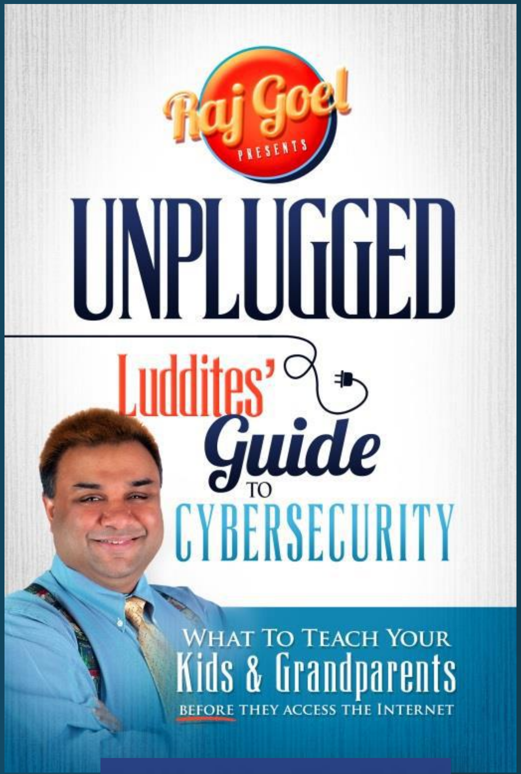
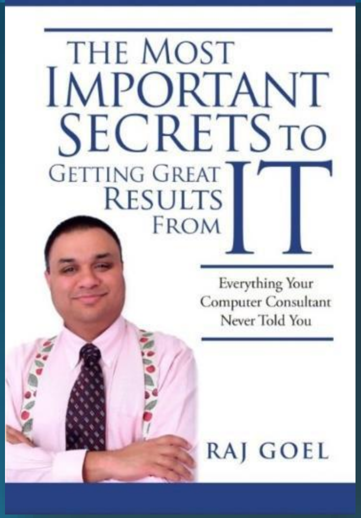
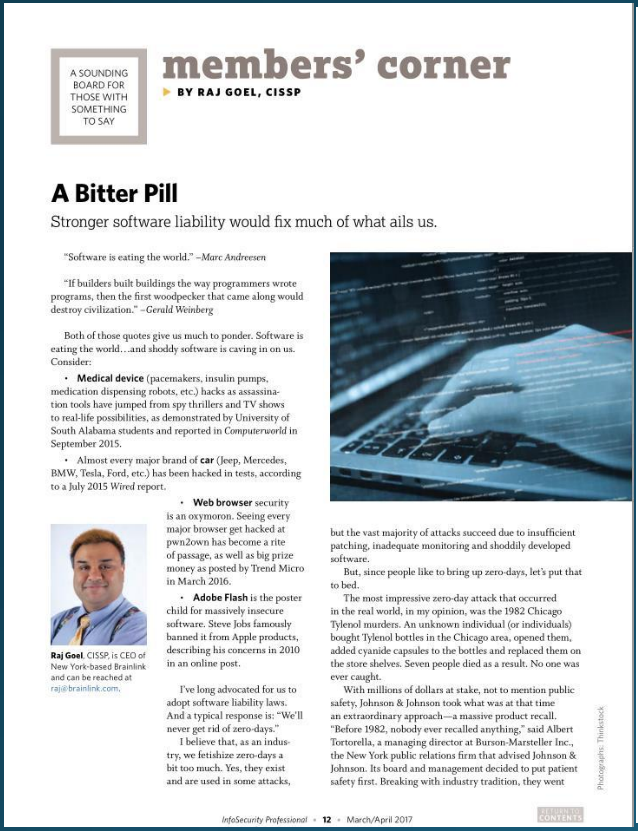
From BOTNETS to HEART ATTACKS: UNSAFE Software is a DANGER to us All

Raj Goel, CISSP
raj@brainlink.com / 917-685-7731
www.RajGoel.com
@rajgoel_ny


Raj Goel!
PRESENTS
UNPLUGGED
Luddites' Guide to CYBERSECURITY
WHAT TO TEACH YOUR Kids & Grandparents
BEFORE THEY ACCESS THE INTERNET


THE MOST IMPORTANT SECRETS TO GETTING GREAT RESULTS FROM IT
Everything Your Computer Consultant Never Told You
RAJ GOEL

ISC2 Article – A Bitter Pill



A SOUNDING BOARD FOR THOSE WITH SOMETHING TO SAY

members' corner

▶ BY RAJ GOEL, CISSP

A Bitter Pill

Stronger software liability would fix much of what ails us.

"Software is eating the world." –*Marc Andreesen*

"If builders built buildings the way programmers wrote programs, then the first woodpecker that came along would destroy civilization." –*Gerald Weinberg*

Both of those quotes give us much to ponder. Software is eating the world…and shoddy software is caving in on us. Consider:

- **Medical device** (pacemakers, insulin pumps, medication dispensing robots, etc.) hacks as assassination tools have jumped from spy thrillers and TV shows to real-life possibilities, as demonstrated by University of South Alabama students and reported in *Computerworld* in September 2015.
- Almost every major brand of **car** (Jeep, Mercedes, BMW, Tesla, Ford, etc.) has been hacked in tests, according to a July 2015 *Wired* report.
- **Web browser** security is an oxymoron. Seeing every major browser get hacked at pwn2own has become a rite of passage, as well as big prize money as posted by Trend Micro in March 2016.
- **Adobe Flash** is the poster child for massively insecure software. Steve Jobs famously banned it from Apple products, describing his concerns in 2010 in an online post.

Raj Goel, CISSP, is CEO of New York-based Brainlink and can be reached at raj@brainlink.com.

I've long advocated for us to adopt software liability laws. And a typical response is: "We'll never get rid of zero-days."

I believe that, as an industry, we fetishize zero-days a bit too much. Yes, they exist and are used in some attacks, but the vast majority of attacks succeed due to insufficient patching, inadequate monitoring and shoddily developed software.

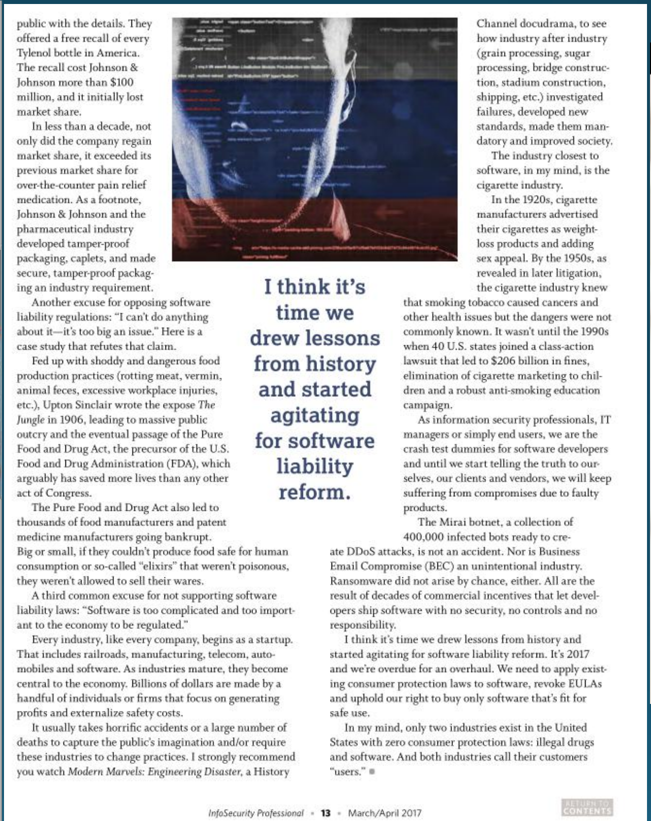
But, since people like to bring up zero-days, let's put that to bed.

The most impressive zero-day attack that occurred in the real world, in my opinion, was the 1982 Chicago Tylenol murders. An unknown individual (or individuals) bought Tylenol bottles in the Chicago area, opened them, added cyanide capsules to the bottles and replaced them on the store shelves. Seven people died as a result. No one was ever caught.

With millions of dollars at stake, not to mention public safety, Johnson & Johnson took what was at that time an extraordinary approach—a massive product recall. "Before 1982, nobody ever recalled anything," said Albert Tortorella, a managing director at Burson-Marsteller Inc., the New York public relations firm that advised Johnson & Johnson. Its board and management decided to put patient safety first. Breaking with industry tradition, they went

Photographs: Thinkstock

RETURN TO CONTENTS



public with the details. They offered a free recall of every Tylenol bottle in America. The recall cost Johnson & Johnson more than $100 million, and it initially lost market share.

In less than a decade, not only did the company regain market share, it exceeded its previous market share for over-the-counter pain relief medication. As a footnote, Johnson & Johnson and the pharmaceutical industry developed tamper-proof packaging, caplets, and made secure, tamper-proof packaging an industry requirement.

Another excuse for opposing software liability regulations: "I can't do anything about it—it's too big an issue." Here is a case study that refutes that claim.

Fed up with shoddy and dangerous food production practices (rotting meat, vermin, animal feces, excessive workplace injuries, etc.), Upton Sinclair wrote the expose *The Jungle* in 1906, leading to massive public outcry and the eventual passage of the Pure Food and Drug Act, the precursor of the U.S. Food and Drug Administration (FDA), which arguably has saved more lives than any other act of Congress.

The Pure Food and Drug Act also led to thousands of food manufacturers and patent medicine manufacturers going bankrupt. Big or small, if they couldn't produce food safe for human consumption or so-called "elixirs" that weren't poisonous, they weren't allowed to sell their wares.

> I think it's time we drew lessons from history and started agitating for software liability reform.

A third common excuse for not supporting software liability laws: "Software is too complicated and too important to the economy to be regulated."

Every industry, like every company, begins as a startup. That includes railroads, manufacturing, telecom, automobiles and software. As industries mature, they become central to the economy. Billions of dollars are made by a handful of individuals or firms that focus on generating profits and externalize safety costs.

It usually takes horrific accidents or a large number of deaths to capture the public's imagination and/or require these industries to change practices. I strongly recommend you watch *Modern Marvels: Engineering Disaster*, a History Channel docudrama, to see how industry after industry (grain processing, sugar processing, bridge construction, stadium construction, shipping, etc.) investigated failures, developed new standards, made them mandatory and improved society.

The industry closest to software, in my mind, is the cigarette industry.

In the 1920s, cigarette manufacturers advertised their cigarettes as weight-loss products and adding sex appeal. By the 1950s, as revealed in later litigation, the cigarette industry knew that smoking tobacco caused cancers and other health issues but the dangers were not commonly known. It wasn't until the 1990s when 40 U.S. states joined a class-action lawsuit that led to $206 billion in fines, elimination of cigarette marketing to children and a robust anti-smoking education campaign.

As information security professionals, IT managers or simply end users, we are the crash test dummies for software developers and until we start telling the truth to ourselves, our clients and vendors, we will keep suffering from compromises due to faulty products.

The Mirai botnet, a collection of 400,000 infected bots ready to create DDoS attacks, is not an accident. Nor is Business Email Compromise (BEC) an unintentional industry. Ransomware did not arise by chance, either. All are the result of decades of commercial incentives that let developers ship software with no security, no controls and no responsibility.

I think it's time we drew lessons from history and started agitating for software liability reform. It's 2017 and we're overdue for an overhaul. We need to apply existing consumer protection laws to software, revoke EULAs and uphold our right to buy only software that's fit for safe use.

In my mind, only two industries exist in the United States with zero consumer protection laws: illegal drugs and software. And both industries call their customers "users." ■

RETURN TO CONTENTS

A MORE 'ARTFUL' APPROACH TO SECURITY ▪ FIRST WOMAN CISSP IN UAE

InfoSecurity PROFESSIONAL

A Publication for the (ISC)² Membership

MARCH/APRIL 2017

MAKE ROOM FOR MILLENNIALS

They are changing the way we work

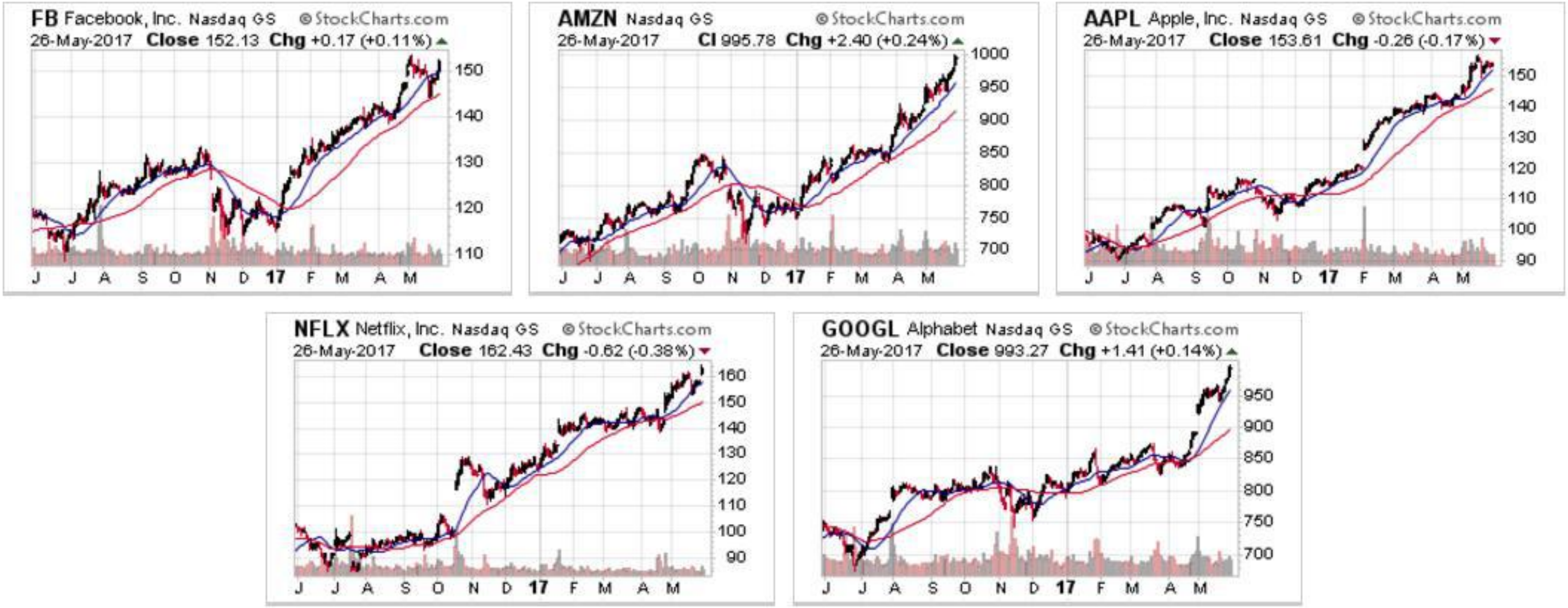
GDPR
PRIVACY BY DESIGN AND BY DEFAULT

CHANGE
FROM RESISTANCE TO ACCEPTANCE

SOFTWARE
LET'S FINALLY DEMAND BETTER

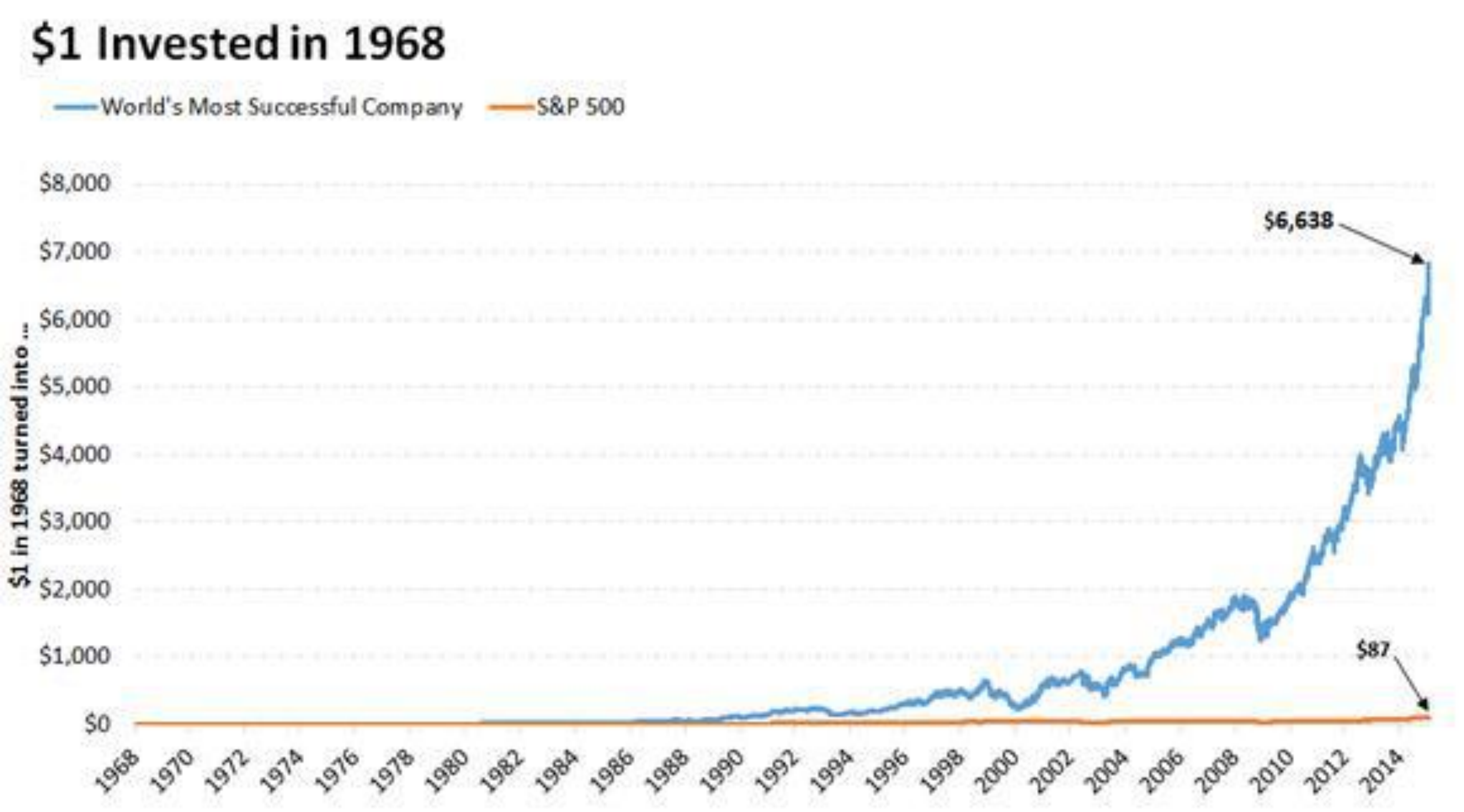
isc2.org facebook.com/isc2fb twitter.com/ISC2

FAANGs 2.0



Simple Moving Averages: 20-period / 50-period

FAANG 1.0


$1 Invested in 1968
World's Most Successful Company
S&P 500
$1 in 1968 turned into ...
$8,000
$7,000
$6,000
$5,000
$4,000
$3,000
$2,000
$1,000
$0
$6,638
$87
1968
1970
1972
1974
1976
1978
1980
1982
1984
1986
1988
1990
1992
1994
1996
1998
2000
2002
2004
2006
2008
2010
2012
2014

“Software is eating the world”
- Marc Andressen

“If builders built buildings the way programmers wrote programs, then the first woodpecker that came along would destroy civilization.” –Gerald Weinberg

ISACA
Trust in, and value from, information systems

The Hidden Internet of Things at Work: RISKS AND REWARDS

63%
Say workplace use of Internet of Things devices has reduced employee privacy

47%
Expect a cyberattack on their organization within the next year

1 in 2
Believe IT department is not aware of all the organization's connected devices

73%
Estimate medium to high likelihood of organization being hacked through Internet of Things device

72%
Believe that Internet of Things device manufacturers do not implement sufficient security

#1
IoT security concern for enterprises is data leakage

#1
Benefit of Internet of Things is better access to information

1 in 3
Believe their organization is unprepared for a sophisticated cyberattack

The Internet of Things will continue to surround and connect people at home, at work and on the road.
The number of B2B Internet of Things devices is expected to expand from 1.2 billion devices in 2015 to 5.4 billion connected devices by 2020 [Verizon/ABI Research]. To view IT and cybersecurity professionals' recommendations for maintaining a cyber-secure workplace and learn the steps that consumers can take to protect their data, visit: **www.isaca.org/risk-reward-barometer**.

CSX
CYBERSECURITY NEXUS

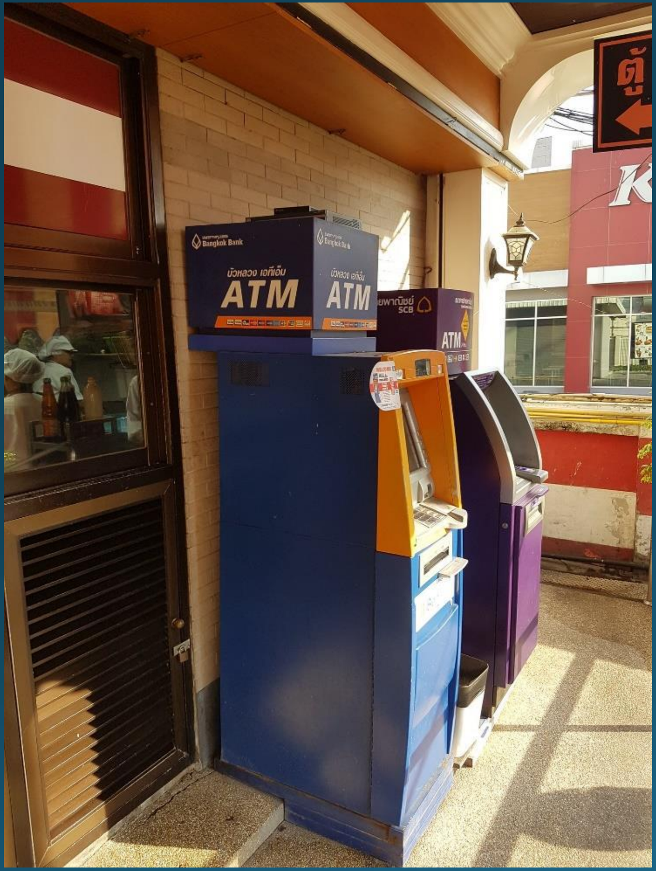
Source: ISACA 2015 IT Risk/Reward Barometer, global member survey

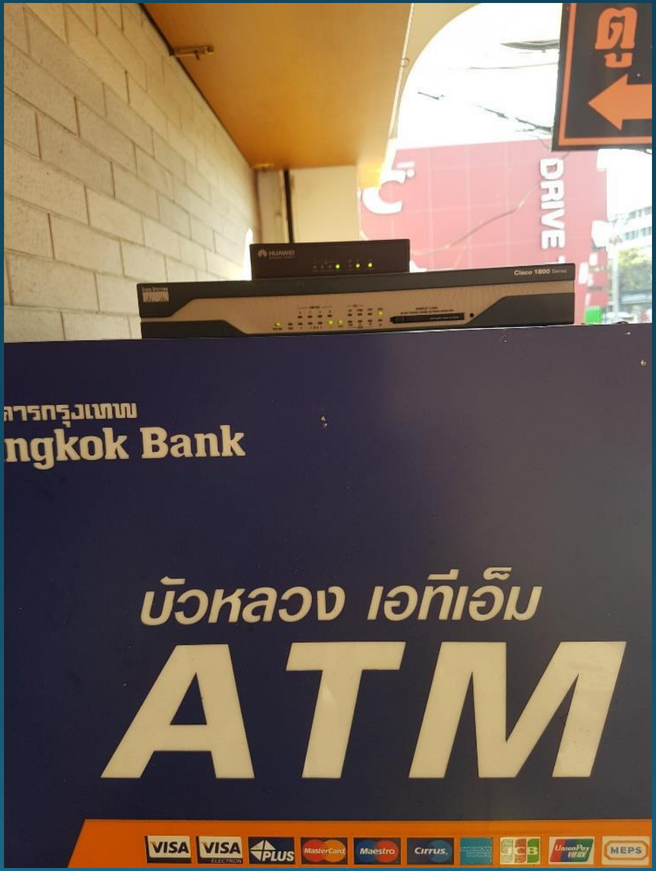
“Humans are incapable of securely storing high-quality cryptographic keys and they have unacceptable speed and accuracy when performing cryptographic operations. They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations.”

From Network Security: Private Communication in a Public World.

Kaufman, Perlman, and Speciner
Prentice Hall, publisher

Deployment Failures





Windows Er
Windows did not shut down successfull
responding, or if the system was shut
able to recover by choosing one of th
menu below:
(Use the arrow keys to highlight your
Safe Mode
Safe Mode with Networking
Safe Mode with Command Prompt
Start Windows Normally
Seconds until the highlighted choice
Description: Start Windows with its r
Choose

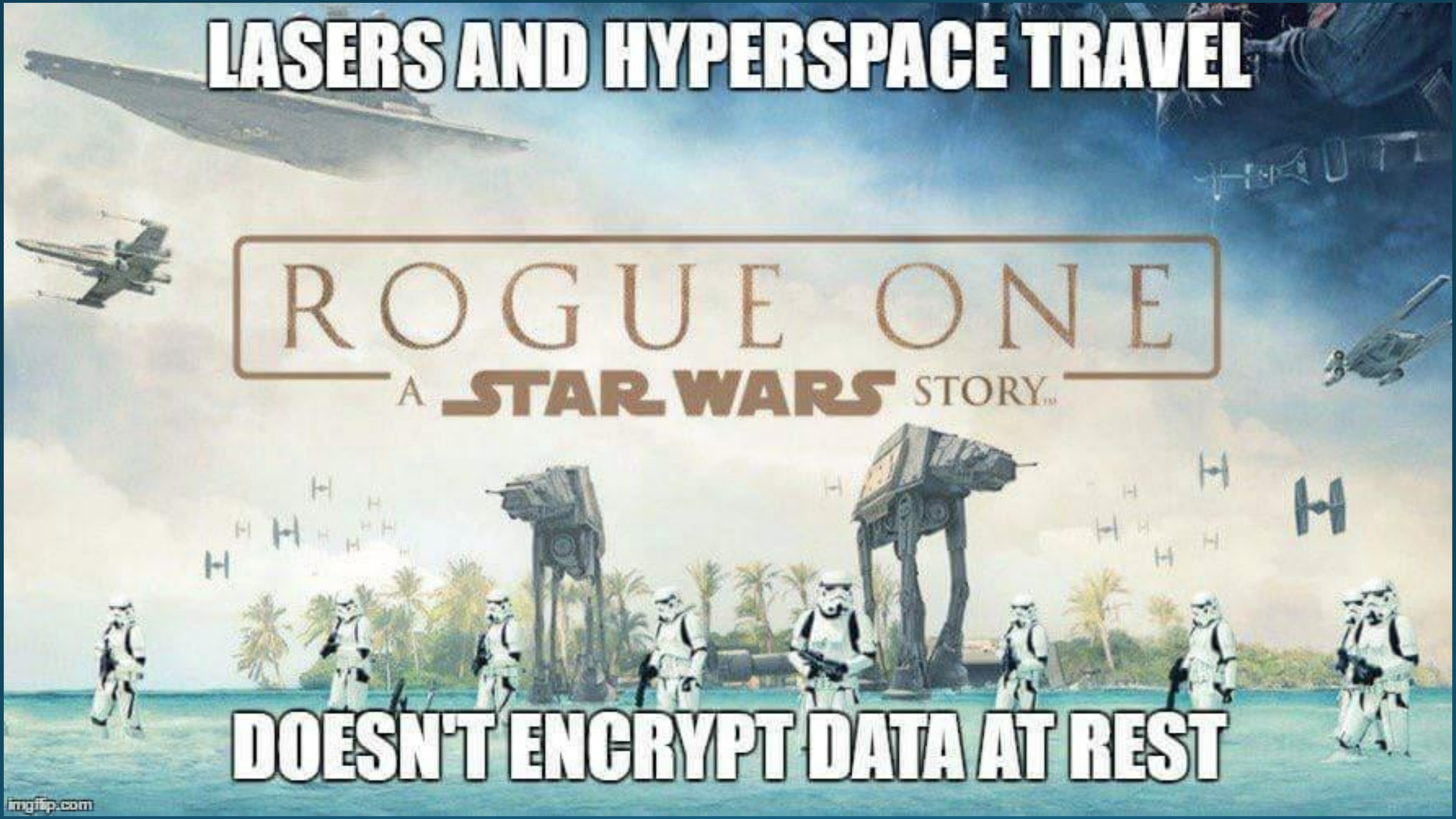
UK Banks warn against storing family finger prints on Apple Pay

- Banks are warning Apple Pay users against storing other people's fingerprints on their iPhones, with a threat that would void terms & conditions agreements.

- While iPhone users can store as many as 10 fingerprints on some iPhones – to allow family members to share their devices – these settings could create several unintended consequences.

- If mobile bank customers fail to heed these notices, banks may opt not to refund disputed transactions or may not assist customers when they if they become victims of fraud.

http://www.scmagazine.com/banks-warn-apple-pay-users-against-storing-family-members-fingerprints-on-iphones/article/451494/


LASERS AND HYPERSPACE TRAVEL
ROGUE ONE
A STAR WARS STORY
DOESN'T ENCRYPT DATA AT REST
imgflip.com

War on Kids

Until we fix our connected homes,
hackers will keep screaming at babies.

Talking Tom app offers naked selfies

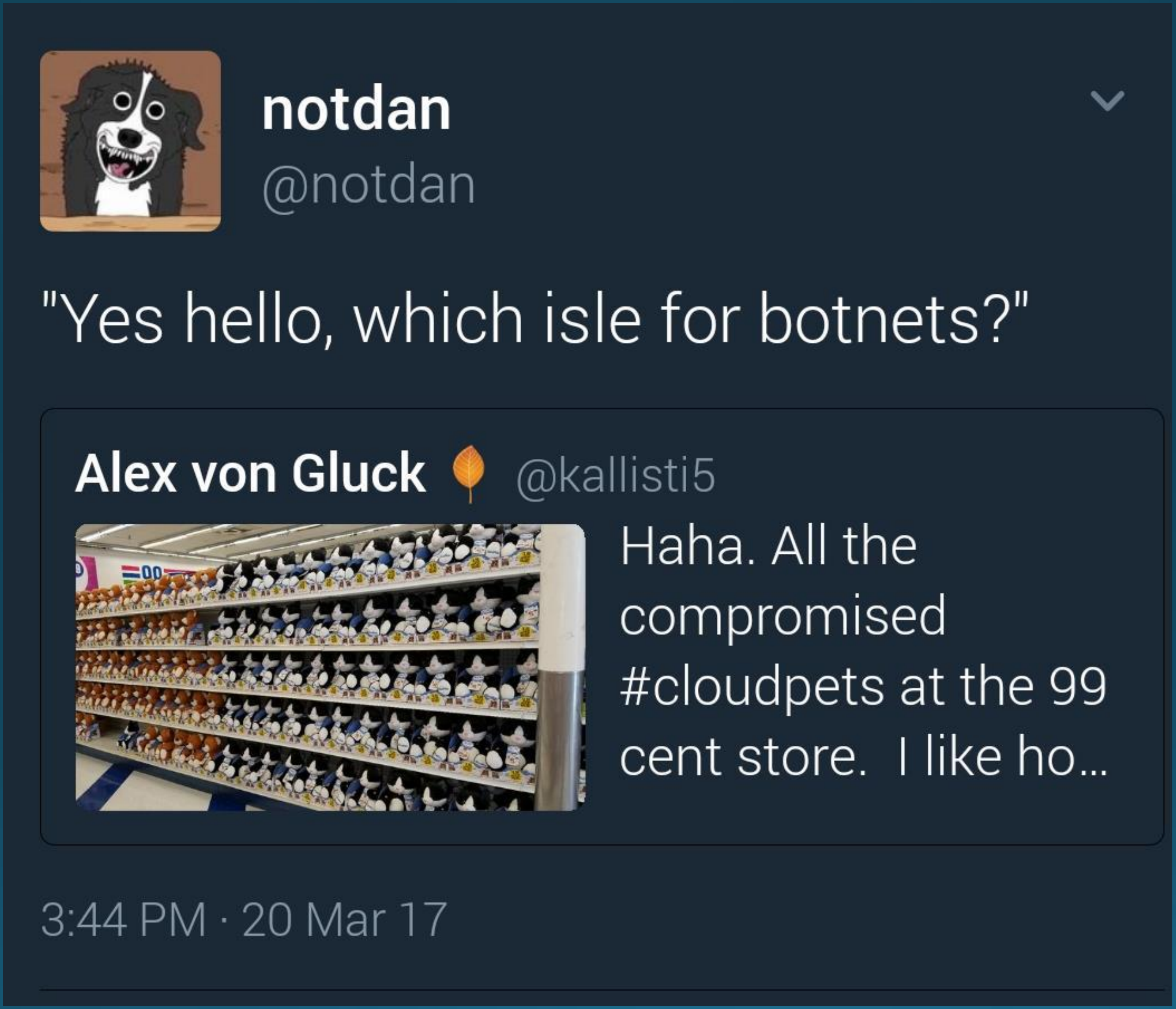
- Company says it's the "world's most popular cat"
- Available on Android & iOS
- Aimed at children
- Affairalert.com bought adult ads on Talking Tom

https://nakedsecurity.sophos.com/2015/12/11/my-talking-tom-offers-up-naked-selfie-ads-to-kids/

Fisher-Price smart bear hacked…

- Researchers at Rapid7, found that the app connected to the Fisher-Price toy had several security flaws that would allow a hacker to steal a **child's name**, **birthdate** and **gender**, along with other data. The toymaker encourages parents to use the app so that the toy can better interact with children.

https://www.theguardian.com/technology/2016/feb/02/fisher-price-mattel-smart-toy-bear-data-hack-technology



notdan
@notdan

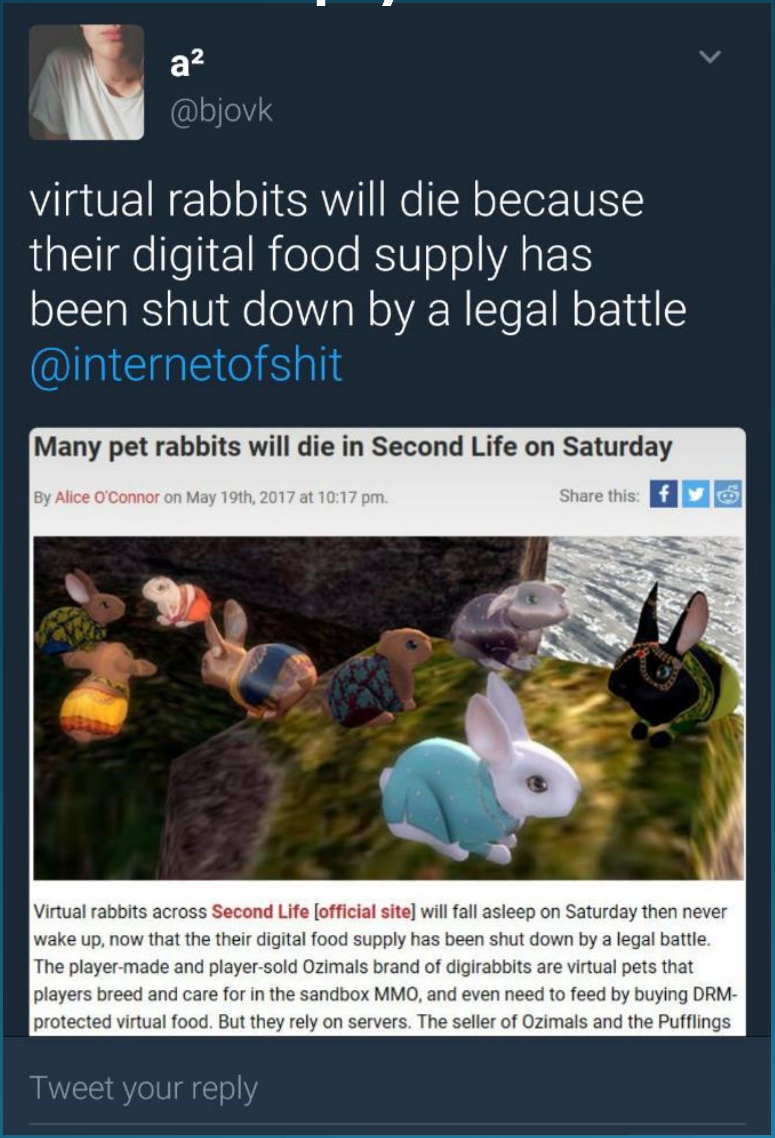
"Yes hello, which isle for botnets?"

Alex von Gluck 🍂 @kallisti5

Haha. All the compromised #cloudpets at the 99 cent store. I like ho…

3:44 PM · 20 Mar 17

Future Therapy Bills…



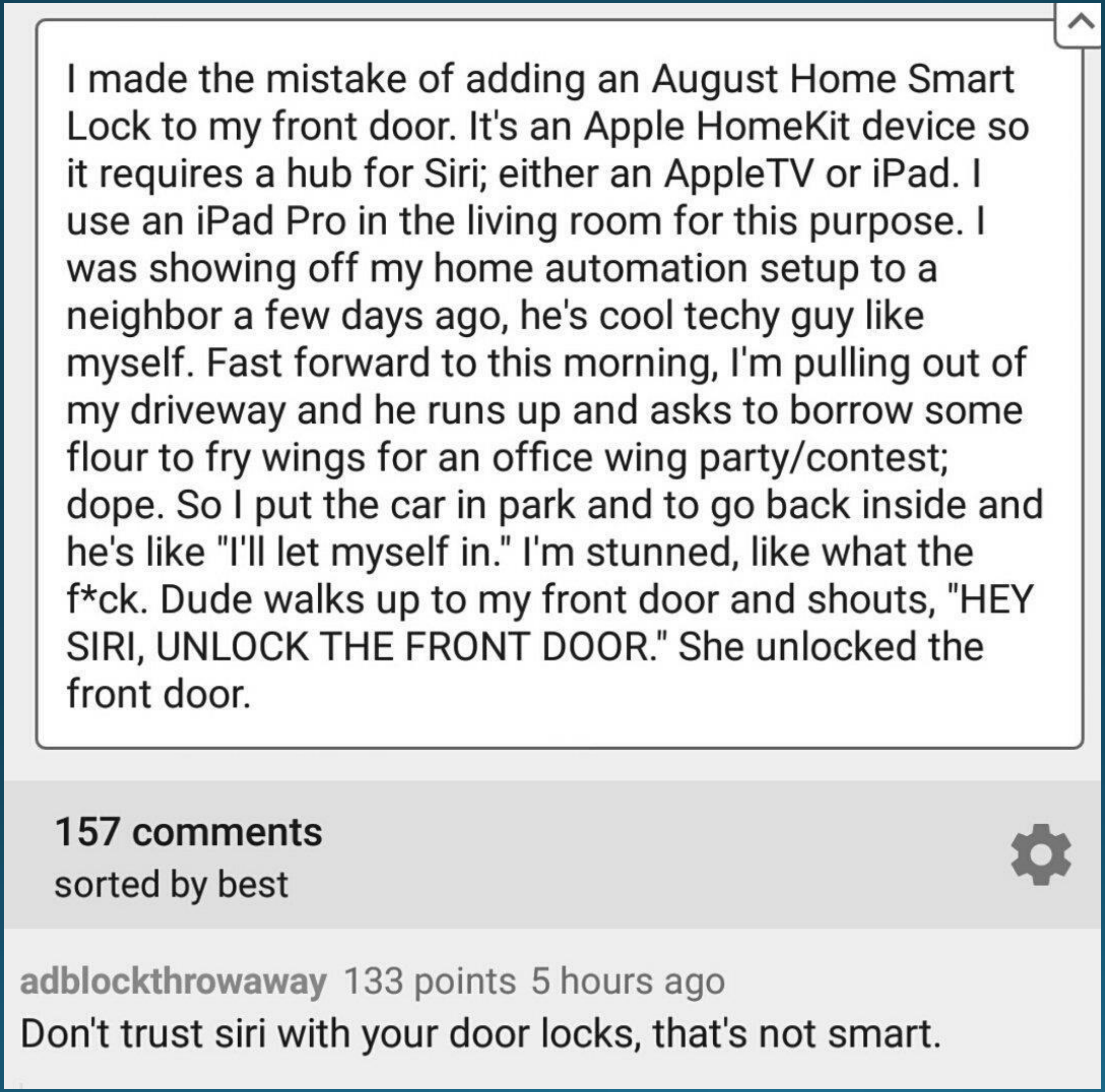
a²
@bjovk

virtual rabbits will die because their digital food supply has been shut down by a legal battle @internetofshit

Many pet rabbits will die in Second Life on Saturday

By Alice O'Connor on May 19th, 2017 at 10:17 pm.

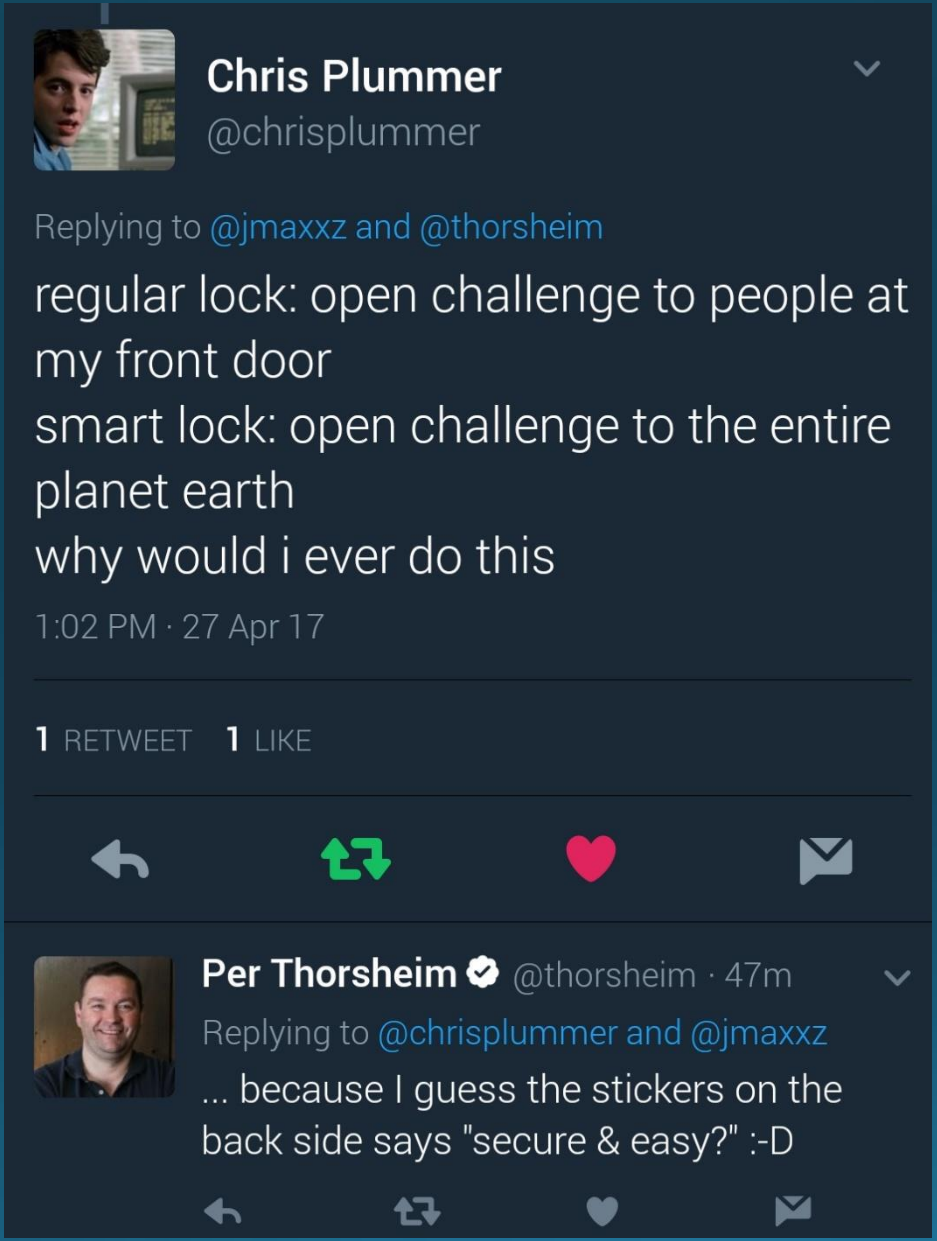
Virtual rabbits across **Second Life** [**official site**] will fall asleep on Saturday then never wake up, now that the their digital food supply has been shut down by a legal battle. The player-made and player-sold Ozimals brand of digirabbits are virtual pets that players breed and care for in the sandbox MMO, and even need to feed by buying DRM-protected virtual food. But they rely on servers. The seller of Ozimals and the Pufflings



I made the mistake of adding an August Home Smart Lock to my front door. It's an Apple HomeKit device so it requires a hub for Siri; either an AppleTV or iPad. I use an iPad Pro in the living room for this purpose. I was showing off my home automation setup to a neighbor a few days ago, he's cool techy guy like myself. Fast forward to this morning, I'm pulling out of my driveway and he runs up and asks to borrow some flour to fry wings for an office wing party/contest; dope. So I put the car in park and to go back inside and he's like "I'll let myself in." I'm stunned, like what the f*ck. Dude walks up to my front door and shouts, "HEY SIRI, UNLOCK THE FRONT DOOR." She unlocked the front door.

157 comments
sorted by best

adblockthrowaway 133 points 5 hours ago
Don't trust siri with your door locks, that's not smart.



Chris Plummer
@chrisplummer

Replying to @jmaxxz and @thorsheim

regular lock: open challenge to people at my front door
smart lock: open challenge to the entire planet earth
why would i ever do this

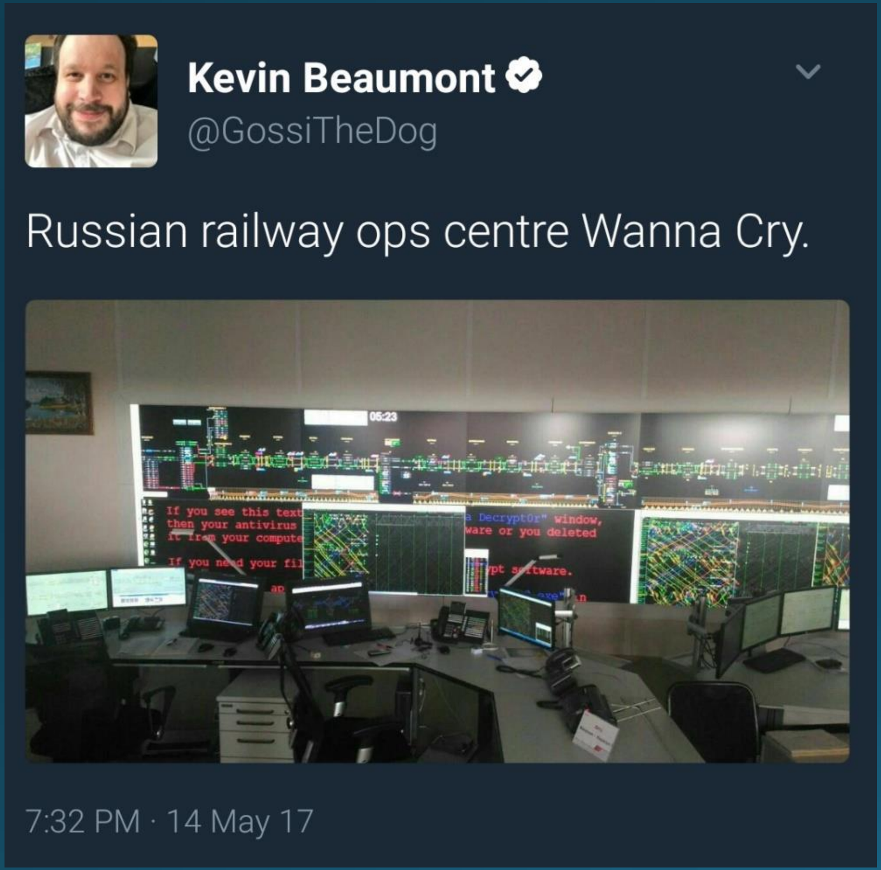
1:02 PM · 27 Apr 17

1 RETWEET 1 LIKE

Per Thorsheim @thorsheim · 47m

Replying to @chrisplummer and @jmaxxz

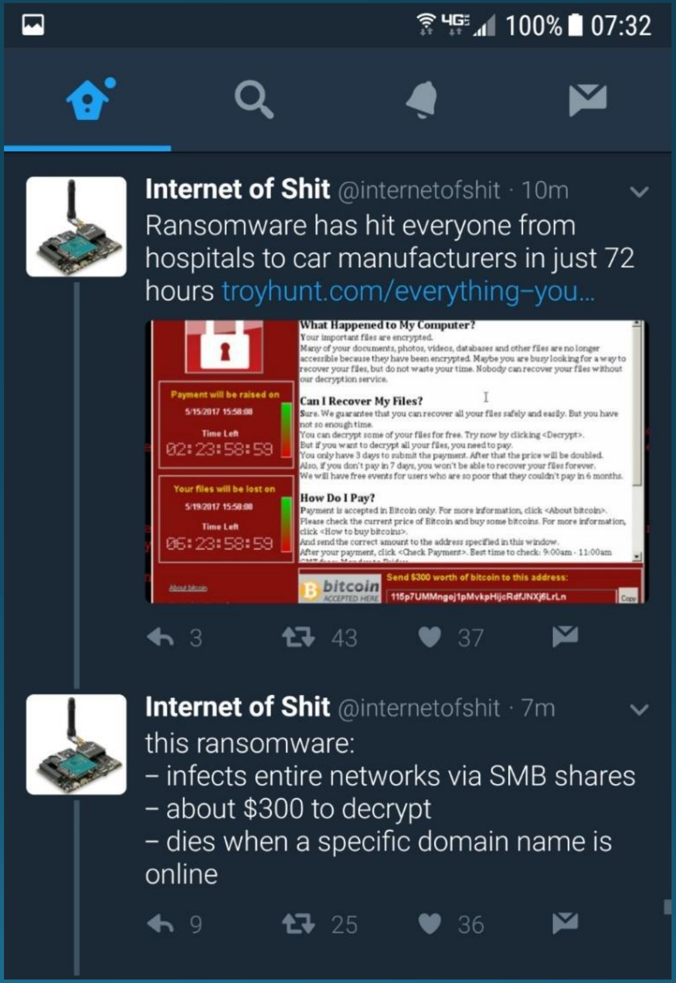
... because I guess the stickers on the back side says "secure & easy?" :-D



Kevin Beaumont @GossiTheDog

Russian railway ops centre Wanna Cry.

7:32 PM · 14 May 17



Internet of Shit @internetofshit · 10m

Ransomware has hit everyone from hospitals to car manufacturers in just 72 hours troyhunt.com/everything-you...

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/15/2017 15:58:08
Time Left
02:23:58:59

Your files will be lost on
5/19/2017 15:58:08
Time Left
06:23:58:59

Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

3 43 37

Internet of Shit @internetofshit · 7m

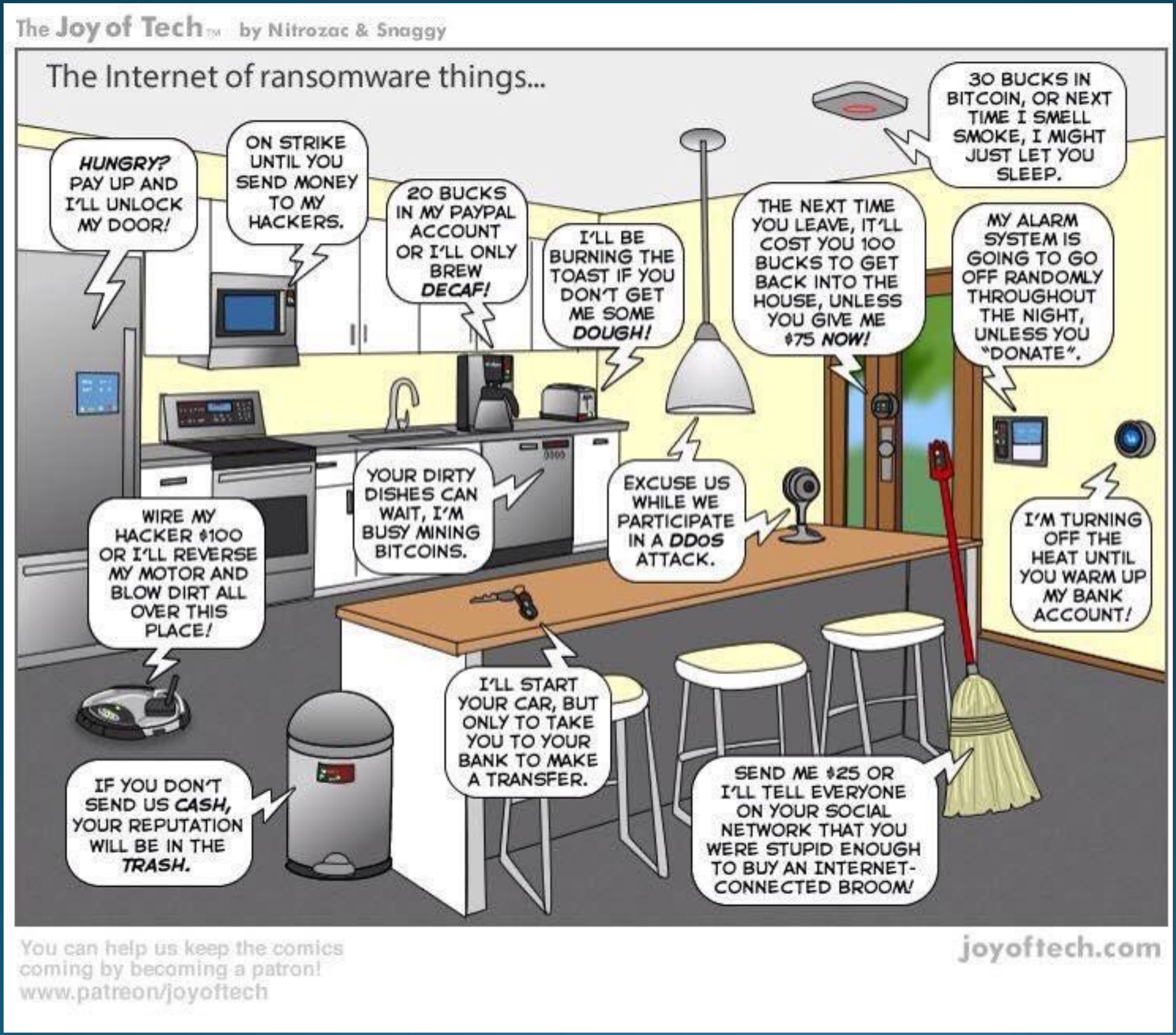
this ransomware:
- infects entire networks via SMB shares
- about $300 to decrypt
- dies when a specific domain name is online

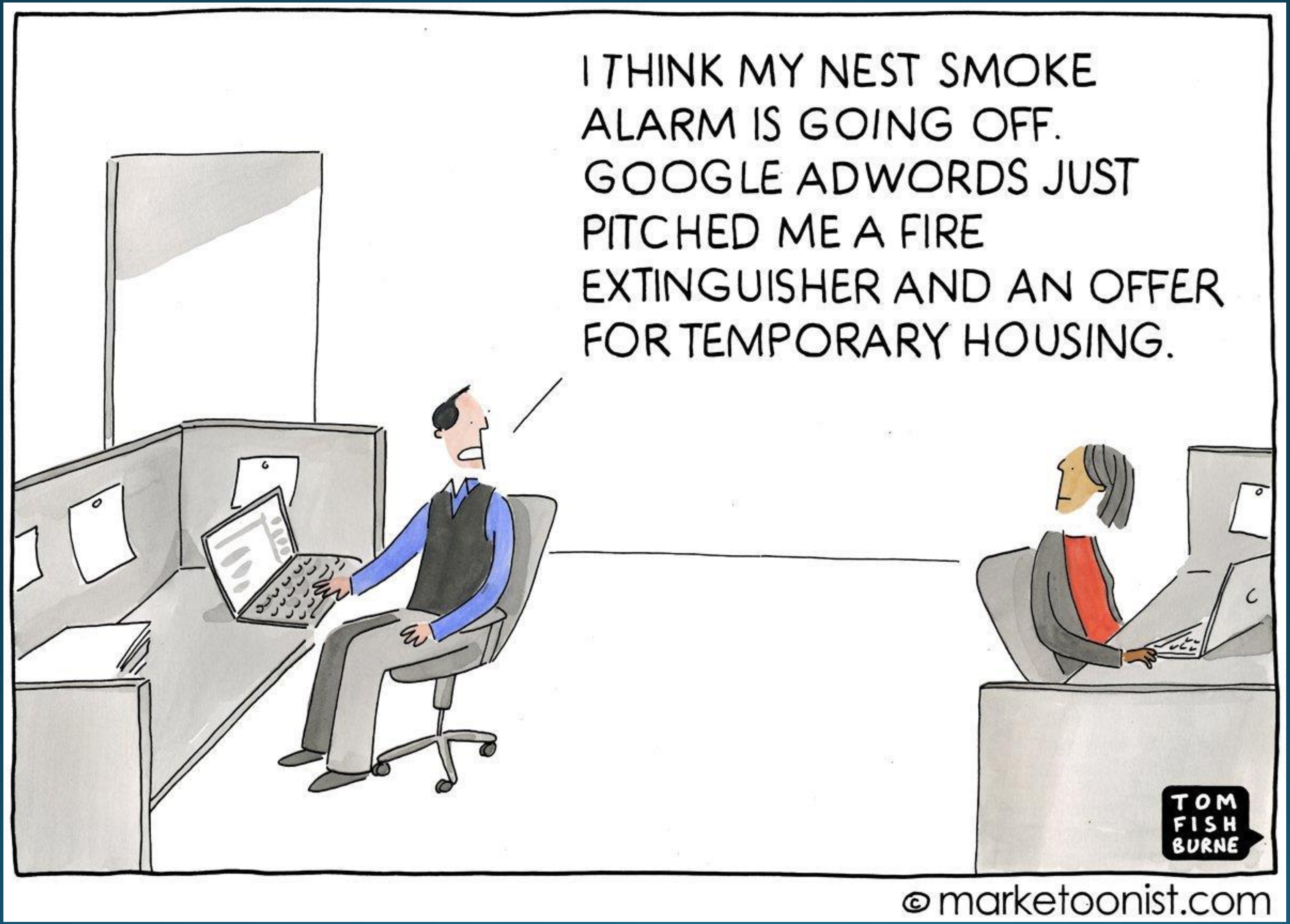
9 25 36

Google's NEST never turns off

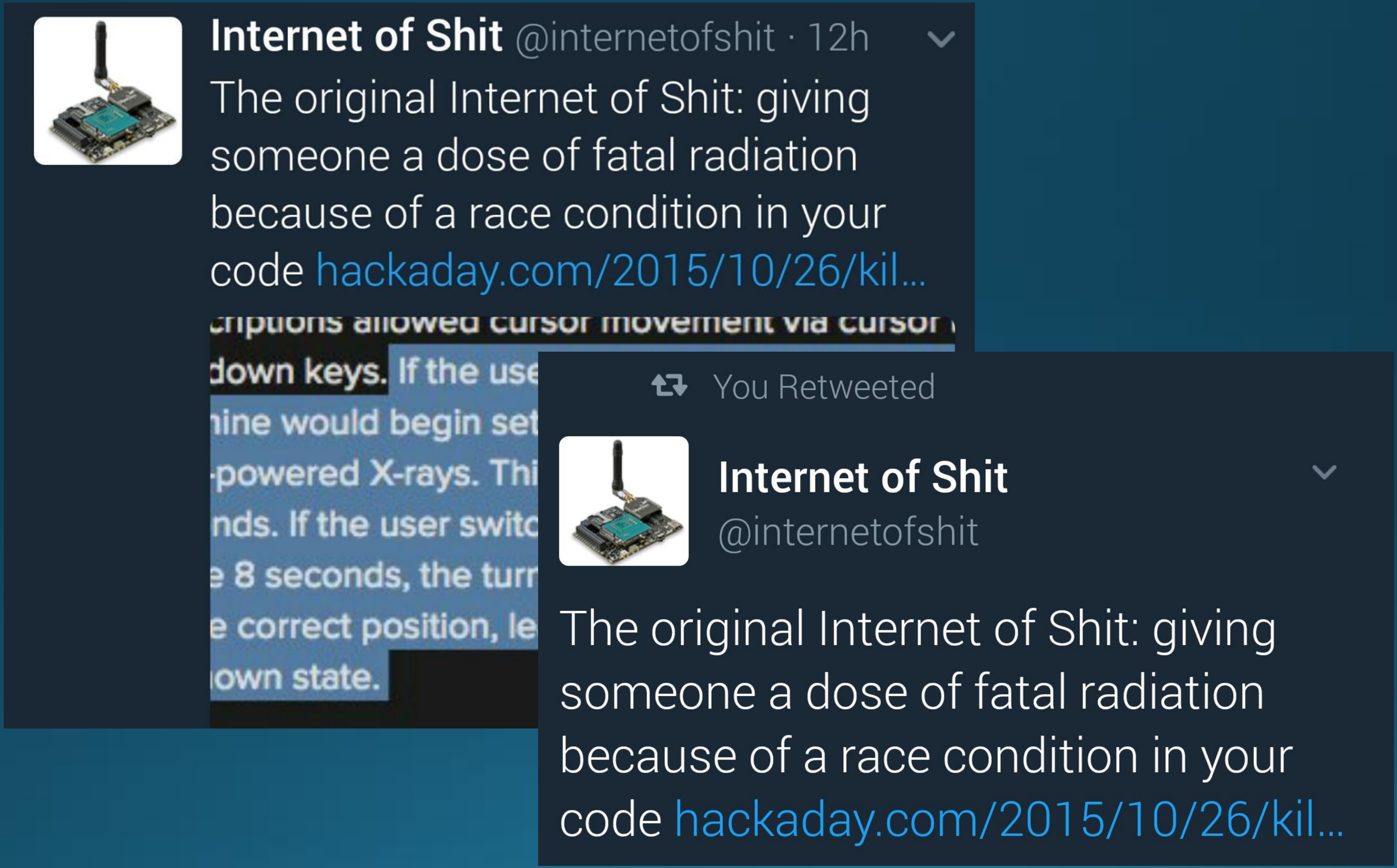
- **ABI Research has inspected Google's Nest Cam and found that when users turn off the camera, only the LED lights shuts down, with other components continuing to run in the background.**
- "This means that even when a consumer thinks that he or she is successfully turning off this camera, the device is still running, which could potentially unleash a tidal wave of privacy concerns."

http://news.softpedia.com/news/google-s-nest-cam-doesn-t-actually-shut-down-continues-to-operate-regardless-of-led-light-496691.shtml


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDoS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech
joyoftech.com


I THINK MY NEST SMOKE ALARM IS GOING OFF. GOOGLE ADWORDS JUST PITCHED ME A FIRE EXTINGUISHER AND AN OFFER FOR TEMPORARY HOUSING.
TOM FISH BURNE
© marketoonist.com

Medical



Internet of Shit @internetofshit · 12h

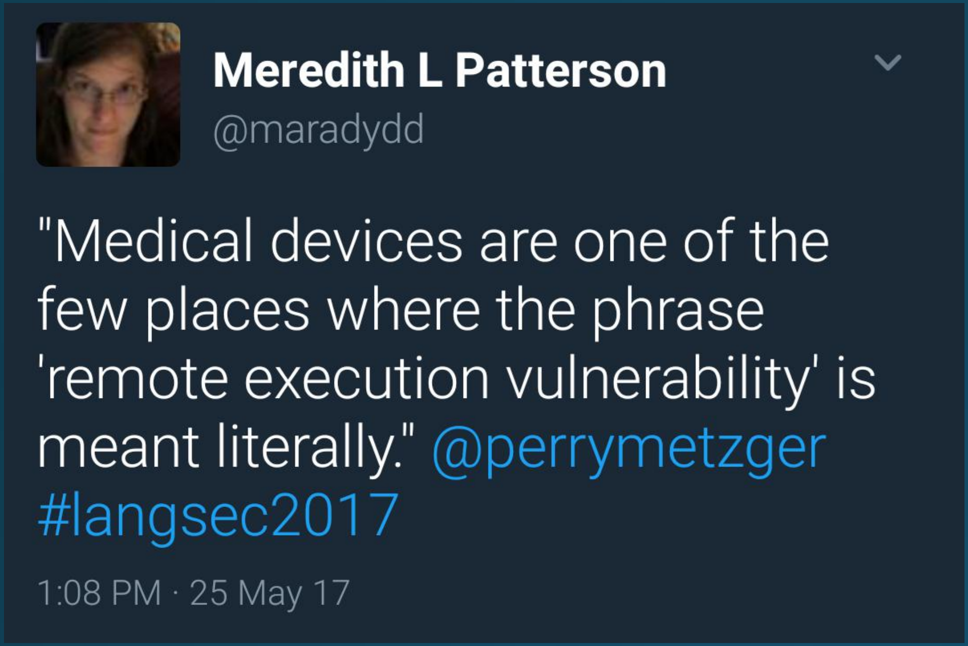
The original Internet of Shit: giving someone a dose of fatal radiation because of a race condition in your code hackaday.com/2015/10/26/kil…

criptions allowed cursor movement via cursor
down keys. If the use
hine would begin set
powered X-rays. Thi
nds. If the user switc
e 8 seconds, the turr
e correct position, le
own state.

You Retweeted

Internet of Shit
@internetofshit

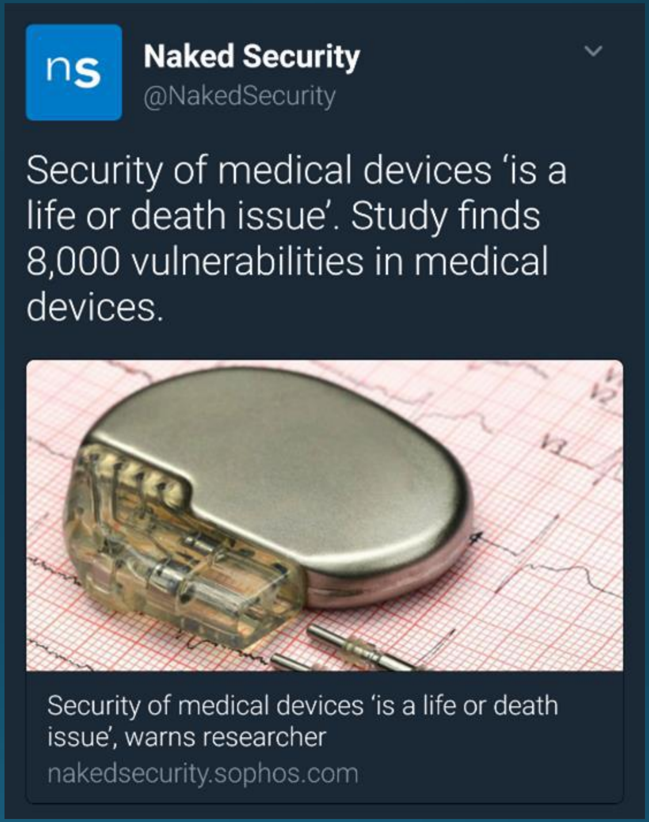
The original Internet of Shit: giving someone a dose of fatal radiation because of a race condition in your code hackaday.com/2015/10/26/kil…



Meredith L Patterson
@maradydd

"Medical devices are one of the few places where the phrase 'remote execution vulnerability' is meant literally." @perrymetzger #langsec2017

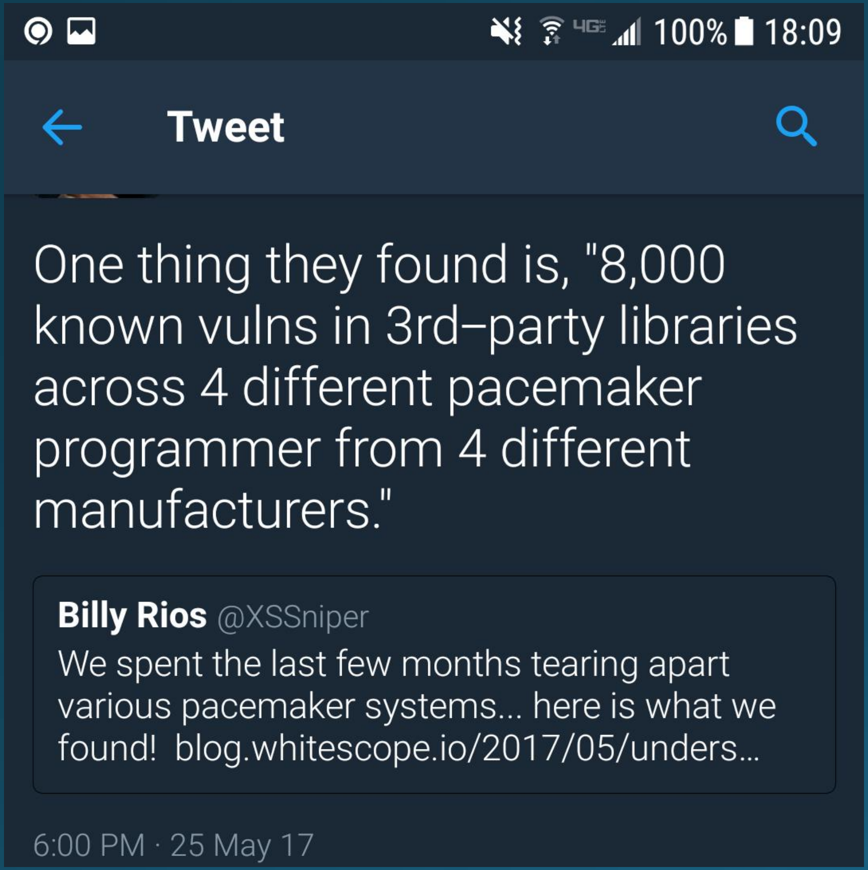
1:08 PM · 25 May 17



Naked Security
@NakedSecurity

Security of medical devices 'is a life or death issue'. Study finds 8,000 vulnerabilities in medical devices.

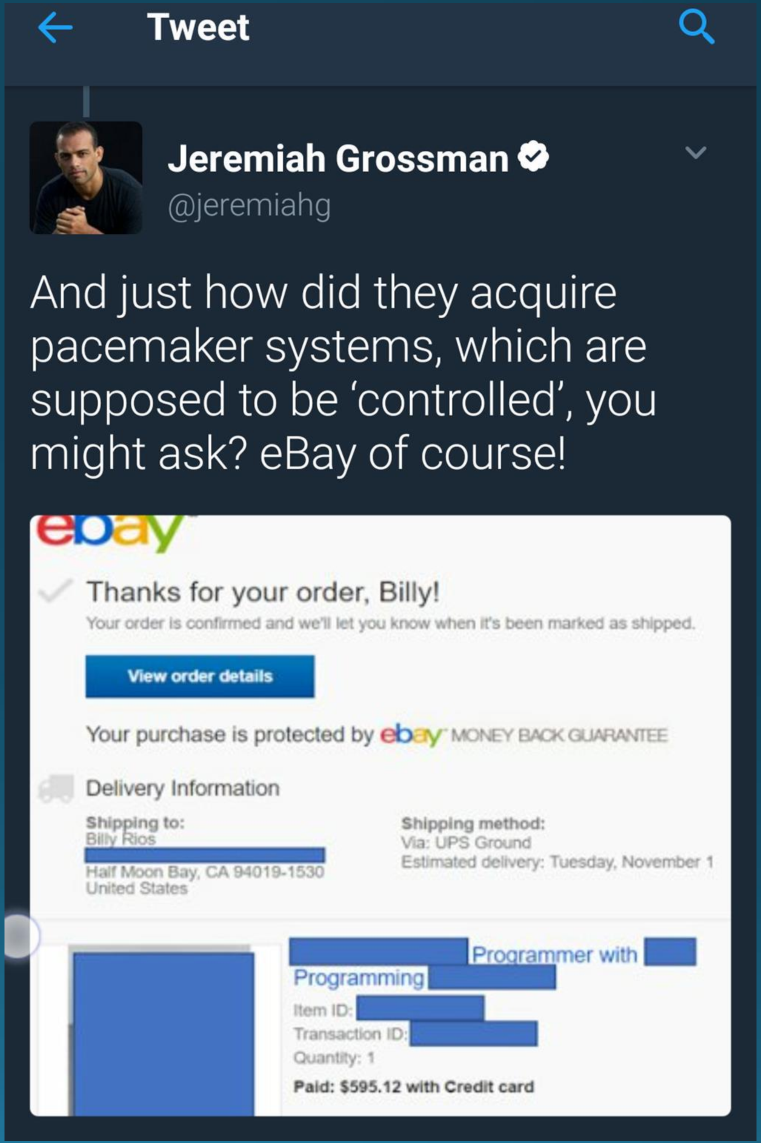
Security of medical devices 'is a life or death issue', warns researcher
nakedsecurity.sophos.com



One thing they found is, "8,000 known vulns in 3rd-party libraries across 4 different pacemaker programmer from 4 different manufacturers."

Billy Rios @XSSniper
We spent the last few months tearing apart various pacemaker systems... here is what we found! blog.whitescope.io/2017/05/unders...

6:00 PM · 25 May 17



Jeremiah Grossman @jeremiahg

And just how did they acquire pacemaker systems, which are supposed to be ‘controlled’, you might ask? eBay of course!

Thanks for your order, Billy!
Your order is confirmed and we'll let you know when it's been marked as shipped.

View order details

Your purchase is protected by ebay MONEY BACK GUARANTEE

Delivery Information

Shipping to:
Billy Rios
[redacted]
Half Moon Bay, CA 94019-1530
United States

Shipping method:
Via: UPS Ground
Estimated delivery: Tuesday, November 1

[redacted]

[redacted] Programmer with [redacted] Programming [redacted]
Item ID: [redacted]
Transaction ID: [redacted]
Quantity: 1
Paid: $595.12 with Credit card

Voice Assistants

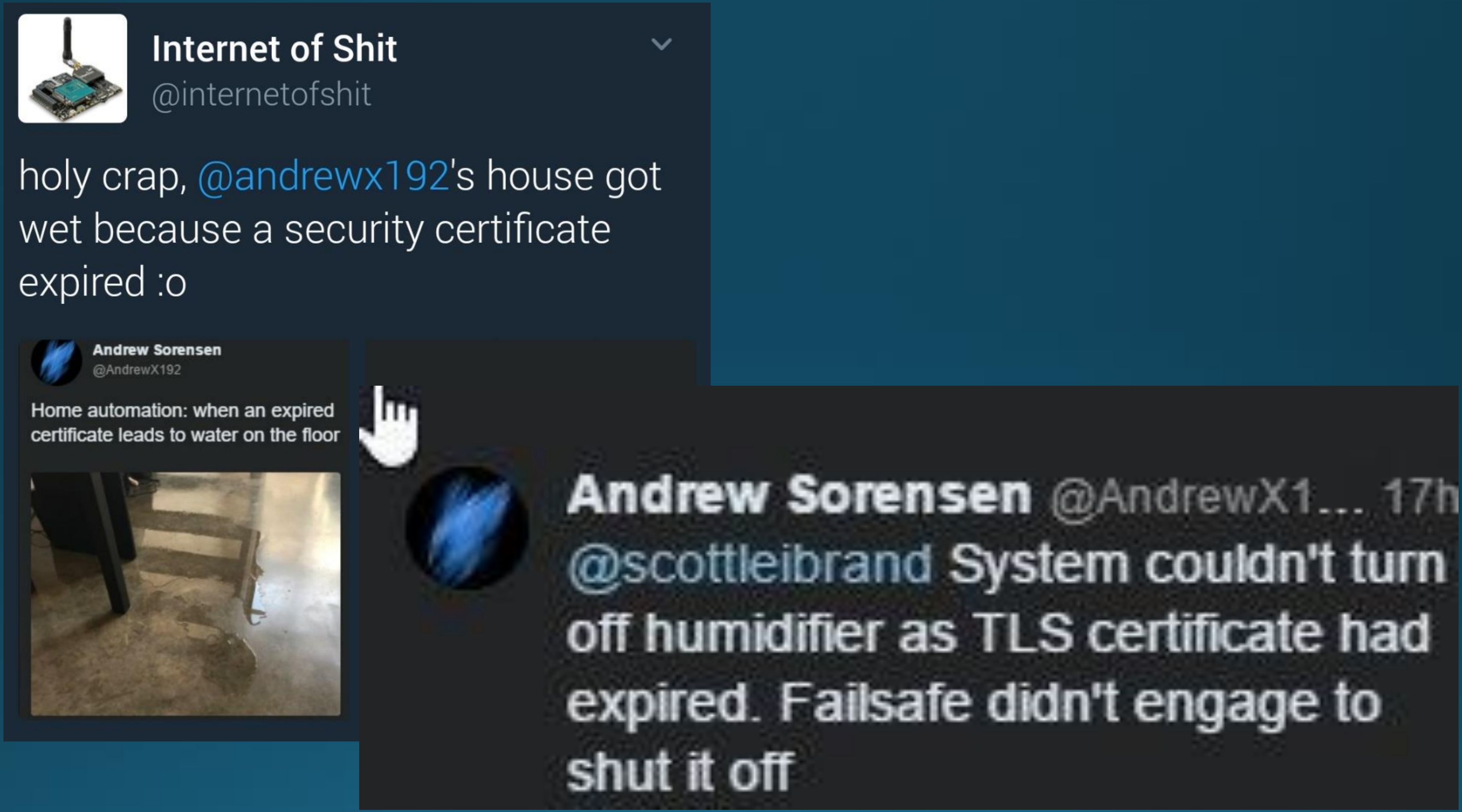
PEOPLE IN THE SIXTIES: THE GOVERNMENT WILL WIRETAP YOUR HOME
amazon
PEOPLE NOW: HEY WIRE TAP, CAN CATS EAT PANCAKES?

HELLO, WELCOME TO OUR HOUSE!
THANKS FOR INVITING US!
ALEXA, ORDER TWO TONS OF CREAMED CORN.
ALEXA, CONFIRM PURCHASE.

WHEN VISITING A NEW HOUSE, IT'S GOOD TO CHECK WHETHER THEY HAVE AN ALWAYS-ON DEVICE TRANSMITTING YOUR CONVERSATIONS SOMEWHERE.

I learned the name of the Amazon Echo and placed an order without asking permission
- Larry Bird

Smart Homes



Internet of Shit
@internetofshit

holy crap, @andrewx192's house got wet because a security certificate expired :o

Andrew Sorensen
@AndrewX192

Home automation: when an expired certificate leads to water on the floor

Andrew Sorensen @AndrewX1... 17h

@scottleibrand System couldn't turn off humidifier as TLS certificate had expired. Failsafe didn't engage to shut it off

SimpliSafe transmits PIN in clear

- It appears SimpliSafe's systems send messages unencrypted in the clear over the air. That means it's trivial to send spoofed sensor readings – such as back-door closed – to fool alarm control boxes into thinking no break-in is happening, and replay PIN codes from keypads to activate or deactivate security systems.

- A thief just has to loiter near a home with some radio equipment, pick up the unencrypted PIN messages transmitted from a keypad to the control box, and later replay the messages to deactivate the alarm when the homeowners are out."

http://www.theregister.co.uk/2016/02/17/simplisafe_wireless_home_alarm_system_cracked

WiFi enabled doorbell…open for all

- The Ring allows people to answer people knocking on your door from your mobile phone
- There’s an optional feature that allows the kit to hook up to some smart door locks, so users can let guests into their home even when they aren’t in.
- The device is secured outside a house using two commonly available Torx T4 screws, leaving it vulnerable to theft. Ring offer a free replacement if the kit is stolen, so homeowners are covered in that scenario (at least).
- An easy attack makes it all too simple to steal a homeowner's Wi-Fi key. To do this, hackers would need to take the kit off the door mounting, flip it over and press the orange "set up" button.
- “Pressing the setup button [puts] the doorbell’s wireless module (a Gainspan wireless unit) into a setup mode, in which it acts as a Wi-Fi access point,” Pen Test Partners consultant David Lodge

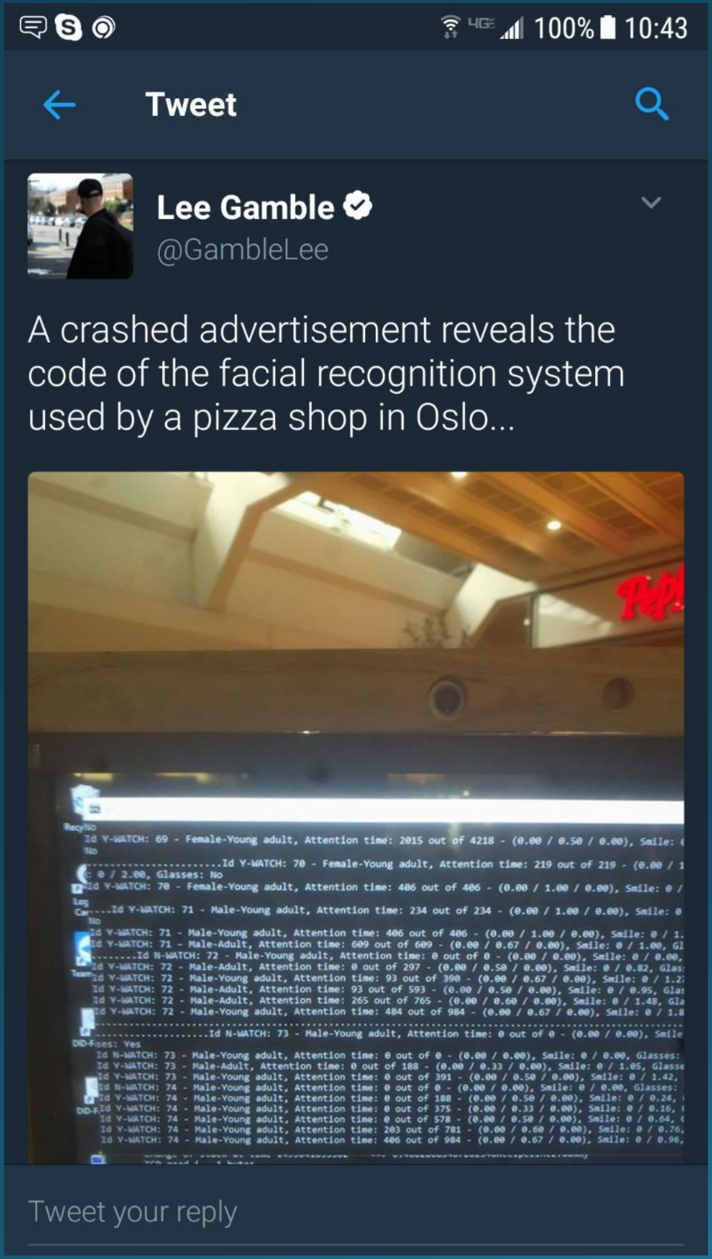
http://www.theregister.co.uk/2016/01/12/ring_doorbell_reveals_wifi_credentials/

Xfinity's Security System Flaws Open Homes to Thieves

- Security researchers at Rapid7 have found vulnerabilities in Comcast's Xfinity Home Security system that would cause it to falsely report that a property's windows and doors are closed and secured even if they've been opened; it could also fail to sense an intruder's motion.

- The system uses a ZigBee-based protocol to communicate and operate over the 2.4 GHz radio frequency band. All a thief has to do is use radio jamming equipment to block the signals that pass from a door, window, or motion sensor to the home's baseband hub
- **"The sign that is designed to deter attackers can now become a sign that invites attackers,"** Beardsley says [Rapid7].
- "***Our home security system uses the same advanced, industry-standard technology as the nation's top home security providers." – Comcast Spokesperson***

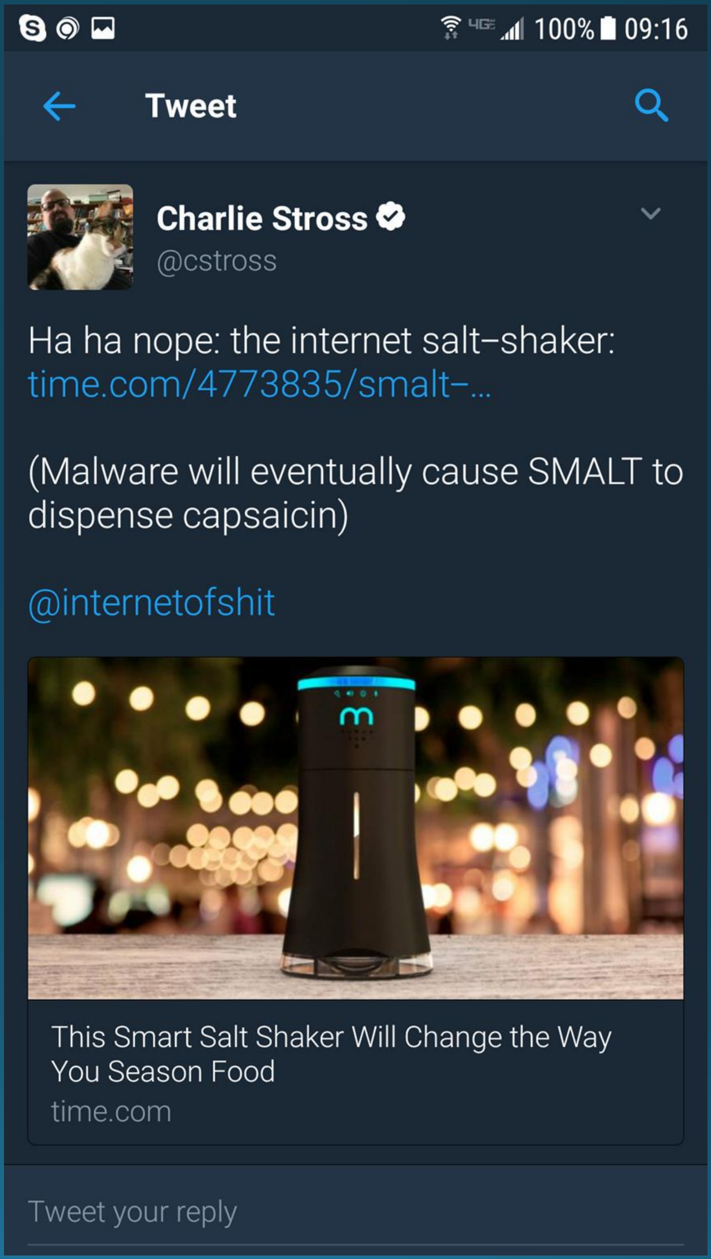
http://www.wired.com/2016/01/xfinitys-security-system-flaws-open-homes-to-thieves/



Lee Gamble
@GambleLee

A crashed advertisement reveals the code of the facial recognition system used by a pizza shop in Oslo...

```
Id Y-WATCH: 69 - Female-Young adult, Attention time: 2015 out of 4218 - (0.00 / 0.50 / 0.00), Smile: 
No
........................Id Y-WATCH: 70 - Female-Young adult, Attention time: 219 out of 219 - (0.00 / 1
: 0 / 2.00, Glasses: No
Id Y-WATCH: 70 - Female-Young adult, Attention time: 406 out of 406 - (0.00 / 1.00 / 0.00), Smile: 0 /
....Id Y-WATCH: 71 - Male-Young adult, Attention time: 234 out of 234 - (0.00 / 1.00 / 0.00), Smile: 0
No
Id Y-WATCH: 71 - Male-Young adult, Attention time: 406 out of 406 - (0.00 / 1.00 / 0.00), Smile: 0 / 1.
Id Y-WATCH: 71 - Male-Adult, Attention time: 609 out of 609 - (0.00 / 0.67 / 0.00), Smile: 0 / 1.00, Gl
........Id N-WATCH: 72 - Male-Young adult, Attention time: 0 out of 0 - (0.00 / 0.00), Smile: 0 / 0.00,
Id Y-WATCH: 72 - Male-Adult, Attention time: 0 out of 297 - (0.00 / 0.50 / 0.00), Smile: 0 / 0.82, Glas
Id Y-WATCH: 72 - Male-Young adult, Attention time: 93 out of 390 - (0.00 / 0.67 / 0.00), Smile: 0 / 1.2
Id Y-WATCH: 72 - Male-Adult, Attention time: 93 out of 593 - (0.00 / 0.50 / 0.00), Smile: 0 / 0.95, Gla
Id Y-WATCH: 72 - Male-Adult, Attention time: 265 out of 765 - (0.00 / 0.60 / 0.00), Smile: 0 / 1.48, Gla
Id Y-WATCH: 72 - Male-Young adult, Attention time: 484 out of 984 - (0.00 / 0.67 / 0.00), Smile: 0 / 1.8
.............................................................................................................
.....................Id N-WATCH: 73 - Male-Young adult, Attention time: 0 out of 0 - (0.00 / 0.00), Smile
ses: Yes
Id N-WATCH: 73 - Male-Young adult, Attention time: 0 out of 0 - (0.00 / 0.00), Smile: 0 / 0.00, Glasses:
Id Y-WATCH: 73 - Male-Adult, Attention time: 0 out of 188 - (0.00 / 0.33 / 0.00), Smile: 0 / 1.05, Glasse
Id Y-WATCH: 73 - Male-Young adult, Attention time: 0 out of 391 - (0.00 / 0.50 / 0.00), Smile: 0 / 1.42,
Id N-WATCH: 74 - Male-Young adult, Attention time: 0 out of 0 - (0.00 / 0.00), Smile: 0 / 0.00, Glasses:
Id Y-WATCH: 74 - Male-Young adult, Attention time: 0 out of 188 - (0.00 / 0.50 / 0.00), Smile: 0 / 0.24,
Id Y-WATCH: 74 - Male-Young adult, Attention time: 0 out of 375 - (0.00 / 0.33 / 0.00), Smile: 0 / 0.16,
Id Y-WATCH: 74 - Male-Young adult, Attention time: 0 out of 578 - (0.00 / 0.50 / 0.00), Smile: 0 / 0.64,
Id Y-WATCH: 74 - Male-Young adult, Attention time: 203 out of 781 - (0.00 / 0.60 / 0.00), Smile: 0 / 0.76,
Id Y-WATCH: 74 - Male-Young adult, Attention time: 406 out of 984 - (0.00 / 0.67 / 0.00), Smile: 0 / 0.96,
```



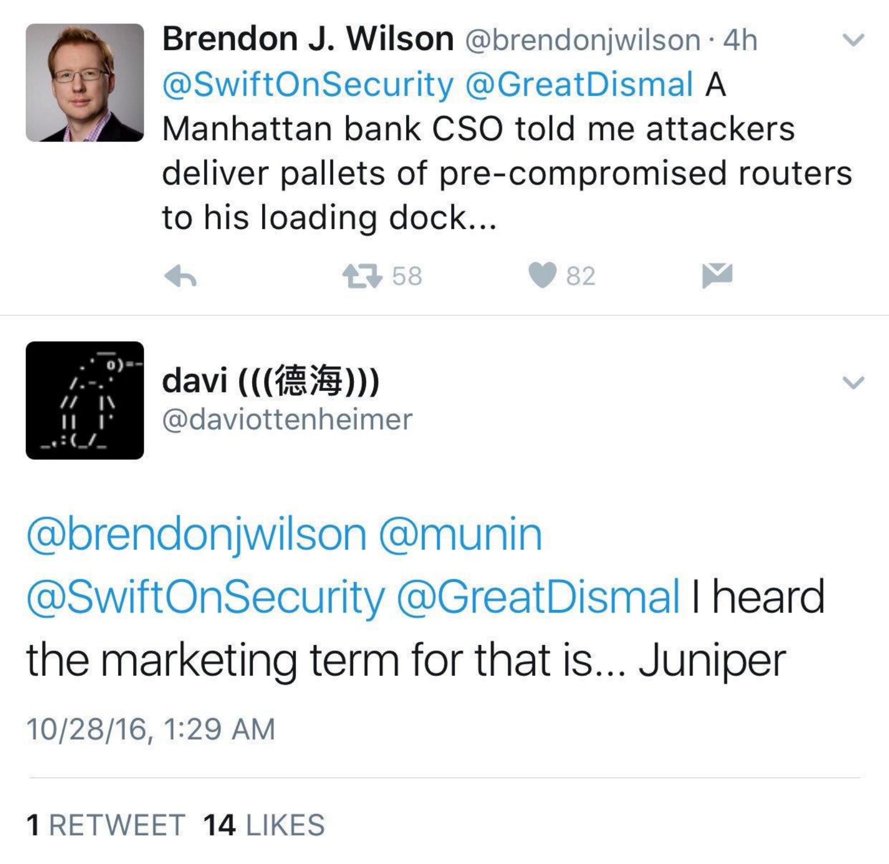
Charlie Stross
@cstross

Ha ha nope: the internet salt–shaker: time.com/4773835/smalt–...

(Malware will eventually cause SMALT to dispense capsaicin)

@internetofshit

This Smart Salt Shaker Will Change the Way You Season Food
time.com



Brendon J. Wilson @brendonjwilson · 4h

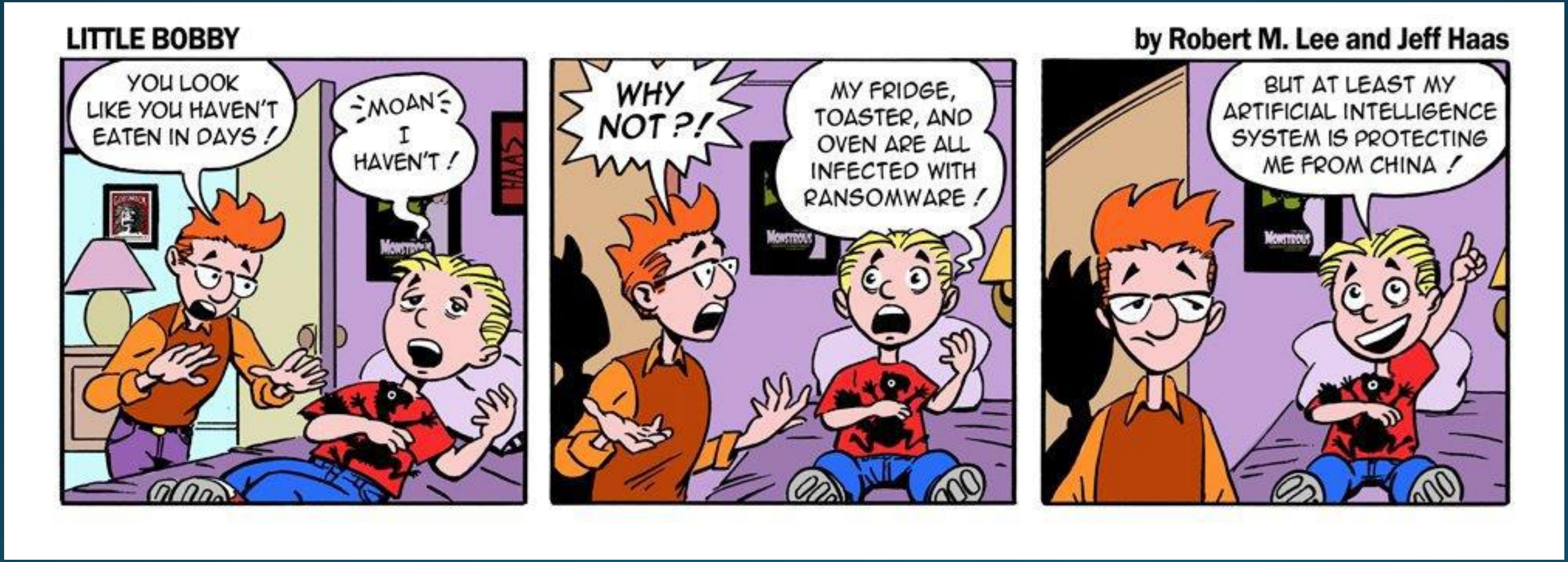
@SwiftOnSecurity @GreatDismal A Manhattan bank CSO told me attackers deliver pallets of pre-compromised routers to his loading dock...

davi (((德海)))
@daviottenheimer

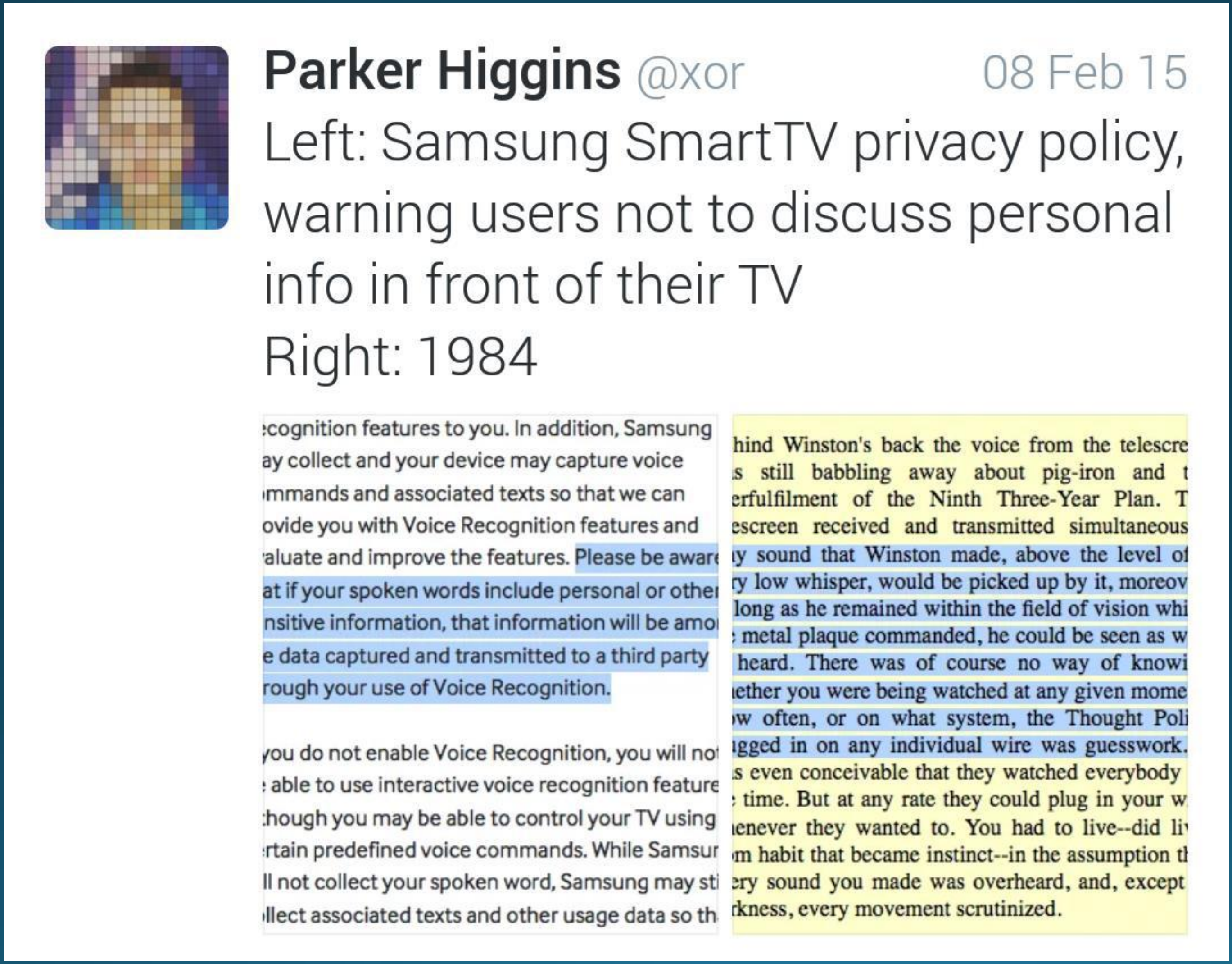
@brendonjwilson @munin @SwiftOnSecurity @GreatDismal I heard the marketing term for that is... Juniper

10/28/16, 1:29 AM

1 RETWEET 14 LIKES


LITTLE BOBBY
by Robert M. Lee and Jeff Haas
YOU LOOK LIKE YOU HAVEN'T EATEN IN DAYS!
MOAN I HAVEN'T!
HAAS
MONSTROUS
WHY NOT?!
MY FRIDGE, TOASTER, AND OVEN ARE ALL INFECTED WITH RANSOMWARE!
BUT AT LEAST MY ARTIFICIAL INTELLIGENCE SYSTEM IS PROTECTING ME FROM CHINA!

SmartTVs



Parker Higgins @xor 08 Feb 15

Left: Samsung SmartTV privacy policy, warning users not to discuss personal info in front of their TV
Right: 1984

:cognition features to you. In addition, Samsung
ay collect and your device may capture voice
ımmands and associated texts so that we can
ovide you with Voice Recognition features and
'aluate and improve the features. Please be aware
at if your spoken words include personal or other
nsitive information, that information will be amo
e data captured and transmitted to a third party
rough your use of Voice Recognition.

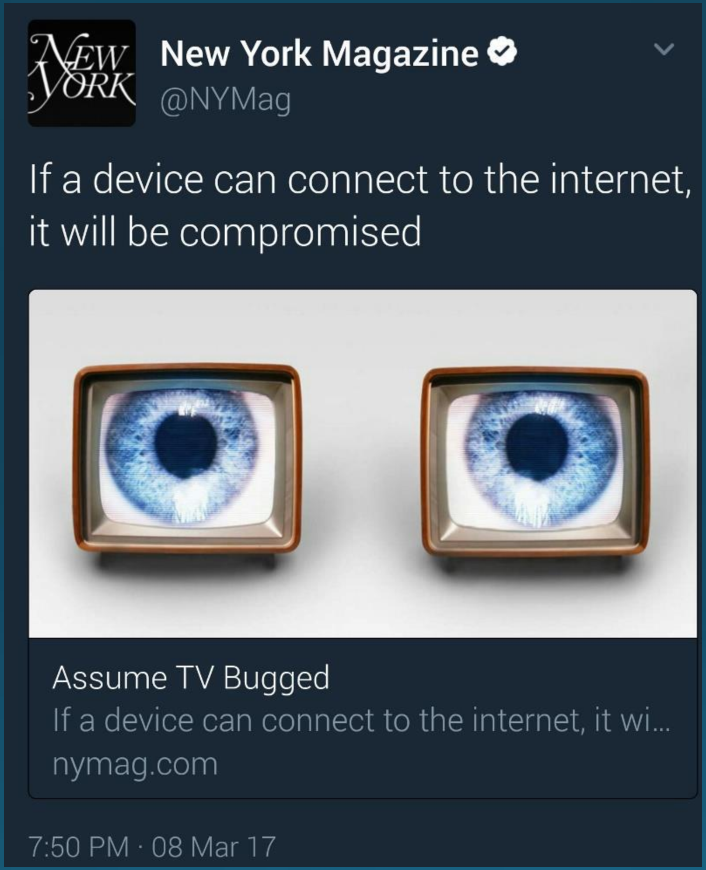
you do not enable Voice Recognition, you will not
: able to use interactive voice recognition feature
:hough you may be able to control your TV using
:rtain predefined voice commands. While Samsur
ll not collect your spoken word, Samsung may sti
ıllect associated texts and other usage data so th

hind Winston's back the voice from the telescre
s still babbling away about pig-iron and t
erfulfilment of the Ninth Three-Year Plan. T
escreen received and transmitted simultaneous
ıy sound that Winston made, above the level of
ry low whisper, would be picked up by it, moreov
long as he remained within the field of vision whi
: metal plaque commanded, he could be seen as w
heard. There was of course no way of knowi
ıether you were being watched at any given mome
ıw often, or on what system, the Thought Poli
ıgged in on any individual wire was guesswork.
s even conceivable that they watched everybody
: time. But at any rate they could plug in your w
ıenever they wanted to. You had to live--did liv
ım habit that became instinct--in the assumption tl
ery sound you made was overheard, and, except
rkness, every movement scrutinized.

Samsung smart fridge leaves Gmail logins open to attack

- Pen Test Partners discovered the MiTM (man-in-the-middle) vulnerability that facilitated the exploit during an IoT hacking challenge at the recent DEF CON hacking conference.
- The hack was pulled off against the RF28HMELBSR smart fridge, part of Samsung's line-up of Smart Home appliances which can be controlled via their Smart Home app. While the fridge implements SSL, it fails to validate SSL certificates, thereby enabling man-in-the-middle attacks against most connections.
- The internet-connected device is designed to download Gmail Calendar information to an on-screen display. Security shortcomings mean that hackers who manage to jump on to the same network can potentially steal Google login credentials from their neighbours.
- "The internet-connected fridge is designed to display Gmail Calendar information on its display," explained Ken Munro, a security researcher at Pen Test Partners. "It appears to work the same way that any device running a Gmail calendar does. A logged-in user/owner of the calendar makes updates and those changes are then seen on any device that a user can view the calendar on."
- "While SSL is in place, the fridge fails to validate the certificate. Hence, hackers who manage to access the network that the fridge is on (perhaps through a de-authentication and fake Wi-Fi access point attack) can Man-In-The-Middle the fridge calendar client and steal Google login credentials from their neighbours, for example."
- http://www.theregister.co.uk/2015/08/24/smart_fridge_security_fubar/

#NYSCybersec @RajGoel_NY Smart Fridge has STUPID Security



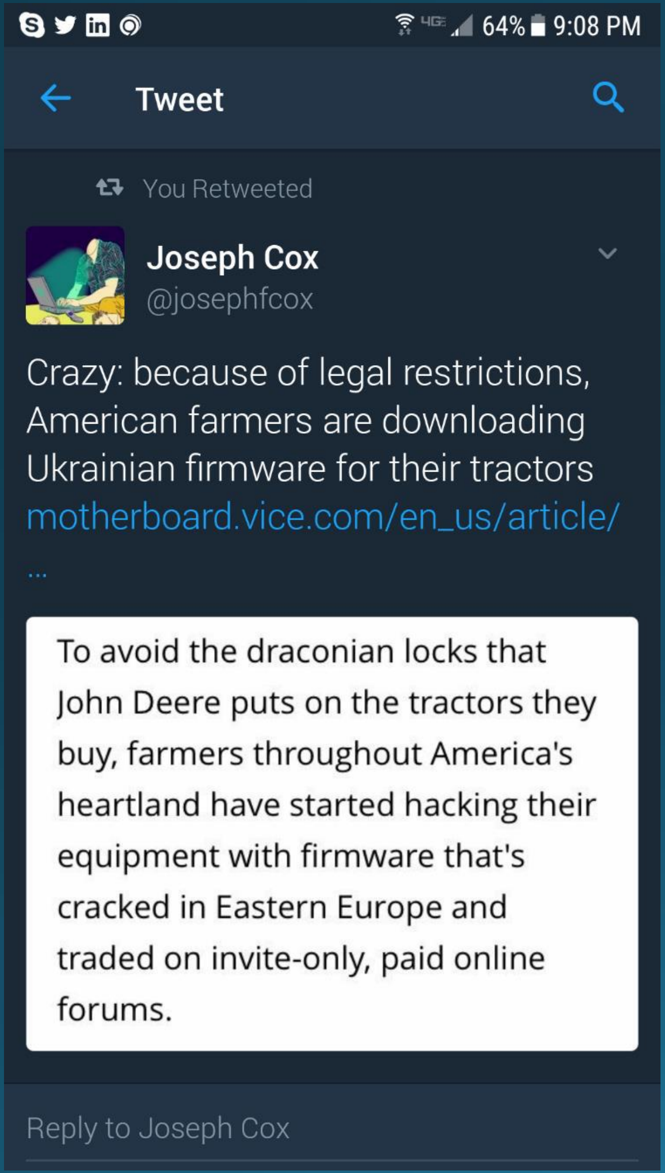
New York Magazine
@NYMag

If a device can connect to the internet, it will be compromised

Assume TV Bugged
If a device can connect to the internet, it wi...
nymag.com

7:50 PM · 08 Mar 17

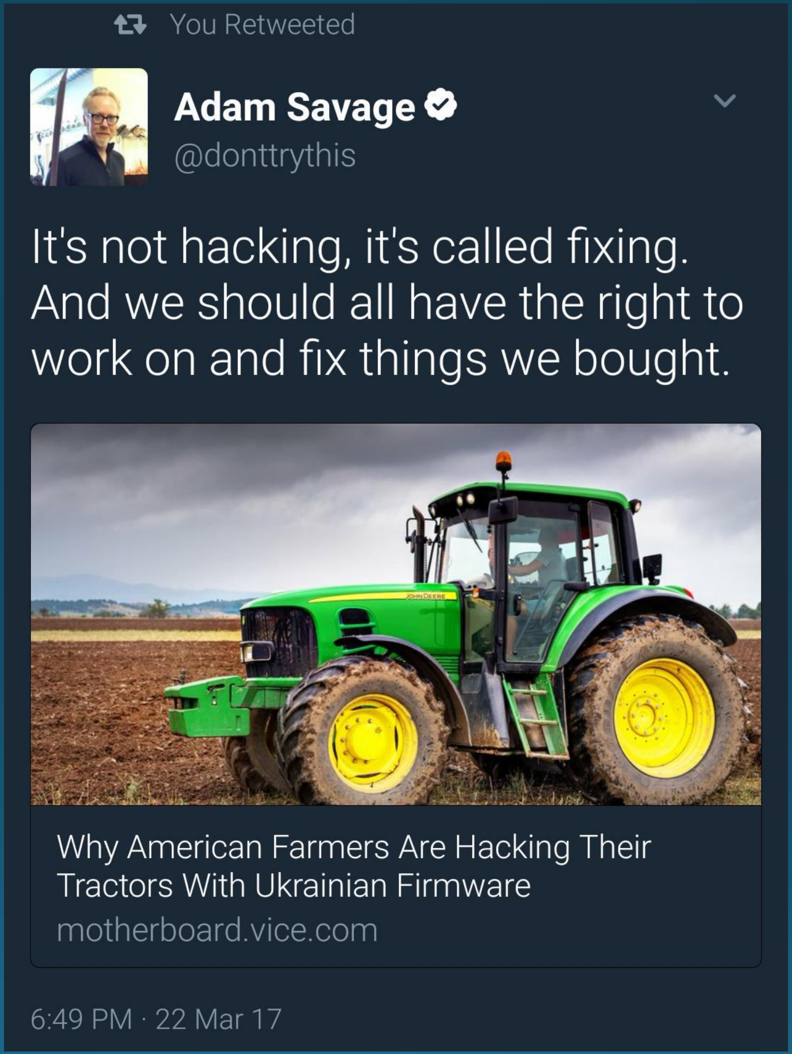
Vehicles – No Keys For YOU!



Joseph Cox
@josephfcox

Crazy: because of legal restrictions, American farmers are downloading Ukrainian firmware for their tractors motherboard.vice.com/en_us/article/ ...

To avoid the draconian locks that John Deere puts on the tractors they buy, farmers throughout America's heartland have started hacking their equipment with firmware that's cracked in Eastern Europe and traded on invite-only, paid online forums.

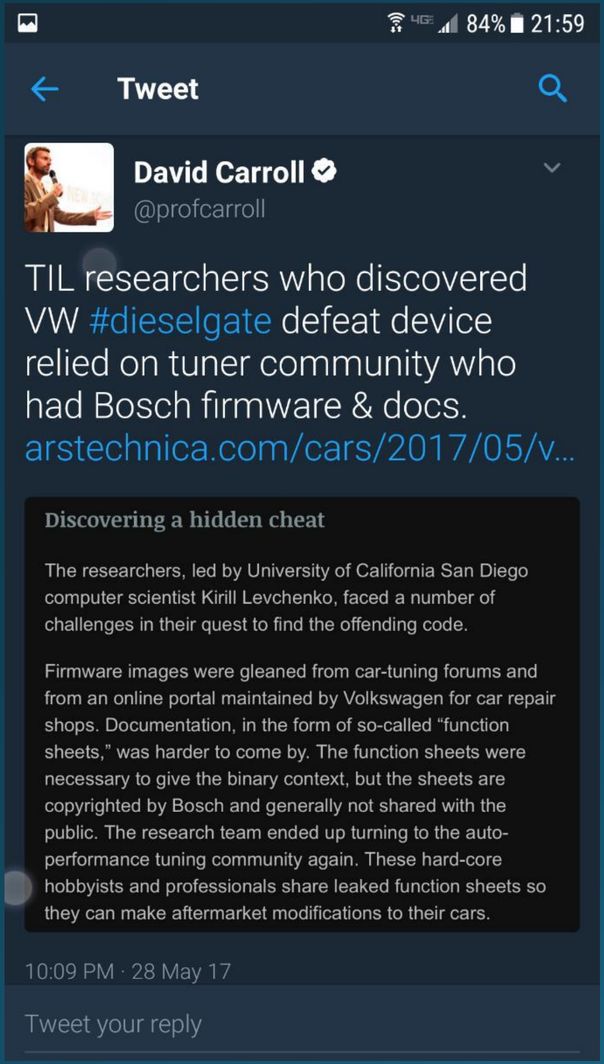


Adam Savage
@donttrythis

It's not hacking, it's called fixing. And we should all have the right to work on and fix things we bought.

Why American Farmers Are Hacking Their Tractors With Ukrainian Firmware
motherboard.vice.com

6:49 PM · 22 Mar 17



David Carroll @profcarroll

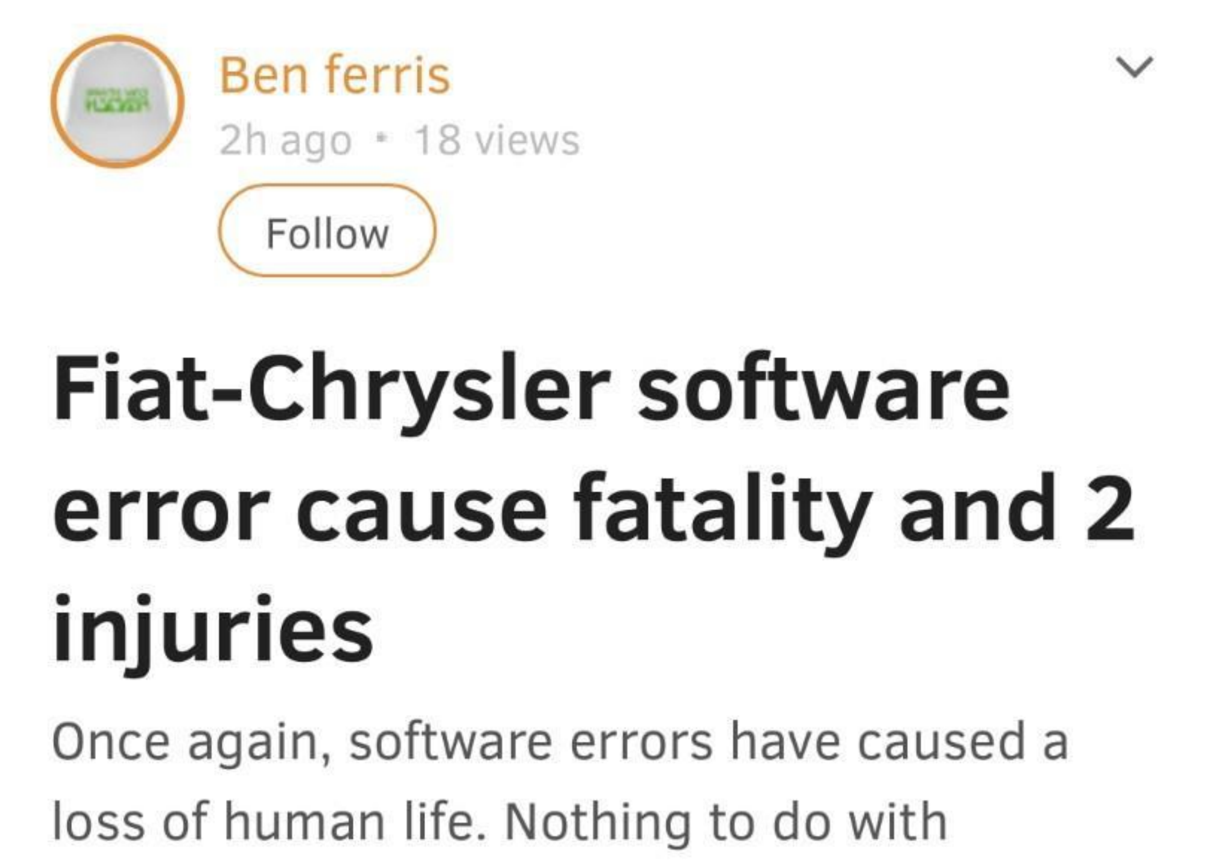
TIL researchers who discovered VW #dieselgate defeat device relied on tuner community who had Bosch firmware & docs. arstechnica.com/cars/2017/05/v...

Discovering a hidden cheat

The researchers, led by University of California San Diego computer scientist Kirill Levchenko, faced a number of challenges in their quest to find the offending code.

Firmware images were gleaned from car-tuning forums and from an online portal maintained by Volkswagen for car repair shops. Documentation, in the form of so-called "function sheets," was harder to come by. The function sheets were necessary to give the binary context, but the sheets are copyrighted by Bosch and generally not shared with the public. The research team ended up turning to the auto-performance tuning community again. These hard-core hobbyists and professionals share leaked function sheets so they can make aftermarket modifications to their cars.

10:09 PM · 28 May 17



Fiat-Chrysler software error cause fatality and 2 injuries

Once again, software errors have caused a loss of human life. Nothing to do with

75% of cars stolen in France…hacked

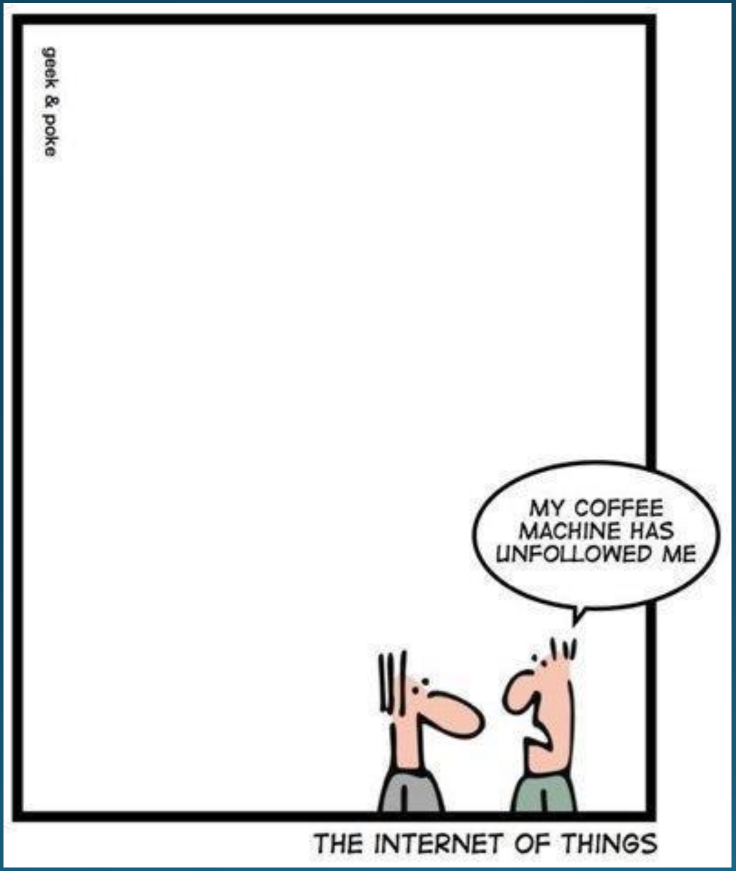
- Three quarters of cars stolen in France are targeted using electronic hacking, it was claimed on Thursday, prompting calls for urgent security improvements in a range of vehicles sold across Europe.

- The Smart Fortwo model was France's most-stolen car, with the Ford Fiesta and Peugeot 406 models also popular among thieves

- The astonishing figures come two months after computer scientists in the UK warned that thousands of cars – including high-end brands such as Porsches and Maseratis - are at risk of electronic hacking. **Their research was suppressed for two years by a court injunction for fear it would help thieves steal vehicles to order.**

http://www.telegraph.co.uk/news/worldnews/europe/france/11964140/Three-quarters-of-cars-stolen-in-France-electronically-hacked.html

Future Therapy #2



Recommendations – Avoid Biometrics

Really good examples of flaws in biometric authentication are demonstrated in the movies:

- DEMOLITION MAN – where they bypass IRIS scans
- SNEAKERS – where they bypass VOICE print

- We shed DNA everywhere; we leave hair, saliva, fingerprints everywhere.

- We cannot change our iris patterns, how we walk (unless we have an injury), etc.

- BIOMETRICS firms would be better off using the biometric markers are REINFORCEMENT factors, not exclusive factors for identification.

Recommendations

- REVOKE EULAs
- pass SOFTWARE SAFETY laws
- hold vendors accountable for shoddy software and pass minimum or mandatory safety standards.
- What we CAN do is make it harder for criminals to steal by building better defenses; making companies and management more liable for breaches; and demanding safer software.

Software, Food, Medicine, Cars

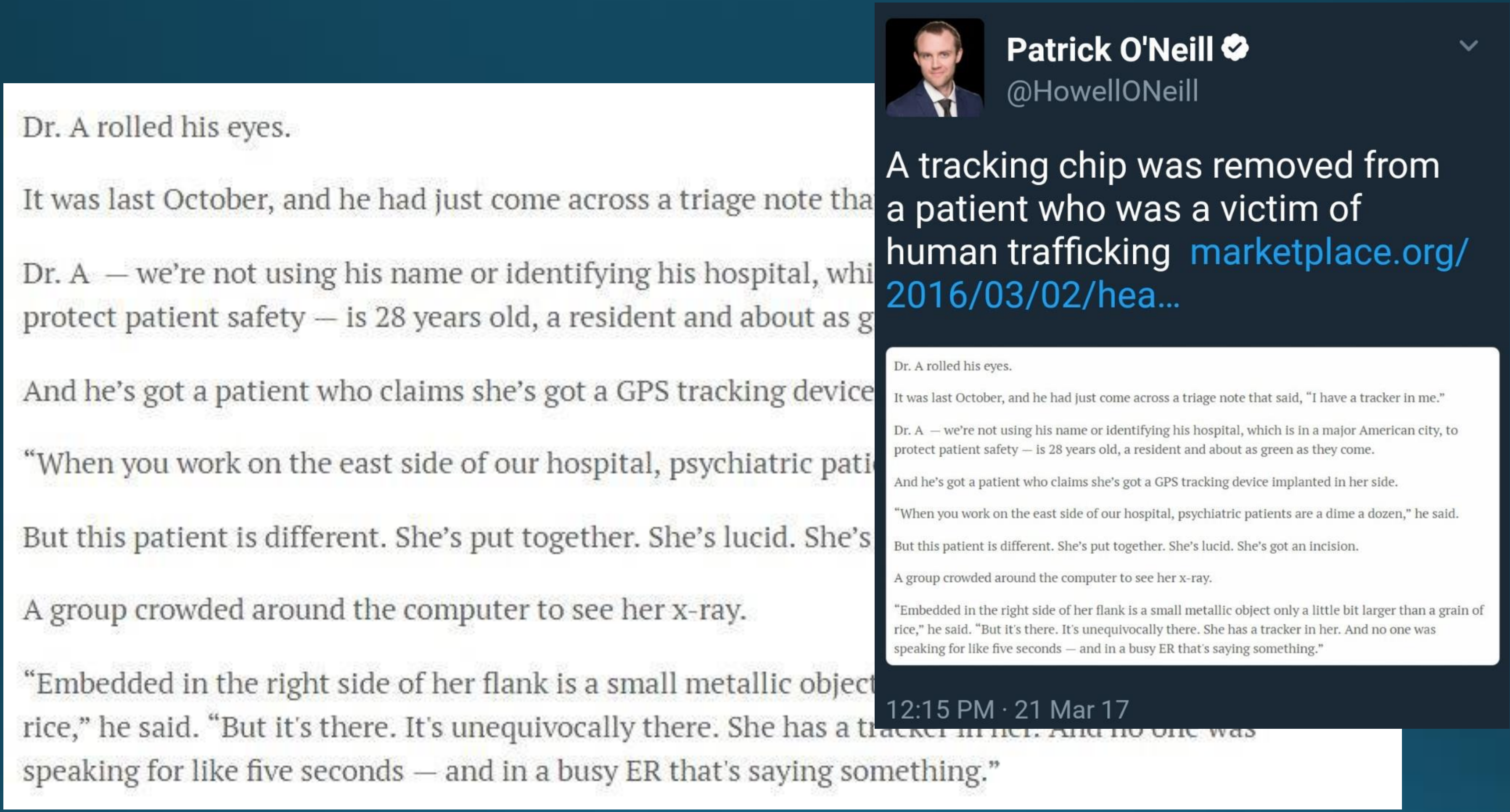
- I see strong parallels between software & food; and software & cars.
- Between 1870 & 1906, the quality of food and medicine sold in the US was frankly, terrible. There were no safety or sanitary practices.
- After the muckrakers agitated, and Upton Sinclair published INTO THE JUNGLE, American society was appalled by the unsanitary food and medicine production practices.

Lessons from FDA

- Congress passed the PURE FOOD AND DRUG ACT (1906)– which led to the creation of the FDA, regulation of FOOD , Medicine, etc.
- A lot of companies died because they could not meet new requirements for cleanliness, safety testing, inspections, etc.
- The net result, however, is that food and medicine in the US became the safest in the world, and influenced food & medical practices worldwide.
- I truly believe that the PURE FOOD & DRUG ACT saved more lives in human history than any other act of Congress.

Lessons from IIHS

- Another parallel to software is the automobile.
- When the automobile was invented, there were no regulations. And for the first few decades, it was seen as a fad; an expensive toy and very much resembled the dotcom economy.
- As cars became central to our lives, the National Highway Safety Commission, driver licensing requirements, mandatory driver's insurance requirements, seat belts, anti-lock brakes, and other safety features were mandated.
- The automakers hated this, and argued that building safer, more efficient cars would destroy the automobile industry.
- What we saw instead, is that some manufacturers died; the industry consolidated into a handful of big brands, and cars produced in 2016 are much safer, more efficient and frankly better than anything produced in 1950, 1970 or even 1990.



Patrick O'Neill

@HowellONeill

A tracking chip was removed from a patient who was a victim of human trafficking marketplace.org/2016/03/02/hea...

Dr. A rolled his eyes.

It was last October, and he had just come across a triage note that said, “I have a tracker in me.”

Dr. A — we're not using his name or identifying his hospital, which is in a major American city, to protect patient safety — is 28 years old, a resident and about as green as they come.

And he's got a patient who claims she's got a GPS tracking device implanted in her side.

“When you work on the east side of our hospital, psychiatric patients are a dime a dozen,” he said.

But this patient is different. She's put together. She's lucid. She's got an incision.

A group crowded around the computer to see her x-ray.

“Embedded in the right side of her flank is a small metallic object only a little bit larger than a grain of rice,” he said. “But it's there. It's unequivocally there. She has a tracker in her. And no one was speaking for like five seconds — and in a busy ER that's saying something.”

12:15 PM · 21 Mar 17

Dr. A rolled his eyes.

It was last October, and he had just come across a triage note tha

Dr. A — we're not using his name or identifying his hospital, whi
protect patient safety — is 28 years old, a resident and about as g

And he's got a patient who claims she's got a GPS tracking device

“When you work on the east side of our hospital, psychiatric pati

But this patient is different. She's put together. She's lucid. She's

A group crowded around the computer to see her x-ray.

“Embedded in the right side of her flank is a small metallic object
rice,” he said. “But it's there. It's unequivocally there. She has a tracker in her. And no one was
speaking for like five seconds — and in a busy ER that's saying something.”

Smartest Man in IoT

Are You
CHENEY
Smart???

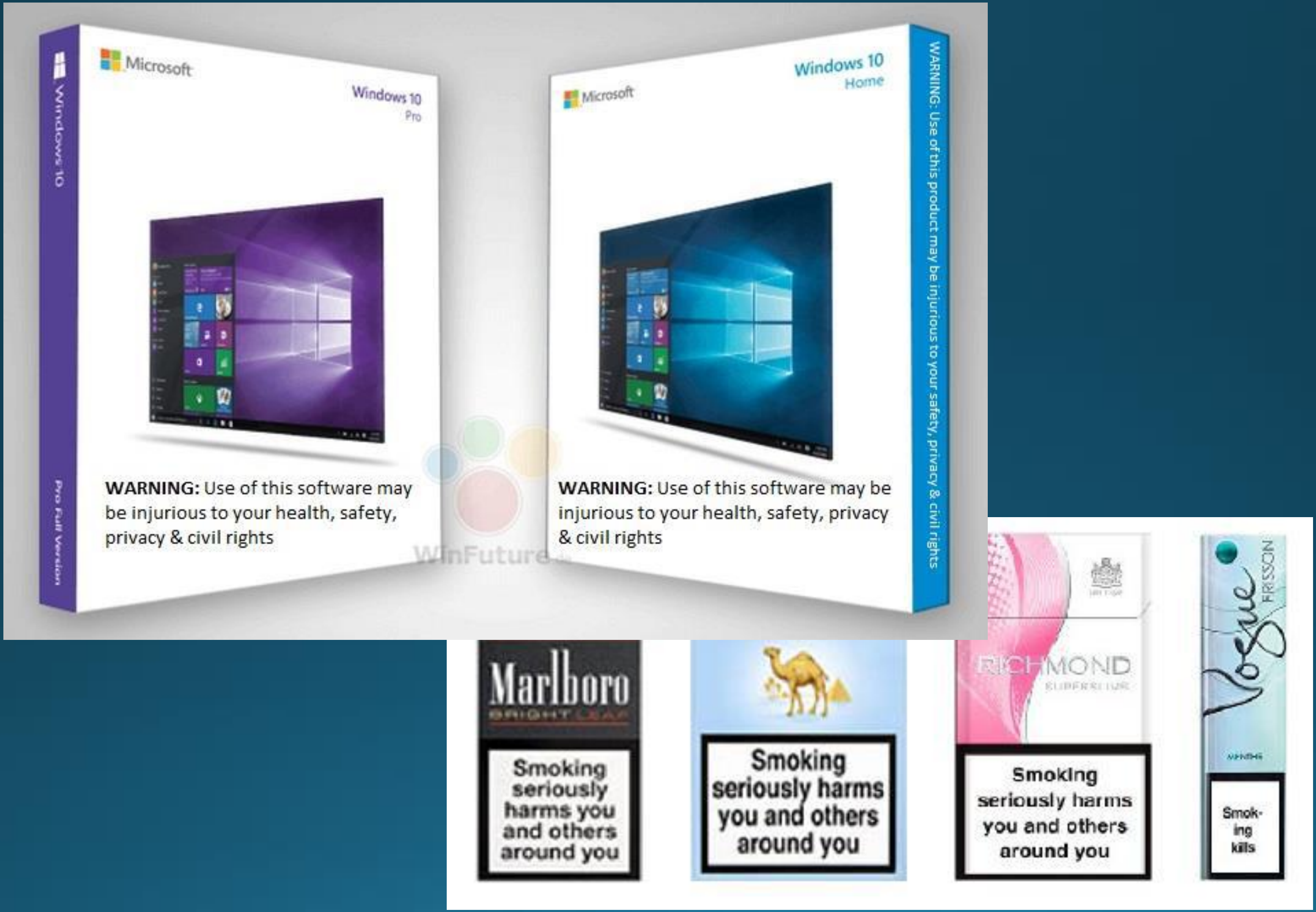
- 2007 - Doctors disabled wireless in Dick Cheney's pacemaker to thwart hacking

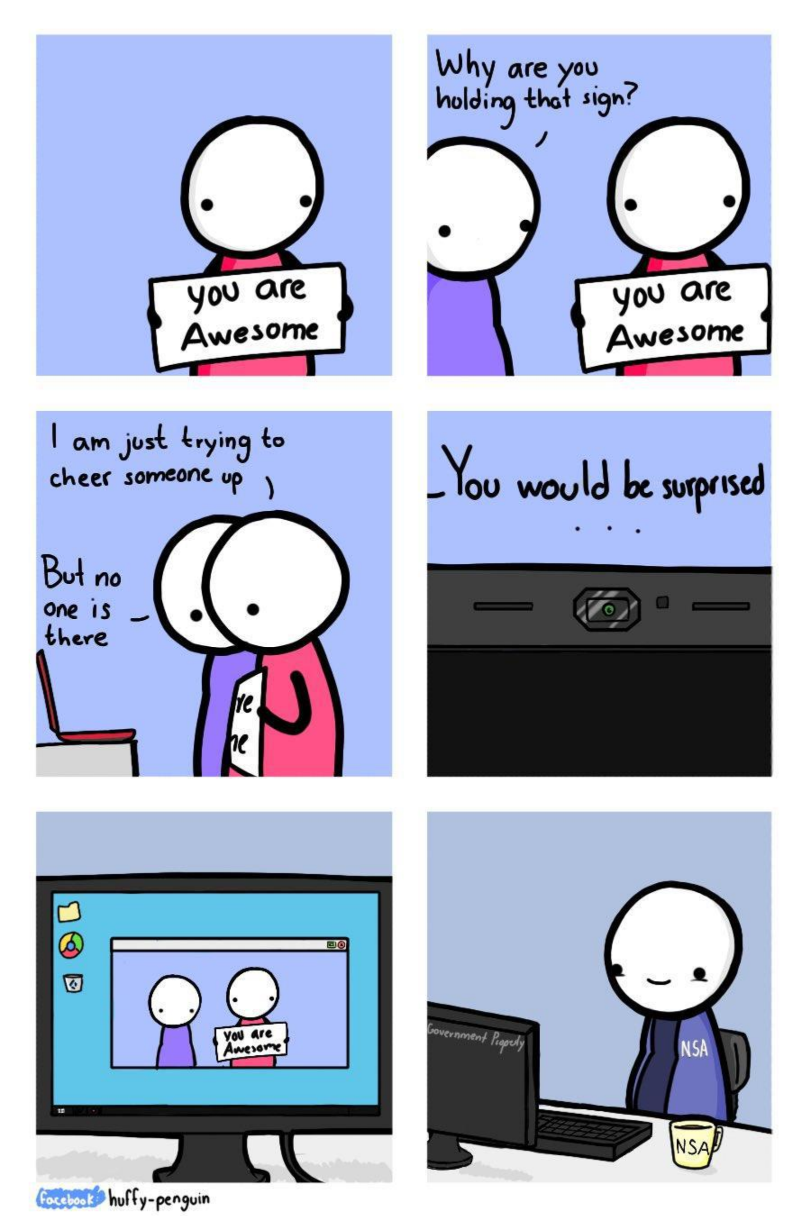
https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/

What We HAVE

VIRGINIA SL
FILTER
L&M
20 CLASS A CIGARETTES
FILTER CIGARETTES
Marlboro
20 CLASS A CIGARETTES
Parliament
Basic
Microsoft
Windows 10
Windows 10 Pro
Pro Full Version
WinFuture
Microsoft
Windows 10 Home

What We WANT


Microsoft
Windows 10
Pro
Windows 10
Pro Full Version
WARNING: Use of this software may be injurious to your health, safety, privacy & civil rights
Microsoft
Windows 10
Home
WARNING: Use of this software may be injurious to your health, safety, privacy & civil rights
WARNING: Use of this product may be injurious to your safety, privacy & civil rights
WinFuture
Marlboro
BRIGHT LEAF
Smoking seriously harms you and others around you
Smoking seriously harms you and others around you
RICHMOND
SUPERKING
Smoking seriously harms you and others around you
Vogue
FRISSON
Smoking kills


you are Awesome
Why are you holding that sign?
you are Awesome
I am just trying to cheer someone up
But no one is there
You would be surprised . . .
You are Awesome
Government Property
NSA
NSA
facebook huffy-penguin

My next presentation

5215 – AMERICA GOT PENTESTED – The Blueteam Report (Did Facebook, Twitter and Google Undermine Democracy?)

- ISC2 SecureCongress
- Sept 25-27, 2017
- Austin, Tx
- Tue Sep 28, 1:45 – 2:45 PM

Contact Information

Raj Goel, CISSP

Chief Technology Officer

Brainlink International, Inc.

C: 917-685-7731

raj@brainlink.com

www.RajGoel.com

www.linkedin.com/in/rajgoel

@rajgoel_ny

Author of

UNPLUGGED Luddites Guide To Cybersecurity

http://www.amazon.com/UNPLUGGED-Luddites-Guide-CyberSecurity-Grandparents/dp/0984424830/

The Most Important Secrets To Getting Great Results From IT

http://www.amazon.com/gp/product/0984424814