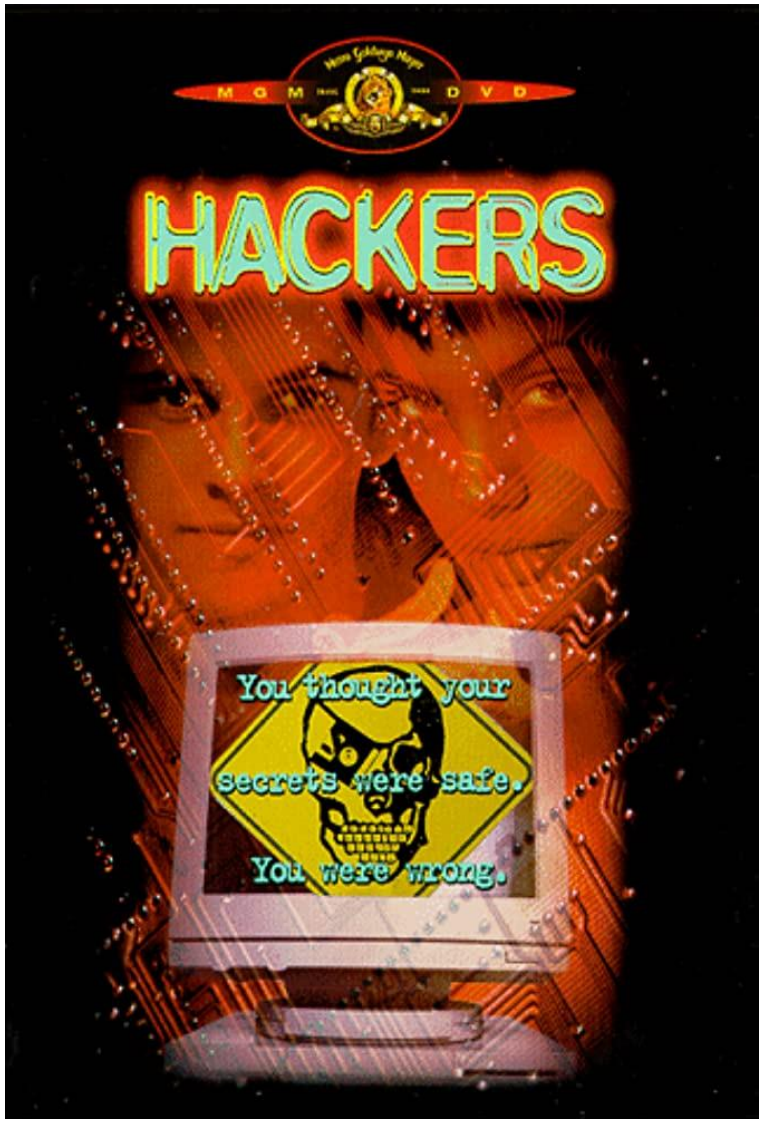
2023
BSides Dublin
27 May 2023

The Gibson



Hackers (1995)

the gibson hotel

stay eat connect offers

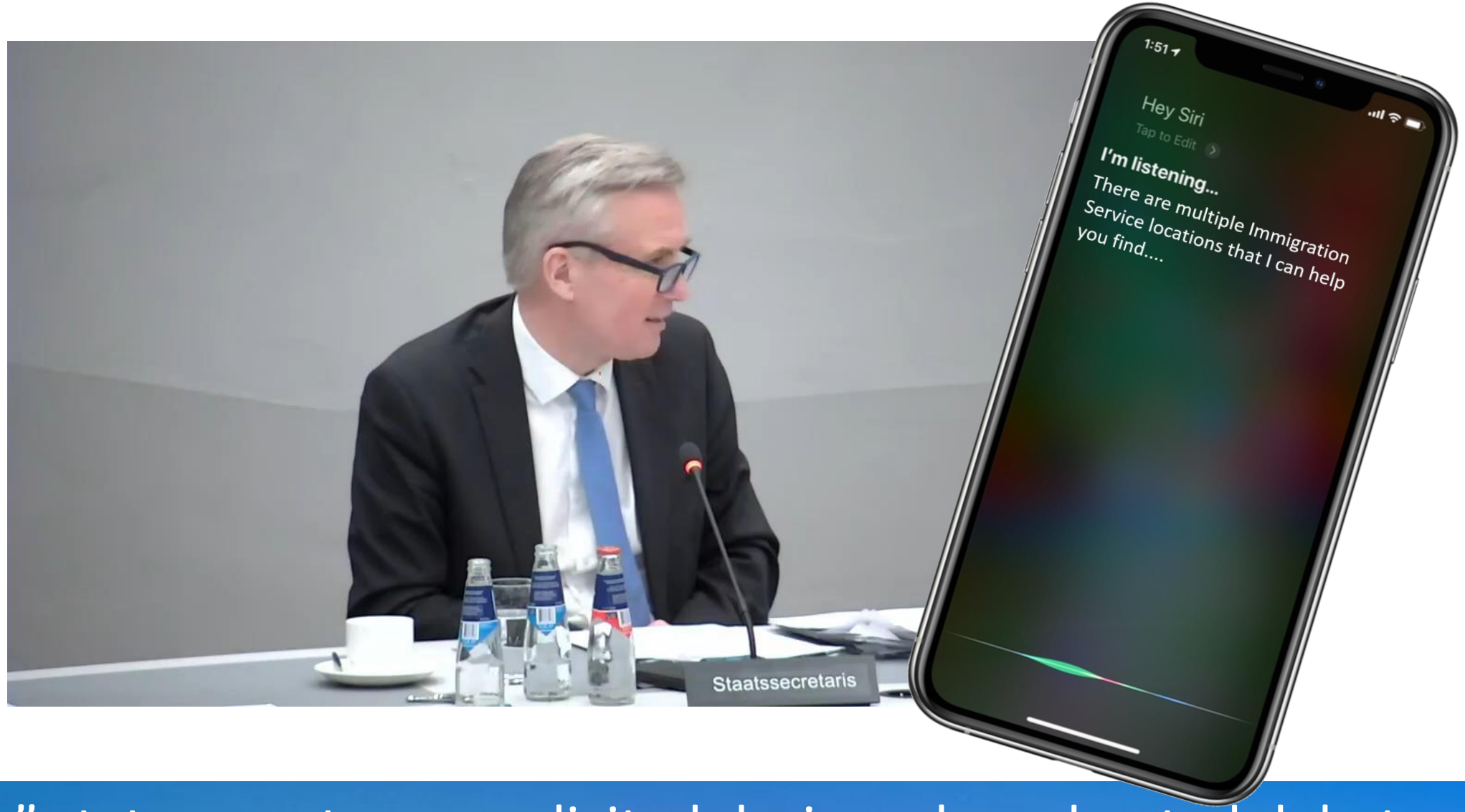
ID.IOT or…
The ID(ea) of IoT


HI!

INTRODUCTION

Richard Zwienenberg, ESET

IoT is EVERYWHERE…



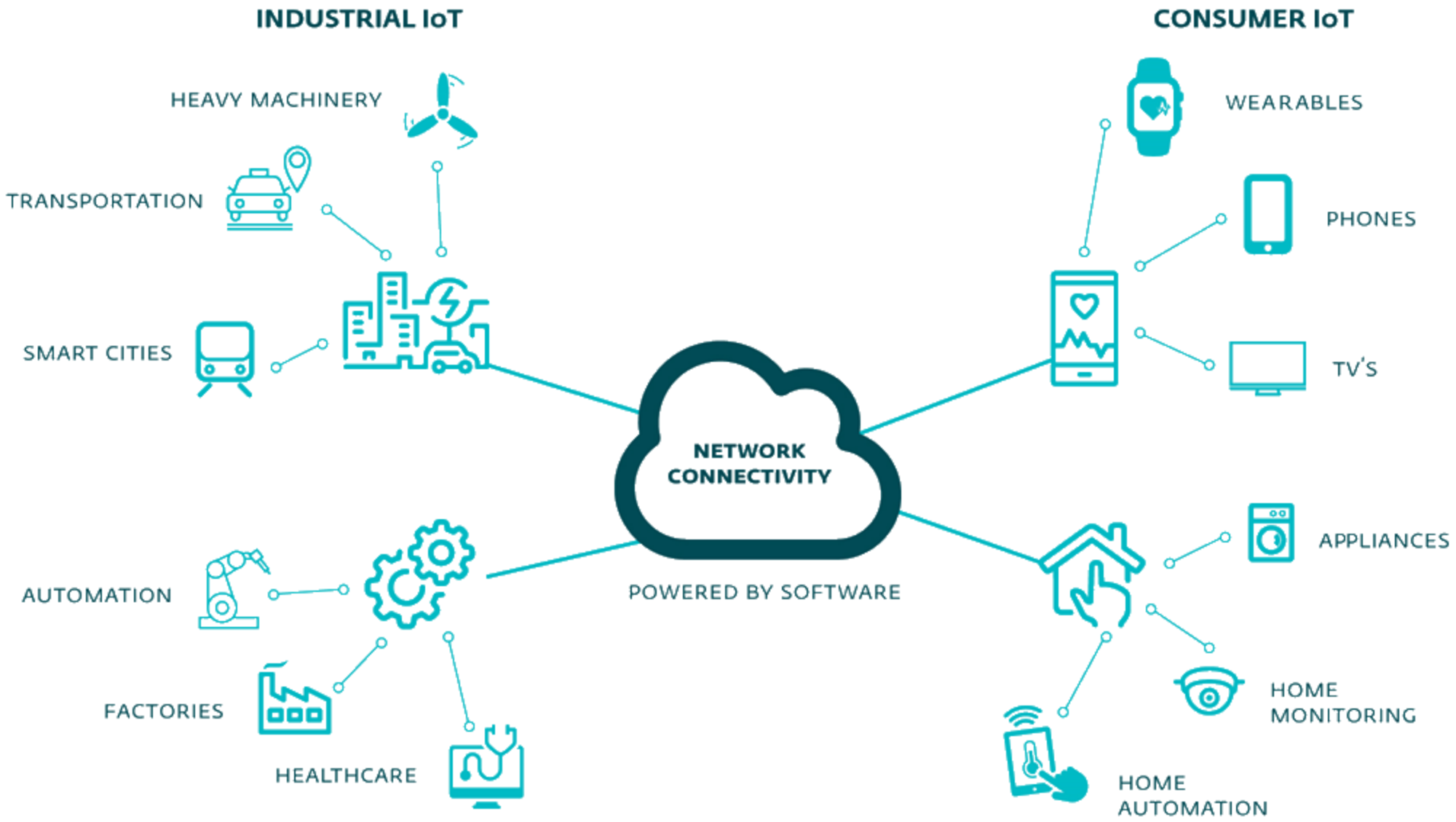
Siri “helps” state secretary unsolicited during a broadcasted debate

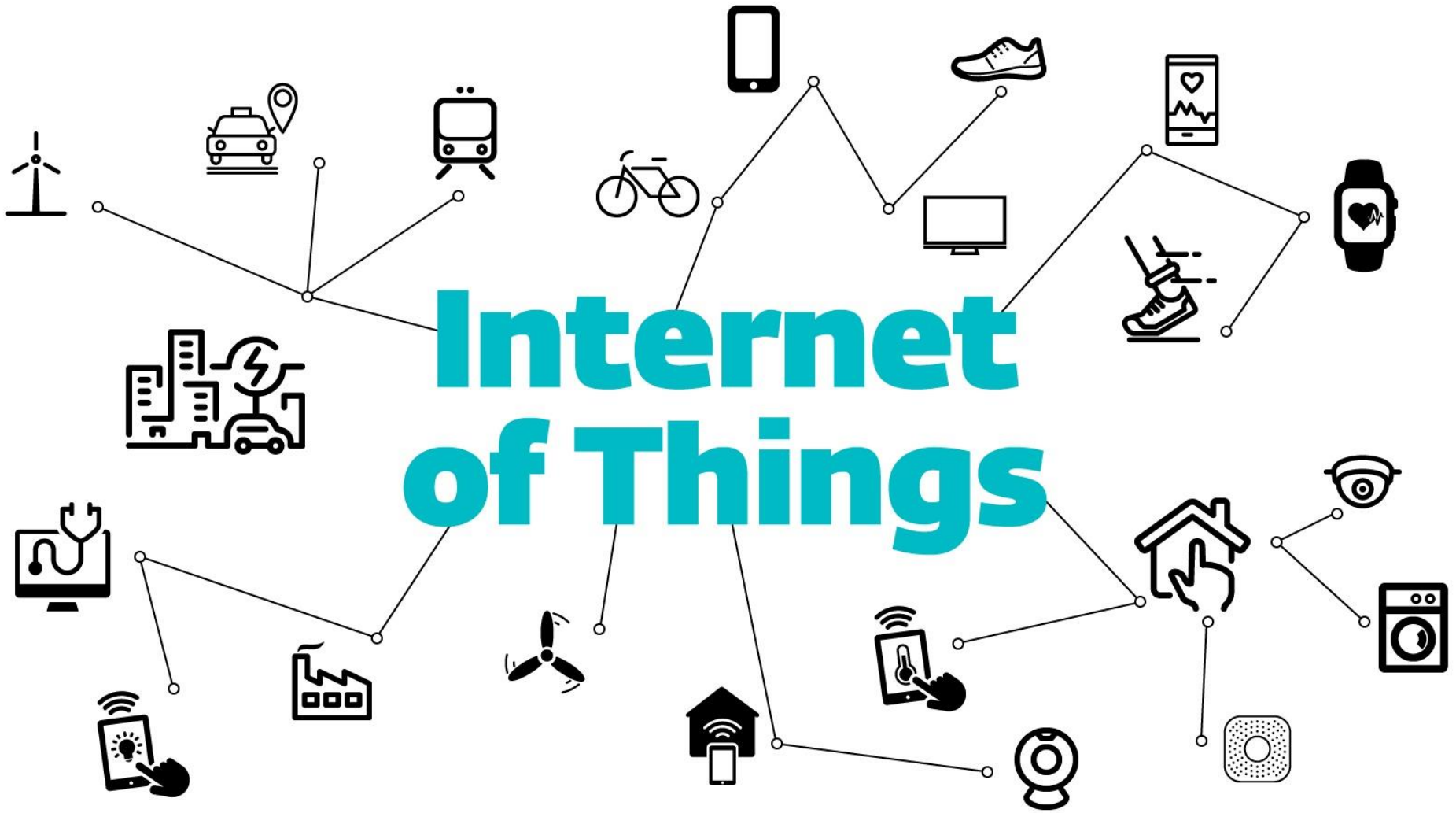
An Experiment: Let’s try it here …

alexa

Hey Siri

Ok Google


INDUSTRIAL IoT
HEAVY MACHINERY
TRANSPORTATION
SMART CITIES
AUTOMATION
FACTORIES
HEALTHCARE
NETWORK CONNECTIVITY
POWERED BY SOFTWARE
CONSUMER IoT
WEARABLES
PHONES
TV'S
APPLIANCES
HOME MONITORING
HOME AUTOMATION



What is it?

Industrial Automation

Smart Health

Smart Home

Smart City

Views on the Internet of Things?

IoT and History

Views on the Internet of Things?

THE X-10 POWERHOUSE DOES EVERYTHING BUT PUT OUT THE CAT.

Model CP290

THE X-10 POWERHOUSE INTERFACES WITH YOUR COMMODORE TO CONTROL YOUR HOME...FOR SECURITY, COMFORT AND ENERGY SAVINGS.

This remarkable Interface lets you run your home through your Commodore 64 or 128 and a keyboard or joystick.

When you're away, it makes your home look and sound lived in. When you're home, it can turn off the TV at night and wake you up to stereo and fresh brewed coffee in the morning. It can

and then plug the Module into an outlet. The Interface can control up to 256 Modules throughout your home and won't interfere with normal use of lights and appliances.

There are plug-in Appliance Modules, Lamp Modules, Wall Switch Replacement Modules and Special 220V Modules for heavy duty appliances such as water heaters and room air conditioners. Plus Thermostat Controllers for central heating and air conditioning, Telephone Responders to control your home from any phone, and much more.

IT WON'T TIE UP YOUR COMPUTER. Use your computer only

Late 1970's

X10

by Pico Electronics

IoT Failures

Smart phones

- Original iPhone, 29 June 2007 (USA)
- Oct/Nov 2009 “Dutch hack”
- Only jailbroken phones
- Abused default SSH password
- Changed device wallpaper
- Asked for €5 “ransom”

http://arstechnica.com/apple/2009/11/dutch-hacker-holds-jailbroken-iphones-hostage-for-5/

Smart phones

- First Android phone, 22 Oct 2008 (USA)
- Aug 2010 Android/FakePlayer.A
- Fake media player app
- From Russian porn sites
- Sent premium-rate SMSes

Smartwatch security fails to impress: Top devices vulnerable to cyberattack

A new study into the security of smartwatches found that 100 percent of popular device models contain severe vulnerabilities.

By Charlie Osborne for Zero Day | July 22, 2015 -- 17:25 GMT (03:25 AEST) | Topic: Security

Apple

A research study conducted by Hewlett-Packard has found serious security issues in today's top smartwatch wearable devices.

Smartwatches are part of the wearable device trend, which extends from medical devices and fitness trackers to acting as an extension of your smartphone.

The Apple Watch and Android Wear are examples of popular wearable devices on the market which can pair with smartphones and allow you to view online notifications, send messages and control apps through either the small display or through voice control.

Wearables can be useful and have grown in popularity with the arrival of the Internet of Things (IoT) concept in the marketplace. However, as smartwatches become mainstream,

Smart watches

COMPUTERWORLD
FROM IDG

SECURITY IS SEXY

By Darlene Storm, Computerworld | JUL 7, 2016 8:27 AM PT

About

Most security news is about insecurity, hacking and cyber threats, bordering on scary. But when security is done right, it's a beautiful thing...sexy even. Security IS sexy.

NEWS ANALYSIS

Hackers can exploit smartwatches, fitness trackers to steal your ATM PIN

Smartwatches and fitness trackers can be exploited to give attackers your ATM PIN and passwords.

Smart watches

6-DAY

Samsung's Tizen said to be riddled with vulnerabilities. Is your smartwatch safe?

BY JERRY HILDENBRAND Tuesday, Apr 4, 2017 at 7:00 am EDT

25 Comments

A report from Motherboard is some very bad news for fans of Samsung's *other* operating system, Tizen.

Speaking with Israeli security researcher *Amihai Neiderman* of Equus Software, Motherboard tells us that there are currently 40 unreported security vulnerabilities that would allow remote execution and hacking of every Samsung TV, watch or phone that uses Tizen as the operating system. More serious are some allegations about the how and why behind many of these exploits.

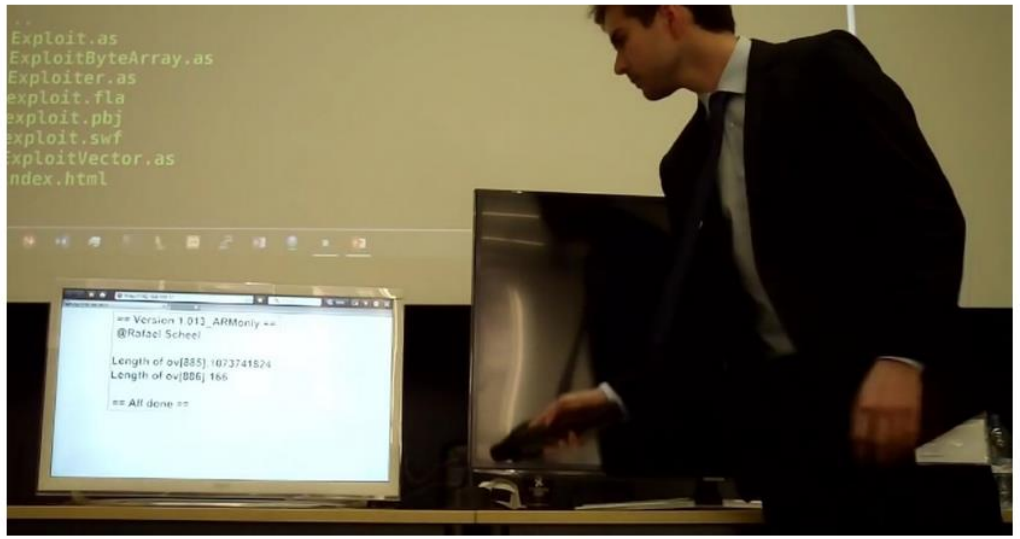
It may be the worst code I've ever seen.

While Samsung may not be thinking about replacing Android with Tizen on its phones and tablets, the current ecosystem is about to be expanded in a big way: Samsung is committed to using Tizen on most every smart appliance it sells going forward. Smart refrigerators sound like a great idea until someone hacks your email through one.

Smart watches: Samsung’s Tizen

About 90% of Smart TVs Vulnerable to Remote Hacking via Rogue TV Signals

By Catalin Cimpanu March 29, 2017 01:30 PM 4



A new attack on smart TVs allows a malicious actor to take over devices using rogue DVB-T (Digital Video Broadcasting — Terrestrial) signals, get root access on the smart TV, and use the device for all sorts of nasty actions, ranging from DDoS attacks to spying on end users.

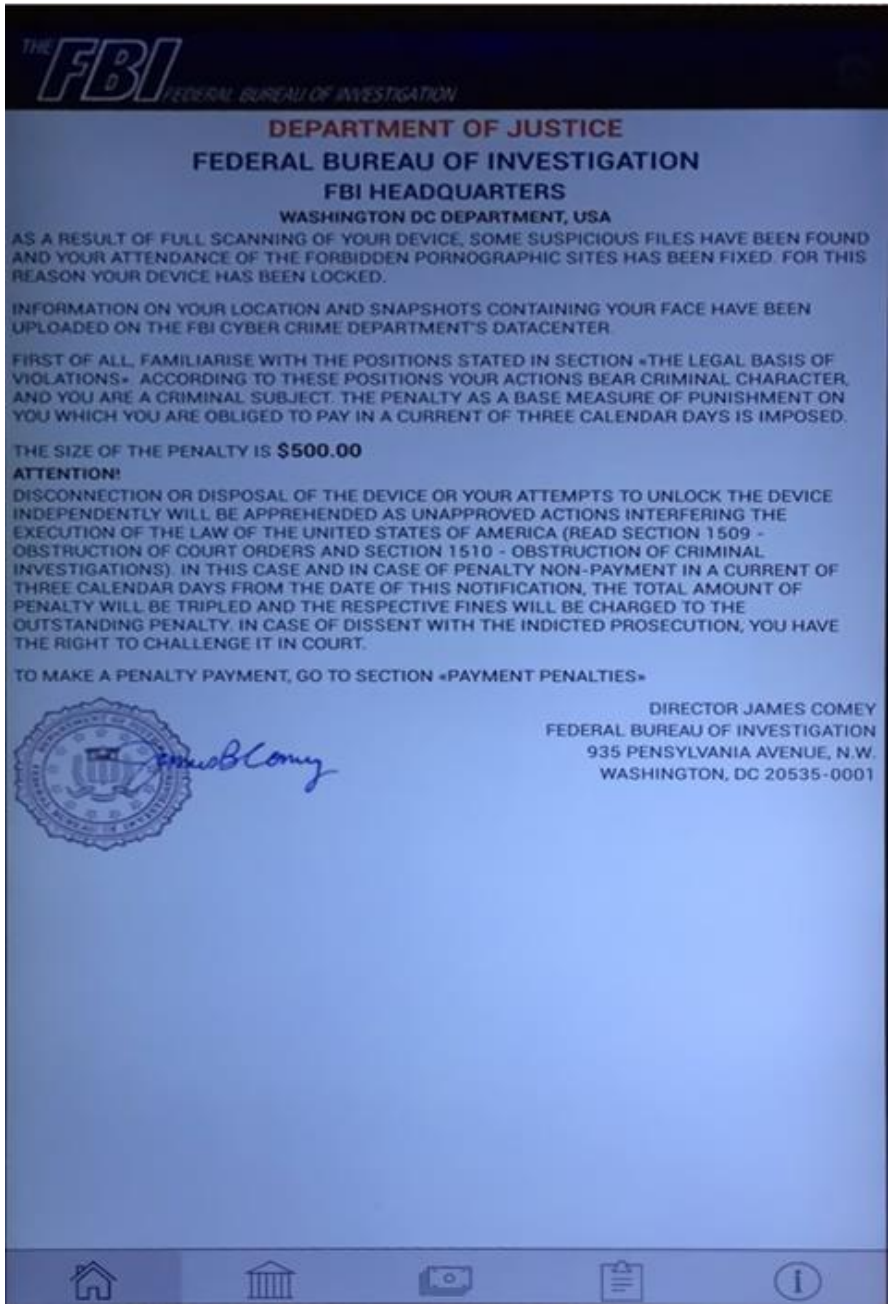
The attack, developed by Rafael Scheel, a security researcher working for Swiss cyber security consulting company Oneconsult, is unique and much more dangerous than previous smart TV hacks.

Current smart TV hacks aren't not really "dangerous"

Until now, all smart TV exploits relied on attackers having physical access to the device, in order to plug in an USB that executes malicious code. Other attacks relied on social engineering, meaning attackers had to trick users into installing a malicious app on their TV.

Smart TVs


Darren Cauthon
@darrencauthon
Follow
Family member's tv is bricked by Android malware. #lg wont disclose factory reset. Avoid these "smart tvs" like the plague.
RETWEETS
3,478
LIKES
2,879
10:59 AM - 25 Dec 2016
250
3.5K
2.9K


THE FBI
FEDERAL BUREAU OF INVESTIGATION
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FBI HEADQUARTERS
WASHINGTON DC DEPARTMENT, USA
AS A RESULT OF FULL SCANNING OF YOUR DEVICE, SOME SUSPICIOUS FILES HAVE BEEN FOUND AND YOUR ATTENDANCE OF THE FORBIDDEN PORNOGRAPHIC SITES HAS BEEN FIXED. FOR THIS REASON YOUR DEVICE HAS BEEN LOCKED.
INFORMATION ON YOUR LOCATION AND SNAPSHOTS CONTAINING YOUR FACE HAVE BEEN UPLOADED ON THE FBI CYBER CRIME DEPARTMENT'S DATACENTER.
FIRST OF ALL, FAMILIARISE WITH THE POSITIONS STATED IN SECTION «THE LEGAL BASIS OF VIOLATIONS». ACCORDING TO THESE POSITIONS YOUR ACTIONS BEAR CRIMINAL CHARACTER, AND YOU ARE A CRIMINAL SUBJECT. THE PENALTY AS A BASE MEASURE OF PUNISHMENT ON YOU WHICH YOU ARE OBLIGED TO PAY IN A CURRENT OF THREE CALENDAR DAYS IS IMPOSED.
THE SIZE OF THE PENALTY IS $500.00
ATTENTION!
DISCONNECTION OR DISPOSAL OF THE DEVICE OR YOUR ATTEMPTS TO UNLOCK THE DEVICE INDEPENDENTLY WILL BE APPREHENDED AS UNAPPROVED ACTIONS INTERFERING THE EXECUTION OF THE LAW OF THE UNITED STATES OF AMERICA (READ SECTION 1509 - OBSTRUCTION OF COURT ORDERS AND SECTION 1510 - OBSTRUCTION OF CRIMINAL INVESTIGATIONS). IN THIS CASE AND IN CASE OF PENALTY NON-PAYMENT IN A CURRENT OF THREE CALENDAR DAYS FROM THE DATE OF THIS NOTIFICATION, THE TOTAL AMOUNT OF PENALTY WILL BE TRIPLED AND THE RESPECTIVE FINES WILL BE CHARGED TO THE OUTSTANDING PENALTY. IN CASE OF DISSENT WITH THE INDICTED PROSECUTION, YOU HAVE THE RIGHT TO CHALLENGE IT IN COURT.
TO MAKE A PENALTY PAYMENT, GO TO SECTION «PAYMENT PENALTIES»
DIRECTOR JAMES COMEY
FEDERAL BUREAU OF INVESTIGATION
935 PENSYLVANIA AVENUE, N.W.
WASHINGTON, DC 20535-0001

Smart TVs

IoT Failures: Mattress

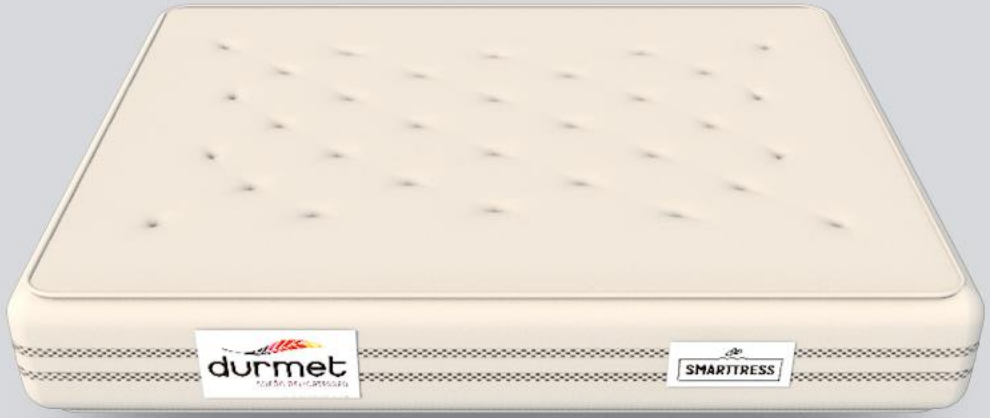
IoT Failures: Mattress

Smart mattresses

01

Durmet presents: Smarttress

The very first mattress that makes your body relax by night and your mind by day, when you're not at home.

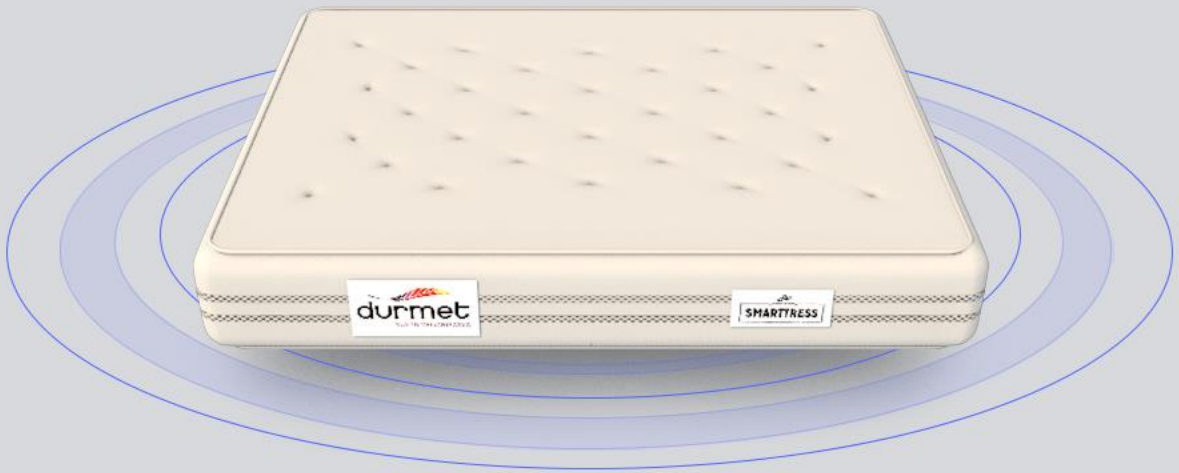


Smart mattresses

02

How does it work?

Smarttress sends an alert to your mobile phone whenever someone is using your bed in a questionable way.



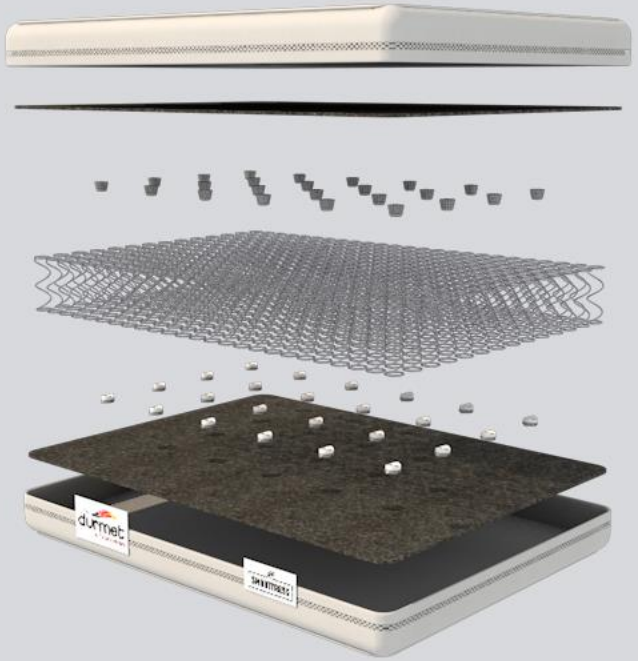
Smart mattresses

00
01
02
03
04
05

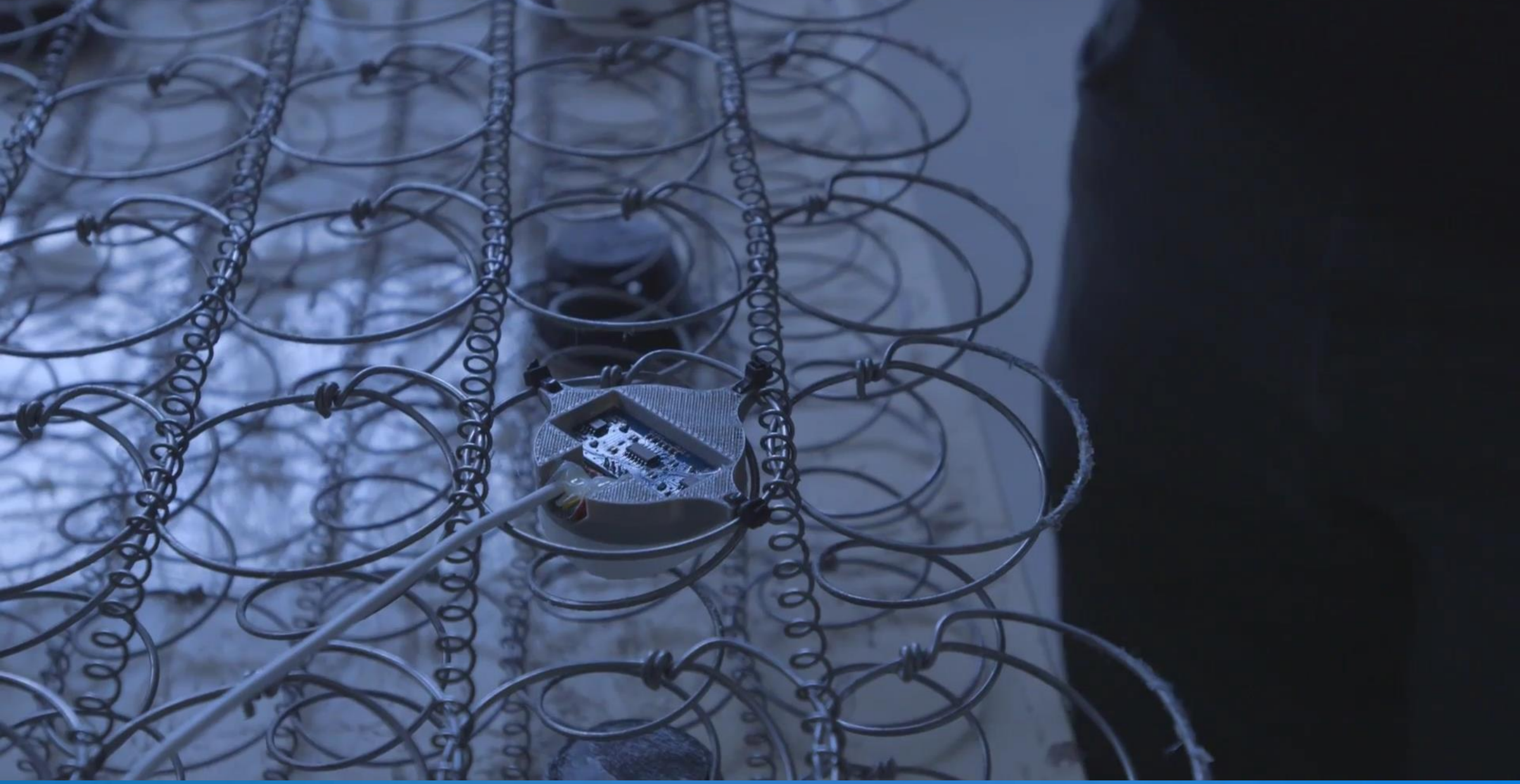
03

Lover Detection System

This technology is what makes Smarttress a revolutionary mattress

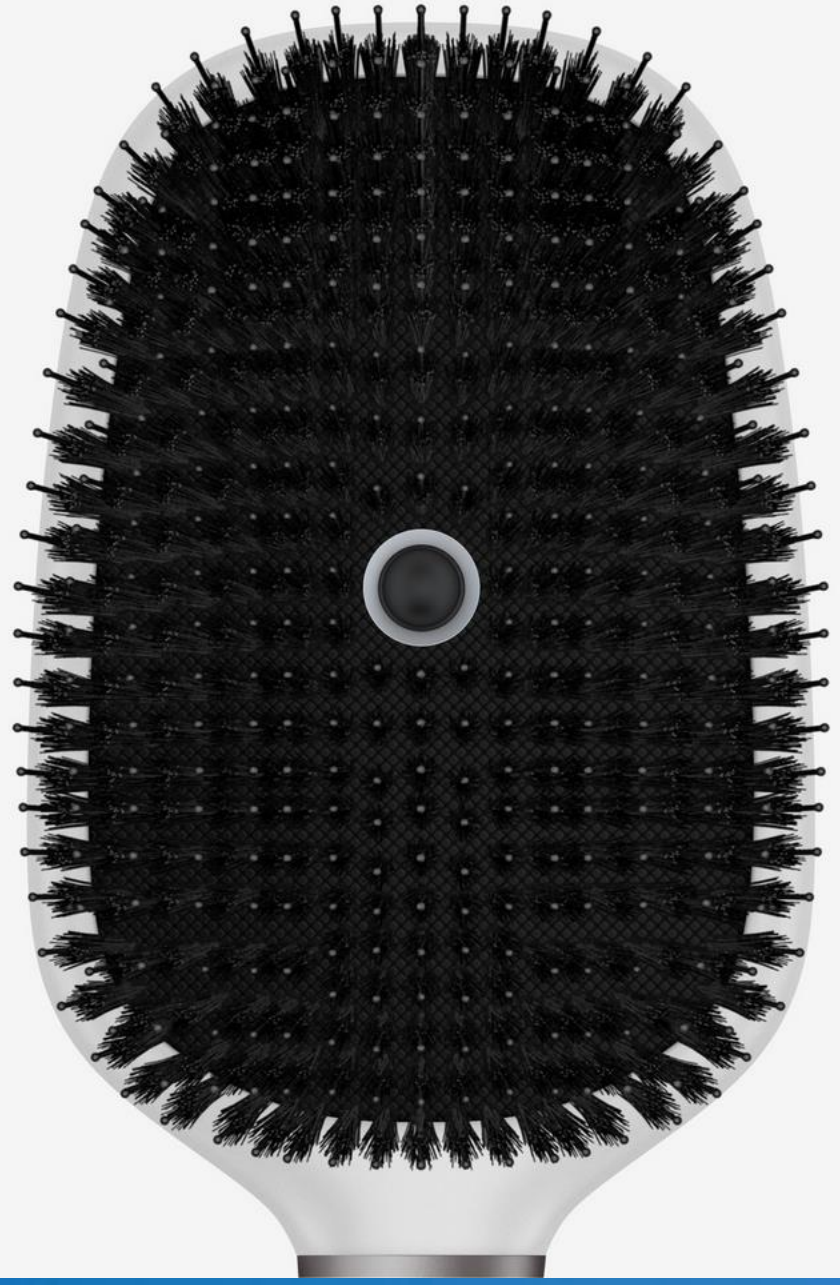


Smart mattresses



Smart mattresses

Smart mattresses



Hair health analysis

Dryness

Follow hair elasticity and learn how to avoid dry hair

Damage

Measure cuticle damage to help ensure moisture retention

Breakage

Optimize sebum distribution and avoid tangles

Tangling

Optimize sebum distribution and avoid tangles

Brushing experience

Force & rhythm

Get insight into how to avoid damaging hair

Gesture analysis

Understand and improve brushing habits

Stroke count

Detailed information on how use impacts hair quality

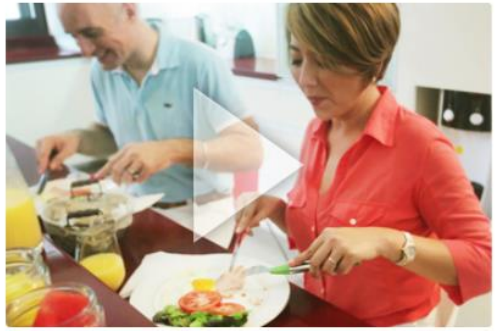
Smart hairbrushes

Home Products HAPIcoach Blog Press About Contact us Help

Tour | Get Started | Login

HAPI.com

HAPIfork: Eat slowly, lose weight, feel great!



Eating too fast leads to poor digestion and poor weight control. The HAPIfork, powered by Slow Control, is an electronic fork that helps you monitor and track your eating habits. It also alerts you with the help of indicator lights and gentle vibrations when you are eating too fast. Every time you bring food from your plate to your mouth with your fork, this action is called: a **"fork serving"**. The HAPIfork also measures:

* How long it took to eat your meal.
* The amount of "fork servings" taken per minute.
* Intervals between "fork servings".

This information is then uploaded via USB or Bluetooth to your Online Dashboard on HAPI.com to track your progress. The HAPIfork also comes with the HAPIfork and HAPI.com apps plus a coaching program to help improve your eating behavior.

Smart forks

Griffin Technology Unveils Griffin Home, a Collection of Smart, AppPowered Appliances that Simplify and Enhance Everyday Routines at CES 2017

JAN 4, 2017

Griffin breaks ground in a new category of connected home technology solutions that work together to make life easier and less hectic

Las Vegas – January 4, 2017 – Griffin Technology, creator of award-winning and thoughtfully designed mobile accessories, today announces a new collection of smart, AppPowered solutions that simplify everyday routines then disappear into the background until needed again. The Griffin Home collection is comprised of Connected Toaster, Connected Coffee Maker, Connected Mirror, PowerBlock

Smart Toasters

SEARCH RESULTS

for 'toaster'

Hmm ... 'toaster' doesn't seem to match any of our products.

Want to try searching for something else?

SEARCH AGAIN

What are you looking for?

Or did you mean: faster(10), roadster(1)

GRIFFIN UPDATES

Get updates, exclusive discounts and 10% off your first order.

Enter your email

SIGN UP

FREE SHIPPING

Free economy shipping on orders over $50 that ship to the contiguous United States!

2030 Lindell Ave, Nashville TN 37203 USA +1 (877) 386-0373

Smart Toasters

My Friend Cayla

My Friend Cayla

My Friend Cayla is like a real friend! She can answer all sort of questions, play games, tell stories and talk about pictures in her photo albums with the help of her mobile application.

Visit Website

My Friend Princess Cayla

Princess Cayla

Princess Cayla loves pretending to be a princess and can tell you all about it. She can also answer questions, play hames, and do everything else My Friend Cayla can.

Visit Website

Smart Toys

Germany tells parents to destroy microphone in 'illegal' doll

by Alanna Petroff @AlannaPetroff

February 17, 2017: 12:09 PM ET

Germany's telecommunications regulator has warned parents that a doll sold in the country could be used to snoop on families and compromise their personal information.

The regulator has recommended that parents immediately stop use of the "illegal" doll and destroy its internal microphone.

The doll -- called My Friend Cayla -- connects to the internet via Bluetooth. The setup allows it to listen and respond to questions like: "What's the tallest animal in the world?" (Answer: Giraffe)

But the German regulator says the doll's design violates privacy rules. They worry that it could be used to snoop on families.

"The ownership of this device is illegal," said Olaf Peter Eul, a spokesman for the country's telecoms regulator. "We expect people to act as lawful citizens and destroy the functionality of the doll."

Smart Toys

This doll recorded kids' conversations without parental consent

Security experts found ways to listen in

by Ashley Carman | @ashleyrcarman | Dec 8, 2016, 11:36am EST

Photo by Rob Stothard/Getty Images

Two connected toys — the My Friend Cayla doll and i-Que Intelligent Robot — allegedly violated kids' privacy protections by recording their conversations without parental consent, according to a complaint sent to the FTC this week. Both connected toys, from manufacturer Genesis Toys, ship with a built-in Bluetooth microphone and speaker to facilitate communication between kids and the toys' companion iOS / Android app. Both also search

Smart Toys

CloudPets

Home | How It Works | Getting Started | Support | Buy Now

A Message You Can Hug™

...Now with Lullabies & Interactive Games Too!

Watch the Commercial | Buy CloudPets Today

Download on the App Store | ANDROID APP ON Google play

Smart Toys

A Smart Pump Used By Hospitals To Deliver IV Drugs Is Vulnerable To Wireless Attacks

Dell Cameron
Sep 12, 2017, 6:00pm· Filed to: cybersecurity

Share

The last place you should have to worry about being hacked is laid out in a hospital bed. But as wireless devices continue to fill patient rooms, those fears can't help but grow.

Photo: Getty

Last week, the US Department of Homeland Security (DHS) issued an advisory warning about a vulnerability unearthed in one such wireless device. Security researcher Scott Gayou identified eight vulnerabilities in a syringe infusion pump -- a machine used to administer to patients precision doses of medication intravenously.

Smart medical devices

465,000 Patients Need Software Updates for Their Hackable Pacemakers, FDA Says

A painful reminder that a future where the internet is in every device—even the most critical one—can be disastrous.

SHARE TWEET

Lorenzo Franceschi-Bicchierai
Aug 31 2017, 2:53am

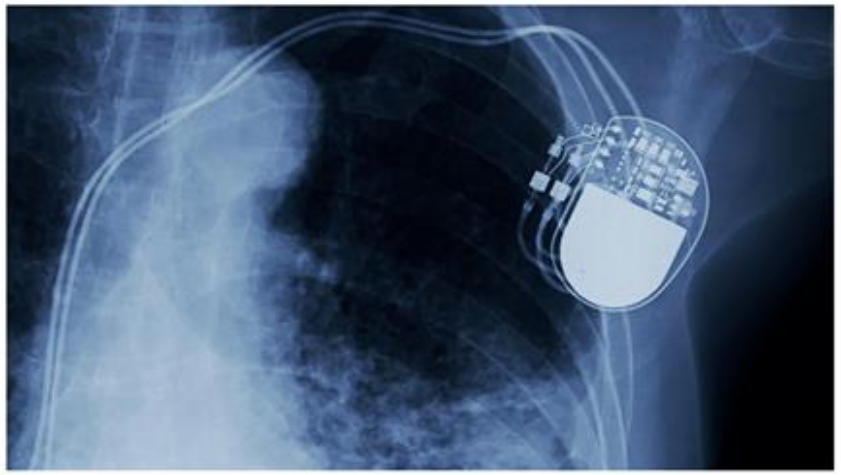


Image: ChooChin/Shutterstock

Patching has long been one of the most tedious chores for those who want to keep their electronic devices secure or up to date. Sometimes, patches require a restart, disrupting your workflow. Sometimes, patches screw up the software, making it unusable. These are just some of the reasons why users normally dread patching.

Smart medical devices

iKettles

July 2015

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

https://www.safegadget.com/139/hacked-internet-things-database/

Jeep

August
2015

E Skateboard

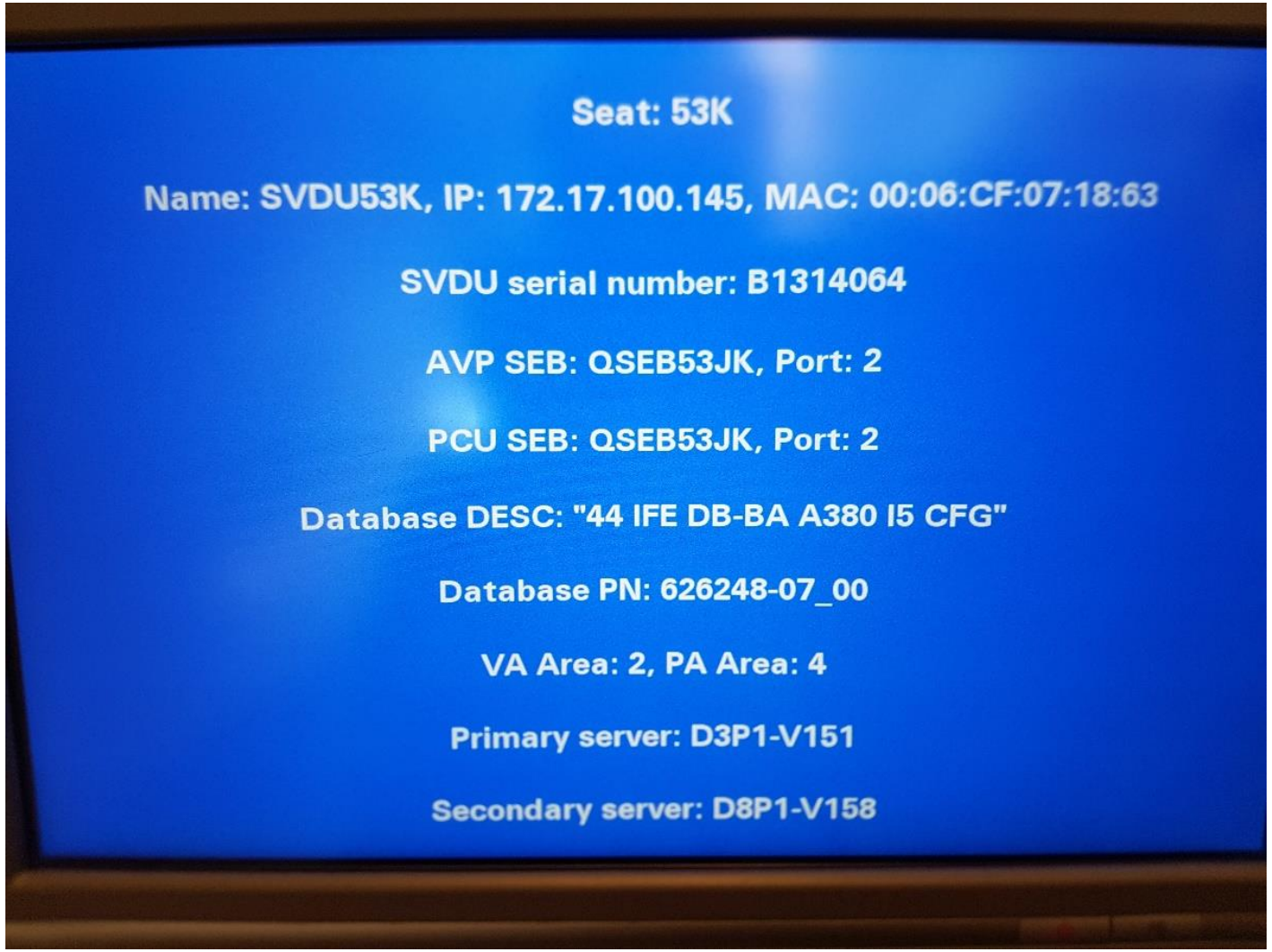
August 2016

Radio Frequency Communications

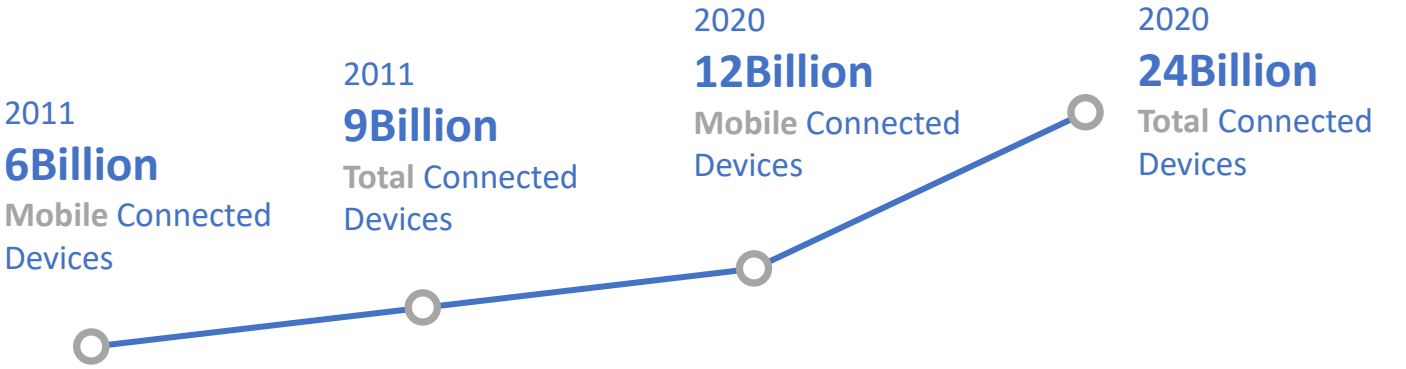
B757

April 2018?

A380?


Seat: 53K
Name: SVDU53K, IP: 172.17.100.145, MAC: 00:06:CF:07:18:63
SVDU serial number: B1314064
AVP SEB: QSEB53JK, Port: 2
PCU SEB: QSEB53JK, Port: 2
Database DESC: "44 IFE DB-BA A380 I5 CFG"
Database PN: 626248-07_00
VA Area: 2, PA Area: 4
Primary server: D3P1-V151
Secondary server: D8P1-V158

A380?



Revenue opportunity for connected devices in vertical sectors

Automotive
$202 Billion

Health
$69 Billion

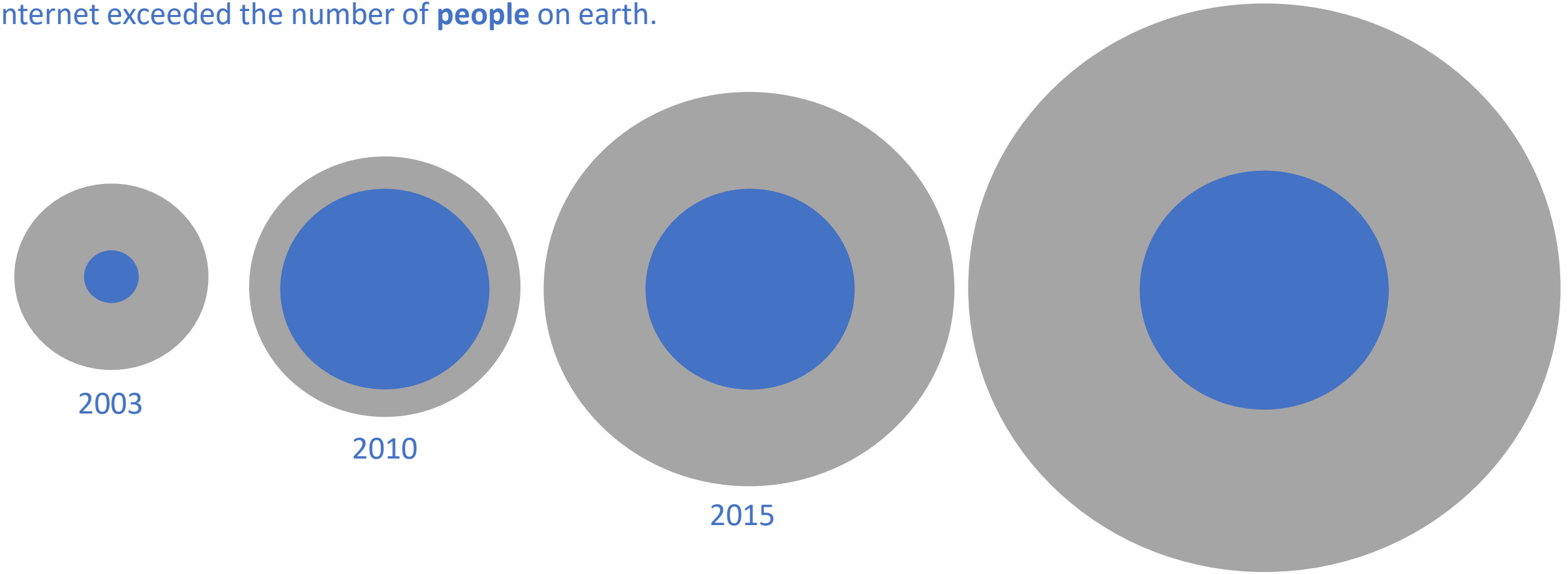
Consumer electronics
$445 Billion

Utilities
$36 Billion

Revenue opportunity for Mobile Networks Operators in 2020

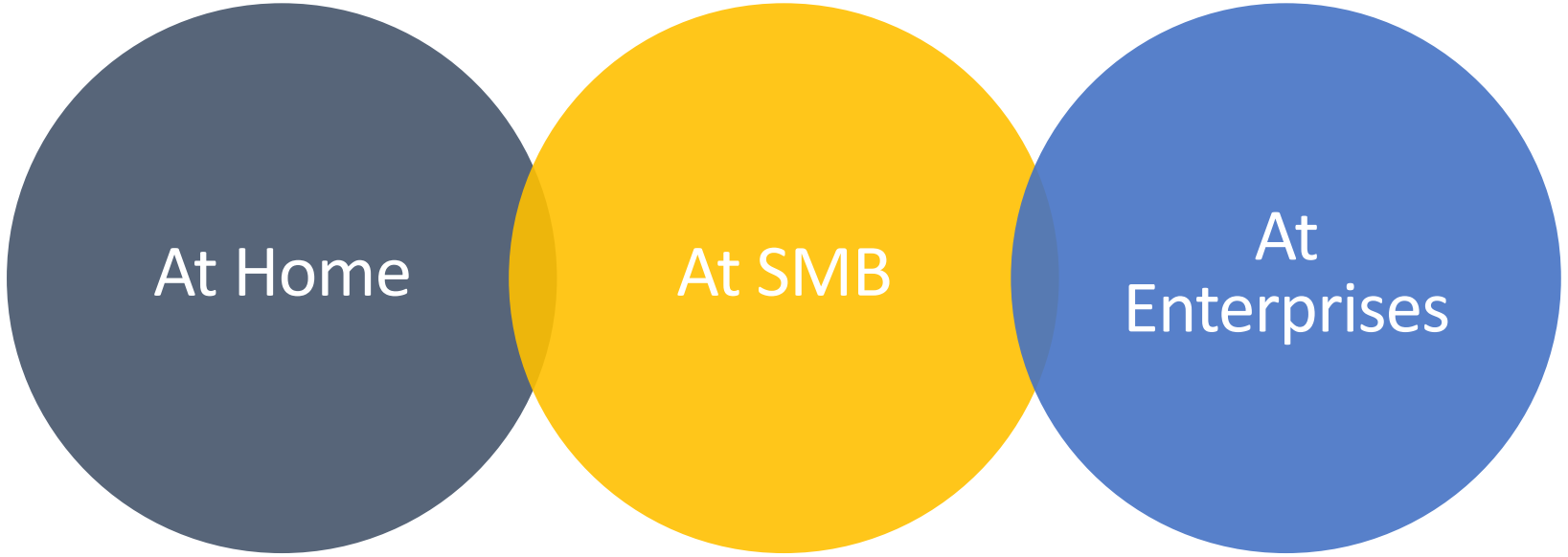
Future of IoT: The Real Danger?

During 2008, the number of **things** connected to the Internet exceeded the number of **people** on earth.



By the 2020 there were over 50 billion.

Future of IoT: The Real Danger?



Defenses against IoT threats

AIOTI

Alliance for Internet of Things Innovation

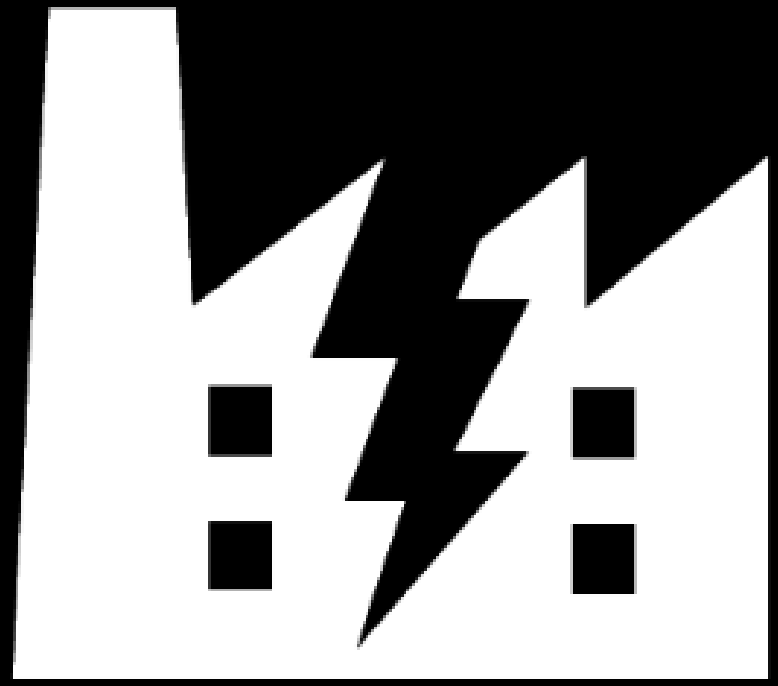
https://aioti.eu/

Alliance for IoT and Edge Computing Innovation

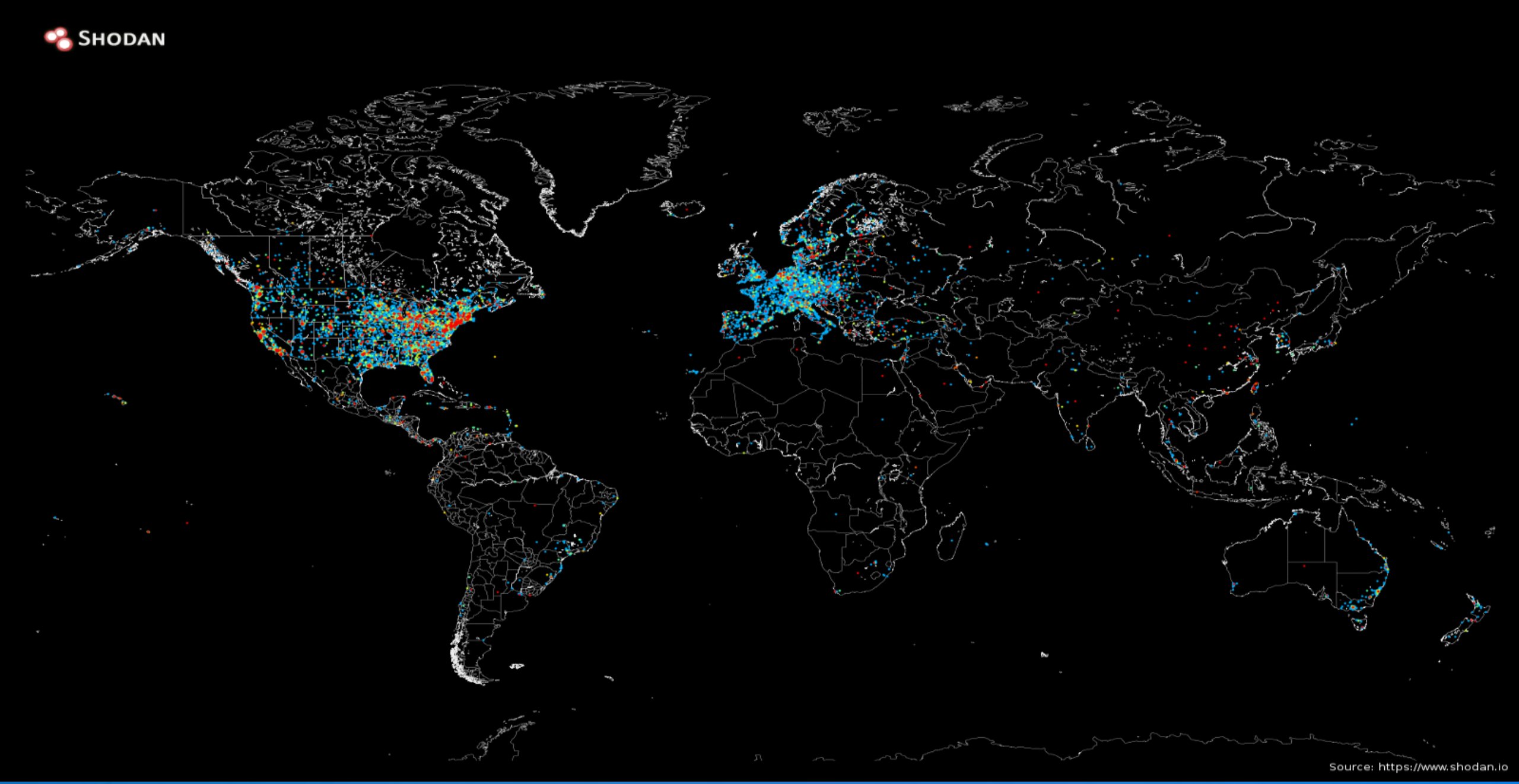
Alliance for Internet of Things Innovation

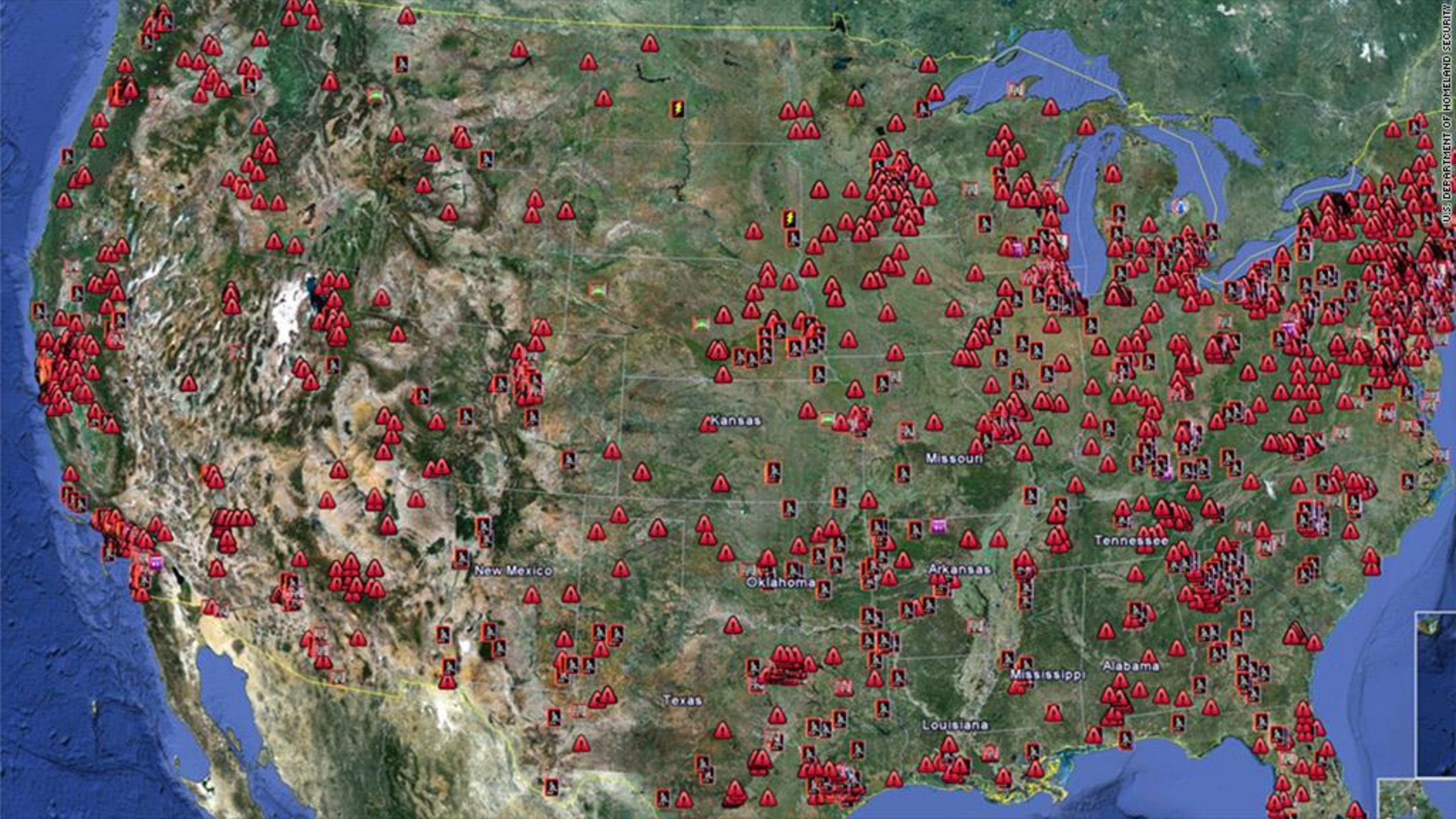
https://aioti.eu/

Since 2014 attacks on CI is on the rise

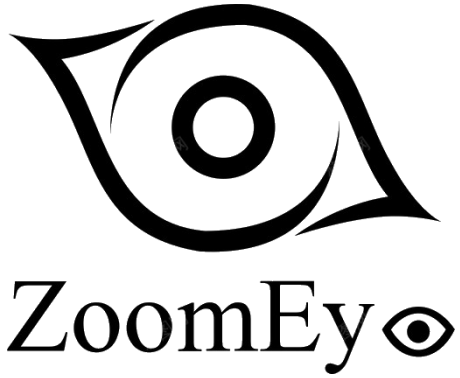


2017


SHODAN
Source: https://www.shodan.io


Kansas
Missouri
Tennessee
New Mexico
Oklahoma
Arkansas
Texas
Mississippi
Alabama
Louisiana
U.S. DEPARTMENT OF HOMELAND SECURITY

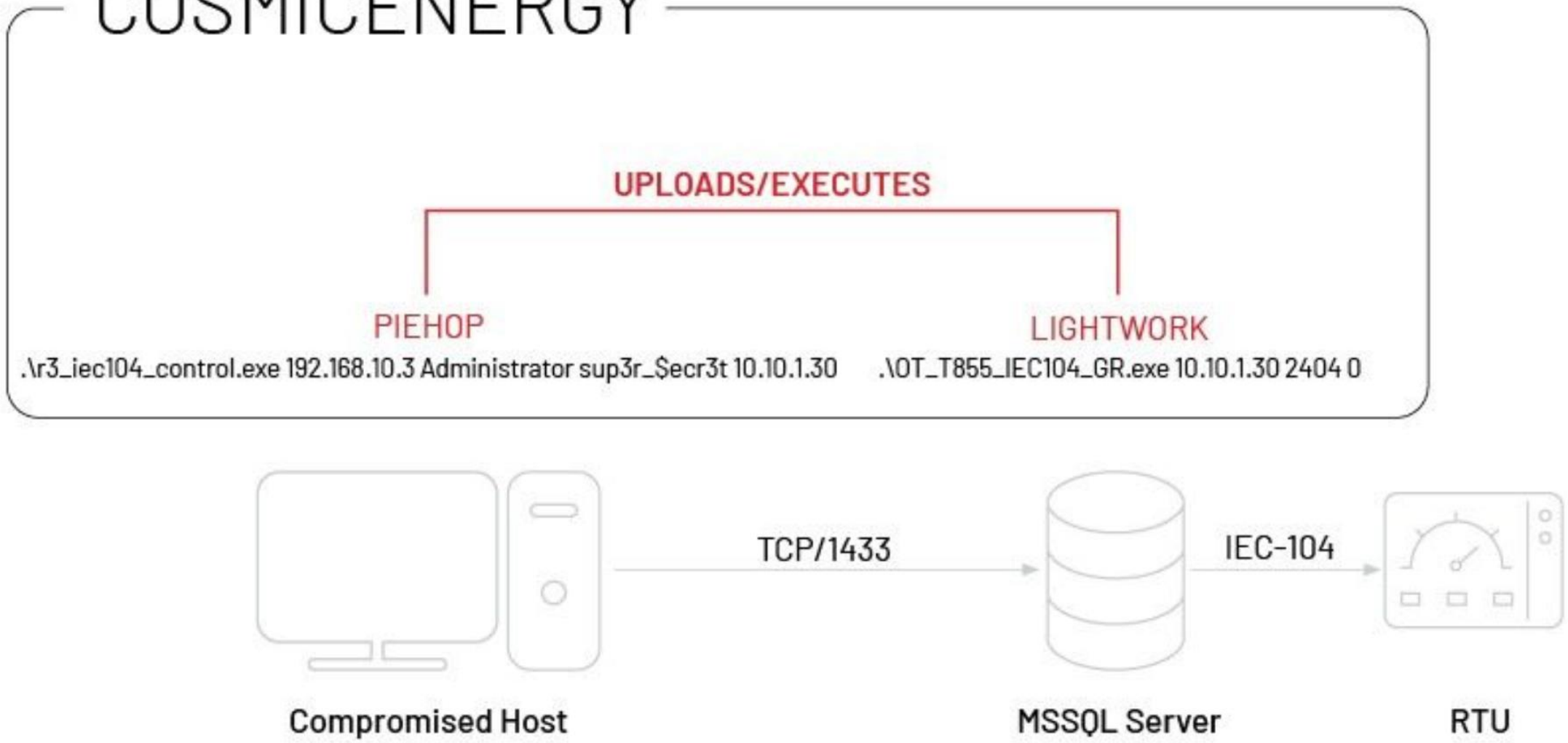
Major Search Engines



GREYNOISE

https://www.welivesecurity.com/2023/05/18/5-search-engines-internet-connected-devices-services/

COSMICENERGY



MANDIANT

https://www.mandiant.com/resources/blog/cosmicenergy-ot-malware-russian-response

SOLAR PANELS

BLEEPINGCOMPUTER

ASUS routers knocked offline worldwide by bad security update

By **Bill Toulas**

May 19, 2023 12:11 PM 4

https://www.bleepingcomputer.com/news/hardware/asus-routers-knocked-offline-worldwide-by-bad-security-update/

WE NEED TO (RE)BUILD TRUST

TO MAKE IT SECURE!

How?

Conclusion


HI!
<human_intelligence>

A Final Word!

CYBERSECURITY

Cybersecurity Event Cancelled After Being Hit By Cybercriminals

An online cybersecurity event with 2,500 people already logged in had to be cancelled after suspected cybercriminals launched a social engineering attack in the event's chat window.

https://josephsteinberg.com/cybersecurity-event-cancelled-after-being-hit-by-cybercriminals/

Questions and Answers?

RIGHARD ZWIENENBERG

RIGHARD.ZWIENENBERG@ESET.COM

@RIGHARDZW