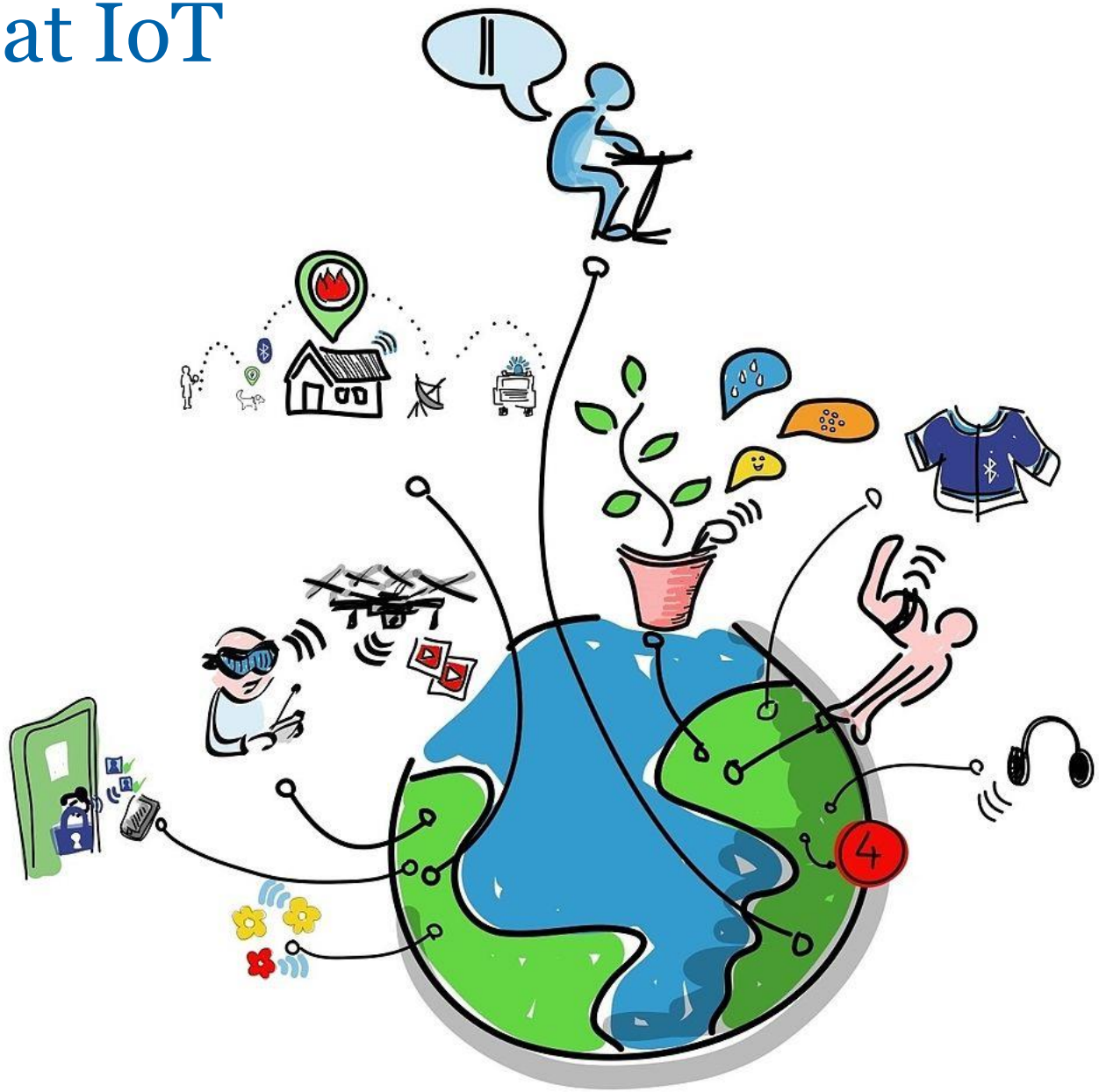
Your Things Are Shouting At Me

The evolving security landscape of the IoT

Jelte Jansen | SIDN Connect 2019

SIDN LABS

So, about that IoT



Should we even still be talking about 'the IoT'?

- It's really 'just' more computers
- A lot more…
- With dubious track-records, so far…..

SIDN LABS

The future of the Internet (of Things)

- Prediction: 21 billion IoT devices in 2025
- source: IoT Analytics 2019

- Prediction: 42 billion IoT devices in 2025
- Source: International Data Corporation

- Prediction: lots and lots of devices in the future
- Source: me

Attributed to @tkadlec

SDN LABS

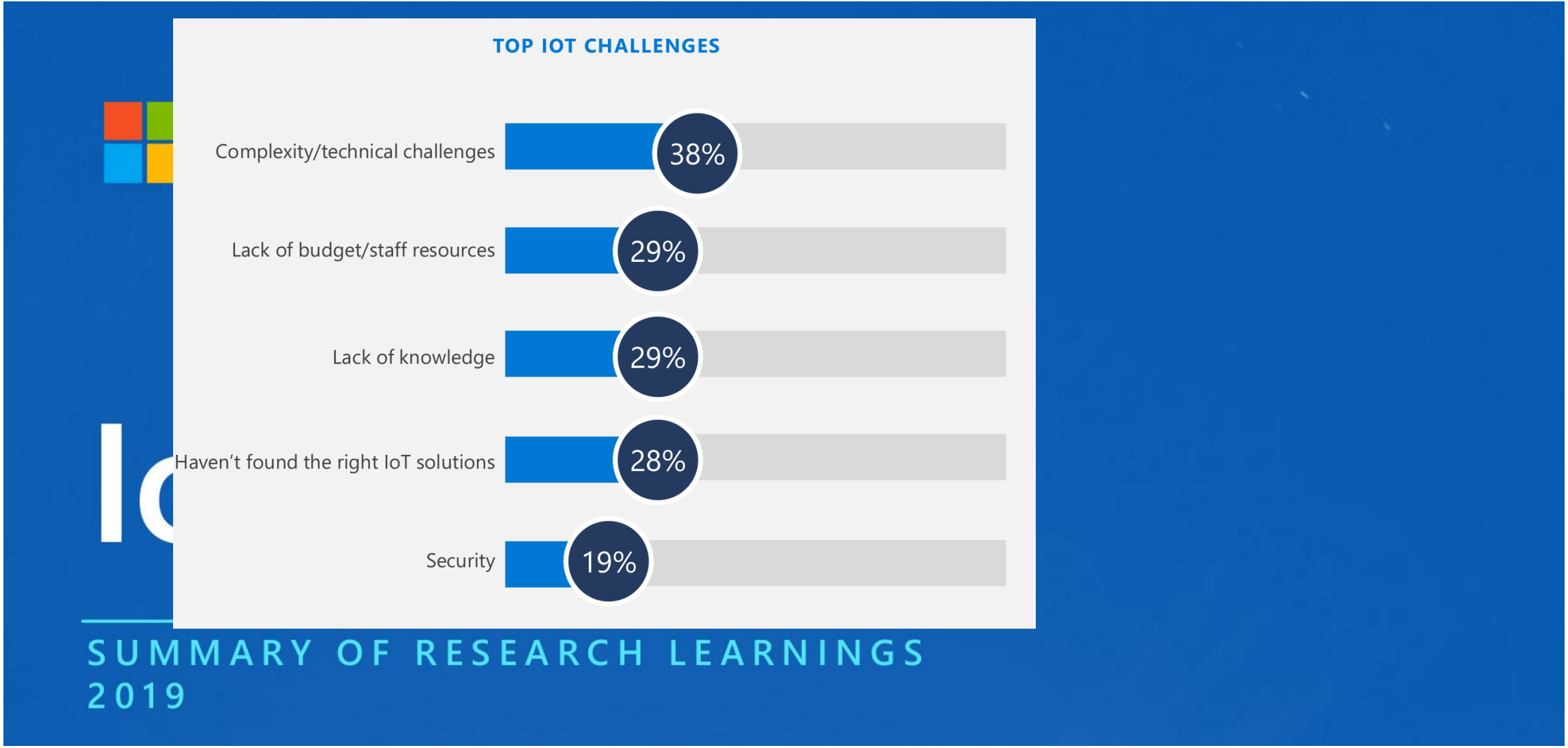
Hacked IoT Devices Internet Services

Microsoft

IoT Signals

SUMMARY OF RESEARCH LEARNINGS
2019

Security concerns around IoT adoption are universal: 97% of companies are concerned about security when implementing IoT (though this is not hindering adoption). Collectively, the top security priority is



Security concerns around IoT adoption are universal: 97% of companies are concerned about security when implementing IoT (though this is not hindering adoption). Collectively, the top security priority is

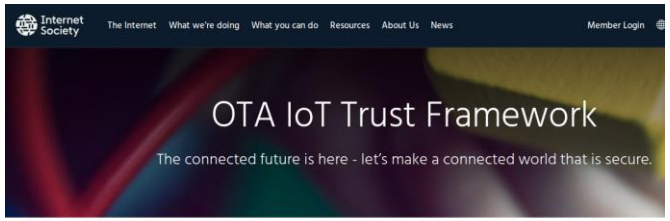
NEWS

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

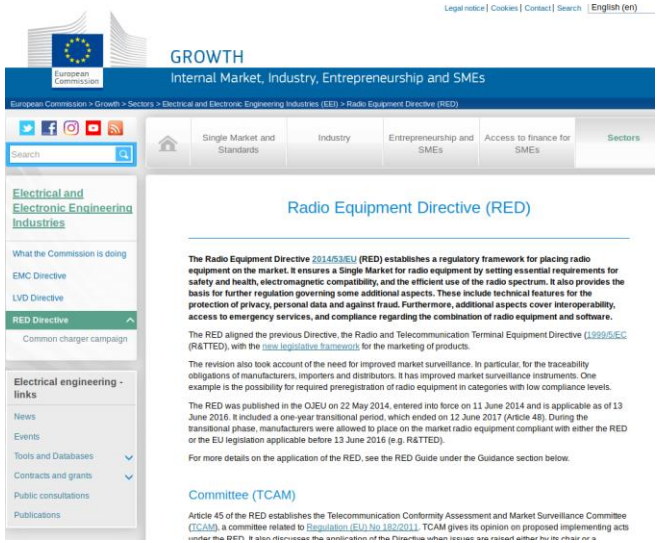
By **Sooraj Shah** - April 27, 2017

Source: Internet of business

Initiatives around the world, on many levels



The Internet of Things (IoT) offer consumers, businesses, and governments across the globe countless benefits. As is true with most emerging technology, however, there remain some significant challenges. The Online Trust Alliance (OTA), an Internet Society initiative, believes that through **leadership, innovation**, and **collaboration,** we can overcome these challenges and create a safer and more trustworthy connected world. This requires a shared responsibility including industry embracing security and privacy by design, and adopting responsible privacy practices.



OPEN SECURITY KNOWLEDGE

FOR COMPLETE SOLUTIONS: END-TO-END

The IoT Security Initiative provides comprehensive guidance and tools for ensuring that the right levels of security and privacy are instilled into created and deployed products, systems, and services.

The security controls and guidelines recommended here are based upon an understanding of overall threat and risk to the technology asset, and how this risk can be mitigated in both the direct system and broader solution context.

The IoT Security Initiative provides broad, high-level material - that is at the same time direct, specific and actionable - to practitioners in various roles of solution development, management, IT, and information security.

AVAILABLE SECURITY GUIDANCE

Cybersecurity Principles of IoT
Security Design Best Practices
Device Security Level Agreement
Privacy Design Best Practices
Secure-Me: Digital-OPSEC
** Product Security Pre-Launch Checklist
** Cybersecurity Health-Check: Network & Cloud
** Cybersecurity Health-Check: Product Development

Home » Blogs en Nieuws » Naar geautomatiseerde DDoS-bescherming met MUD

Naar geautomatiseerde DDoS-bescherming met MUD

Gepubliceerd op: maandag 29 oktober 2018

Onveilige Internet of Things apparaten (IoT-apparaten) worden gebruikt om Distributed Denial of Service (DDoS) aanvallen uit te voeren. Een bekend voorbeeld hiervan is de Mirai-botnet aanval op DNS-operator Dyn, die leidde tot grootschalige uitval van DNS-diensten. Om het schaderisico van onveilige IoT-apparaten te beperken, lanceerde SIDN Labs het SPIN-project. Hierbij evalueerden we de bruikbaarheid van de Manufacturer Usage Description (MUD) specificatie, die momenteel wordt ontwikkeld door de Operations and Management Area Working Group (OPSAWG) binnen de Internet Engineering Task Force (IETF).

De achterliggende gedachte hierbij is dat wanneer een IoT-apparaat verbinding zoekt met een netwerk, het apparaat doorgeeft welke resources het nodig heeft om goed te kunnen functioneren. Deze informatie wordt vastgelegd in een *MUD-profiel*, dat het beoogde netwerkgedrag van het apparaat beschrijft op basis van een 'whitelist'. Deze whitelist zou compleet moeten zijn en dus kan de toegang tot andere netwerkresources worden geweigerd zonder dat dit de goede werking van het apparaat belemmert.

In dit onderzoek bestudeerden we de toepasbaarheid van MUD voor het beveiligen van IoT-apparaten tegen hackpogingen. Ook onderzochten we of de bruikbaarheid van IoT-apparaten voor DDoS-aanvallen afneemt door een profiel te handhaven. De MUD-specificatie is echter nog niet klaar voor gebruik en dus nog nergens geïmplementeerd. Om MUD-profielen te

Home » Blogs en Nieuws » SPIN: A User-centric Security Extension for In-home Networks

SPIN: A User-centric Security Extension for In-home Networks

Gepubliceerd op: woensdag 28 juni 2017

The internet of things (IoT) will connect billions of devices to the internet that we normally do not think of as computers, such as fridges, cameras, and light bulbs. At SIDN Labs, we are developing a system called SPIN (Security and Privacy for In-home Networks) that aims to reduce the security risks that these devices pose to core internet systems, service providers, and end-users. We discuss our ongoing work on the design and implementation of the system in a technical report, which we released today.

Threat to the DNS

While the internet of things (IoT) promises to enable many new types of services and applications, IoT devices are often poorly secured and as a result pose a threat to the security and stability of the core systems of the internet, such as to the Domain Name System (DNS). In October 2016, for example, DNS operator Dyn was hit by a Denial of Service (DoS) attack carried out through millions of IoT devices compromised with the Mirai botnet that allegedly reached an aggregate magnitude of 1.2 Tbps. Other potential targets of such attacks include operators of top-level domains (such as .nl, operated by SIDN), hosting providers, and application service providers.

Threat to end-users

Accountability in the Internet of Things (IoT): Systems, law & ways forward

Jatinder Singh*♦, Christopher Millard+, Chris Reed+, Jennifer Cobbe*, Jon Crowcroft*

*Dept. of Computer Science & Technology (Computer Laboratory), University of Cambridge
+Centre for Commercial Law Studies, Queen Mary University of London

Abstract

Accountability is key to realising the full potential of the IoT. This is for reasons of adoption and public acceptability, and to ensure that the technologies deployed are, and remain, appropriate and fit for purpose. Though technology generally is subject to increasing legal and regulatory attention, the physical, pervasive and autonomous nature of the IoT raises specific accountability challenges; for instance, relating to safety and security, privacy and surveillance, and general questions of governance and responsibility. This article considers the emerging 'systems of systems' nature of the IoT, giving the broad legal context for these concerns, to indicate technical directions and opportunities for improving levels of accountability regarding technologies that will increasingly underpin and pervade society.

Adviesraad kabinet: verbod op onveilige 'slimme' apparaten

Joost Schellevis
redacteur Tech

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.

But what WE like is research

So let's focus on that!

IoT (Collaboration) projects at SIDN

- INTERSECT An Internet of Secure Things
- DINET DNS-Based Trust, Security, Accountability, and Privacy for IoT
- MINIONS Mitigating IOT-Based DDoS Attacks via DNS

Cleaning up the Internet of Evil things

https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_02B-2_Cetin_paper.pdf

Paper by TUD, YNU, and NICT into the effectiveness of remediation strategies, such as notification and quarantining infected networks.

Tracked Mirai infections through several sources, and the rate of cleanup for several methods.

SIDN LABS

Cleaning up the Internet of Evil things: Mirai

- 87% of infections in broadband access networks
- 58-74% natural cleanup rate (no action taken) over several control groups
- 77% cleanup on email notification
- 92% cleanup on quarantine
- Only 5% reinfection rate after 5 months

SIDN LABS

The SPIN project at SIDN Labs

- Security and Privacy for In-home Networks

- Research and prototype of SPIN functionality:
  - Visualising network traffic
  - (Automatic) blocking of 'bad' traffic
  - Allow 'good' traffic

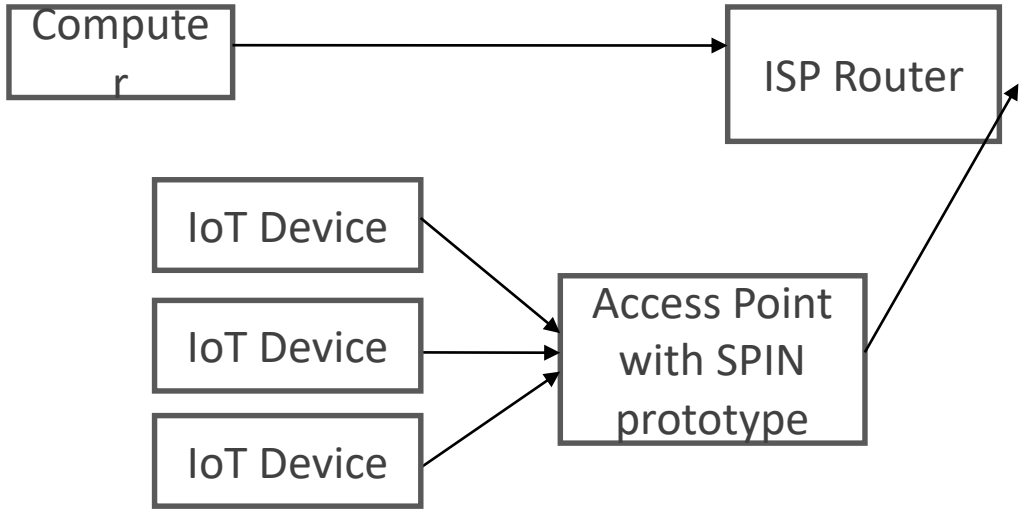
The SPIN project at SIDN Labs

- Open source in-home router/AP software that
- Helps protect DNS operators (like SIDN!) and other service providers against IoT-powered DDoS attacks
- Helps end-users controls the security of their home networks

Prototype built on OpenWRT

- https://spin.sidnlabs.nl
- https://github.com/SIDN/spin
- Currently working on better instructions for Raspberry Pi

prototype 2, GL-Inet hardware

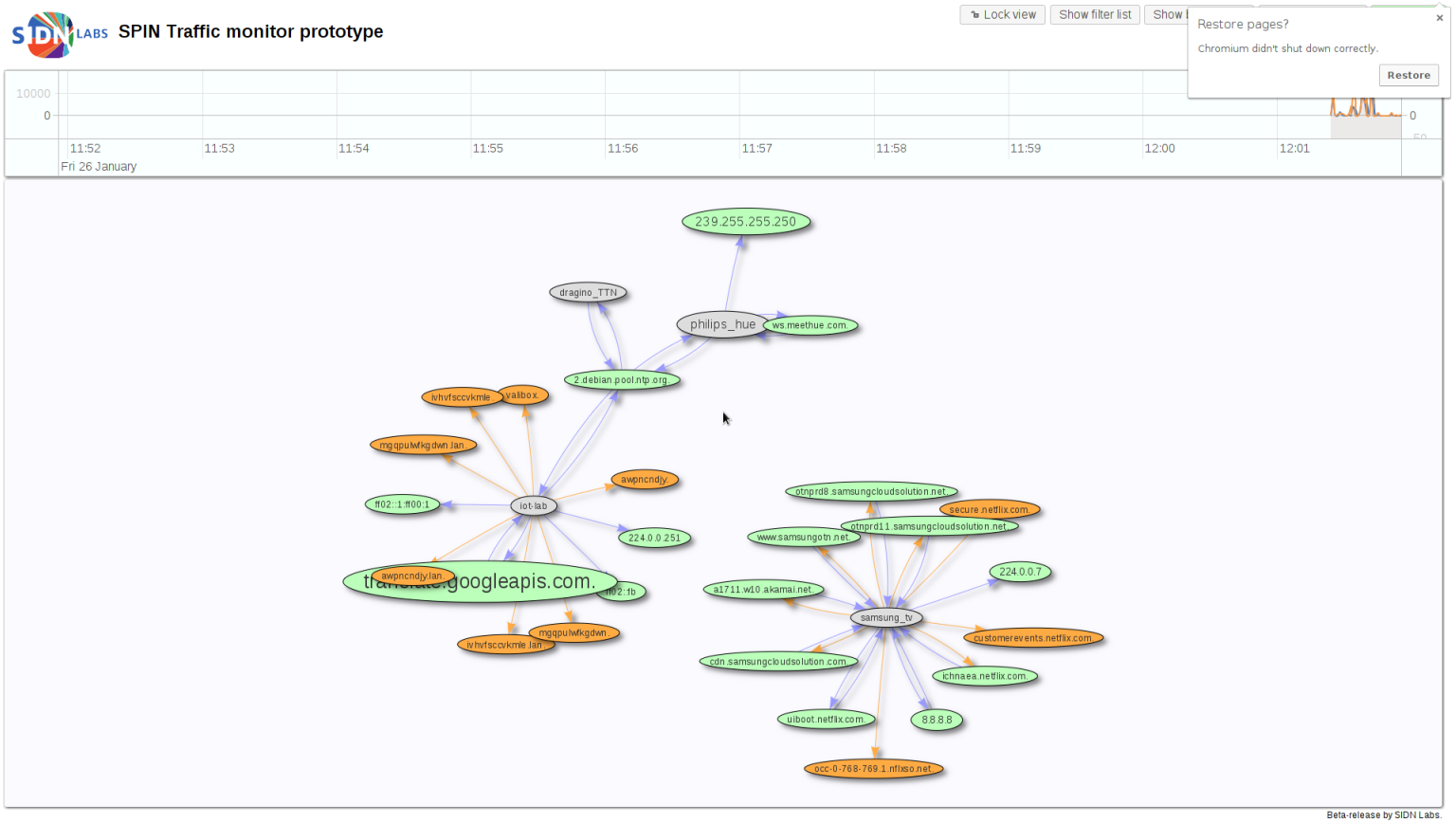


SIDN LABS

Running prototype: visualiser

- Shows DNS queries
- Shows data traffic
- User can block traffic based on source or destination, or both
- Download traffic from specific
- devices

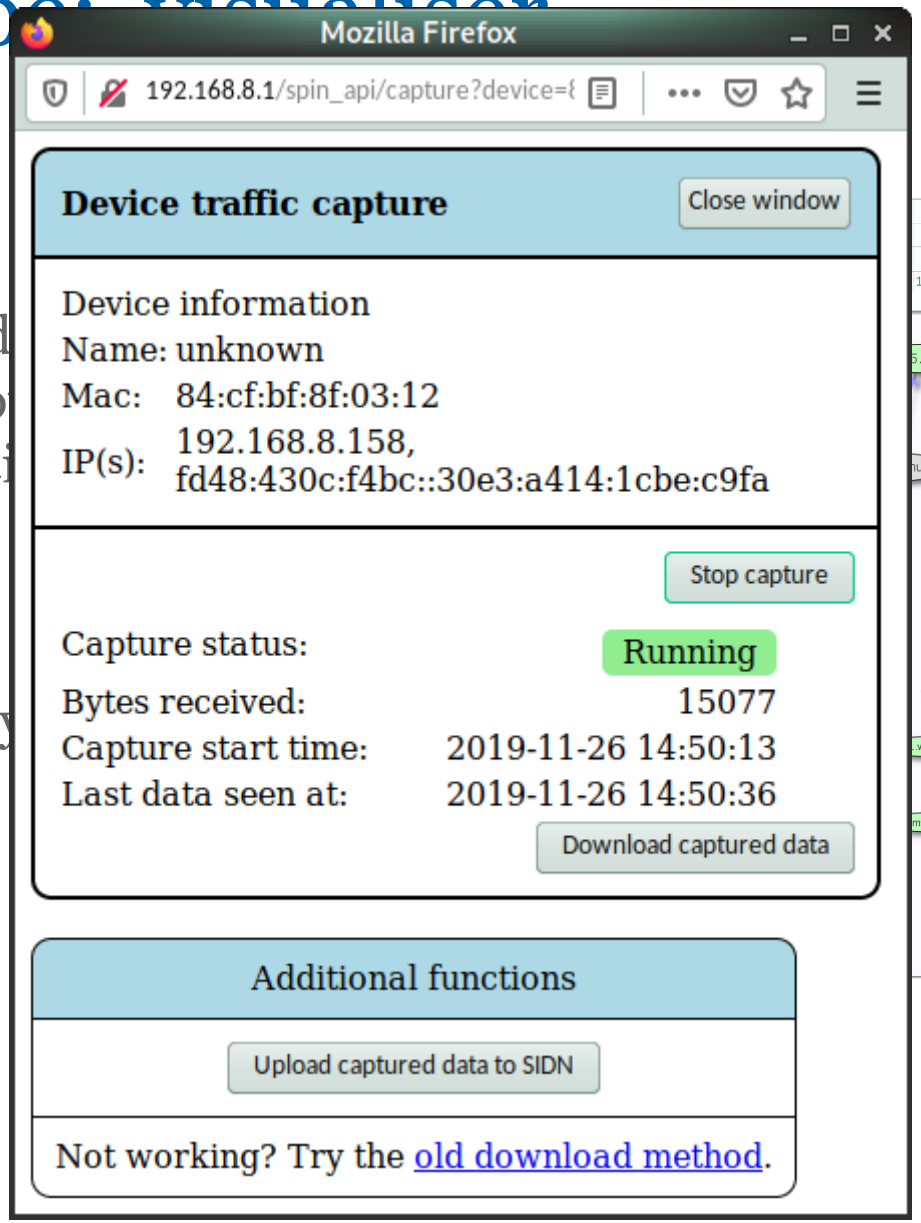
- Next research topics:
  - In-depth device traffic analysis
  - Time-series based analysis



Running prototype: visualiser

- Shows DNS queries
- Shows data traffic
- User can block traffic based
  source or destination, or bo
- Download traffic from speci
- devices

- Next research topics:
  - In-depth device traffic analy
  - Time-series based analysis



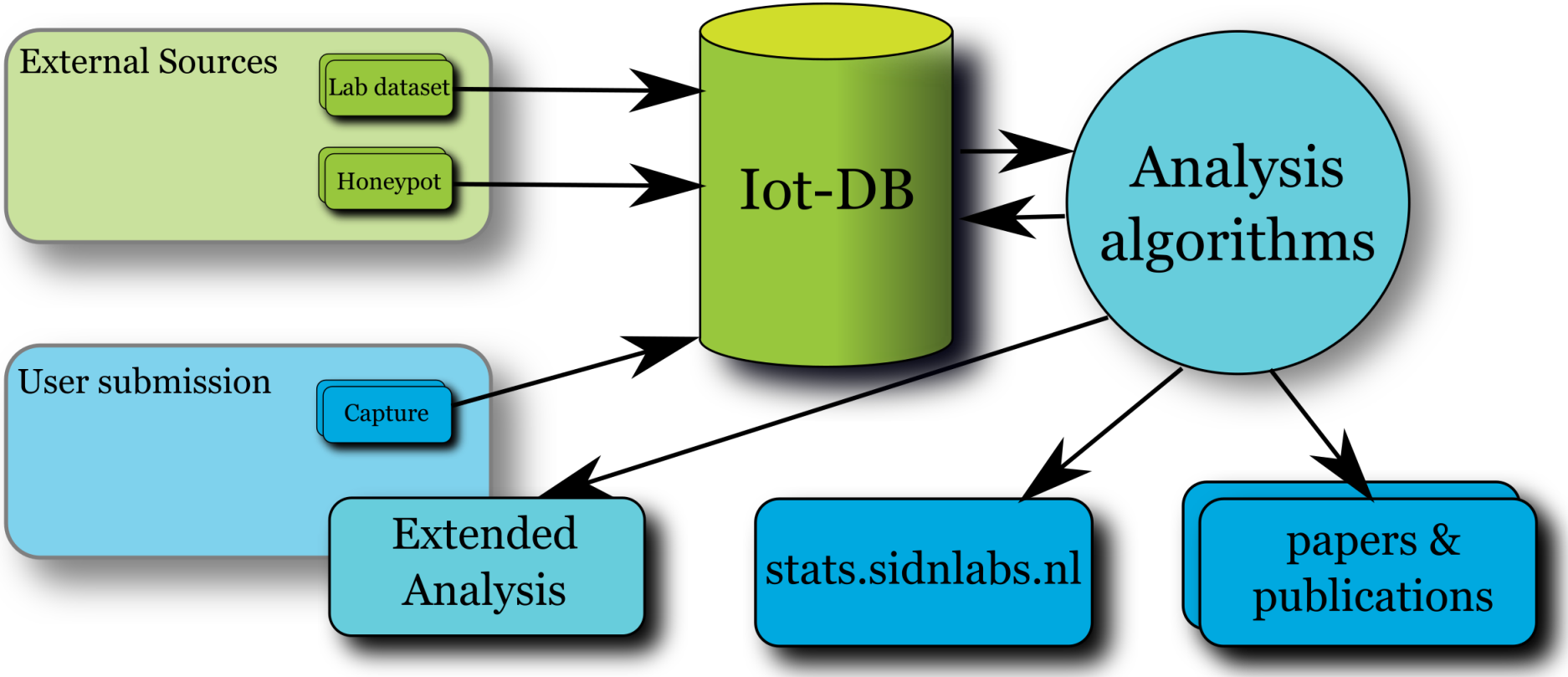
SPIN project focus change

- Renewed focus on research and analysis aspect

- Basic visualisation locally
- Sharing platform for further analysis (fully optional)

- Start out with other datasets:
  - Large dataset of honeypot data
  - Collected data from our lab devices

Potential goal: “IoT-DB”



Thank you for your attention!

Any questions?

Follow us


sidnlabs.nl


@SIDN @sidnlabs @twitjeb


SIDN

dr. João Ceron
UNIVERSITY OF TWENTE.

Your Things Are Shouting At Me - Malicious traffic from IoT devices

SIDN LABS

What is a malicious traffic?

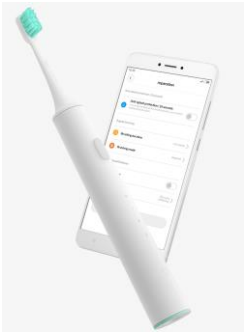
How to measure malicious traffic?

How to detect it?

How to analyze it?

Malicious traffic

- The Internet network traffic is composed by all sort of communication
  - clients/server
  - tunnels/overlays
  - distinct protocols
  - good/bad guys



Any kind of unauthorized network traffic

Network traffic aiming to compromise a system

Anything that I do not want it

SDN LABS

IoT device communication

- Make it easy for the users
  - Auto-configuration protocols
  - A lot of packets on the wire
  - Centralization (cloud)

How many packets when you turn the device on?

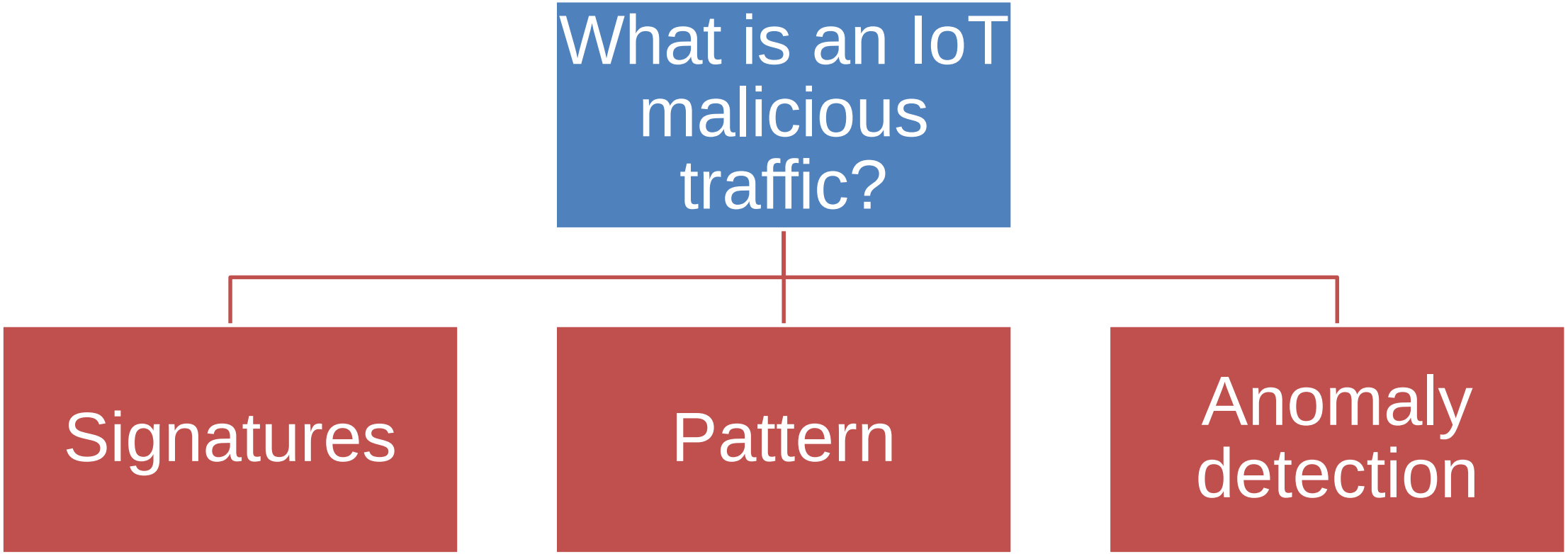
TP Link Plug

WeMoLink

HueSwitch

https://arxiv.org/abs/1611.04880

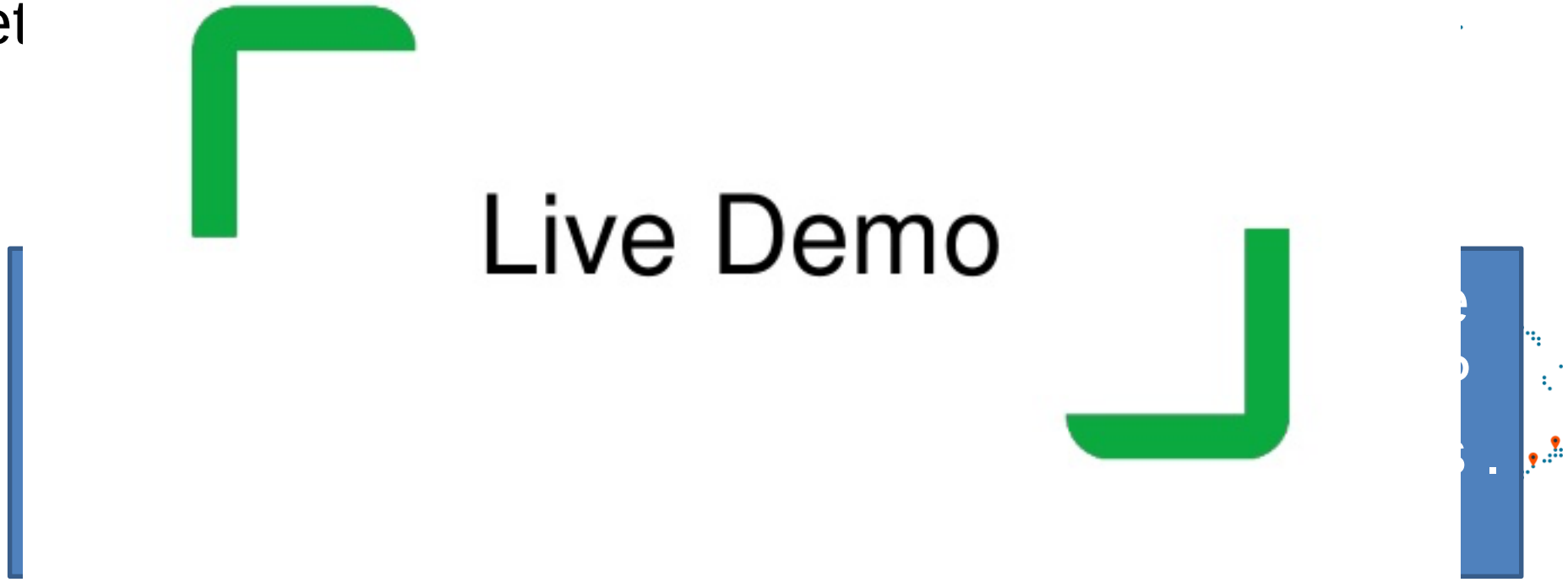
Challenges to monitor IoT malicious traffic



Investigating malicious traffic in large scale

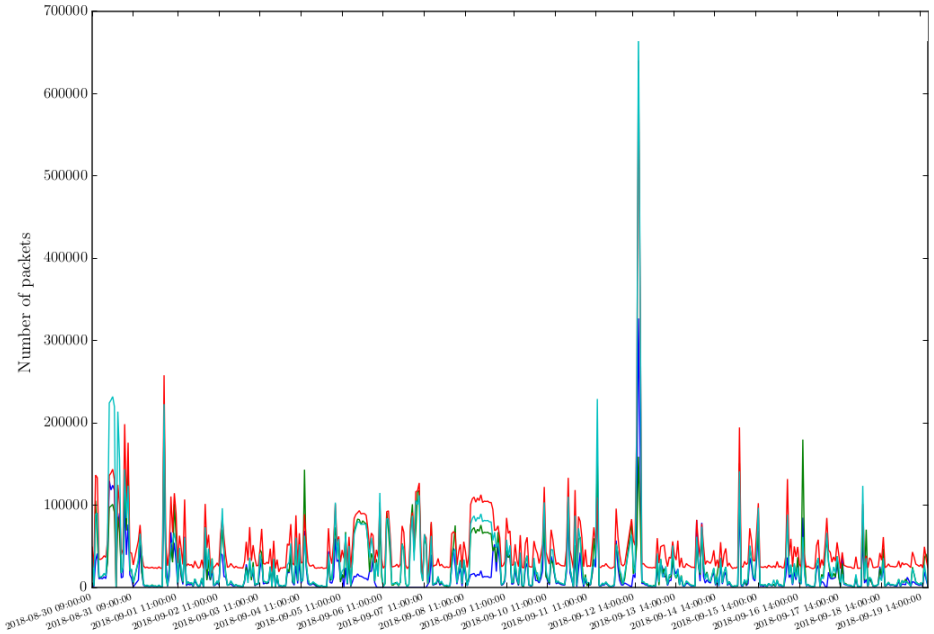
- Networ
- Darkne

Live Demo



Malicious traffic collected

- 3 Gigabytes data per day
- ~44 Millions of packets per day



Protocol	Brazil
TCP(6)	94.33%
UDP(17)	5.2%
ICMP(1)	0.34%
Others	0.13%

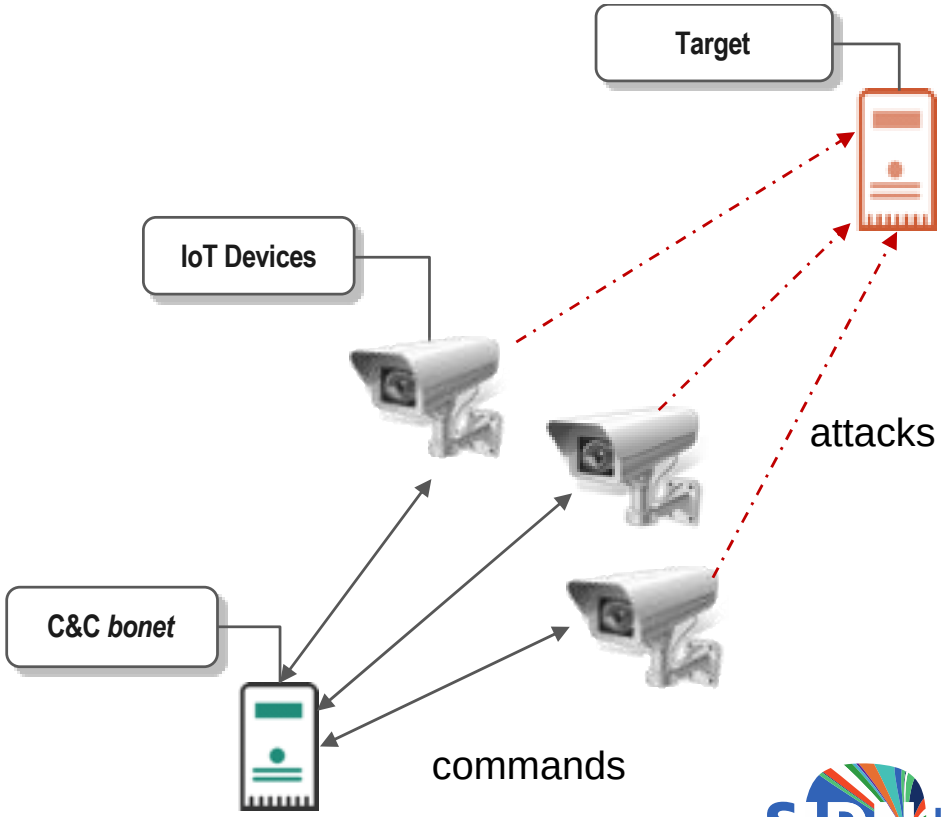
IoT malicious traffic

- Malware
  - Bashlite
  - Mirai

Home > News >

New Variant of Mirai Malware Exploits Weak IoT Device Passwords to Conduct Brute-Force Attacks

January 2, 2019 @ 1:00 PM



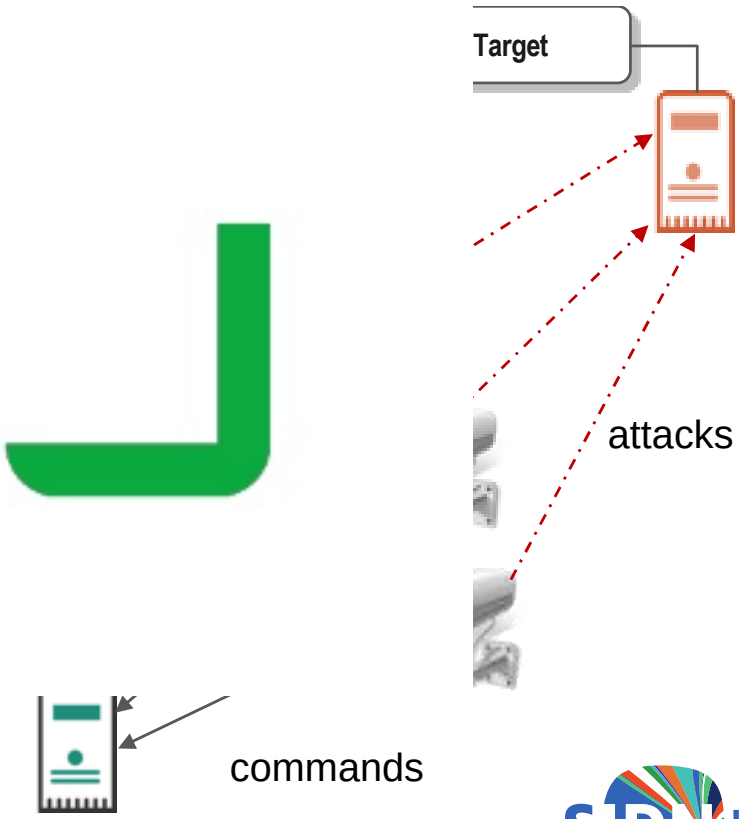
IoT malicious traffic

- Mirai Si

```
1  for (i = 0;
   {
     struct so
     struct ipl
5    struct tcp
     iph->id =
     iph->saddr
     iph->daddr
     iph->check
10   iph->check
     if (i % 10
     {
         tcph->
     }
15   else
     {
         tcph->dest = htons(23);
     }
     tcph->seq = iph->daddr;
```

Live Demo

Source: mirai/bot/scanner.c



Conclusion

- Internet is a noisy place
- Malicious traffic identification is not trivial
  - Partial view
  - Many actors
- Some tools that help in the process
  - Darknets
  - Network sensors
- Identify IoT traffic pattern is essential

Thank you

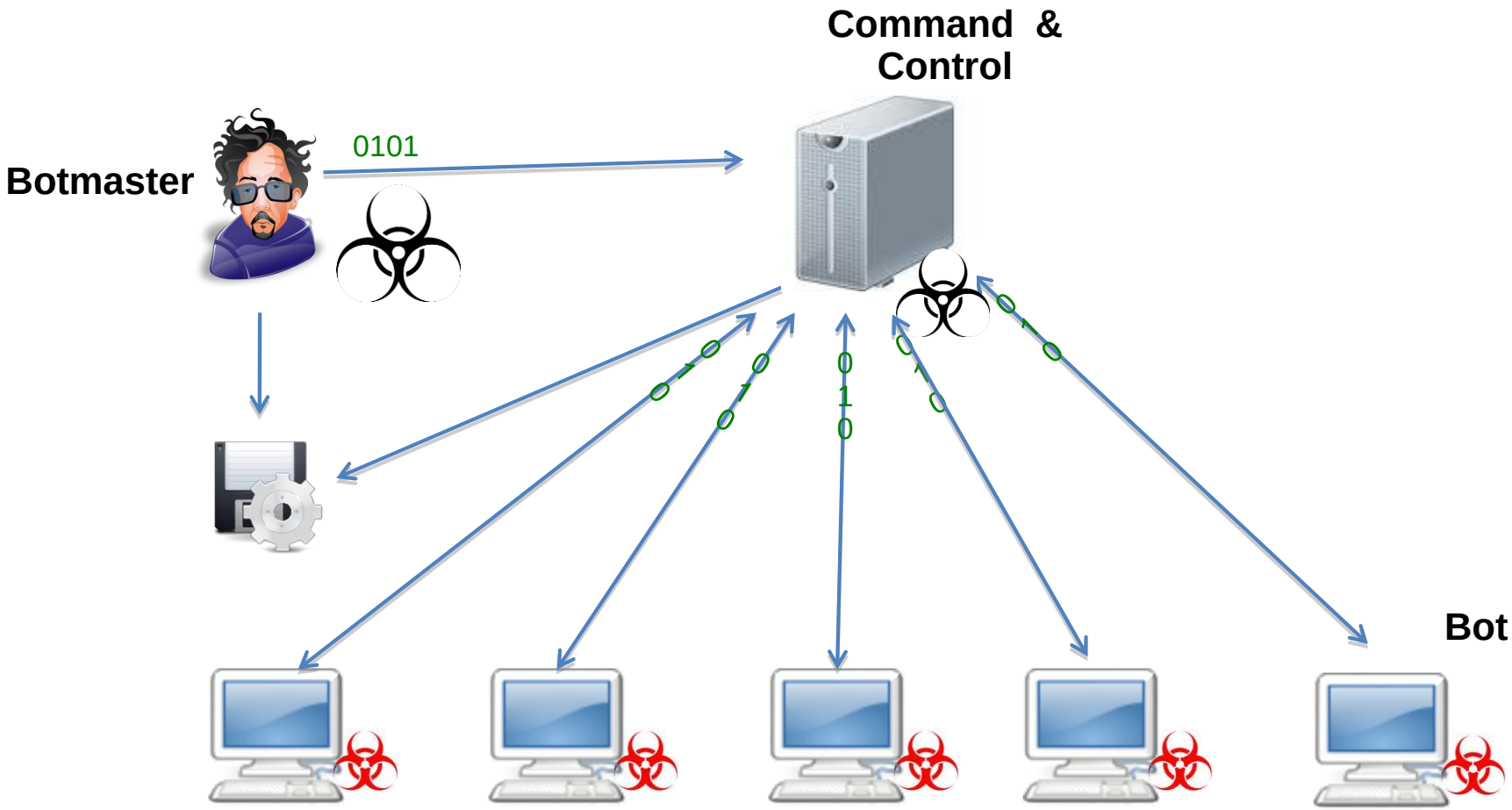
http://www.botlog.org/

UNIVERSITY OF TWENTE.

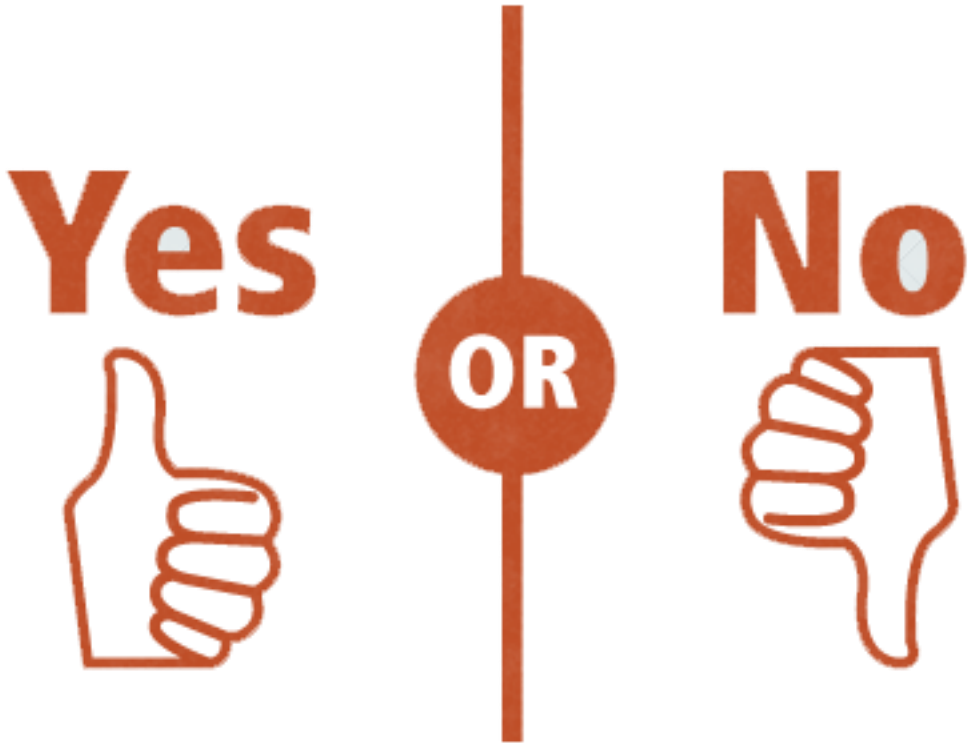
SIDN LABS

Backup

Malicious traffic



Network SCAN



Network SCAN

Scanning for SSH Can Cause a Crash - Cisco Systems

HIGH Nessus Plugin ID 48967

Synopsis

The remote device is missing a vendor-supplied security patch

Description

While fixing vulnerabilities mentioned in the Cisco Security Advisory cisco-sa-20010627-ssh, a new vulnerability was introduced in some products. When an attacker tries to exploit the vulnerability VU#945216 (described in the CERT/CC Vulnerability Note at http://www.kb.cert.org/vuls/id/945216) the SSH module will consume too much of the processor's time, effectively causing a DoS. In some cases the device will reboot. In order to be exposed SSH must be enabled on the device.
It is possible to mitigate this vulnerability by preventing, or having control over, the SSH traffic.

Solution

Apply the relevant patch referenced in Cisco Security Advisory cisco-sa-20020627-ssh-scan.

See Also

http://www.nessus.org/u?fab8dcf4

http://www.nessus.org/u?b9451893

Plugin Details

Severity: High

ID: 48967

File Name: cisco-sa-20020627-

Version: 1.19

Type: local

Family: CISCO

Published: 2010/09/01

Updated: 2018/11/15

Dependencies: 47864

Risk Information

Risk Factor: High

CVSS v2.0

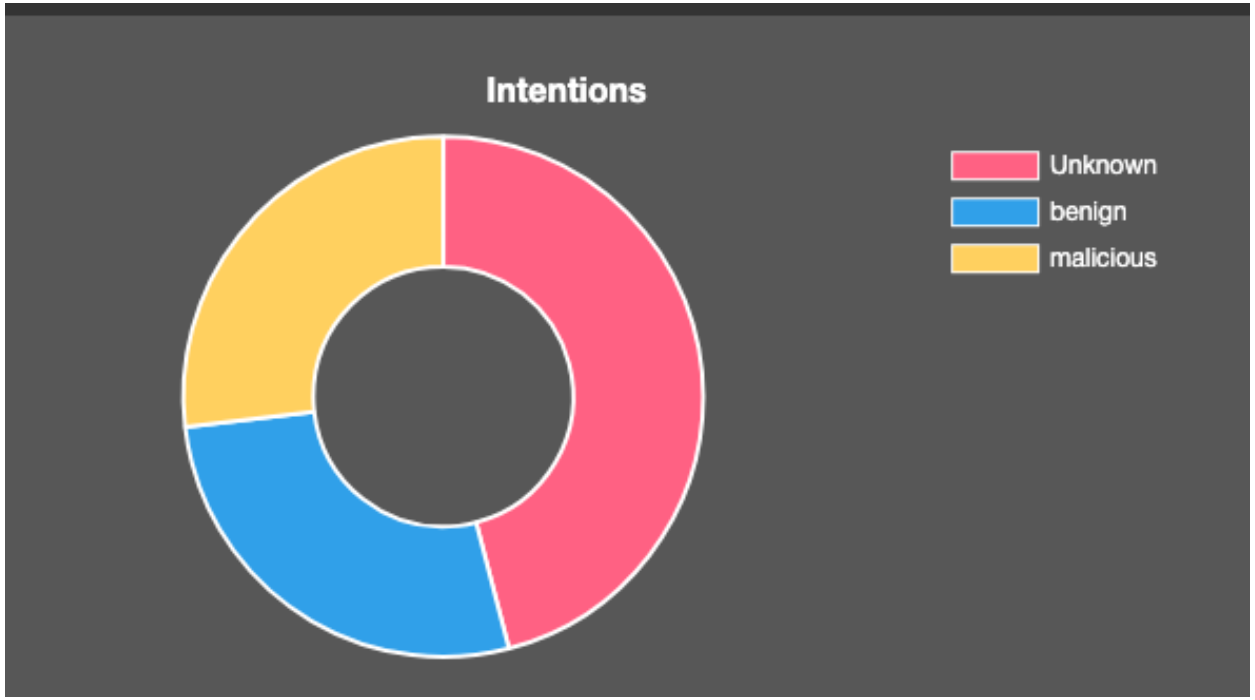
Base Score: 7.1

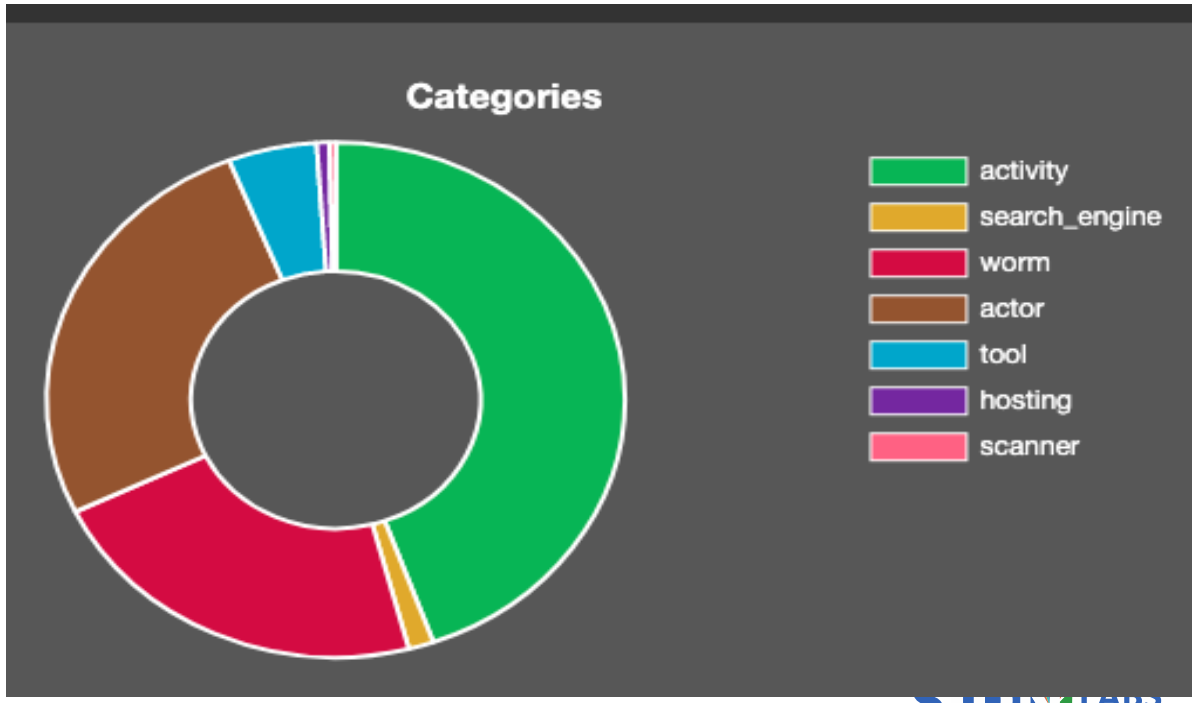
SDN LABS

How to measure malicious traffic?

- http://www.greyNoise.io/

GREY NOISE





How to measure malicious traffic?

- http://www.greyNoise.io/

BINGBOT
GOOGLEBOT
YANDEX_SEARCH_ENGINE
BAIDU_SPIDER

SHODAN — actor

IP	Organization	ASN	rDNS
107.6.151.194	Shodan LLC	AS32475	security.census.shodan.io
107.6.151.194	Shodan LLC	AS32475	security.census.shodan.io
185.181.102.18	M247 Europe SRL	AS9009	turtle.census.shodan.io
66.240.219.146	CariNet, Inc.	AS10439	burger.census.shodan.io
89.248.172.16	Quasi Networks LTD.	AS29073	house.census.shodan.io
82.221.105.7	Thor Data Center ehf	AS50613	census11.shodan.io
198.20.99.130	Shodan LLC	AS32475	census4.shodan.io
94.102.49.193	Quasi Networks LTD.	AS29073	cloud.census.shodan.io
107.6.151.194	Shodan LLC	AS32475	security.census.shodan.io
107.6.151.194	Shodan LLC	AS32475	security.census.shodan.io
71.6.199.23	CariNet, Inc.	AS10439	ubuntu1619923.aspadmin.com
162.243.164.235	DigitalOcean, LLC	AS14061	ns-05-nyc1.dns.shodan.io
162.243.164.234	DigitalOcean, LLC	AS14061	ns-04-nyc1.dns.shodan.io

RUHR_UNIVERSITTT_BOCHUM
AIHIT
UNIVERSITY_OF_THE_FREE_STATE
INTERNET_CENSUS
QWANT
ARCHIVE
UNIVERSITY_OF_NEW_MEXICO
PINGDOM
EXPOSURE_MONITORING
PINGZAPPER
IPIP
LTX71
CHECKMARKNETWORK
TALAIA
PROJECT_SONAR
SHADOWSERVER
SAFEDNS
CLIQZ
ONYPHE
FINDMALWARE

Shodan.io

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

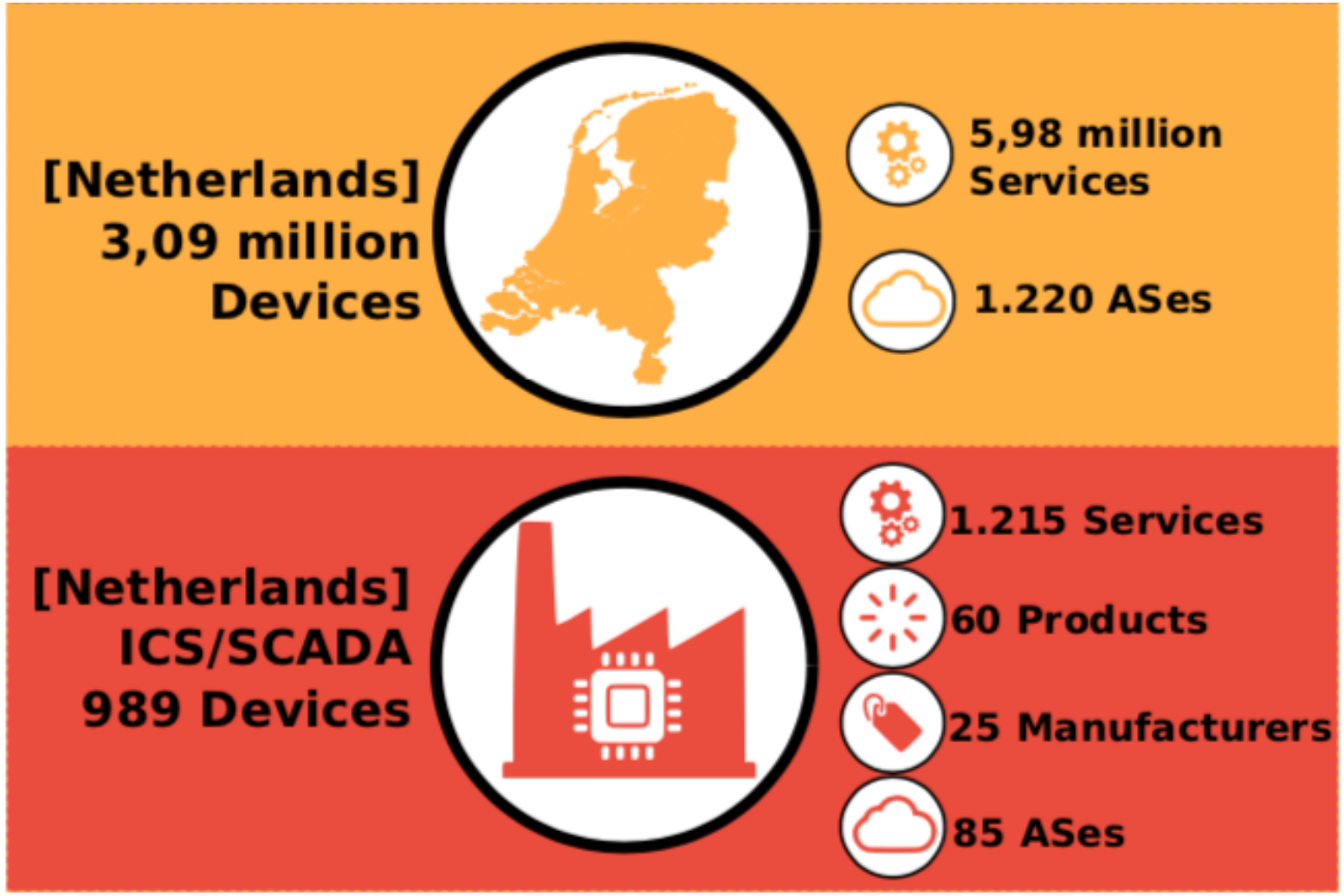
Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

Case Study

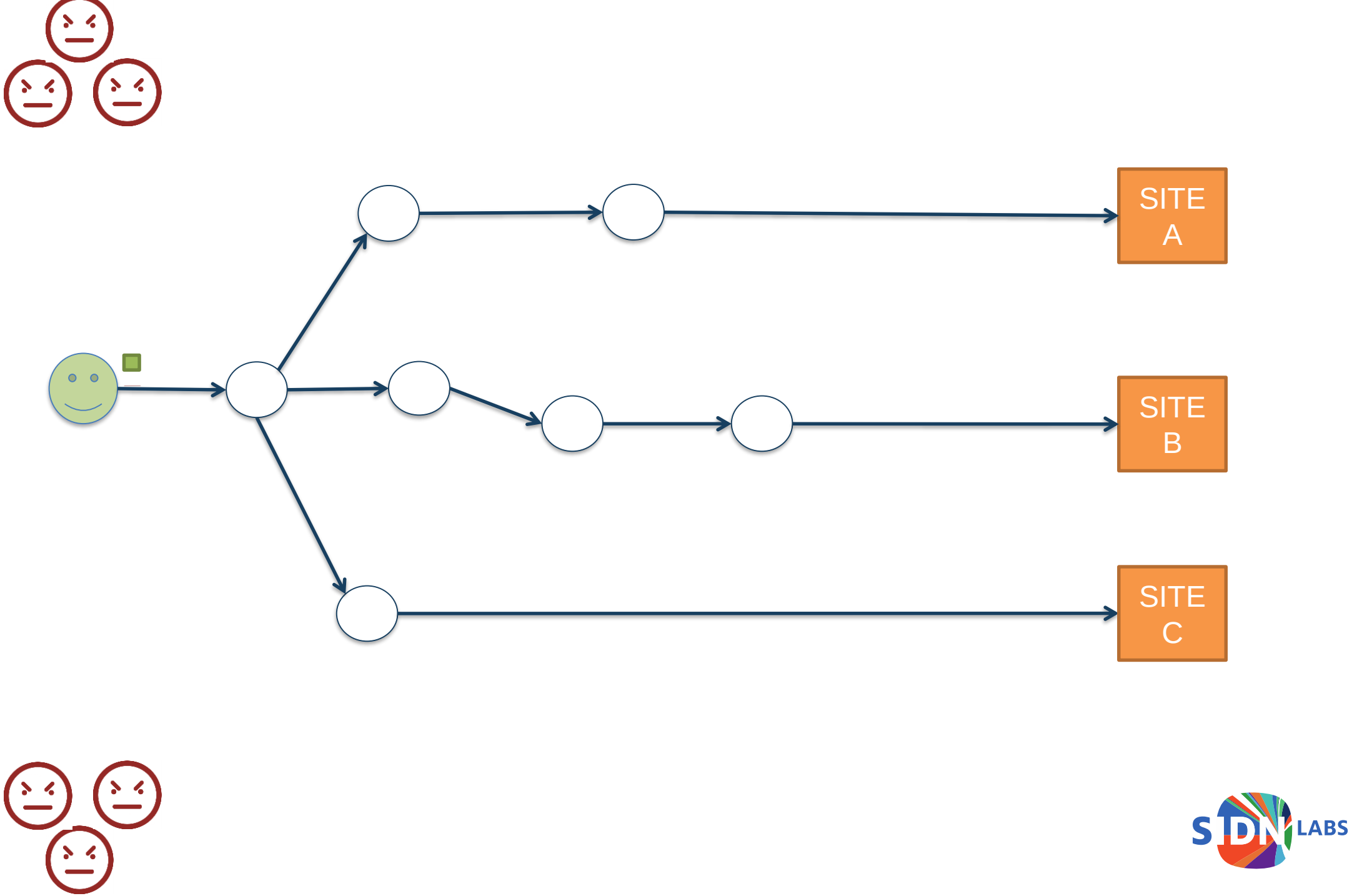

[Netherlands]
3,09 million
Devices
5,98 million
Services
1.220 ASes
[Netherlands]
ICS/SCADA
989 Devices
1.215 Services
60 Products
25 Manufacturers
85 ASes

Darknet

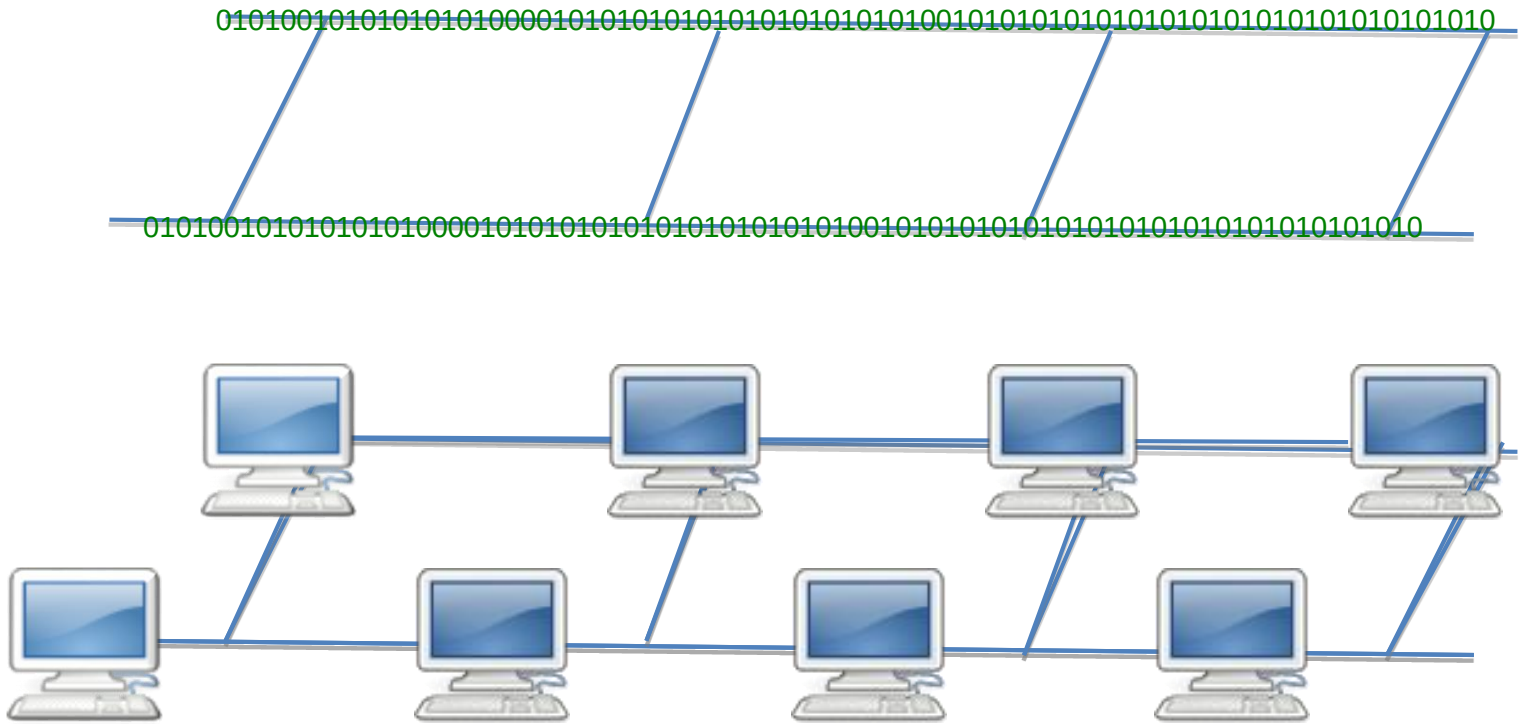
- 8192 IP address

Malicious traffic

- Network scanners
- Research groups
- Other groups
- Compromised machines
  - DDoS
  - Botnets


SITE
A
SITE
B
SITE
C

Malicious traffic



Estado da Arte

- Correlação Vertical