uc3m | Universidad Carlos III de Madrid

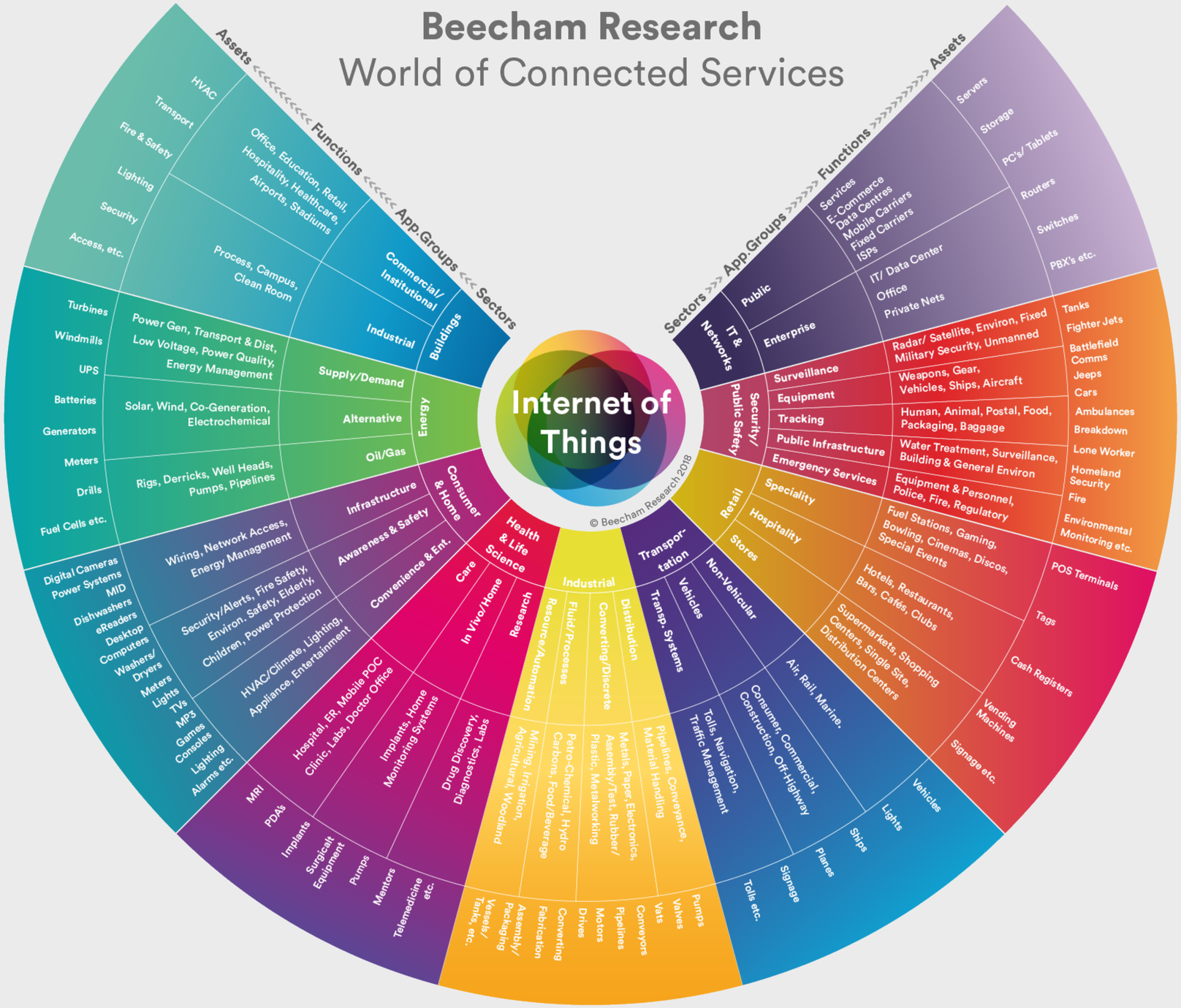
Security & Privacy in the Internet of Things: A Drama in 70 Tweets

Juan Tapiador
@0xjet

May 2019

vision

Beecham Research
World of Connected Services

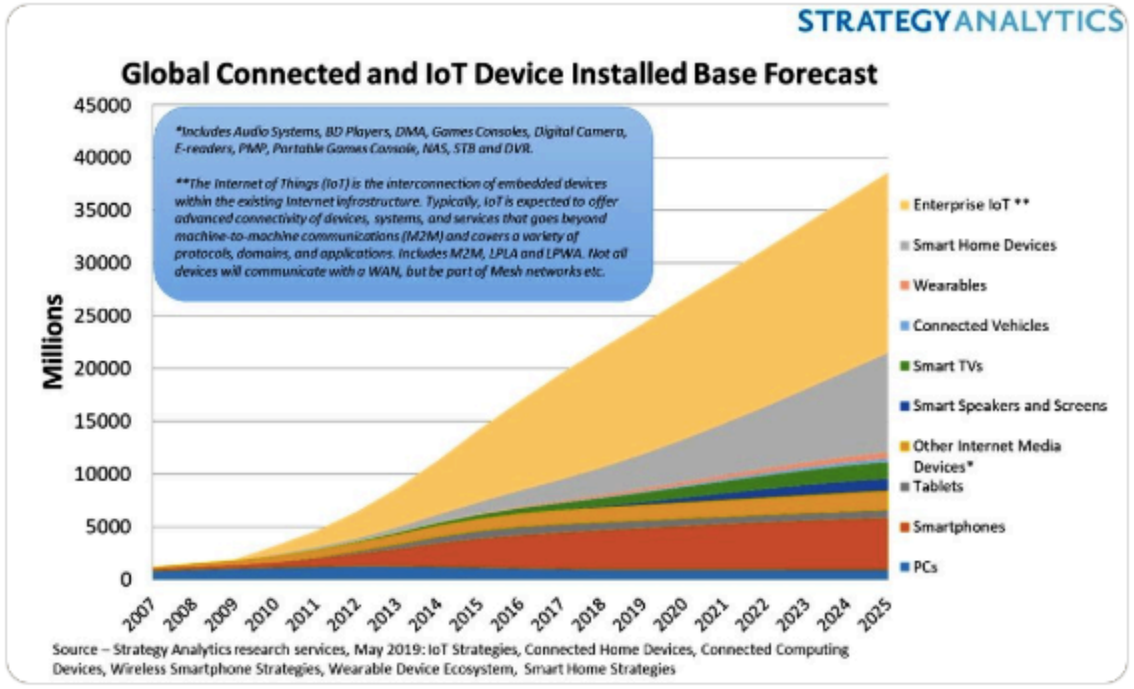


numbers

Digital TV News
@digitaltvnews

Follow

IoT now numbers 22 billion devices, but where is the revenue? bit.ly/2LVPgUy #DigitalTV #MarketResearch #SmartHome #Worldwide

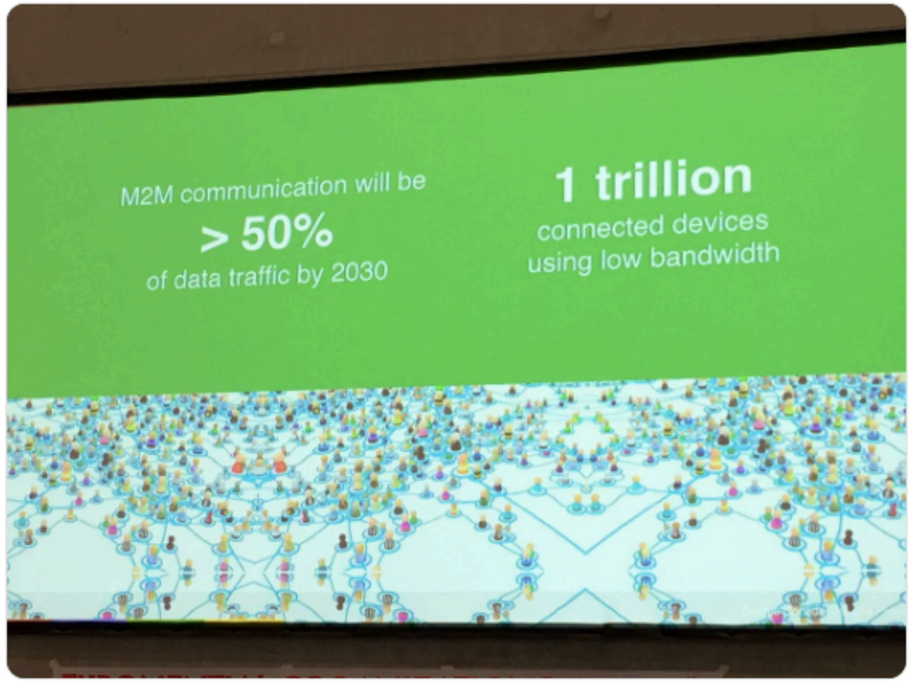


7:33 AM - 21 May 2019

Carsten Stöcker
@CarstenStoecker

Follow

By 2030:
1 trillion #connecteddevices,
M2M >50% of all data traffic. In need for decentral Tx layer.
@salimismail



1:40 AM - 22 Aug 2016

11 Retweets **13** Likes

Stephen Chey
@CheyStephen

Follow

Japan assigns eleven-digit numbers starting ‘070’, ‘080’ and ‘90’ for mobile handsets (including smartphones), while eleven-digit numbers beginning ‘020’ have been used for IoT devices since January 2017.

TeleGeography

Japan reveals plan to create ten billion 14-digit mobile pho...
The Japan Times writes that Japan’s Ministry of Internal Affairs and Communications (MIC) has revealed plans to create around ten billion 14-digit mobile phone numbers starting with ‘020’ for...
telegeography.com

4:46 AM - 16 May 2019

Gerri Elliott
@gerri_elliott

Follow

Predictions to ground us as we start Mobile World Congress in Barcelona. By 2022:
- There will be 5.7B global mobile users.
- Data from mobile devices will increase 7x. 79% will be video.
- IOT/M2M traffic will increase 8x.
Cisco VNI 2019 #MWC2019 #WeAreCisco

12:43 AM - 25 Feb 2019

35 Retweets **114** Likes

35 114

Chetan Bhawani
@chetanbhawani

Follow

Some of the recent achievements of Xiaomi. Big numbers there for their IoT products and ecosystem. #GizmoTimesatMWC

1:48 AM - 24 Feb 2019

50 Retweets **64** Likes

34 50 64

smart

Internet of Shit
@internetofshit

Following

Alexa in a toilet. The literal internet connected shitter has arrived.

Kohler's smart toilet promises a 'fully-immersive experience'
Truly, we live in an age of wonders
theverge.com

2:13 PM - 6 Jan 2019

565 Retweets **1,713** Likes

133 565 1.7K

Tim Bradshaw
@tim

Follow

CES, we may already have a winner. Meet @Kohler's Numi 2.0, the Alexa-enabled "intelligent toilet", with "personalized cleansing and dryer functions, a heated seat, and high-quality built-in speakers" AND "dynamic and interactive multi-colored ambient and surround lighting"

6:39 AM - 4 Jan 2019

98 Retweets **226** Likes

The Verge
@verge

Follow

Samsung's new fridge will ping your phone if you leave the door open
theverge.com/2019/1/7/18169 …

8:56 AM - 13 Jan 2019

246 Retweets **947** Likes

200 246 947

Internet of Shit
@internetofshit

Following

why the fuck doesn't it just close the door itself if it's so smart

The Verge @verge
Samsung's new fridge will ping your phone if you leave the door open theverge.com/2019/1/7/18169…

1:42 PM - 13 Jan 2019

38,634 Retweets **105,842** Likes

592 39K 106K

promises


Telefónica
@Telefonica
Follow
Building a secure future for the IoT
m2m.telefonica.com/blog/building- ... #IoT
@m2mtelefonica
4:25 AM - 16 Jan 2015
4 Retweets 5 Likes
4
5
S IN IOT STANDS FOR SECURITY
The S in IoT stands for Security
The 'S' in IoT stands for security.

The future is private.

Martin Moschek
@MartinMoschek

Follow

Mark Zuckerberg: “The future is private.”
Sundar Pichai: “The present is private."
#GoogleIO #F8 tcrn.ch/2WCI0xY

11:45 PM - 16 May 2019

2 Likes

2


THIS IS FINE.
THIS ISN'T GONNA END WELL.

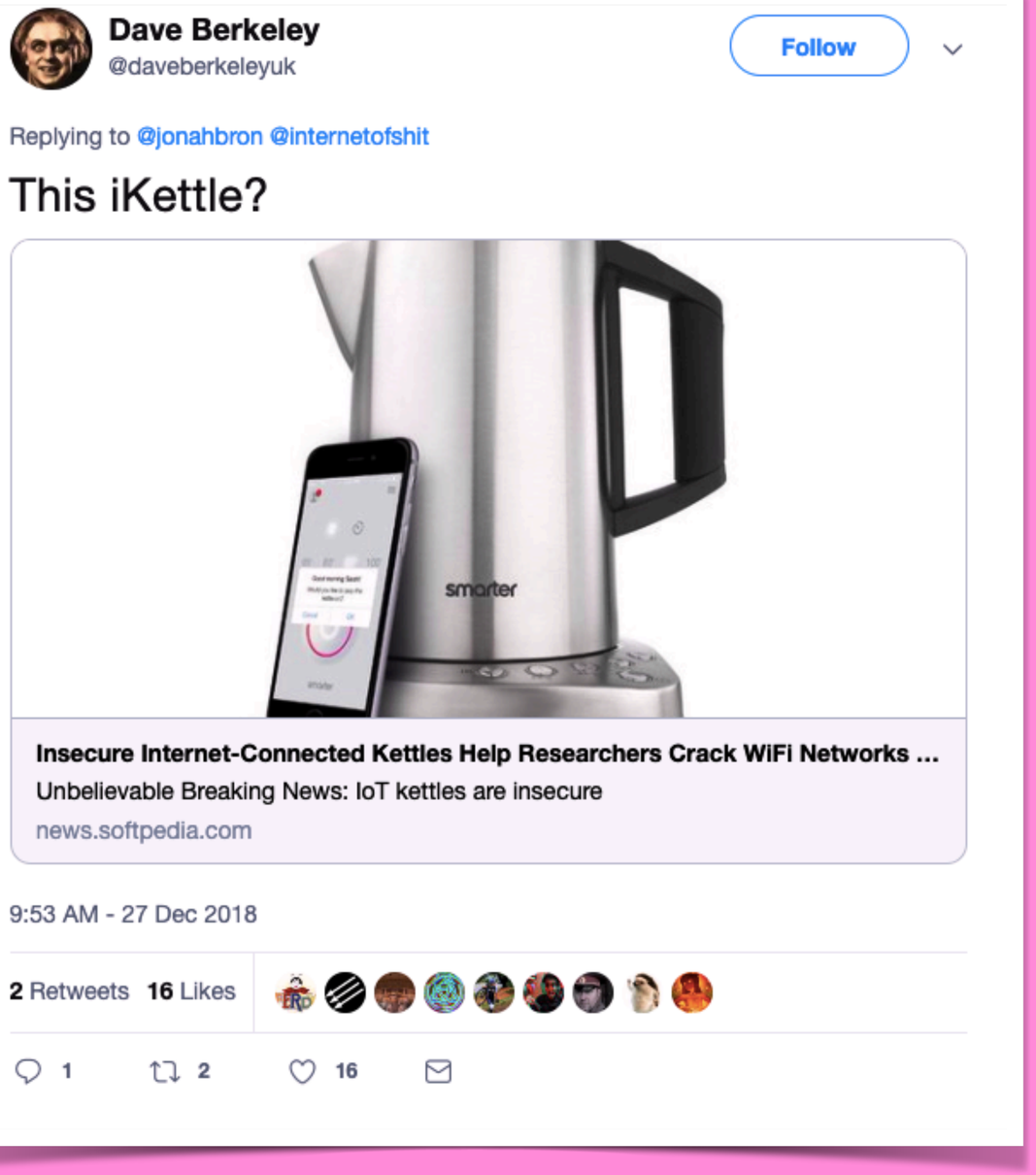
home

Insecure Internet-Connected Kettles Help Researchers Crack WiFi Networks Across London

Unbelievable Breaking News: IoT kettles are insecure

Oct 20, 2015 09:14 GMT · By Catalin Cimpanu · Share:

Security researchers at Pen Test Partners have found a security vulnerability in the iKettle Wi-Fi Electric Kettle that allows attackers to crack the password of the WiFi network to which the kettle is connected.



BBC News (UK)
@BBCNews

Follow

MiSafes' child-tracking smartwatches are 'easy to hack'

Hi-tech watches let children be spied on

Researchers find a way to reveal the locations of children wearing MiSafes watches and call them.

bbc.com

6:50 PM - 14 Nov 2018

23 Retweets **19** Likes

4 23 19

Pen Test Partner's Ken Munro and Alan Monie learned of the product's existence when a friend bought one for his son earlier this year.

Out of curiosity, they probed its security measures and found that easy-to-find PC software could be used to mimic the app's communications.

This software could be used to change the assigned ID number, which was all it took to get access to others' accounts.

This made it possible to see personal information used to register the product, including:

- a photo of the child
- their name, gender and date of birth
- their height and weight
- the parents' phone numbers
- the phone number assigned to the watch's Sim card

"It's probably the simplest hack we have ever seen," he told the BBC.

"Once a hacker has the parent's number, they could spoof a call to appear to come from it and the child would now think it's their mum or dad dialling," said Mr Munro.

"This is another example of unsecure products that should never have reached the market," said Gro Mette Moen, the watchdog's acting director of digital services.

click me

Techgear Online
@TechgearOnline

Follow

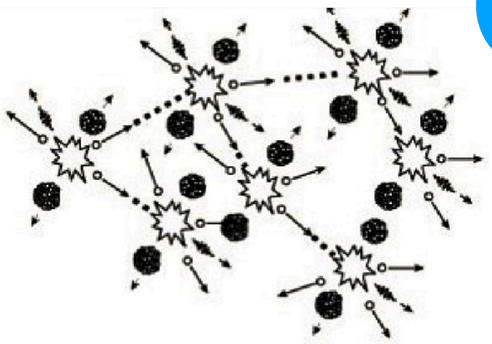
#hack #nerd Smart bulb 7W E27 Wifi Smart LED Light Wireless Bulb Lamp Works with Amazon Alexa Google Home IFFFT RGB Remote Control

11:34 AM - 2 Apr 2019

IoT Goes Nuclear: Creating a ZigBee Chain Reaction

Nov 21, 2018

PDF Slides Video



Eyal Ronen, Colin O'Flynn, Adi Shamir and Achi-Or Weingarten

Creating an IoT worm

Hakin9
@Hakin9

Follow

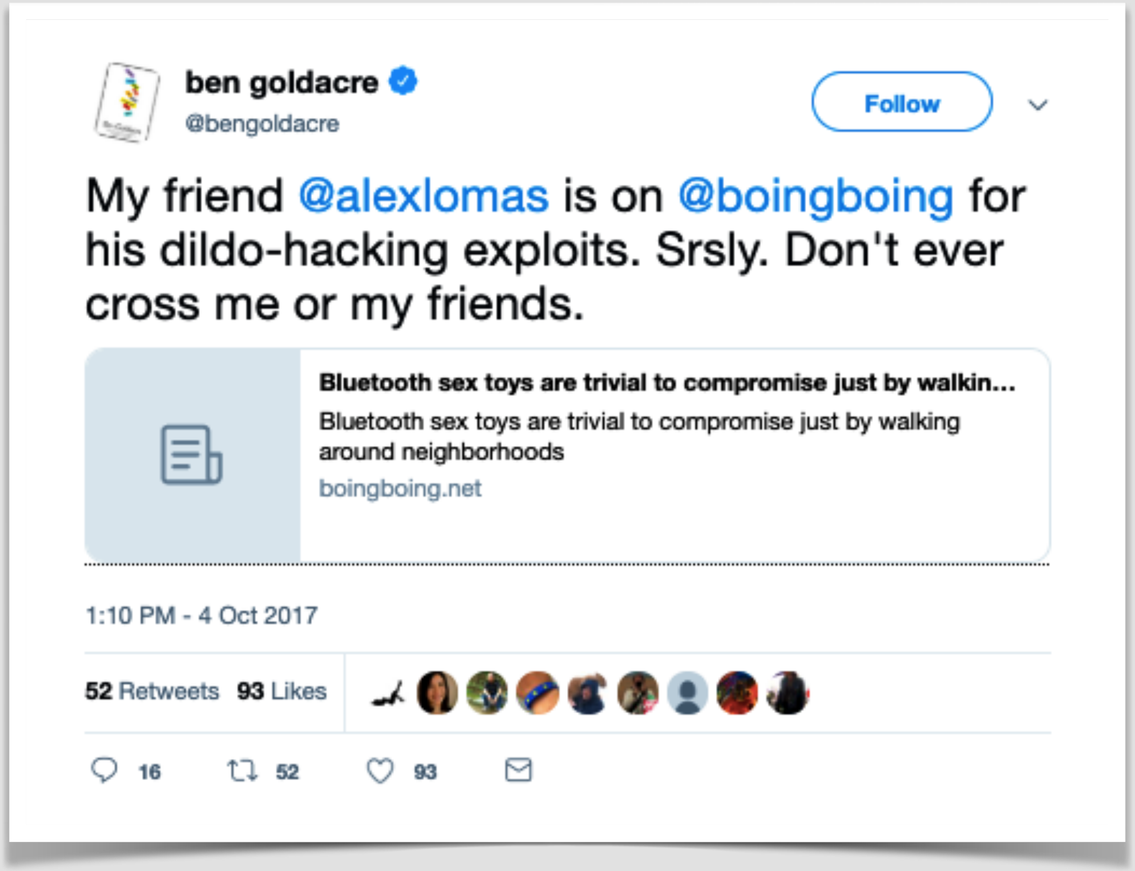
How To Hack A Smart Bulb Using Bluetooth bit.ly/2fXaE9N #infosec #hacking #hackers #pentesting #pentest #programming #coding #data #DataProtection #DataSecurity #cybersecurity #RaspberryPi #linux #opensource #Bluetooth

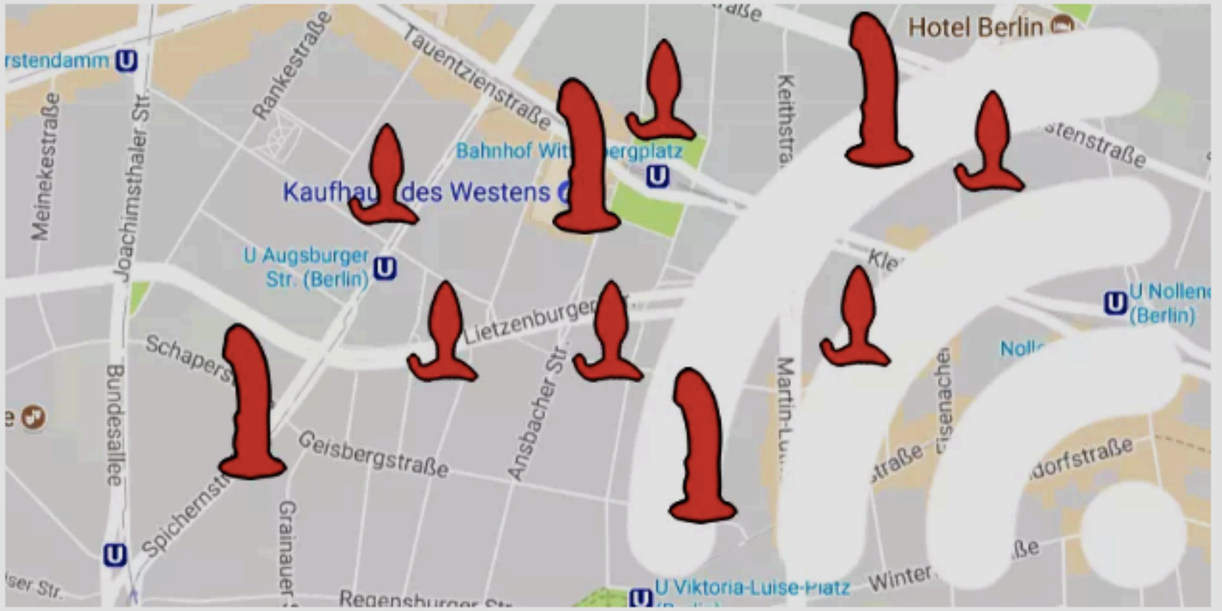
2:30 PM - 18 Apr 2018

12 Retweets 12 Likes

boingboing / CORY DOCTOROW / 11:57 AM TUE OCT 3, 2017

Bluetooth sex toys are trivial to compromise just by walking around neighborhoods





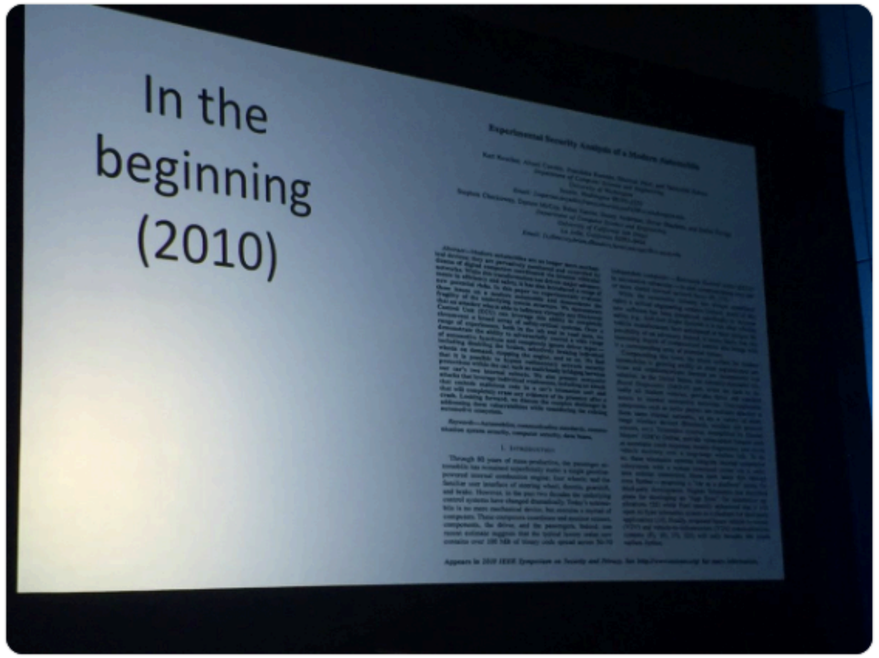
Bluetooth Low Energy (BLE) is the go-to protocol for low-powered networking in personal devices, so "smart" sex-toy manufacturers have adopted it -- despite the protocol's many vulnerabilities. That means that hackers can now wander city streets, detecting and compromising sex toys from the sidewalk, in a practice that Pentest Partners' Alex Lomas has dubbed "Screwdriving" (analogous to "Wardriving").

cars

Arm
@Arm

Follow

"Car hacking really began with an academic paper in 2010. It was not well received at the time." - Charlie Miller #ARMTechCon



9:36 AM - 27 Oct 2016

2 Retweets 1 Like

2 1

Doug Olenick
@DougOlenick

Follow

Car hackers Charlie Miller and Chris Valasek announced their retirement from car hacking at Black Hat. @SCMagazine

3:40 PM - 4 Aug 2016

1 Retweet 2 Likes

1 2

click me

Daniel W. Dieterle
@Cyberarms

Follow

Charlie Miller & Chris Valasek have published all their car hacking tools, data and research notes for FREE!
illmatics.com/carhacking.html

1:11 PM - 25 Apr 2017

87 Retweets 82 Likes

1 87 82

OccupytheWeb
@three_cube

Follow

Automobile Hacking, Part 4: Hacking the Vehicle Keyless Entry System #carhacking #autohacking #iot #cybersecurity bit.ly/2Uh5SWZ

6:52 AM - 19 May 2019

12 Retweets **27** Likes

12 27

The Guardian
@guardian

Follow

Is your car the most stolen model in England and Wales?

Is your car the most stolen model in England and Wales?
Hi-tech thieves are using computers to outsmart electronic security systems, with the Audi S3 and Land Rover Defender most at risk
theguardian.com

1:49 AM - 25 Jun 2016

19 Retweets **17** Likes

6 19 17

click me

THE PRIVACY PROJECT

Companies and governments are gaining new powers to follow people across the internet and around the world, and even to peer into their genomes. The benefits of such advances have been apparent for years; the costs — in anonymity, even autonomy — are now becoming clearer. The boundaries of privacy are in dispute, and its future is in doubt. Citizens, politicians and business leaders are asking if societies are making the wisest tradeoffs. The Times is embarking on this monthslong project to explore the technology and where it's taking us, and to convene debate about how it can best help realize human potential.

Privacy Project ✓
@PrivacyProject

Following

Your driving habits — how fast you drive, how hard you brake, whether you always use your seatbelt — could be valuable to insurance companies. But while you can turn off location data on your phone, there's no opt-out feature for your car.

Opinion | Your Car Knows When You Gain Weight
Vehicles collect a lot of unusual data. But who owns it?
nytimes.com

4:00 AM - 20 May 2019

74 Retweets **90** Likes

What Do They Know, and How Do They Know It?

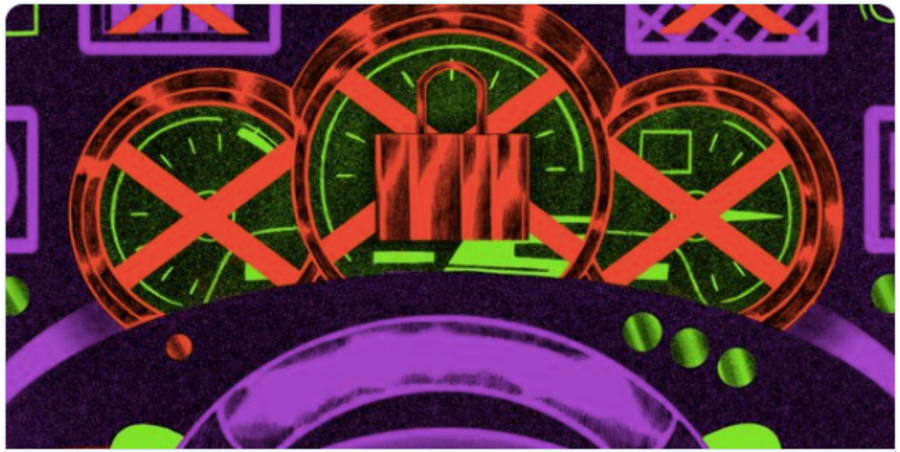
DEBATE
What Should Be Done About This?

ACTION
What Can I Do?

Privacy Project
@PrivacyProject

Following

Today's cars are equipped with an always-on wireless transmitter that constantly sends vehicle performance and maintenance data to the manufacturer. Modern cars collect as much as 25 gigabytes of data per hour.



Opinion | Your Car Knows When You Gain Weight
Vehicles collect a lot of unusual data. But who owns it?
nytimes.com

1:00 PM - 20 May 2019

15 Retweets **20** Likes

2 15 20

to follow
even to peer
e been
tonomy — are
in dispute,
ness leaders
. The Times is
echnology
how it can

best help realize human potential.

IDEAS
Does Privacy Matter?

BASICS
What Do They Know, and How Do They Know It?

DEBATE
What Should Be Done About This?

ACTION
What Can I Do?

medical

THE PRIVACY PROJECT

Companies and governments are gaining new powers to follo
people across the internet and around the world, and even to
into their genomes. The benefits of such advances have been
apparent for years; the costs — in anonymity, even autonomy
now becoming clearer. The boundaries of privacy are in dispu
and its future is in doubt. Citizens, politicians and business lea
are asking if societies are making the wisest tradeoffs. The Ti
embarking on this monthslong project to explore the technolo
and where it's taking us, and to convene debate about how it c
best help realize human potential.

Privacy Project ✓
@PrivacyProject

Following

We've given up so much of our privacy for so many bad reasons. Here's a good one: the potential for a longer, healthier life.

Opinion | For a Longer, Healthier Life, Share Your Data
Privacy protections are standing in the way of artificial-intelligence programs that could diagnose cancers and screen for genetic disorders.
nytimes.com

4:07 PM - 22 May 2019

2 Retweets **10** Likes

1 2 10

What Can I Do?

EECS at Michigan
@EECSatMI

Follow

In 2008 @DrKevinFu & collaborators demonstrated that defibrillators in patients could be fatally manipulated—the field of medical device security has since grown into a global effort. That landmark paper is now recognized w/ an @IEEESSP Test of Time Award.
news.engin.umich.edu/2019/05/resear ...

6:37 AM - 22 May 2019

10 Retweets **10** Likes

HIPAA Journal
@HIPAAJournal

Follow

Two vulnerabilities have been identified in the Conexus telemetry protocol used by Medtronic MyCareLink monitors

1:01 PM - 22 May 2019

1 Retweet **1** Like

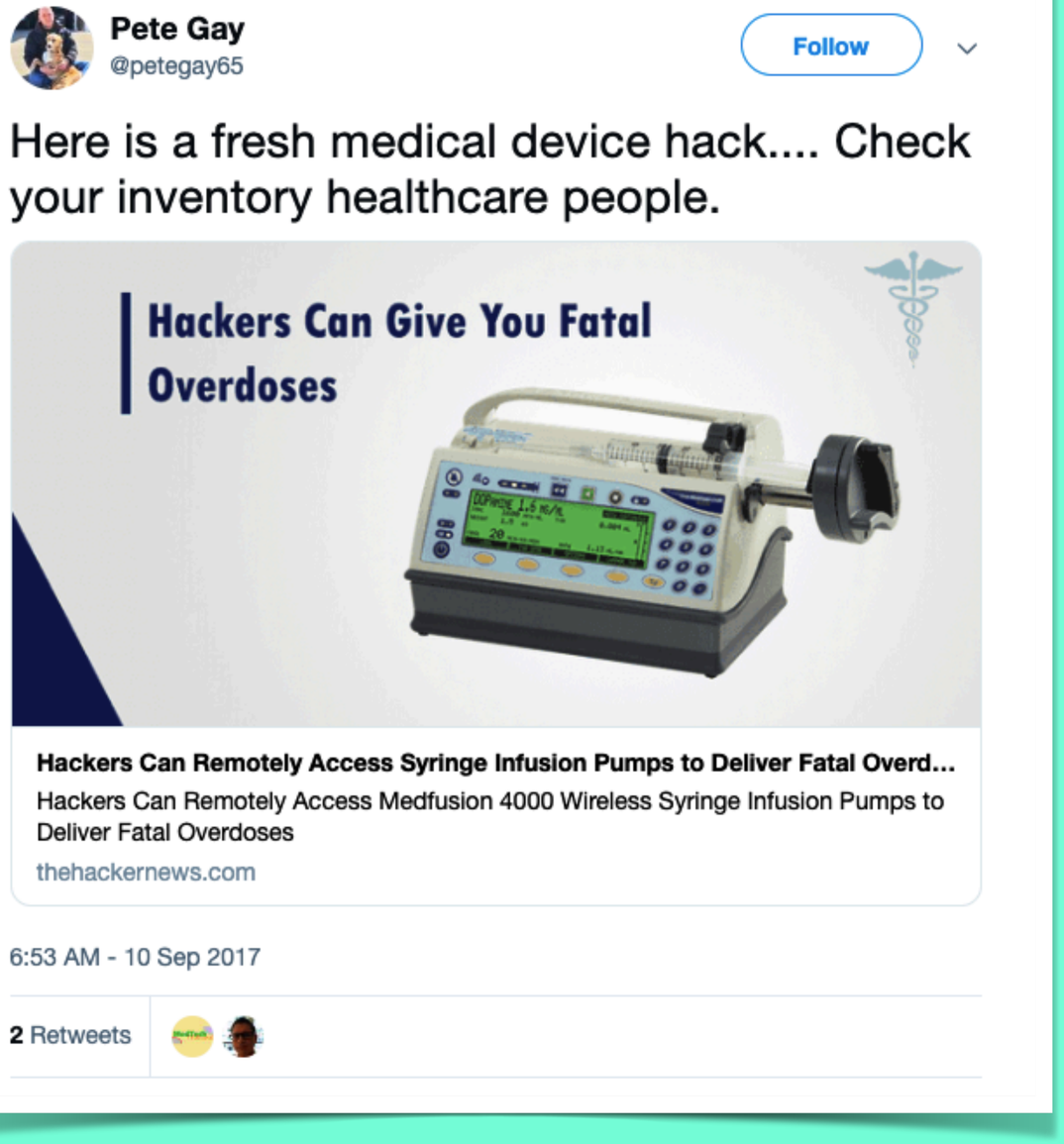
1 1

Two vulnerabilities have been identified in the Conexus telemetry protocol used by Medtronic MyCarelink monitors, CareLink monitors, CareLink 2090 programmers, and 17 implanted cardiac devices. Both vulnerabilities require a low level of skill to exploit, although adjacent access to a vulnerable device would be required to exploit either vulnerability.

The most serious vulnerability, rated critical, is a lack of authentication and authorization controls in the Conexus telemetry protocol which would allow an attacker with adjacent short-range access to a vulnerable device to inject, replay, modify, and/or intercept data within the telemetry communication when the product's radio is turned on.

An attacker could potentially change memory in a vulnerable implanted cardiac device which could affect the functionality of the device.

A second, medium severity vulnerability concerns the transmission of sensitive information in cleartext. Since the Conexus telemetry protocol does not use encryption, an attacker with adjacent short-range access to a vulnerable product could intercept communications and obtain sensitive patient data.

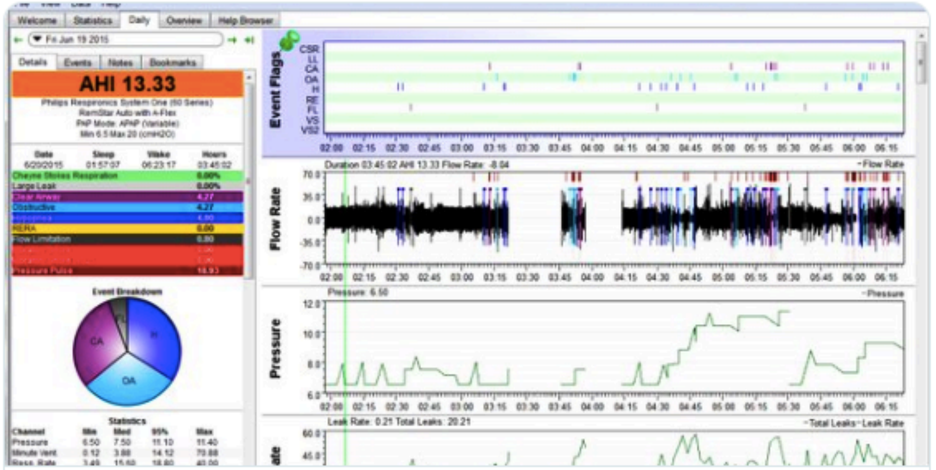

Pete Gay
@petegay65
Follow
Here is a fresh medical device hack.... Check your inventory healthcare people.
Hackers Can Give You Fatal Overdoses
Hackers Can Remotely Access Syringe Infusion Pumps to Deliver Fatal Overd...
Hackers Can Remotely Access Medfusion 4000 Wireless Syringe Infusion Pumps to Deliver Fatal Overdoses
thehackernews.com
6:53 AM - 10 Sep 2017
2 Retweets


Ben Ransford
@br_
Follow
NOBODY PANIC! yrs truly quoted in a thoroughly researched @_JoeCarlson news story about a #medtronic implantable cardiac device vulnerability announced today: startribune.com/750-000-medtro … [1/8]
750,000 Medtronic defibrillators are vulnerable to hacking
A Homeland Security alert cites two types of computer-hacking vulnerabilities in 16 different models of Medtronic implantable defibrillators.
By Joe Carlson Star Tribune | MARCH 21, 2019 — 12:54PM
11:57 AM - 21 Mar 2019
16 Retweets 22 Likes

Xeni Jardin
@xeni

Follow

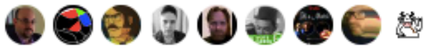
Thousands of sleep apnea sufferers rely on a lone CPAP hacker in Australia whose code circumvents DRM that the medical device makers force on the machines. The hack lets patients modify life-altering settings that doctors are too busy to pay attention to.



Thousands of sleep apnea sufferers rely on a lone Australian CPAP hacker to ...
Thousands of sleep apnea sufferers rely on a lone Australian CPAP hacker to stay healthy
boingboing.net

11:01 AM - 16 Nov 2018

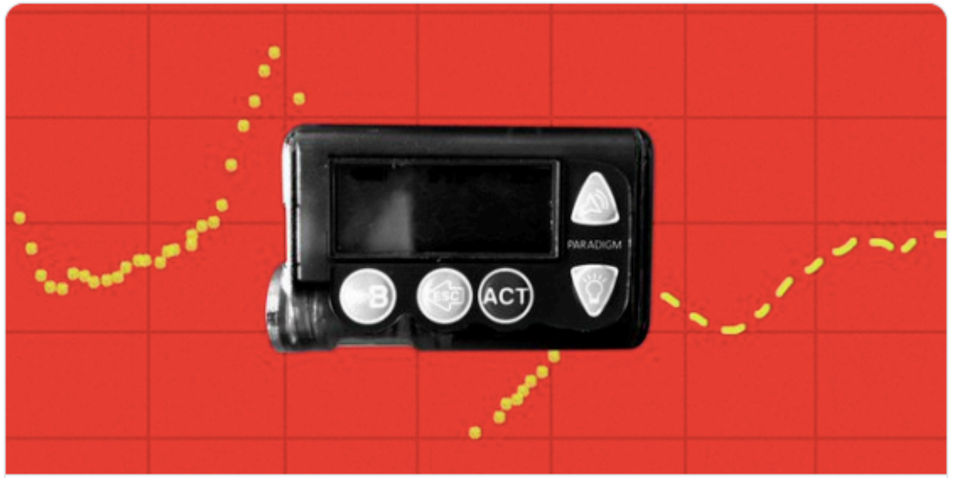
29 Retweets **29** Likes



Daniel W. Dieterle
@Cyberarms

Follow

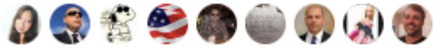
Hacking Insulin Pumps - How an obsolete medical device with a security flaw became a must-have for some patients with type 1 diabetes



People Are Clamoring to Buy Old Insulin Pumps
How an obsolete medical device with a security flaw became a must-have for some patients with type 1 diabetes
theatlantic.com

10:39 AM - 30 Apr 2019

61 Retweets **67** Likes



Beau Woods
@beauwoods

Follow

"We're tremendously concerned about infrastructure being targeted for health care… We didn't learn the lessons of #WannaCry in the United States."

6:23 AM - 21 May 2019

5 Retweets **2** Likes

1 5 2

Beau Woods
@beauwoods

Follow

"The medical device industry is 10-15 years behind on security. I will be candid because by being candid, it allows us to help accelerate and move the industry in the right direction" Michael McNeil @PhilipsHealth

6:23 AM - 21 May 2019

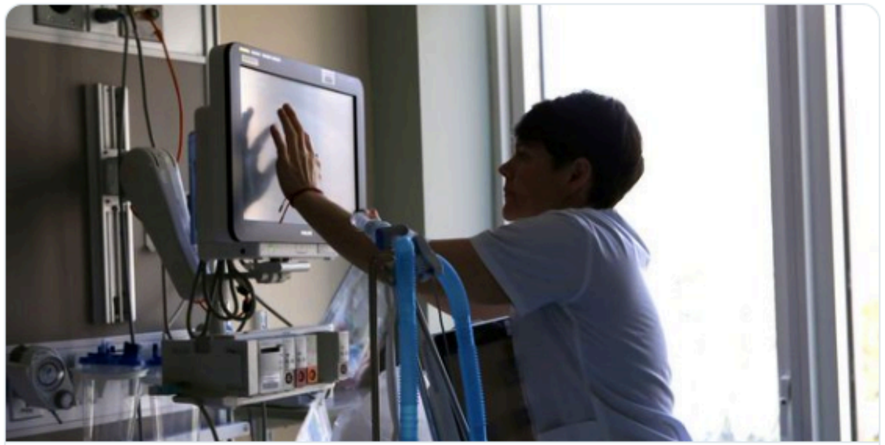
3 Retweets **4** Likes

1 3 4

The Wall Street Journal
@WSJ

Follow

As reports of cyberattacks rise, hospitals are pressing medical-device makers to disclose proprietary software and step up security commitments



Rattled by Cyberattacks, Hospitals Push Device Makers to Improve Security

U.S. hospitals are pressing medical-device makers to improve cyber defenses of their internet-connected infusion pumps, biopsy imaging tables and other health...

wsj.com

7:40 AM - 12 May 2019

57 Retweets **74** Likes

9 57 74

JamiOh
@Mitosucks

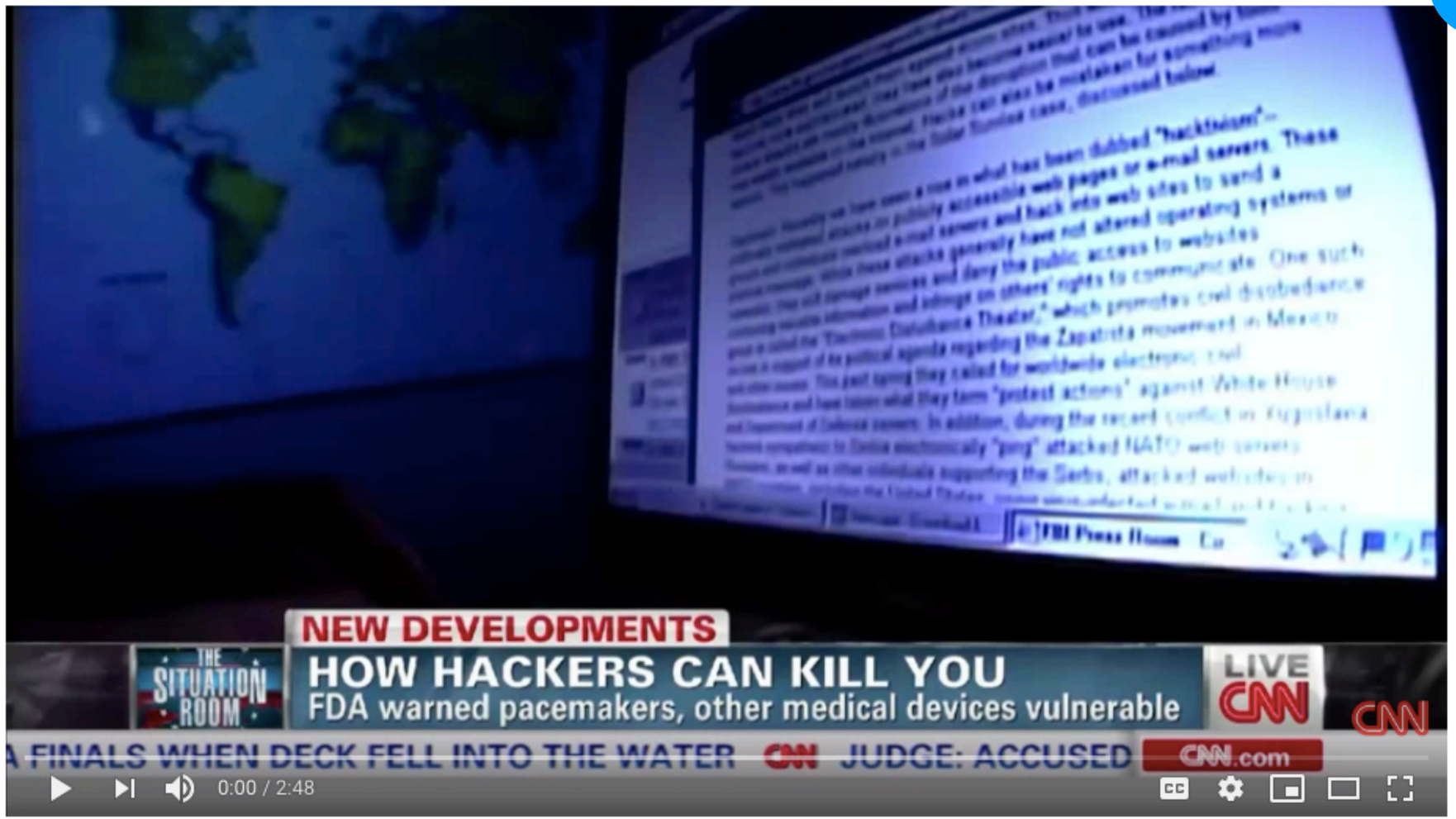
Follow

Replying to @WSJ

I have an implanted defibrillator that my doctor does remote device checks on. Wondering if someone can hack that and shock me to death.

7:42 AM - 12 May 2019

click me



How hackers can kill you

7,800 views

35 13 SHARE SAVE

infrastructure

Catalin Cimpanu
@campuscodi

Follow

Ukraine blames Russia for malware attack that crippled its electric grid on Christmas buff.ly/1ZAf6Kr #Russia #malware #hacking

3:55 PM - 29 Dec 2015

Teresa Rothaar
@trothaar

Follow

I mentioned in a blog I wrote for a client last November that hackers don't take holidays. The Ukraine #SCADA system attack took place on Christmas, and #NotPetya was timed with a Ukrainian national holiday. #Cybersecurity #Infosec #hacking

Proofpoint @proofpoint
Holiday lull? Not so much...

For years, threat actors typically avoided sending large, broad-based campaigns on major American and UK holidays and...

11:20 AM - 12 Jan 2018

2 Likes

2

Visualizing Pipeline Impacts
@PipelineImpacts

Follow

In 1982, the C.I.A. hacked into the software that controlled Soviet natural gas pipelines...The result...was the largest nonnuclear explosion and fire ever seen from space and a major blow to Soviet sales of natural gas to Western Europe.

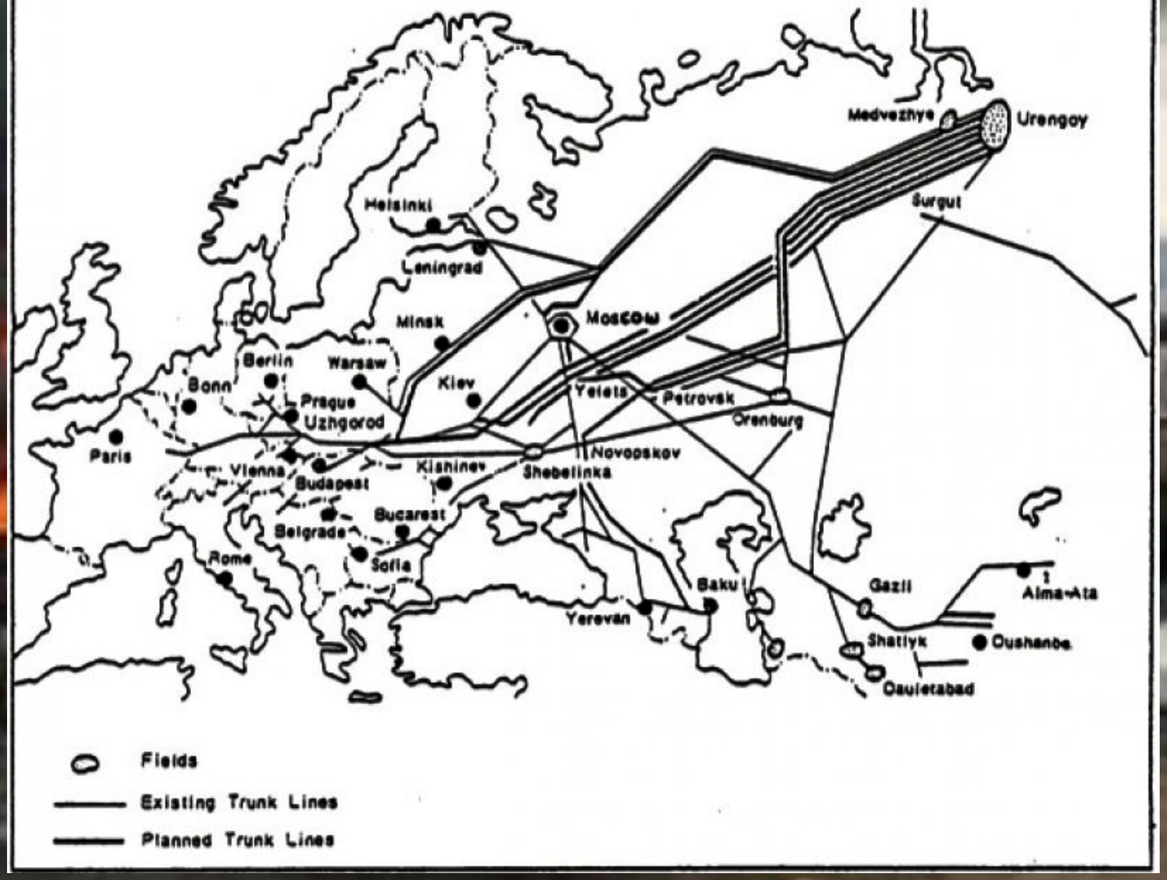
Mapping Natural Gas Lines: Advise the Public, Tip ...
Tensions mount in New York City as officials try to straddle fence dividing two important natural gas issues; explosiveness of natural gas requires that public be a...
nytimes.com

5:12 AM - 28 May 2018

2 Retweets **1** Like

1 2 1

Urengoy-Surgut-Chelyabinsk pipeline



backdoors

CVE Updates
@cvebot

Follow

CVE-2014-0354 The ZyXEL Wireless N300 NetUSB NBG-419N router with firmware 1.00(BFQ.6)C0 has a hardcoded password of qweasdzxc for an u

7:27 AM - 15 Apr 2014

Fortified ICS
@Secured_ICS

Follow

Hardcoded Password Opens Router Backdoor isssource.com/hardcoded-pass …

7:25 AM - 28 Aug 2014

CVE
@CVEnew

Follow

CVE-2017-18373 The Billion 5200W-T TCLinux Fw $7.3.8.0 v008 130603 router distributed by TrueOnline has three user accounts with default passwords, including two hardcoded service accounts: one with the username true and password true, and another with ... cve.mitre.org/cgi-bin/cvenam …

10:45 AM - 2 May 2019

1 Like

Prof Richard Buckland
@ProfBuckland

Follow

I can't believe this is still happening?! Whoever taught these coders needs to hand their head in shame.

Hardcoded root SSH credentials were stored in the binary. Any attacker knowing the default password (oelinux123) can login to the router via SSH as the root user(!)

> **packet storm** @packet_storm
> EE 4GEE HH70VB-2BE8GB3 HH70_E1_02.00_19 Hard-Coded Credentails packetstormsecurity.com/files/150100 #exploit

6:08 PM - 30 Oct 2018

2 Likes

CVE
@CVEnew

Follow

CVE-2017-18374 The ZyXEL P660HN-T1A v1 TCLinux Fw $7.3.15.0 v001 / 3.40(ULM.0)b31 router distributed by TrueOnline has two user accounts with default passwords, including a hardcoded service account with the username true and password true. These accoun... cve.mitre.org/cgi-bin/cvenam …

10:45 AM - 2 May 2019

2 Likes

The Guardian ✓
@guardian

Follow

Huawei says alleged router 'backdoor' is standard network tool

Huawei says alleged router 'backdoor' is standard network tool
Vodafone found security failings in firm's internet routers a decade ago
theguardian.com

1:45 PM - 30 Apr 2019

29 Retweets **49** Likes

11 29 49

Beau Woods
@beauwoods

Follow

Telnet on a router in 2012 is not a backdoor. It's common practice today in telecom and other sectors. There are reasons to be concerned about Huawei equipment. Telnet is not one of them. bloomberg.com/opinion/articl …

> Vodafone managers had concerns with the security of the routers almost right away. They were the topic of an internal presentation from October 2009 that pointed to 26 open bugs in the routers, six identified as "critical" and nine as "major." Vodafone said in the report that Huawei would need to remove or inhibit a so-called telnet service –a protocol used to control devices remotely–that the carrier said was a backdoor giving Huawei access to sensitive data.

8:31 AM - 30 Apr 2019

11 Retweets **33** Likes

PrivacyDigest
@PrivacyDigest

Following

The Time Tim Cook Stood His Ground Against the FBI wired.com/story/the-time …
> The agency wanted a backdoor to crack the iPhone of Syed Farook, a suspect in the 2015 San Bernardino shooting. The Apple CEO said no.

The FBI Wanted a Backdoor to the iPhone. Tim Cook Said No

The agency wanted to crack the iPhone of Syed Farook, a suspect in the 2015 San Bernardino shooting. The Apple CEO took a stand.

wired.com

12:56 PM - 16 Apr 2019

1 Retweet

1

Andrew Ayer
@__agwa

Follow

Headphone software made by Sennheiser has been installing a root certificate, plus the private key, onto people's computers: secorvo.de/publikationen/ …

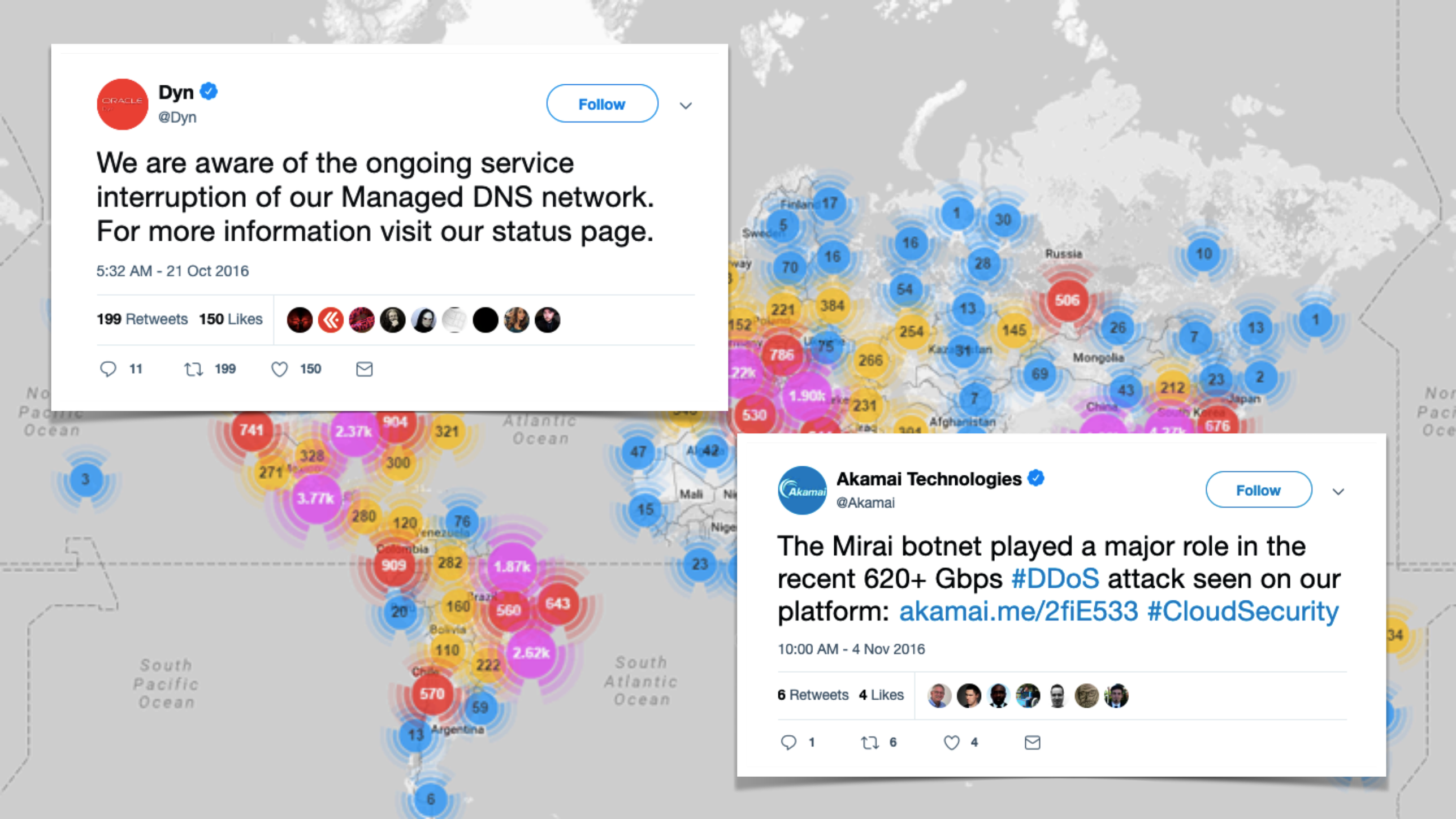
Like Superfish, anyone can use this key, which is the same on all installations, to forge certificates and impersonate websites.

2:59 PM - 27 Nov 2018

2,143 Retweets **2,452** Likes

69 2.1K 2.5K

malware


Dyn
@Dyn
Follow
We are aware of the ongoing service interruption of our Managed DNS network. For more information visit our status page.
5:32 AM - 21 Oct 2016
199 Retweets 150 Likes
11
199
150
Akamai Technologies
@Akamai
Follow
The Mirai botnet played a major role in the recent 620+ Gbps #DDoS attack seen on our platform: akamai.me/2fiE533 #CloudSecurity
10:00 AM - 4 Nov 2016
6 Retweets 4 Likes
1
6
4
Russia
Mongolia
China
Japan
Afghanistan
Mali
Bolivia
Argentina
South Pacific Ocean
South Atlantic Ocean
Atlantic Ocean

Slate
@Slate

Follow

The ransomware attack that locked hotel guests out of their rooms:
slate.me/2kWoOHW

12:34 PM - 1 Feb 2017

11 Retweets **4** Likes

11 4

Archimedes Center
@ARC_MedSec

Follow

Career-ending costly #lessonslearned for this Michigan Practice Forced to Close Following Ransomware Attack @DrKevinFu @br_ #itys #iot #its2019 #CyberSecurity

Michigan Practice Forced to Close Following Ransomware Attack

Following a ransomware attack that encrypted patient data and a refusal to pay the ransom demand, hackers deleted all encrypted files and the practice was forced t...

hipaajournal.com

2:13 PM - 8 Apr 2019 from Rosemount, MN

1 Retweet **4** Likes

1 4

Moshe Vardi
@vardi

Following

Hackers have been holding the city of Baltimore's computers hostage for 2 weeks vox.com/recode/2019/5/ … via @voxdotcom

Hackers have been holding the city of Baltimore's computers hostage for 2 w…

A ransomware attack means Baltimore citizens can't pay their water bills or parking tickets.

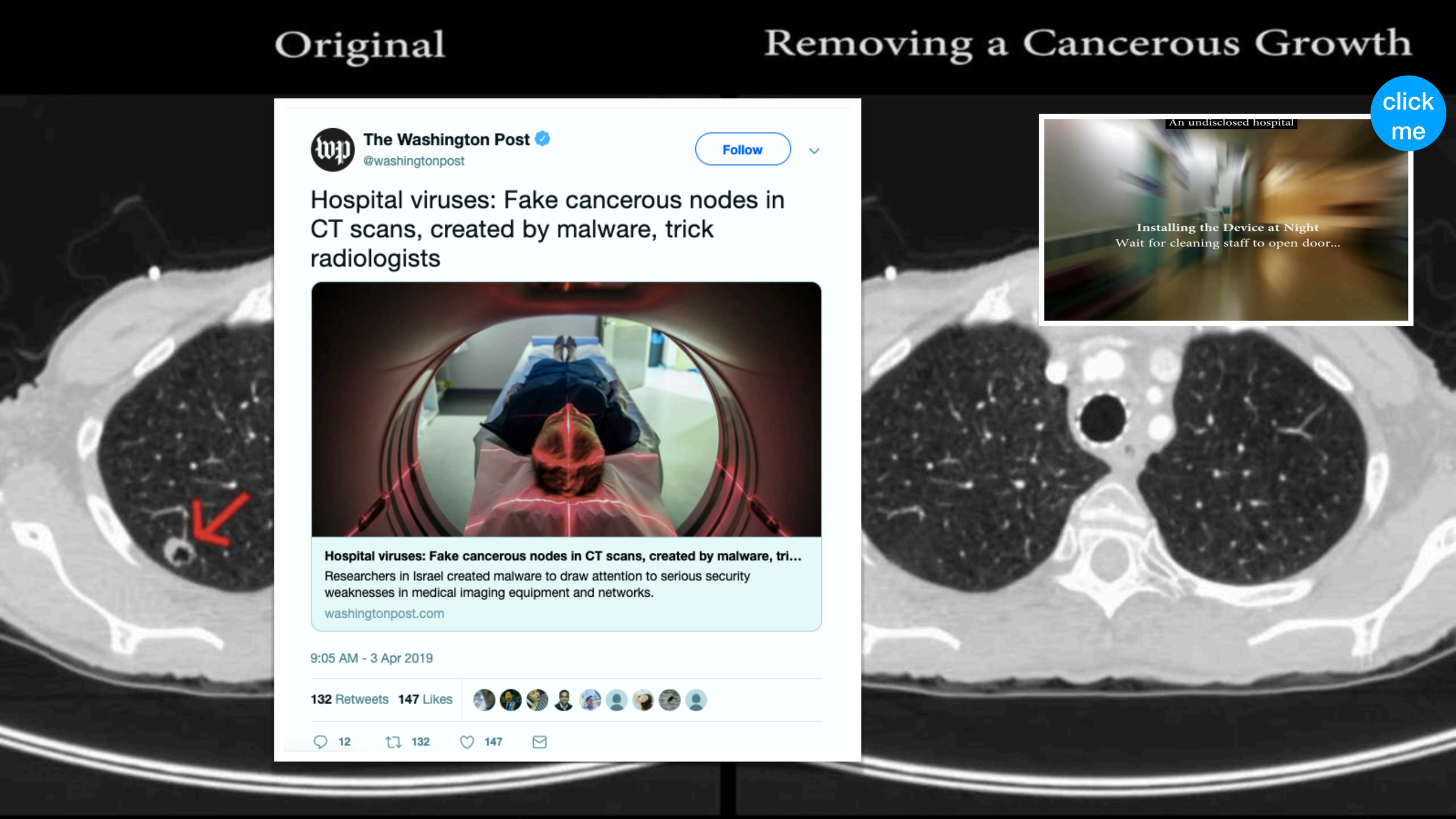
vox.com

12:37 PM - 22 May 2019

1 Retweet **2** Likes

Original

Removing a Cancerous Growth



The Washington Post
@washingtonpost

Follow

Hospital viruses: Fake cancerous nodes in CT scans, created by malware, trick radiologists

Hospital viruses: Fake cancerous nodes in CT scans, created by malware, tri...

Researchers in Israel created malware to draw attention to serious security weaknesses in medical imaging equipment and networks.

washingtonpost.com

9:05 AM - 3 Apr 2019

132 Retweets **147** Likes

12 132 147

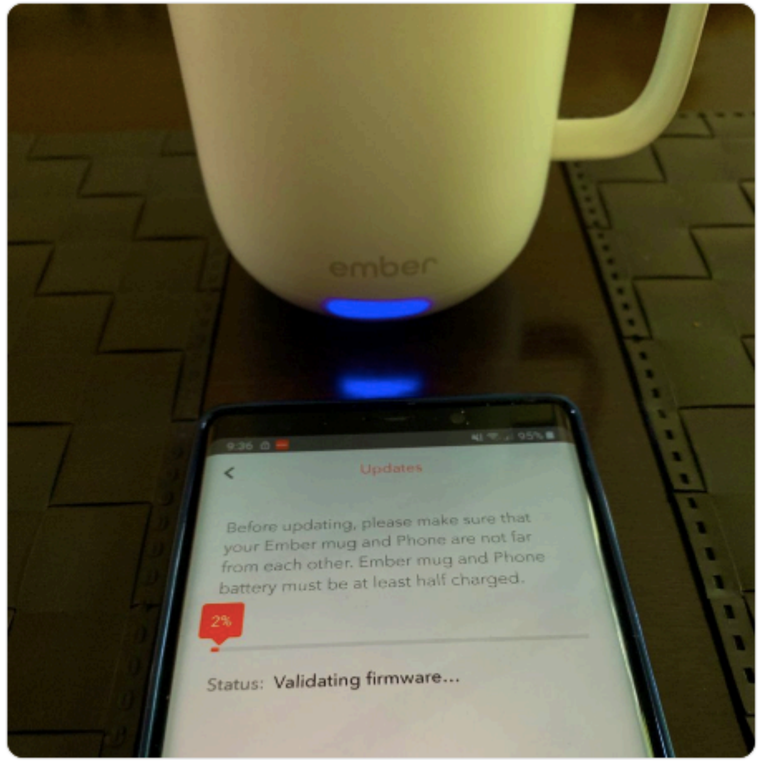
click me

updates

Luca Spolidoro
@Licantrop0

Follow

Updating the firmware of a mug.
What a world we live in! /cc
@internetofshit

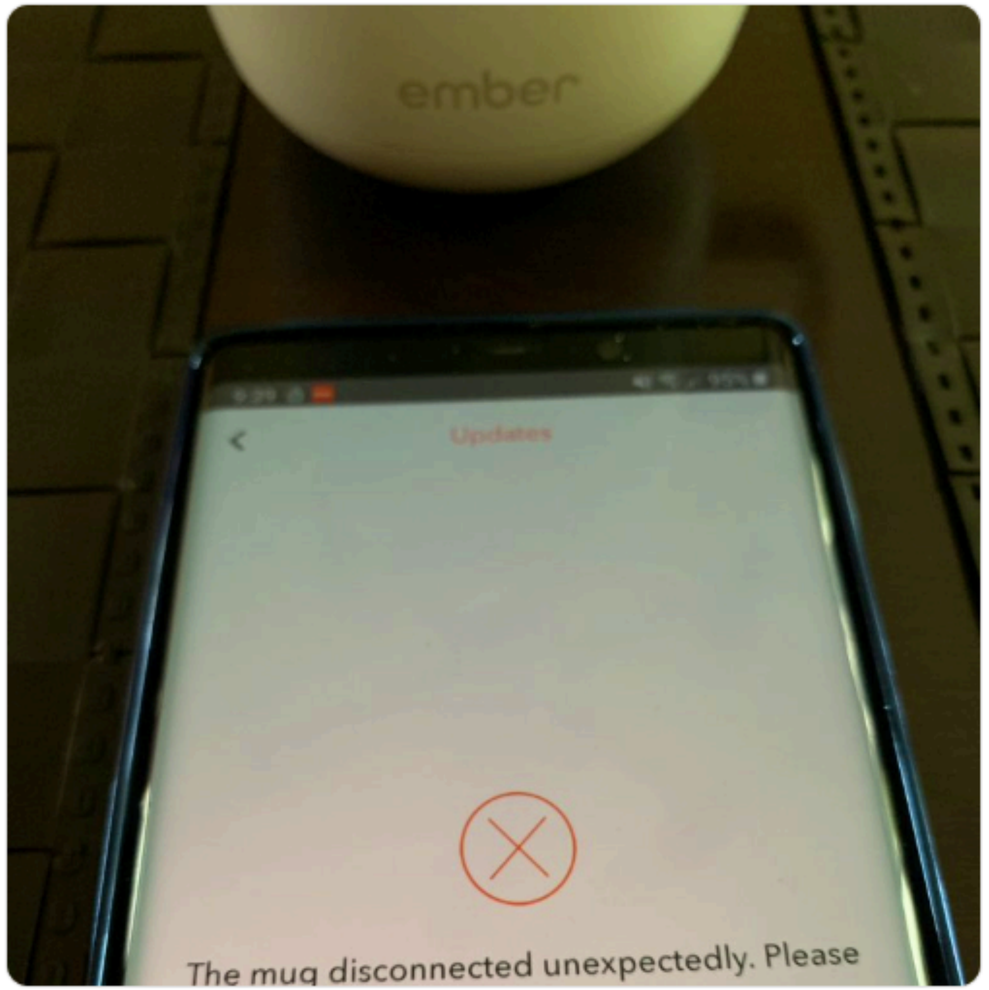


9:37 AM - 14 Apr 2019

310 Retweets **752** Likes

26 310 752

Luca Spolidoro @Licantrop0 · Apr 14
Aaaand it failed.
Now I can't drink from it anymore.



20 106 445

TECH | WEARABLE

circuit breaker

Nike says it's 'actively working' to fix its broken smart sneakers

No timeline on a fix, though

By Ashley Carman | @ashleycarman | Feb 21, 2019, 2:00pm EST

SHARE

Photo by Vjeran Pavic / The Verge

Nike says that a fix is in the works for its broken Adapt BB smart sneakers, days after an Android update rendered some of them unusable.

Ars Technica
@arstechnica

Follow

Why a Windows flaw patched nine days ago is still spooking the Internet arstechnica.com/information-te … by @dangoodin001

Why a Windows flaw patched nine days ago is still spooking the Internet
Researchers warn dangerous BlueKeep vulnerability is almost sure to be exploited.
arstechnica.com

4:29 AM - 23 May 2019

14 Retweets **29** Likes

1 14 29

Kaspersky Lab
@kaspersky

Follow

Exclusive: Kaspersky Lab researchers detect Operation #ShadowHammer - a supplychain attack looking to target high-profile victims. #KLResearch

ShadowHammer: Malicious updates for ASUS laptops
Our technologies detected a threat that seems to be one of the biggest supply-chain attacks ever.
kaspersky.com

6:27 AM - 25 Mar 2019

52 Retweets **65** Likes

4 52 65

Kaspersky Lab
@kaspersky

Follow

In case you missed it: new details have emerged around the recent ASUS #ShadowHammer threat.

Get the deep dive 👇

ShadowHammer: New details
It appears the ASUS incident was just one part of the large-scale operation.
kaspersky.com

4:45 AM - 26 Apr 2019

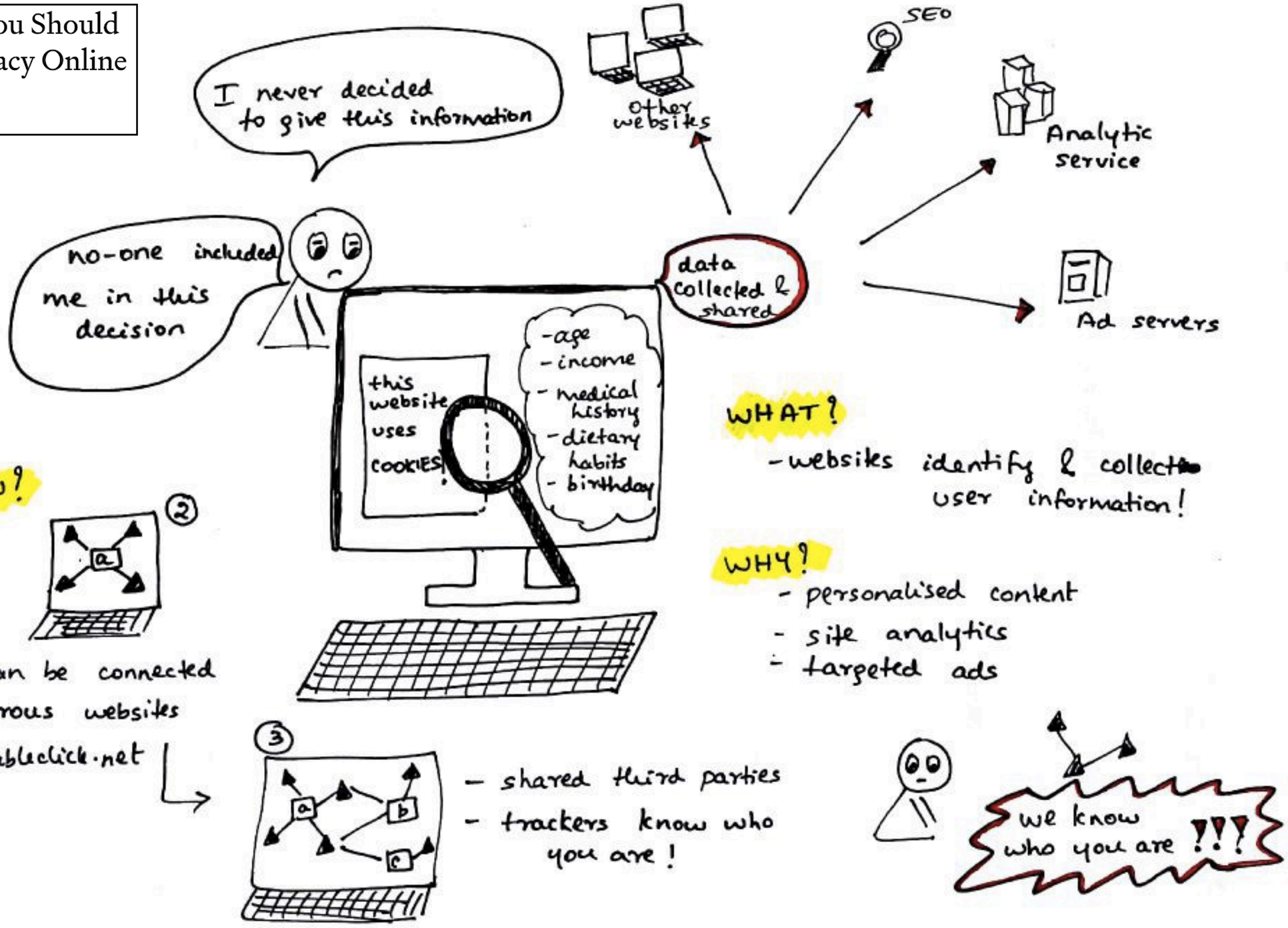
2 Retweets **4** Likes

2 4

tracking

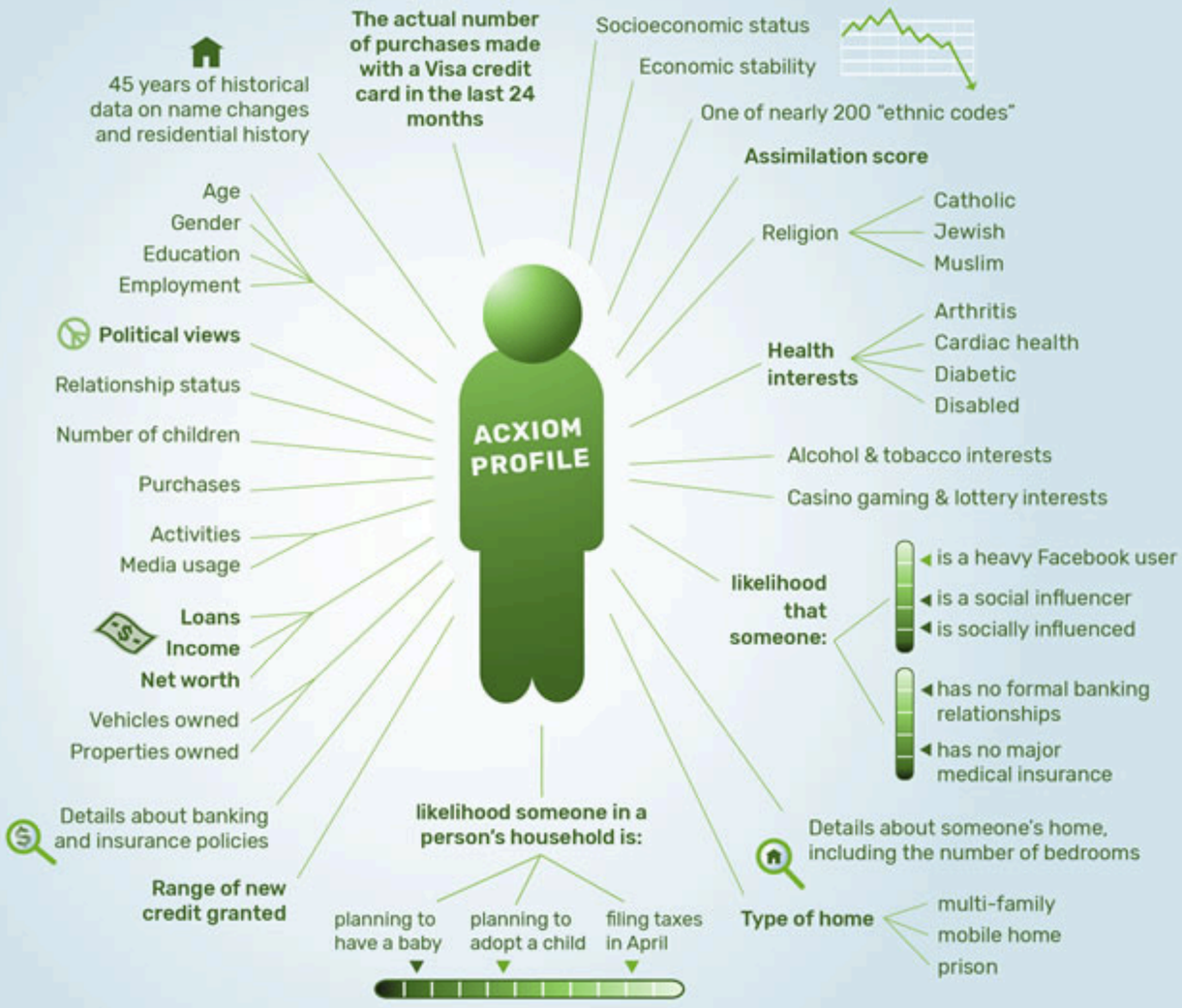
Web Tracking: What You Should Know About Your Privacy Online

Princiya Follow
Apr 23, 2018 · 6 min read

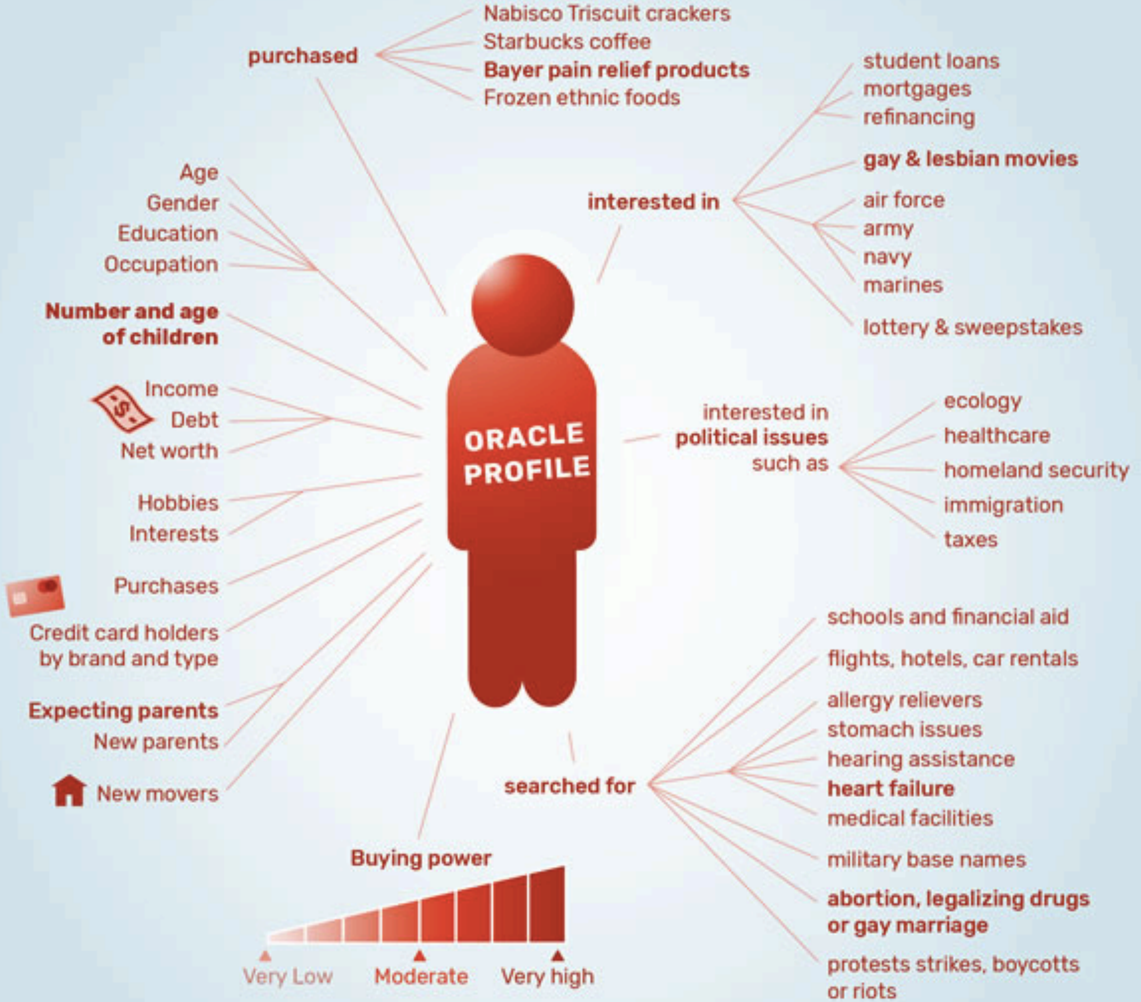


DATA BROKERS HAVE EXTENSIVE PROFILE INFORMATION ON ENTIRE POPULATIONS

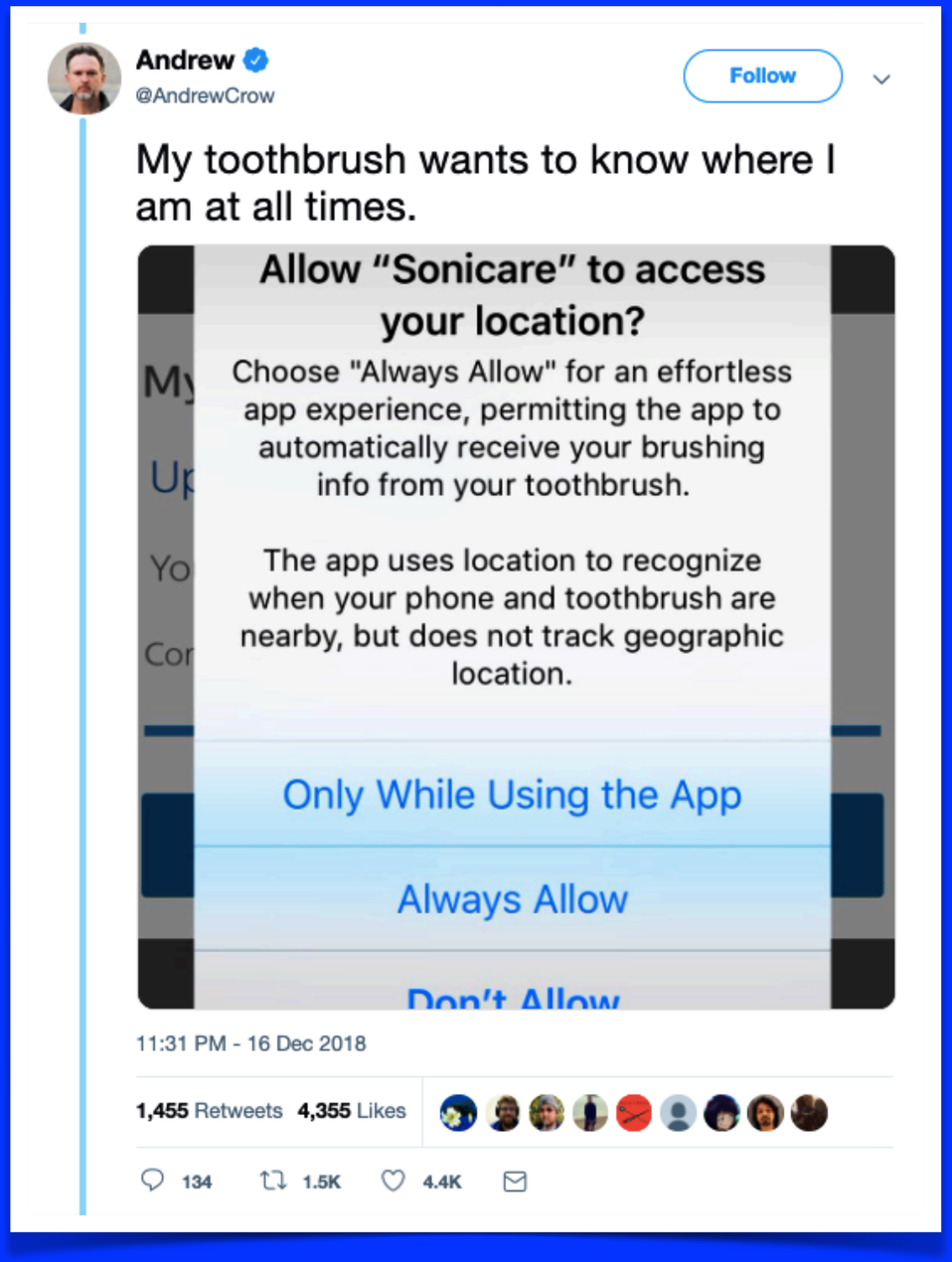
Examples of data on consumers provided by Acxiom and Oracle

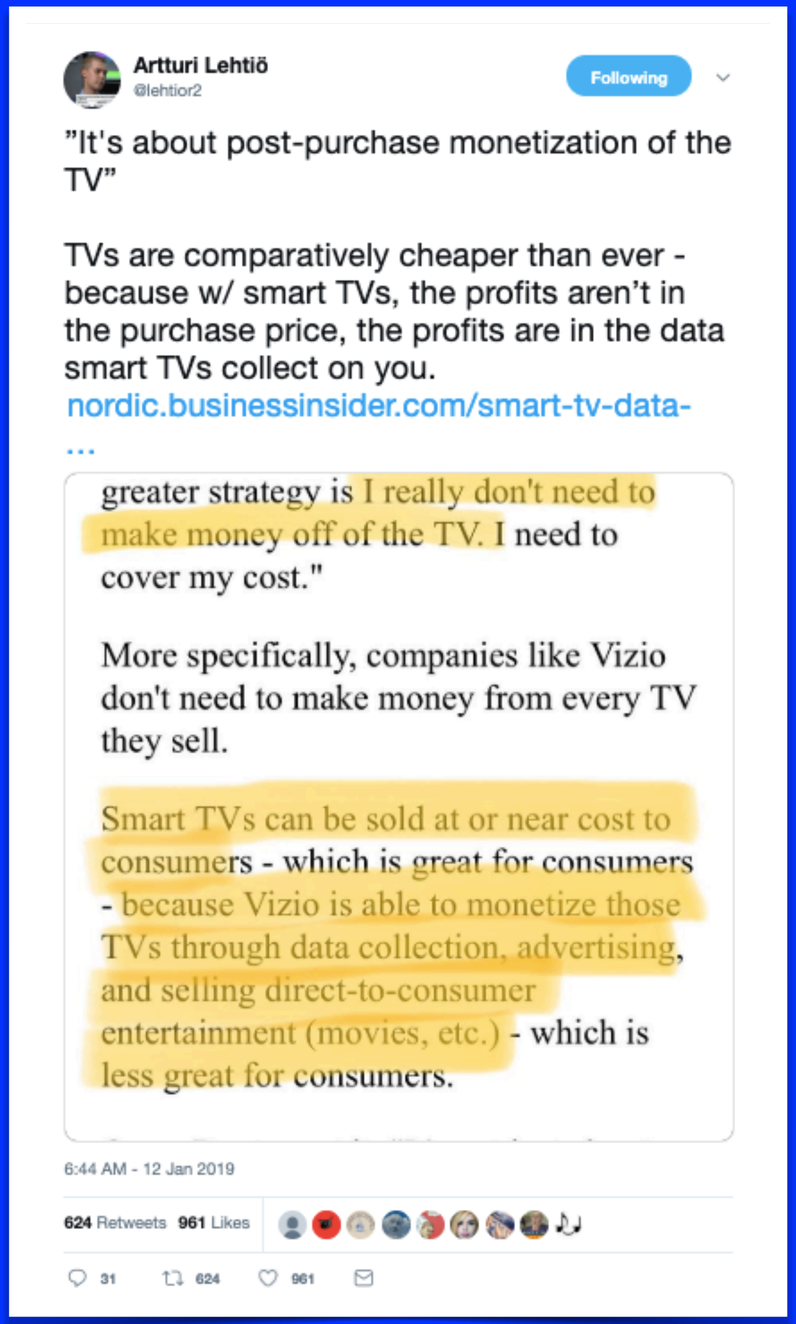


Acxiom provides of up 3,000 attributes and scores
on 700 million people in the US, Europe, and other regions.



Oracle sorts people into thousands of categories
and provides > 30,000 attributes on 2 billion consumer profiles


Andrew
@AndrewCrow
Follow
My toothbrush wants to know where I am at all times.
Allow “Sonicare” to access your location?
Choose "Always Allow" for an effortless app experience, permitting the app to automatically receive your brushing info from your toothbrush.
The app uses location to recognize when your phone and toothbrush are nearby, but does not track geographic location.
Only While Using the App
Always Allow
Don't Allow
11:31 PM - 16 Dec 2018
1,455 Retweets 4,355 Likes
134 1.5K 4.4K

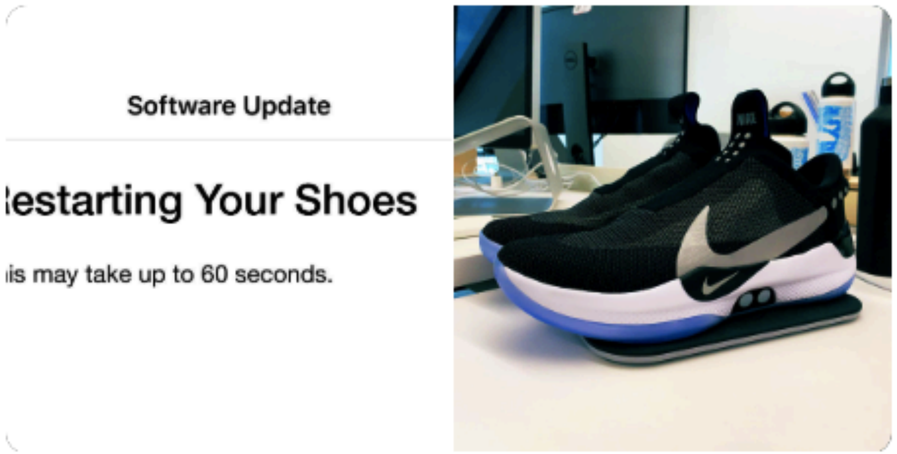

Artturi Lehtiö
@lehtior2
Following
”It's about post-purchase monetization of the TV”
TVs are comparatively cheaper than ever - because w/ smart TVs, the profits aren’t in the purchase price, the profits are in the data smart TVs collect on you.
nordic.businessinsider.com/smart-tv-data-...
greater strategy is I really don't need to make money off of the TV. I need to cover my cost."
More specifically, companies like Vizio don't need to make money from every TV they sell.
Smart TVs can be sold at or near cost to consumers - which is great for consumers - because Vizio is able to monetize those TVs through data collection, advertising, and selling direct-to-consumer entertainment (movies, etc.) - which is less great for consumers.
6:44 AM - 12 Jan 2019
624 Retweets 961 Likes
31 624 961

George Kedenburg III
@GK3

Follow

i just had to download a software update for my shoes which are now getting a charge on their USB-C wireless charging mat

we're living in the future!!! 😲



10:19 AM - 17 Feb 2019 from San Francisco, CA

1,258 Retweets **3,547** Likes

Nike

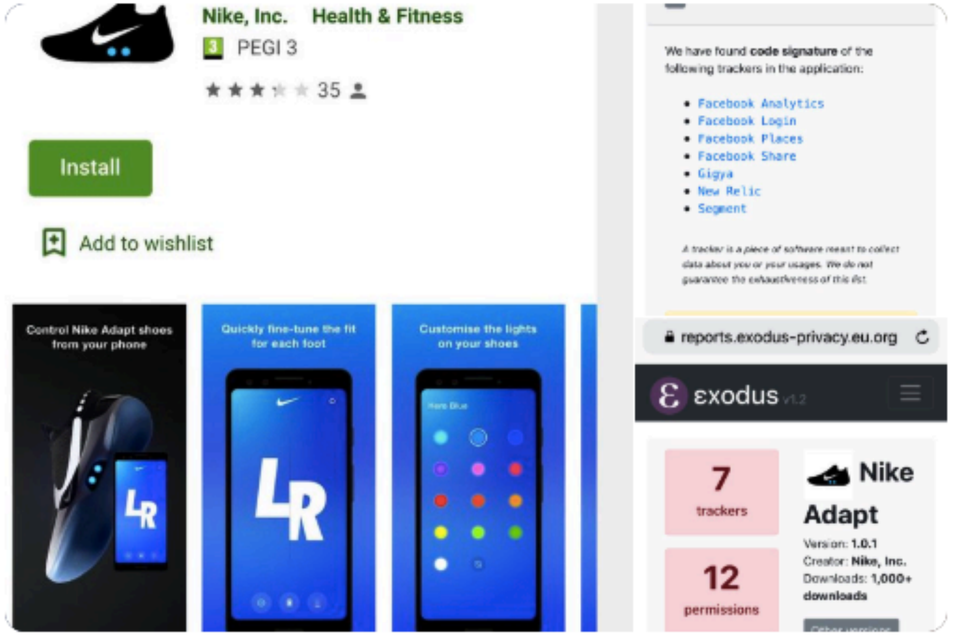
334 1.3K 3.5K

Privacy Matters
@PrivacyMatters

Following

Replying to @GK3 @Nike

Nice bit of tracking in that app too 🤔



11:28 AM - 18 Feb 2019

15 Likes

2 15

HE KNOWS WHEN YOU ARE SLEEPING... —

You snooze, you lose: Insurers make the old adage literally true

Why insurers spy on sleep apnea sufferers via connected CPAP machines.

MARSHALL ALLEN, PROPUBLICA - 11/21/2018, 4:25 PM

Experts who study healthcare costs say insurers' CPAP strategies are part of the industry's playbook of shifting the costs of widely used therapies, devices, and tests to unsuspecting patients.

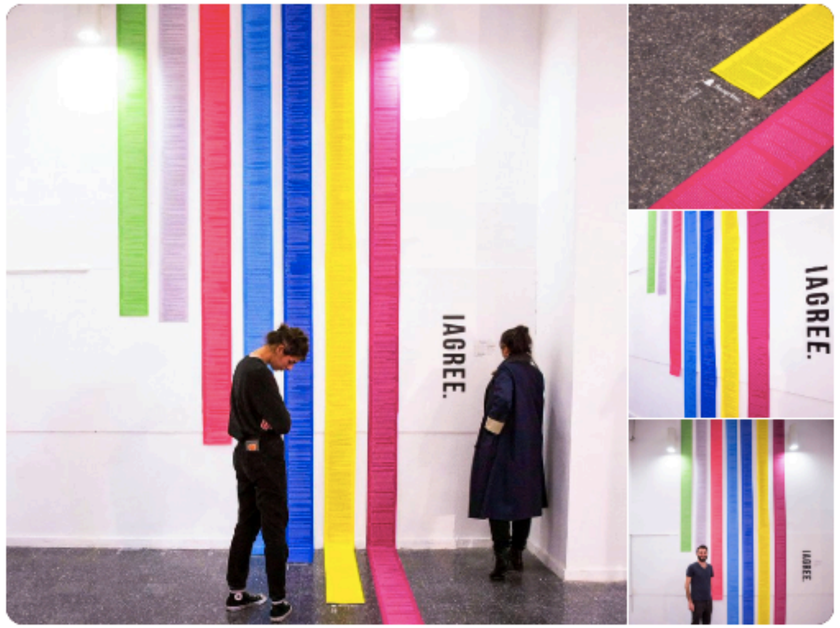
"The doctors and providers are not in control of medicine anymore," said Harry Lawrence, owner of Advanced Oxy-Med Services, a New York company that provides CPAP supplies. "It's strictly the insurance companies. They call the shots."

Dima Yarovinsky
@dimitryarov

Follow

Replying to @hailmika @pop_stefanija

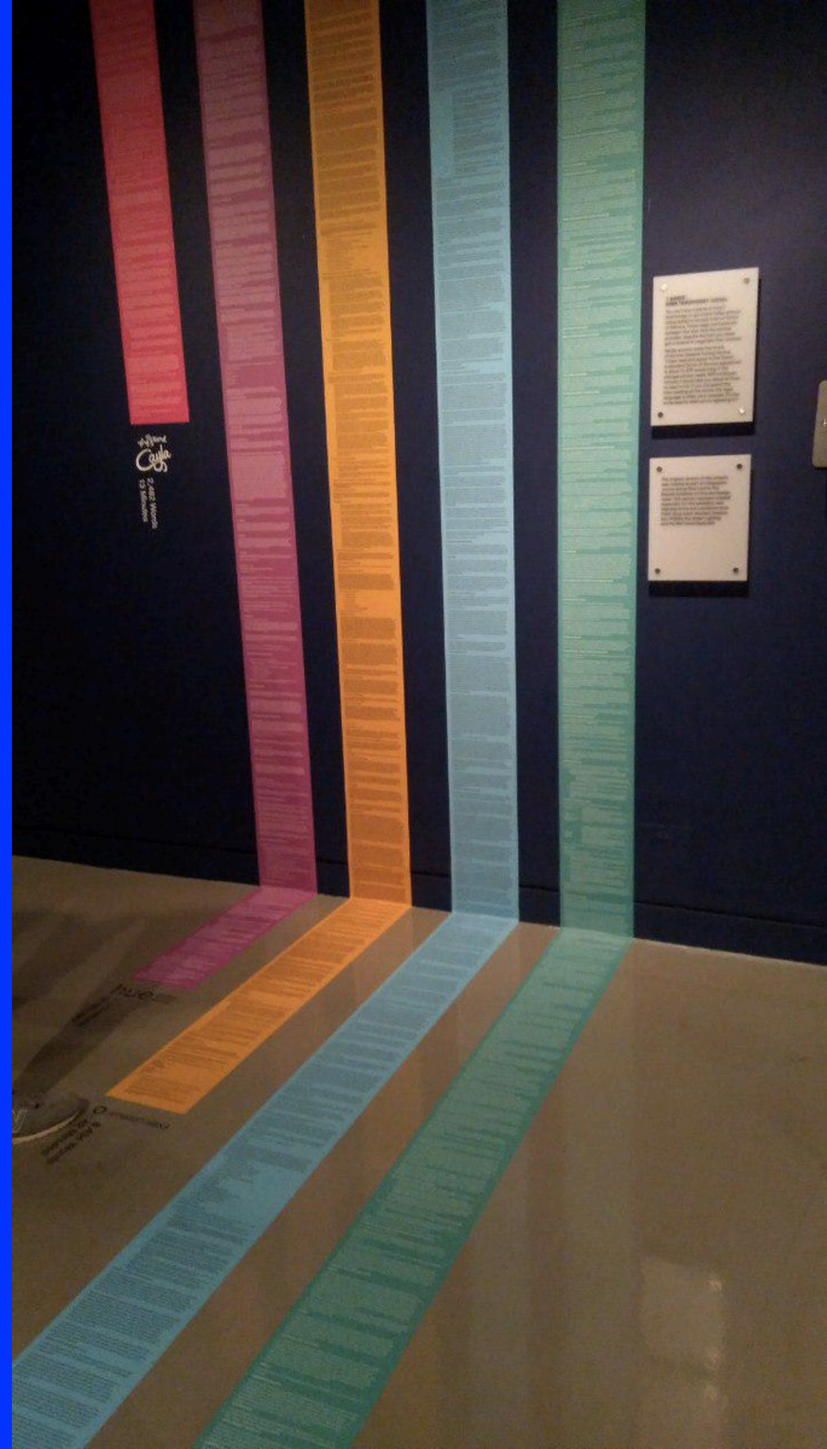
Hey all! thanks for your comments, it's really flattering.
Attaching more photos from the same project as it was presented in the Bezalel art and design academy.



8:17 AM - 5 May 2018

719 Retweets **1,597** Likes

28 719 1.6K



moz://a *privacy not included

click me

Be Smart. Shop Safe.

How creepy is that smart speaker, that fitness tracker, that game console? We created this guide to help you shop for safe, secure connected products. Look for the “Meets Our Minimum Security Standards” badge to get started.

The 😮 below shows how creepy users find these products. Scroll to see it change. Click on a product to rate it.

creepy

LIVE SMARTER

How to Prevent Your Alexa Device From Recording Your Private Conversations

BY EMILY PETSKO DECEMBER 20, 2018

The surest preventative measure you can take is to deny Alexa access to your contacts when you first set up your device. If you've already enabled access, you can call Amazon's customer service department at 877-375-9365 and have them remove the service. Sure, this process is "clunky" and takes about 10 minutes to complete, according to Lifehacker, but it gets the job done. You won't be able to make calls or send texts as quickly, but you'll have some peace of mind knowing that your contacts won't be forced to listen to your conversation about hardwood floors.

When in doubt, you can manually turn off the Echo's microphone at any time. Just press the microphone button on the device to ensure you won't be heard or recorded during particularly sensitive conversations. And if you're going to use your device often, be sure to keep the volume turned up high enough that you can hear it. That way, when Alexa asks to confirm your expletive-laden message to grandma, you can catch it before it's too late.

It's also a good idea to change Alexa's "wake word," which prompts the device to start heeding your command. Unfortunately, Amazon doesn't let you choose your own wake word—so you won't be able to switch it to *supercalifragilistic*—but you can switch it to *Computer*, *Amazon*, or *Echo*. *USA Today* recommends trying out different options to see which one is less likely to be confused for another word in your household. Just call out, "Alexa, change the wake word," or follow these steps to change it in the Alexa app.

Technology

Amazon Workers Are Listening to What You Tell Alexa

A global team reviews audio clips in an effort t d assistant respond to commands.

By Matt Day, Giles Turner, and Natalia Drozdiak
11 April 2019, 00:34 CEST

The wrist-worn gadget is described as a health and wellness product in internal documents reviewed by Bloomberg. It's a collaboration between Lab126, the hardware development group behind Amazon's Fire phone and Echo smart speaker, and the Alexa voice software team.

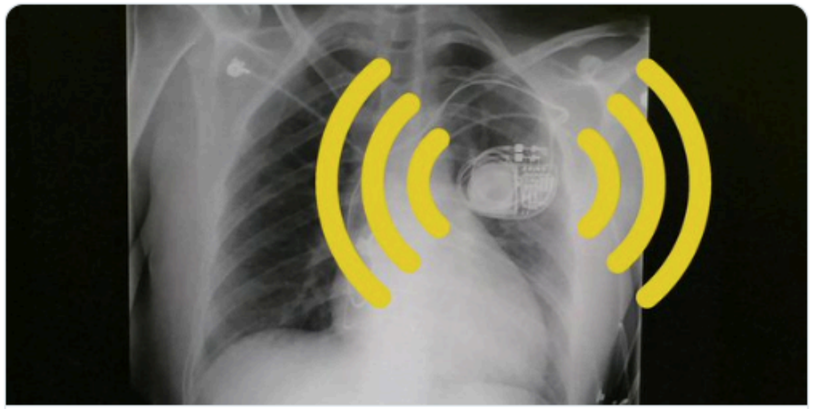
A U.S. patent filed in 2017 describes a system in which voice software uses analysis of vocal patterns to determine how a user is feeling, discerning among "joy, anger, sorrow, sadness, fear, disgust, boredom, stress, or other emotional states." The patent, made public last year, suggests Amazon could use knowledge of a user's emotions to recommend products or otherwise tailor responses.

Amazon declined to comment.

Beau Woods
@beauwoods

Follow

Great to see attention on medical device cyber safety. The article highlights work by people and organizations who have been doing this for over a decade like @MarieGMoe and @ARC_MedSec. We have come a long way, with a long way yet to go.



My Pacemaker Is Tracking Me From Inside My Body

Cloud-connected medical devices save lives, but also raise questions about privacy, security, and oversight.

theatlantic.com

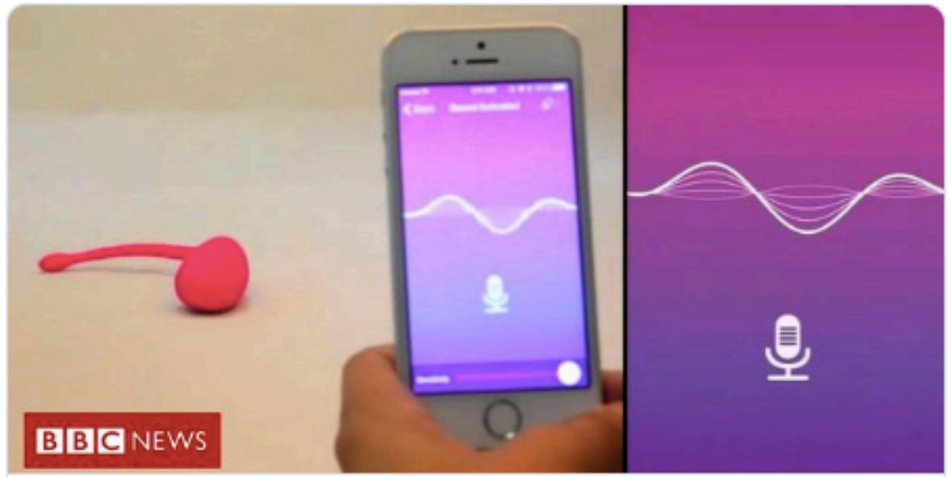
9:27 AM - 28 Jan 2018

56 Retweets **82** Likes

Ken Munro
@TheKenMunroShow

Follow

More dildo hacking stories. Even on the BBC! This one is mostly local only tho. Interesting finding, if fairly low risk



Sex toy app recorded and stored sounds

A smart vibrator-maker blames a bug for causing the software to save audio recordings.

bbc.co.uk

5:35 AM - 13 Nov 2017

1 Retweet **4** Likes

1 1 4

SMART HOME | TECH | COMCAST

Comcast is reportedly developing a device that would track your bathroom h

This probably isn't a company anyone wants to be sharing

By Chris Welch | @chriswelch | May 21, 2019, 3:23pm EDT

"The device will monitor people's basic health metrics using ambient sensors, with a focus on whether someone is making frequent trips to the bathroom or spending more time than usual in bed," CNBC's report says. "Comcast is also building tools for detecting falls, which are common and potentially fatal for seniors."