Conferência Web.br 2017
São Paulo, SP
25 de outubro de 2017

Segurança em IoT: o Pecado Está no Básico

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

cert.br nic.br cgi.br

IoT

Computação Ubíqua

- **Mark Weiser, em 1988**
- **Oposto da "realidade virtual"**
  - pessoas colocadas em realidade gerada por computadores
- **Computador se integra à vida das pessoas**
  - utilizado sem ser notado, tecnologia "calma"
  - pano de fundo de nossas vidas
- **Ainda sem recursos na época para ser usada**

"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it."

The Computer for the 21st Century

http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html

Surgimento do termo IoT

- ***Internet of Things*** **(IoT),** ***Internet of Everything*** **(IoE)**
- **Kevin Ashton, em 1999**
  - apresentação para executivos sobre como facilitar a logística da cadeia de produção usando RFID
- **Ainda com poucos recursos para ser usada**

"We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory."

That 'Internet of Things' Thing

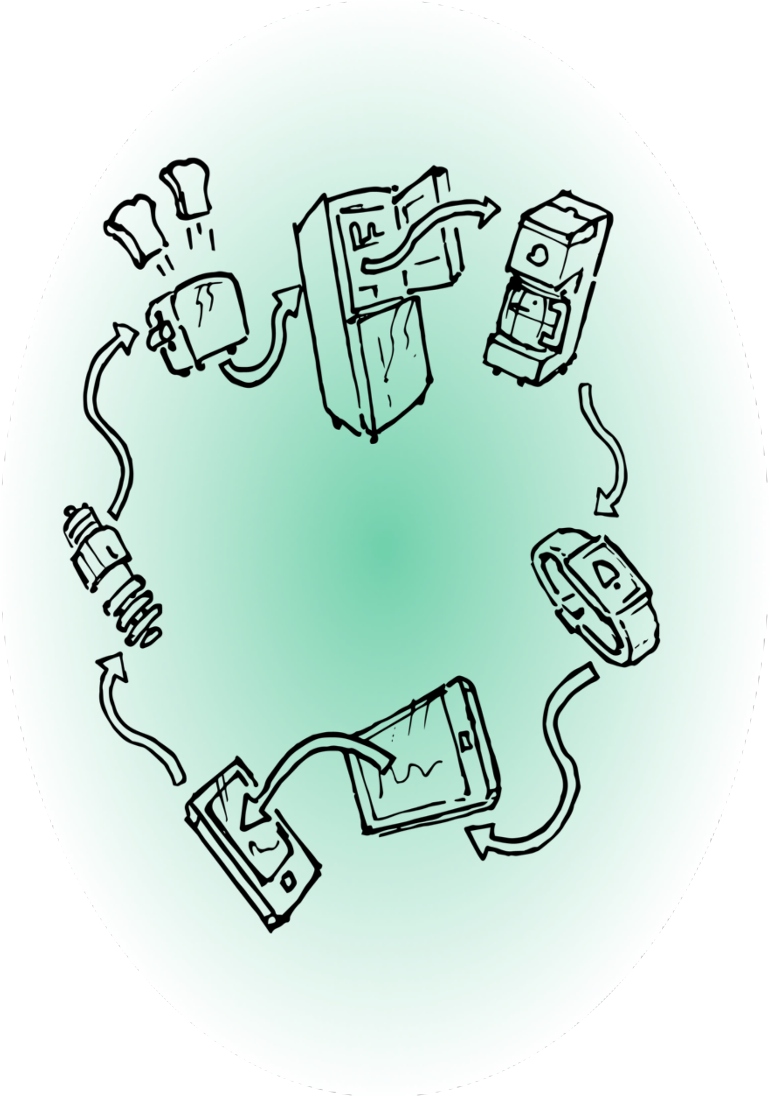
In the real world, things matter more than ideas

http://www.rfidjournal.com/articles/view?4986

Definição IoT

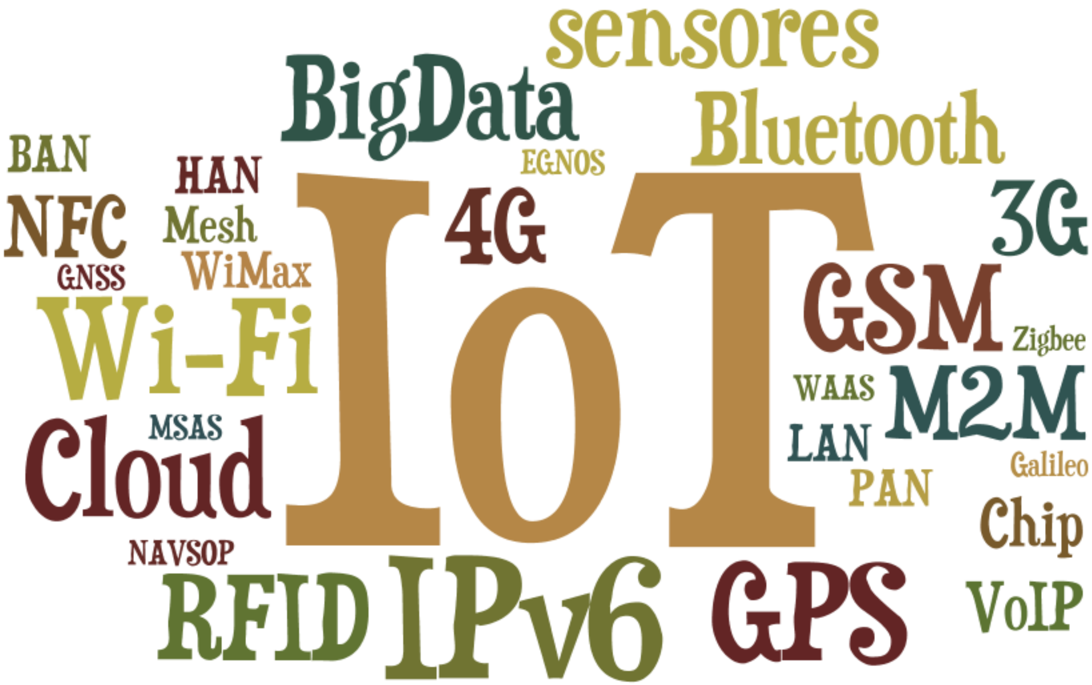
“... é uma rede de objetos físicos, veículos, prédios e outros que possuem tecnologia embarcada, sensores e conexão com rede capaz de coletar e transmitir dados.”

Wikipedia



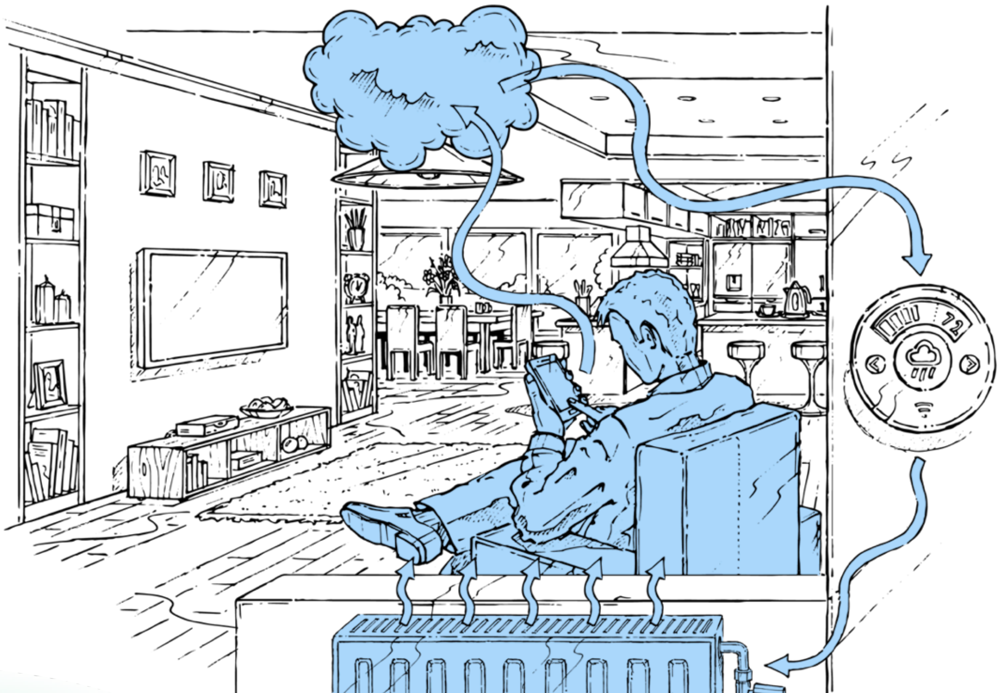
Atualmente

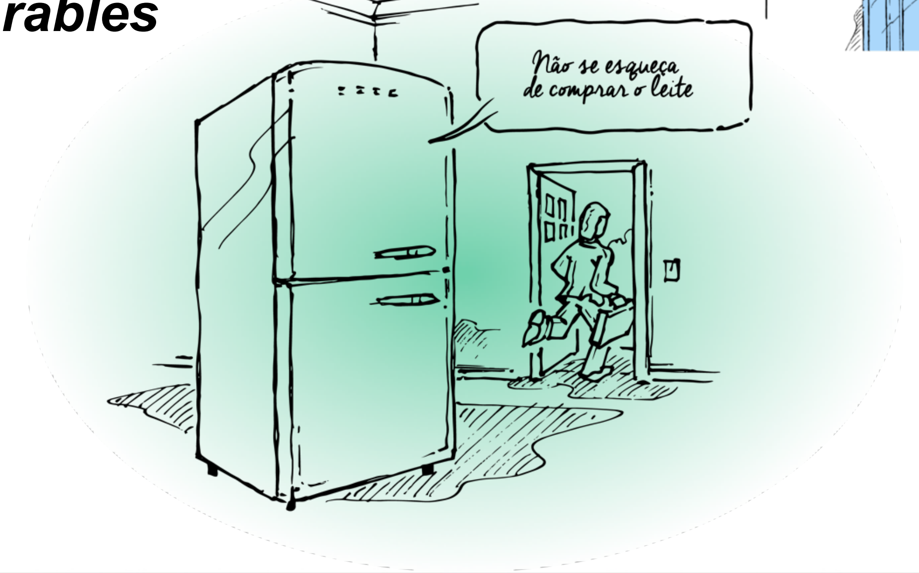
- **As coisas já estão conectadas**
  - sistemas complexos e completos
    - sistema operacional, aplicações Web, permitem acesso remoto, etc
    - múltiplas tecnologias



Usos

- **Casas inteligentes**
- **Cidades inteligentes**
- **Carros conectados**
- **Equipamentos médicos**
- **Agropecuária**
- **Indústria 4.0**
- ***Wearables***





Desafios em Segurança e Privacidade

Principais vulnerabilidades

- **Projetos sem levar em conta segurança**
- **Políticas de atualização inexistentes**
  - *"deploy and forget"*
- **Defeitos de *software* / *firmware***
- **Falhas de configuração**
  - serviços desnecessários ativos por padrão
- **Falta proteção de dados**
  - coleta excessiva
  - criptografia inexistente ou fraca
  - protocolos obsoletos
- **Autenticação falha ou inexistente:**
  - sem senhas, com senhas fracas ou padrão, contas ocultas (*backdoors*)

Mesmos velhos problemas: falhando no "básico"

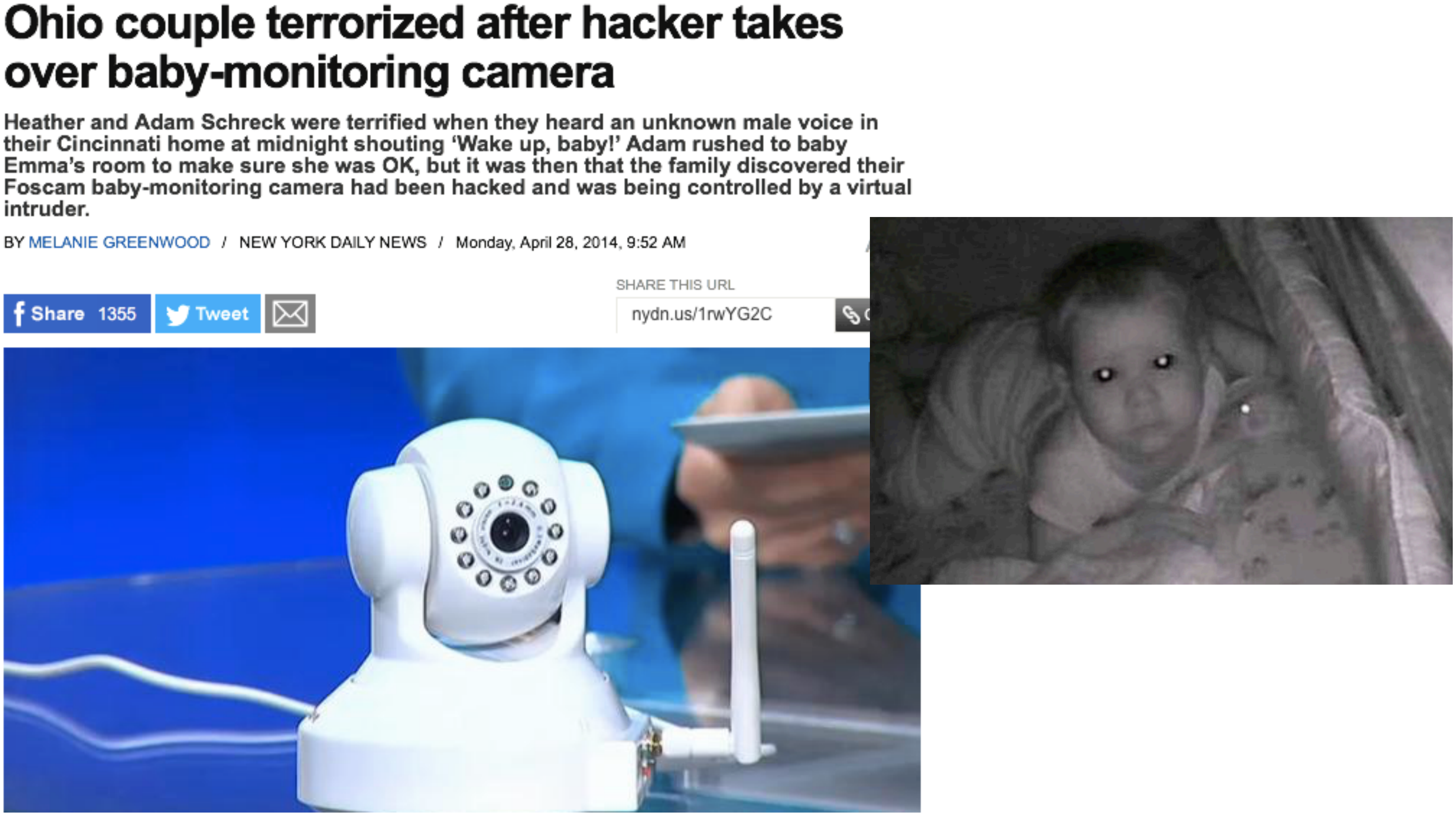
Segurança e Privacidade

- **Riscos:**
  - violação de privacidade
  - furto de dados
  - perdas financeiras
  - danos à imagem
  - perda de confiança na tecnologia
  - indisponibilidade de serviços críticos
  - participação em golpes
  - propagação de códigos maliciosos
  - envio de *spam*
  - morte

Mas por que alguém vai fazer isso?

- **Várias são as motivações:**
  - ganho financeiro / vantagem competitiva
    - golpes
    - espionagem
    - concorrência desleal
  - “*cyberwar*”
    - governos
    - terrorismo
  - vandalismo
  - vingança
  - diversão
  - competição / vaidade

Será que acontece mesmo ou é só paranoia?



Ohio couple terrorized after hacker takes over baby-monitoring camera

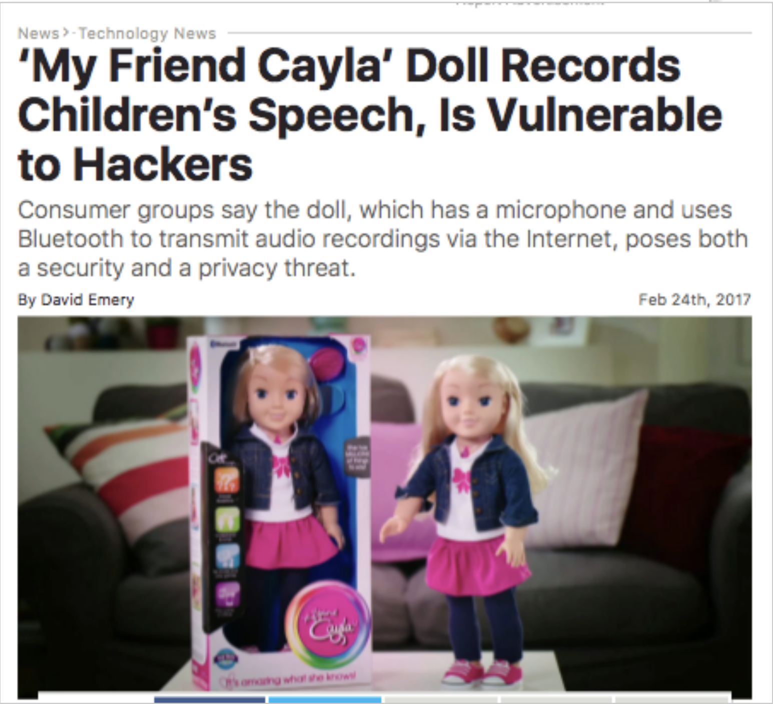
Heather and Adam Schreck were terrified when they heard an unknown male voice in their Cincinnati home at midnight shouting 'Wake up, baby!' Adam rushed to baby Emma's room to make sure she was OK, but it was then that the family discovered their Foscam baby-monitoring camera had been hacked and was being controlled by a virtual intruder.

BY MELANIE GREENWOOD / NEW YORK DAILY NEWS / Monday, April 28, 2014, 9:52 AM

Wake Up, baby

http://www.nydailynews.com/news/national/baby-monitoring-camera-hacked-taunts-family-article-1.1771399

Privacidade

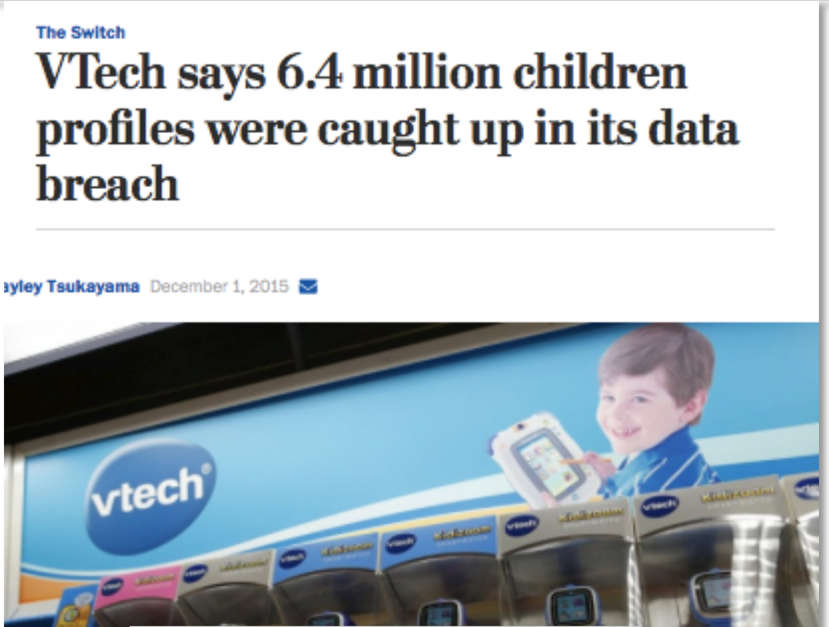


News › Technology News

'My Friend Cayla' Doll Records Children's Speech, Is Vulnerable to Hackers

Consumer groups say the doll, which has a microphone and uses Bluetooth to transmit audio recordings via the Internet, poses both a security and a privacy threat.

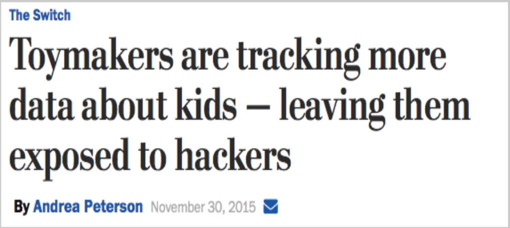
By David Emery Feb 24th, 2017



The Switch

VTech says 6.4 million children profiles were caught up in its data breach

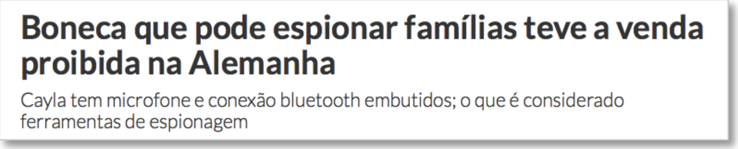
ayley Tsukayama December 1, 2015



The Switch

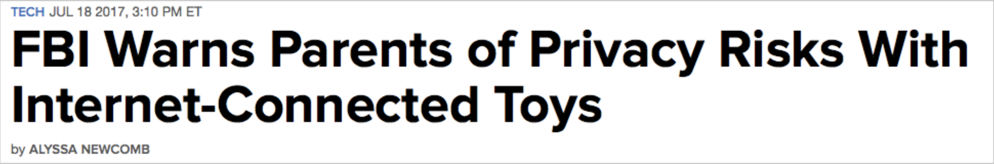
Toymakers are tracking more data about kids – leaving them exposed to hackers

By Andrea Peterson November 30, 2015



Boneca que pode espionar famílias teve a venda proibida na Alemanha

Cayla tem microfone e conexão bluetooth embutidos; o que é considerado ferramentas de espionagem



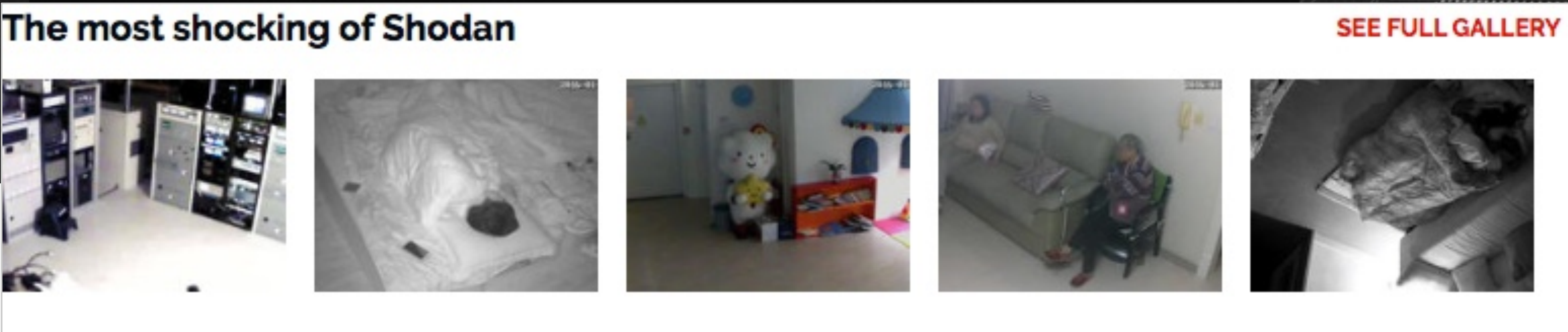
TECH JUL 18 2017, 3:10 PM ET

FBI Warns Parents of Privacy Risks With Internet-Connected Toys

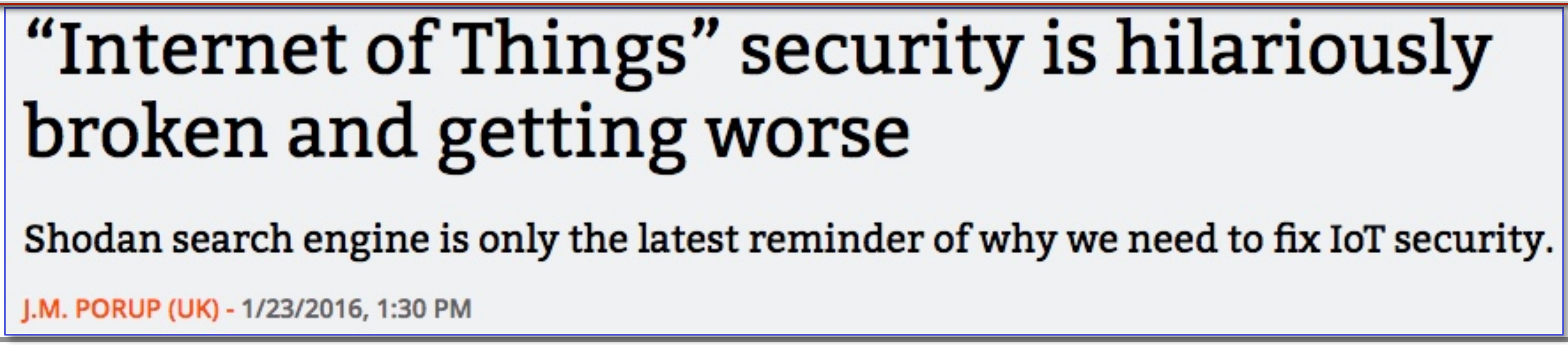
by ALYSSA NEWCOMB

https://www.washingtonpost.com/news/the-switch/wp/2015/12/01/vtech-says-6-4-million-children-were-caught-up-in-its-data-breach/
https://www.washingtonpost.com/news/the-switch/wp/2015/11/30/toymakers-are-tracking-more-data-about-kids-leaving-them-exposed-to-hackers/
http://www.snopes.com/2017/02/24/my-friend-cayla-doll-privacy-concerns/
http://www.em.com.br/app/noticia/internacional/2017/02/17/interna_internacional,848314/boneca-que-pode-espionar-familias-teve-a-venda-proibida-na-alemanha.shtml
https://www.nbcnews.com/tech/security/fbi-warns-parents-privacy-risks-internet-connected-toys-n784126

The search engine for the Internet of Things



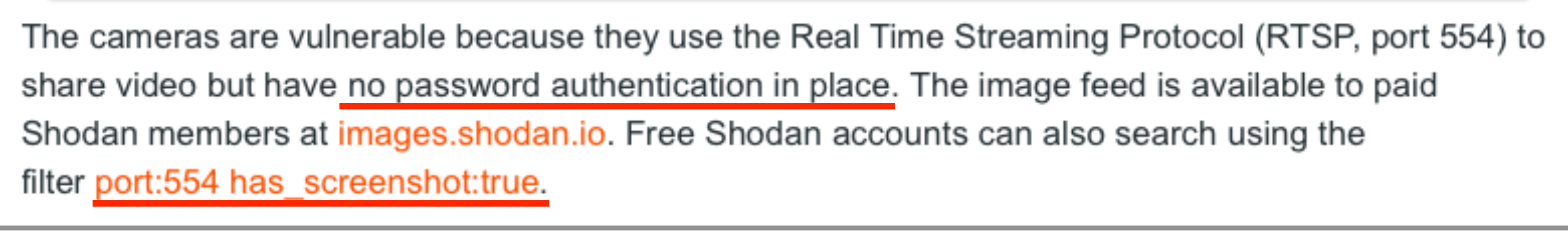
The most shocking of Shodan



“Internet of Things” security is hilariously broken and getting worse

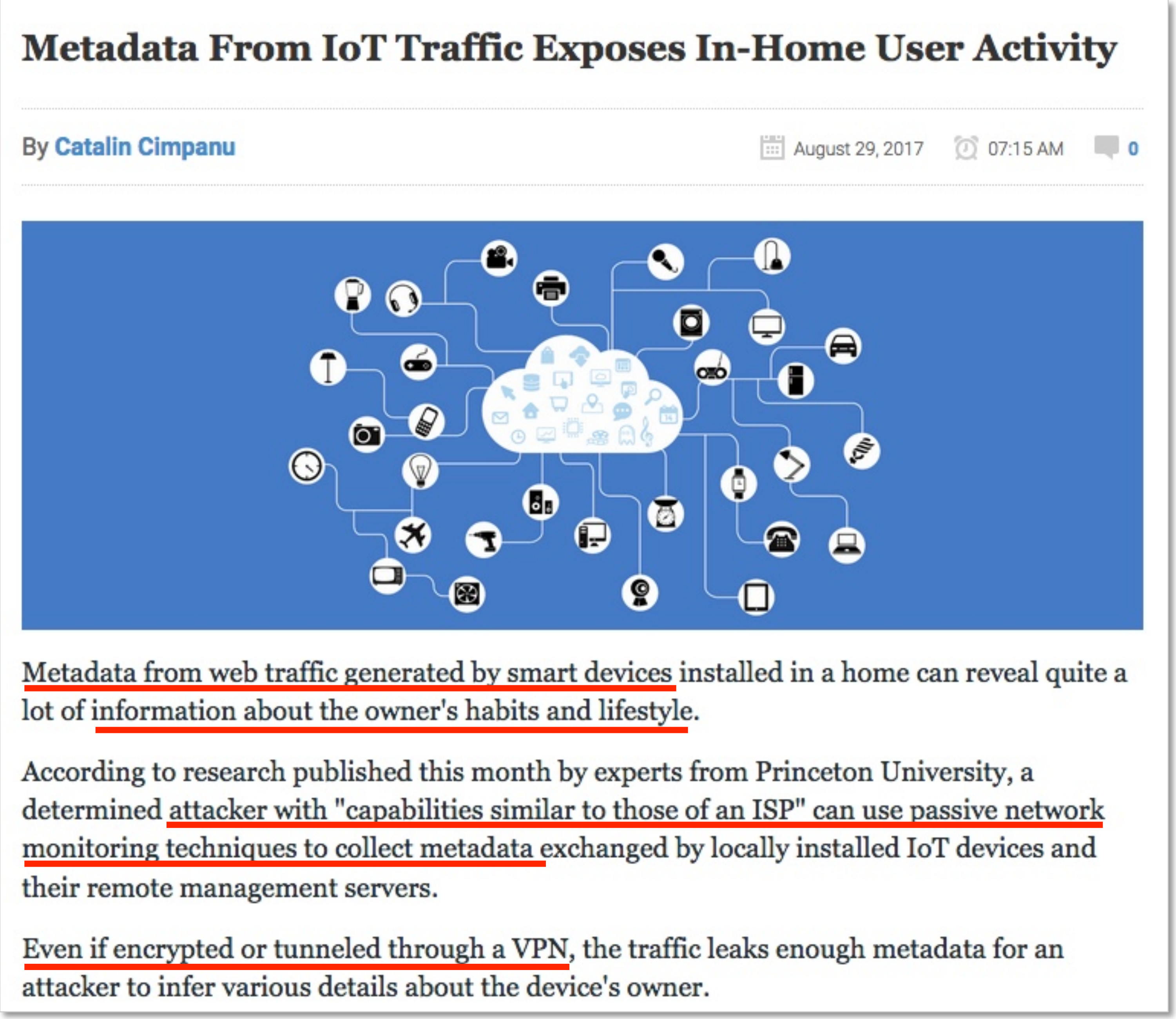
Shodan search engine is only the latest reminder of why we need to fix IoT security.

J.M. PORUP (UK) - 1/23/2016, 1:30 PM



The cameras are vulnerable because they use the Real Time Streaming Protocol (RTSP, port 554) to share video but have no password authentication in place. The image feed is available to paid Shodan members at images.shodan.io. Free Shodan accounts can also search using the filter port:554 has_screenshot:true.

http://www.zdnet.com/article/shodan-the-iot-search-engine-which-shows-us-sleeping-kids-and-how-we-throw-away-our-privacy/
http://arstechnica.com/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/



Metadata From IoT Traffic Exposes In-Home User Activity

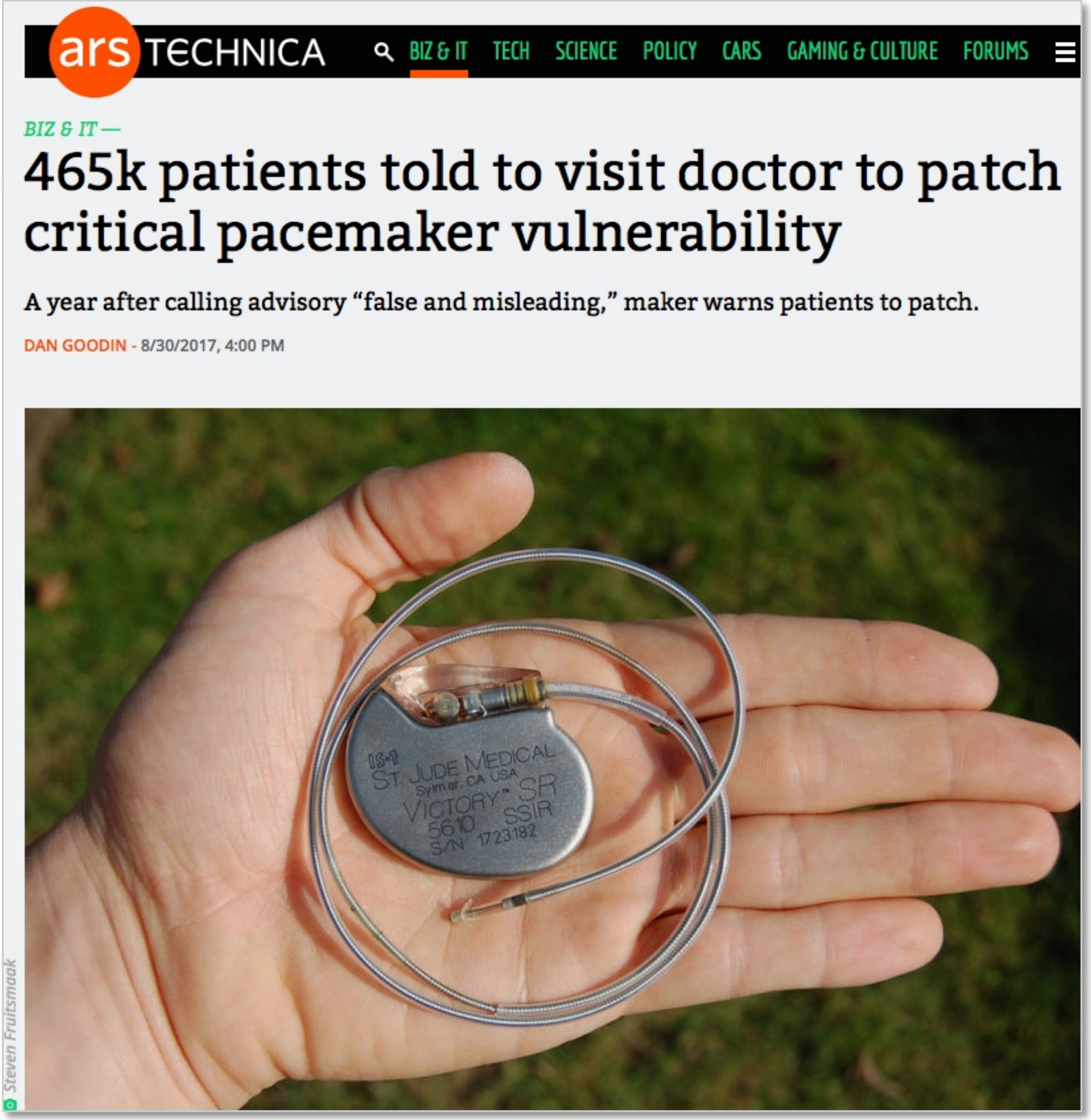
By Catalin Cimpanu August 29, 2017 07:15 AM 0

Metadata from web traffic generated by smart devices installed in a home can reveal quite a lot of information about the owner's habits and lifestyle.

According to research published this month by experts from Princeton University, a determined attacker with "capabilities similar to those of an ISP" can use passive network monitoring techniques to collect metadata exchanged by locally installed IoT devices and their remote management servers.

Even if encrypted or tunneled through a VPN, the traffic leaks enough metadata for an attacker to infer various details about the device's owner.

https://www.bleepingcomputer.com/news/technology/metadata-from-iot-traffic-exposes-in-home-user-activity/



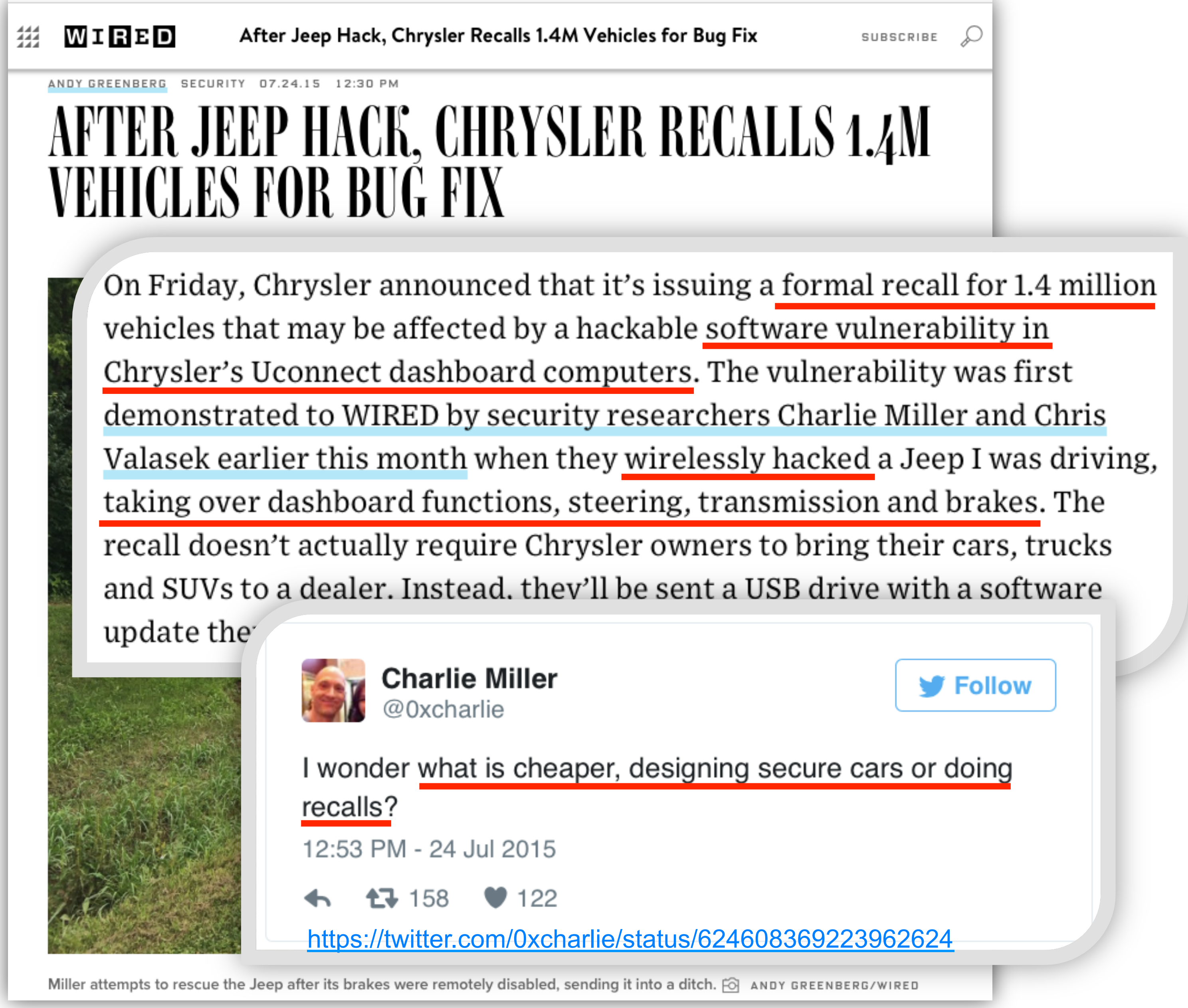
BIZ & IT —

465k patients told to visit doctor to patch critical pacemaker vulnerability

A year after calling advisory "false and misleading," maker warns patients to patch.

DAN GOODIN - 8/30/2017, 4:00 PM

https://arstechnica.com/information-technology/2017/08/465k-patients-need-a-firmware-update-to-prevent-serious-pacemaker-hacks/
https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm
https://ics-cert.us-cert.gov/advisories/ICSMA-17-241-01



WIRED — After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix — SUBSCRIBE

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 the

Charlie Miller
@0xcharlie

Follow

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

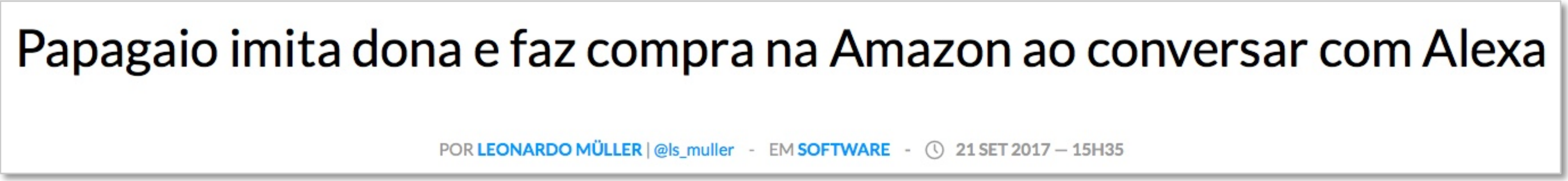
12:53 PM - 24 Jul 2015

158 122

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

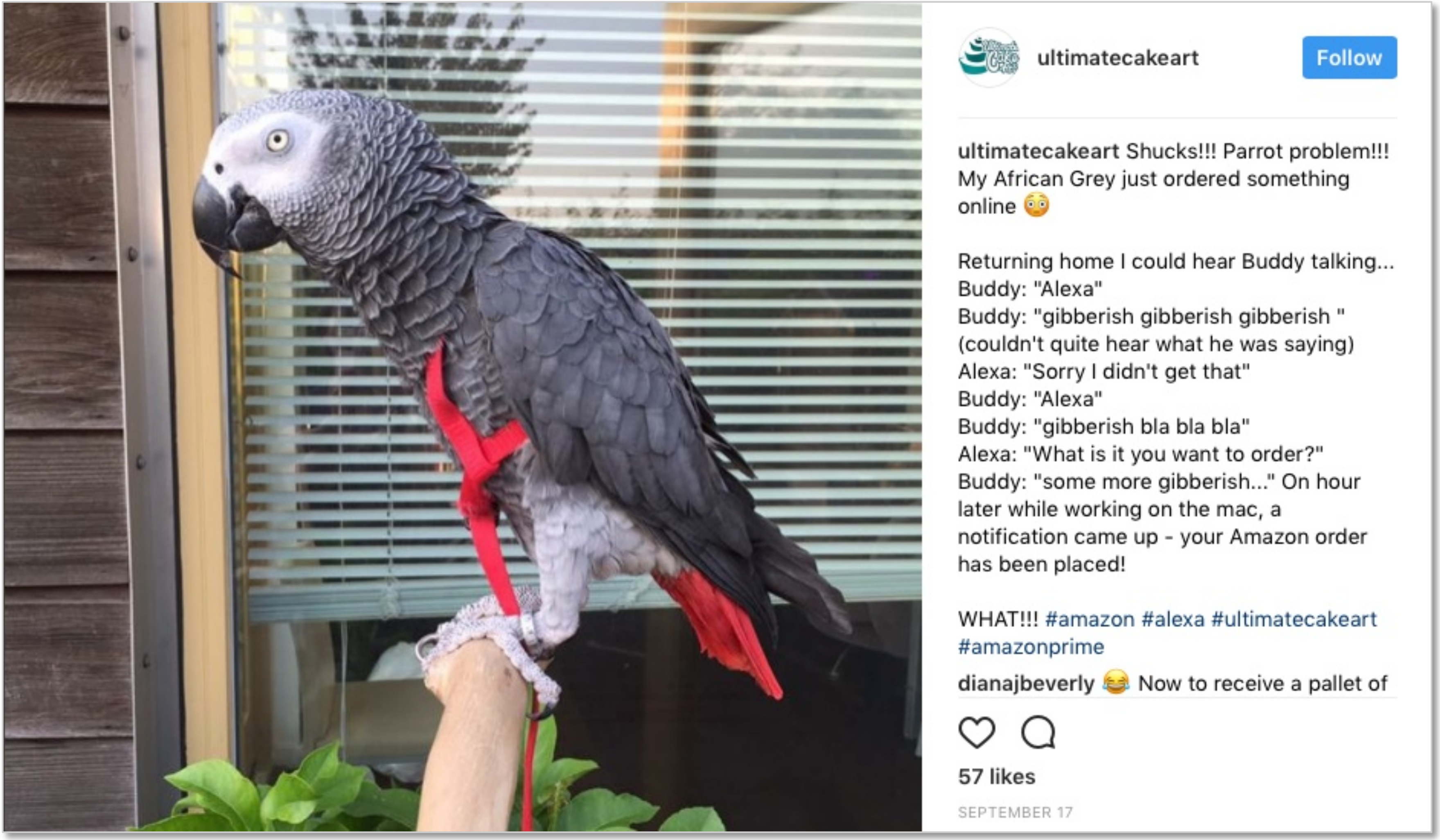
Miller attempts to rescue the Jeep after its brakes were remotely disabled, sending it into a ditch. ANDY GREENBERG/WIRED

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



Papagaio imita dona e faz compra na Amazon ao conversar com Alexa

POR LEONARDO MÜLLER | @ls_muller - EM SOFTWARE - 21 SET 2017 — 15H35



ultimatecakeart Shucks!!! Parrot problem!!! My African Grey just ordered something online 😳

Returning home I could hear Buddy talking...
Buddy: "Alexa"
Buddy: "gibberish gibberish gibberish "
(couldn't quite hear what he was saying)
Alexa: "Sorry I didn't get that"
Buddy: "Alexa"
Buddy: "gibberish bla bla bla"
Alexa: "What is it you want to order?"
Buddy: "some more gibberish..." On hour later while working on the mac, a notification came up - your Amazon order has been placed!

WHAT!!! #amazon #alexa #ultimatecakeart #amazonprime

dianajbeverly 😂 Now to receive a pallet of

57 likes

SEPTEMBER 17

https://www.tecmundo.com.br/software/122278-papagaio-imita-dona-compra-amazon-conversar-alexa.htm
https://www.instagram.com/p/BZJTDnPAcxU/?taken-by=ultimatecakeart

IoT *botnets*

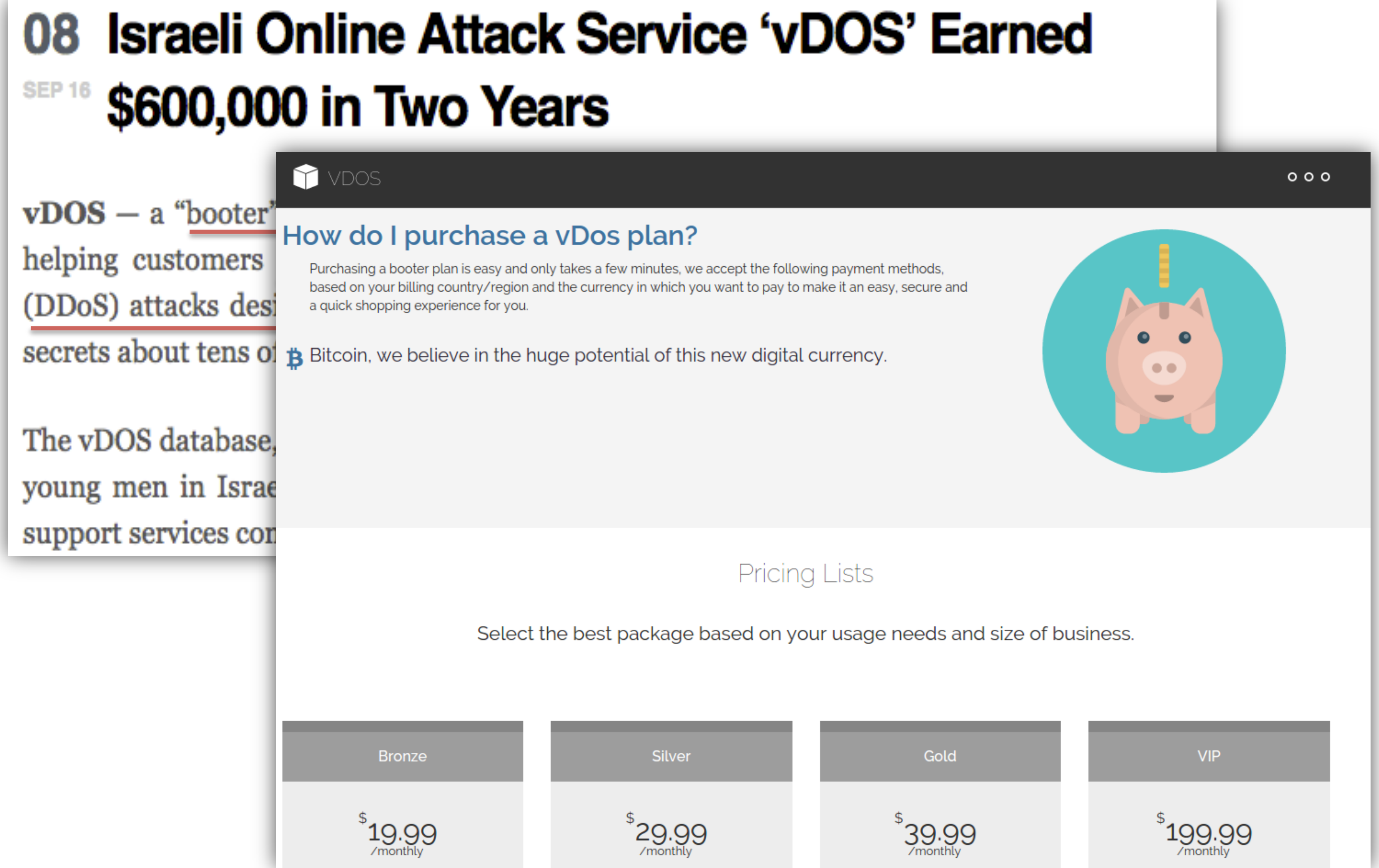
- **CPEs, DVRs, CCTVs, NAS, roteadores domésticos, etc**

- ***Malware* se propaga geralmente via telnet**

- **Explora senhas fracas ou padrão**
  - muitas vezes são "*backdoors*" dos fabricantes

- **Sendo usadas para:**
  - envio de *spams*
  - ataques de negação de serviço (DDoS)

DDoS = Lucro para Criminosos



08 SEP 16

Israeli Online Attack Service ‘vDOS’ Earned $600,000 in Two Years

vDOS — a “booter”
helping customers
(DDoS) attacks desi
secrets about tens o

The vDOS database,
young men in Israe
support services co

How do I purchase a vDos plan?

Purchasing a booter plan is easy and only takes a few minutes, we accept the following payment methods, based on your billing country/region and the currency in which you want to pay to make it an easy, secure and a quick shopping experience for you.

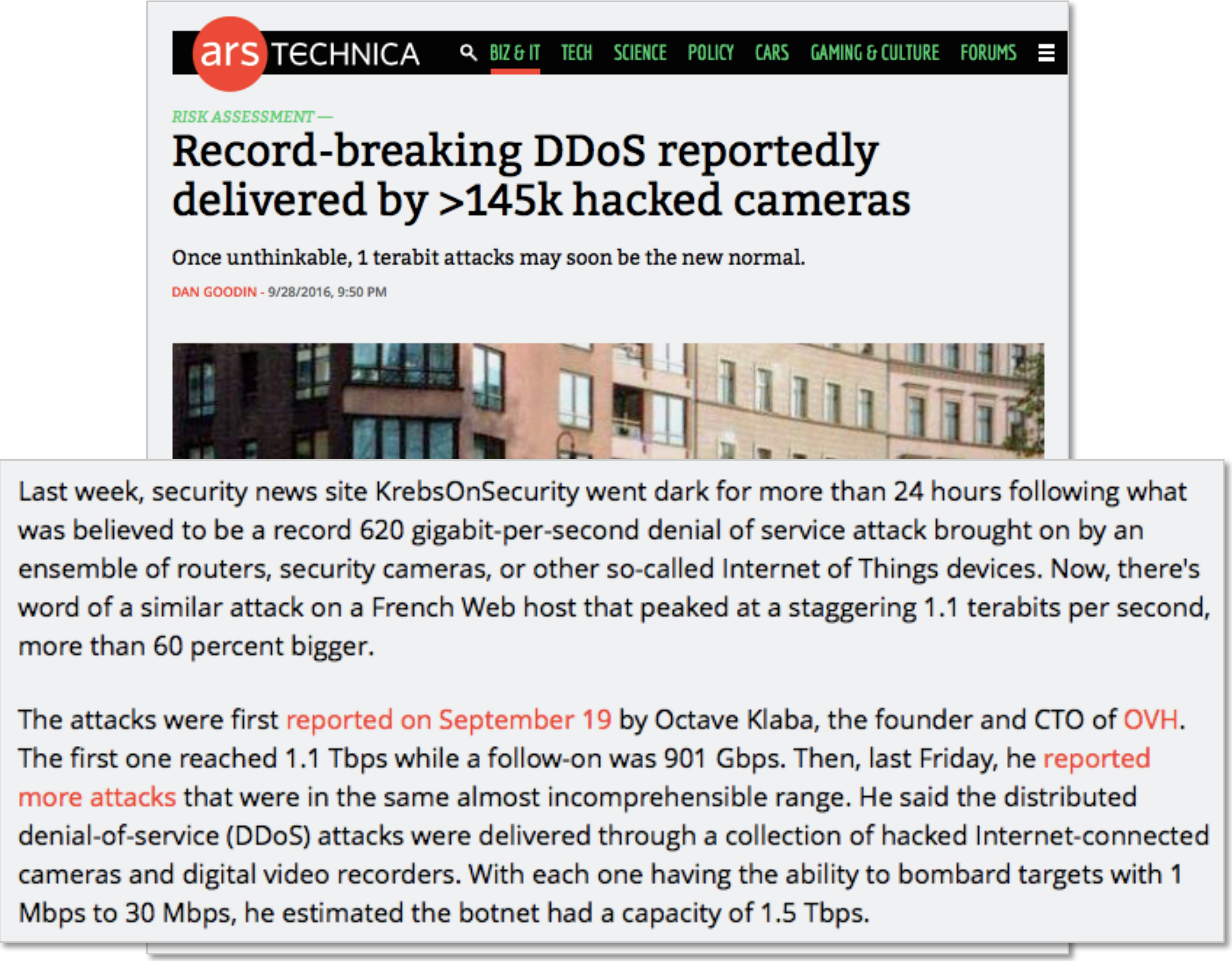
₿ Bitcoin, we believe in the huge potential of this new digital currency.

Pricing Lists

Select the best package based on your usage needs and size of business.

Bronze	Silver	Gold	VIP
$19.99 /monthly	$29.99 /monthly	$39.99 /monthly	$199.99 /monthly

https://krebsonsecurity.com/2016/09/israeli-online-attack-service-vdos-earned-600000-in-two-years/



RISK ASSESSMENT —

Record-breaking DDoS reportedly delivered by >145k hacked cameras

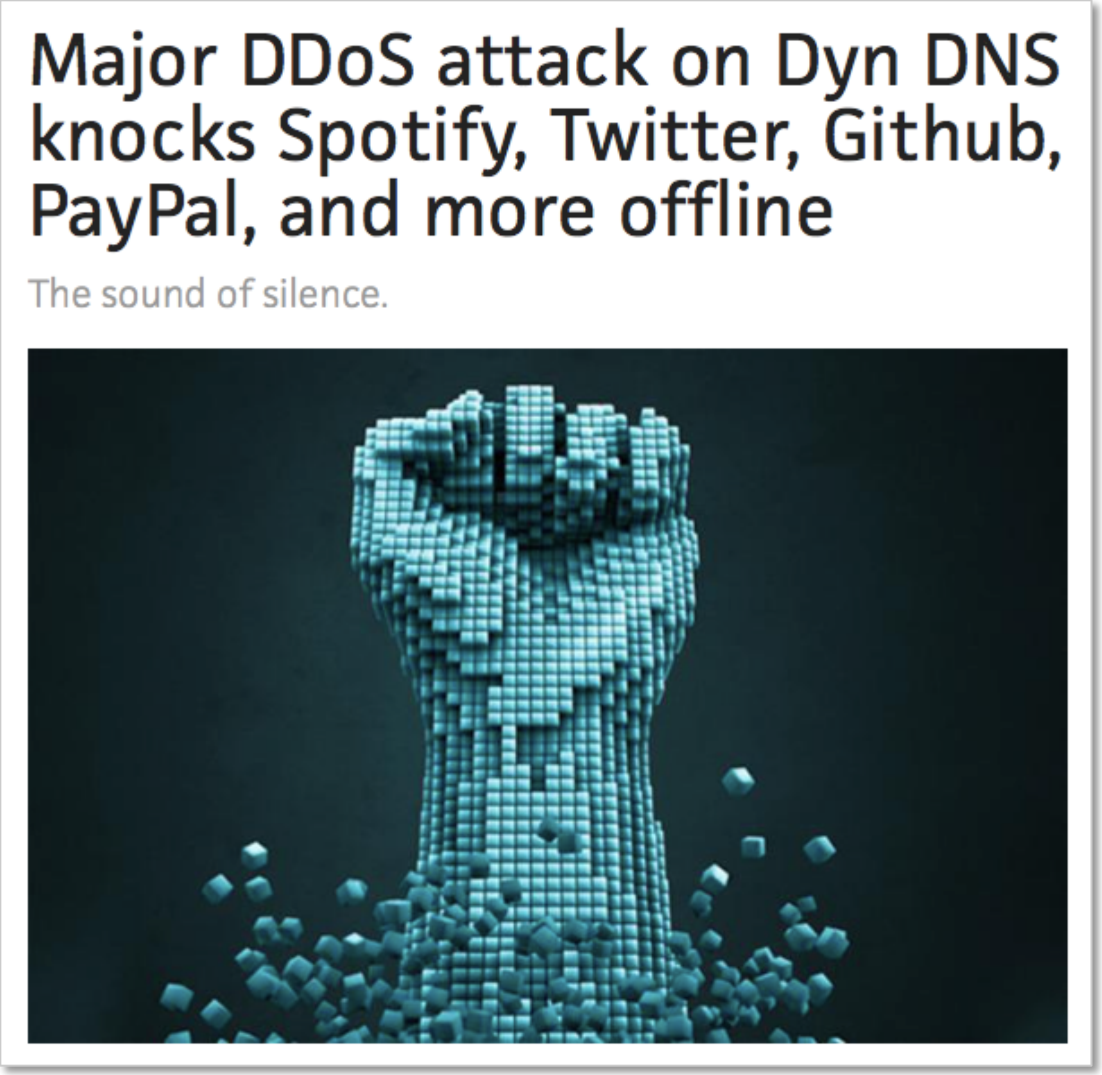
Once unthinkable, 1 terabit attacks may soon be the new normal.

DAN GOODIN - 9/28/2016, 9:50 PM

Last week, security news site KrebsOnSecurity went dark for more than 24 hours following what was believed to be a record 620 gigabit-per-second denial of service attack brought on by an ensemble of routers, security cameras, or other so-called Internet of Things devices. Now, there's word of a similar attack on a French Web host that peaked at a staggering 1.1 terabits per second, more than 60 percent bigger.

The attacks were first reported on September 19 by Octave Klaba, the founder and CTO of OVH. The first one reached 1.1 Tbps while a follow-on was 901 Gbps. Then, last Friday, he reported more attacks that were in the same almost incomprehensible range. He said the distributed denial-of-service (DDoS) attacks were delivered through a collection of hacked Internet-connected cameras and digital video recorders. With each one having the ability to bombard targets with 1 Mbps to 30 Mbps, he estimated the botnet had a capacity of 1.5 Tbps.

http://arstechnica.com/security/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/



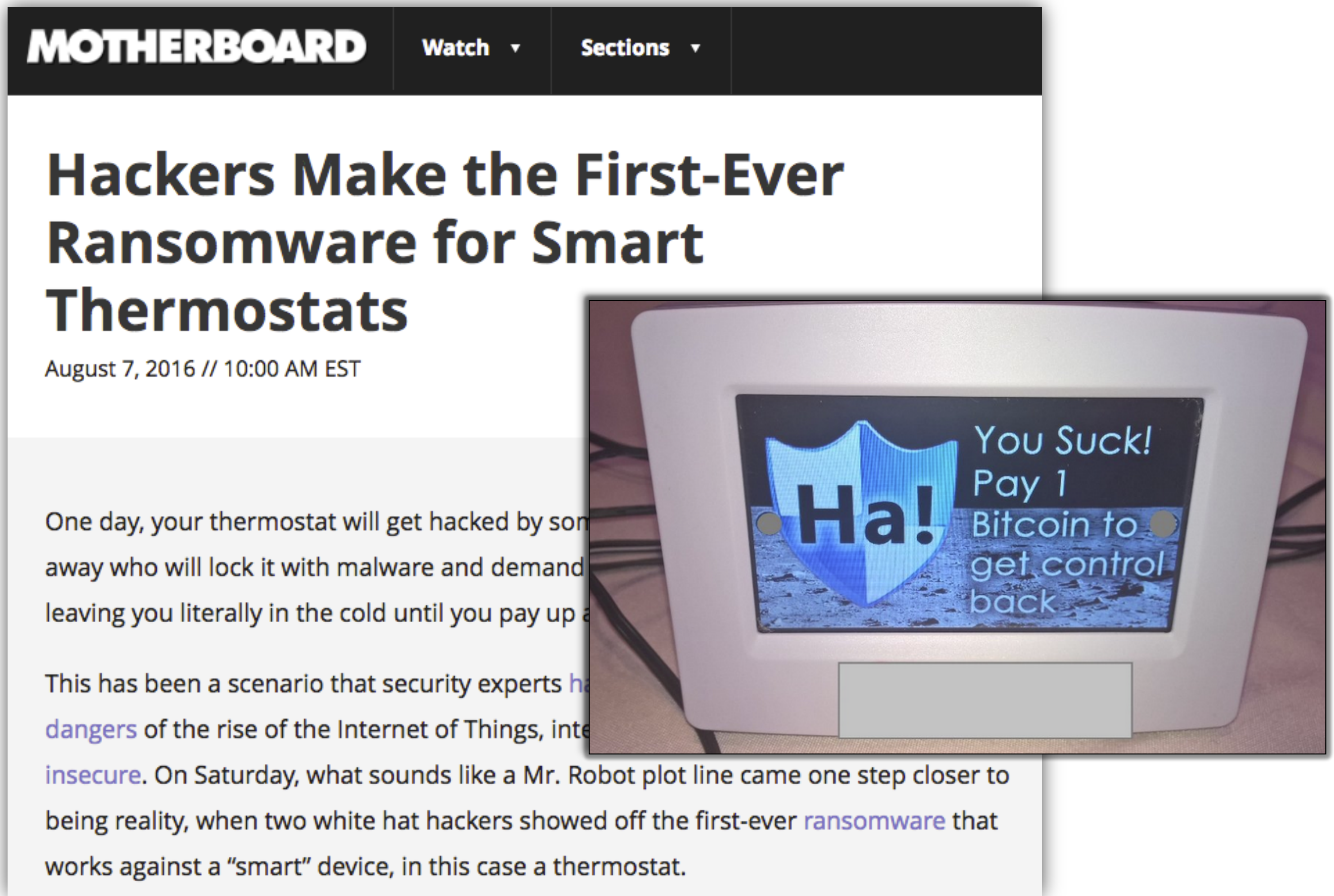
Major DDoS attack on Dyn DNS knocks Spotify, Twitter, Github, PayPal, and more offline

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



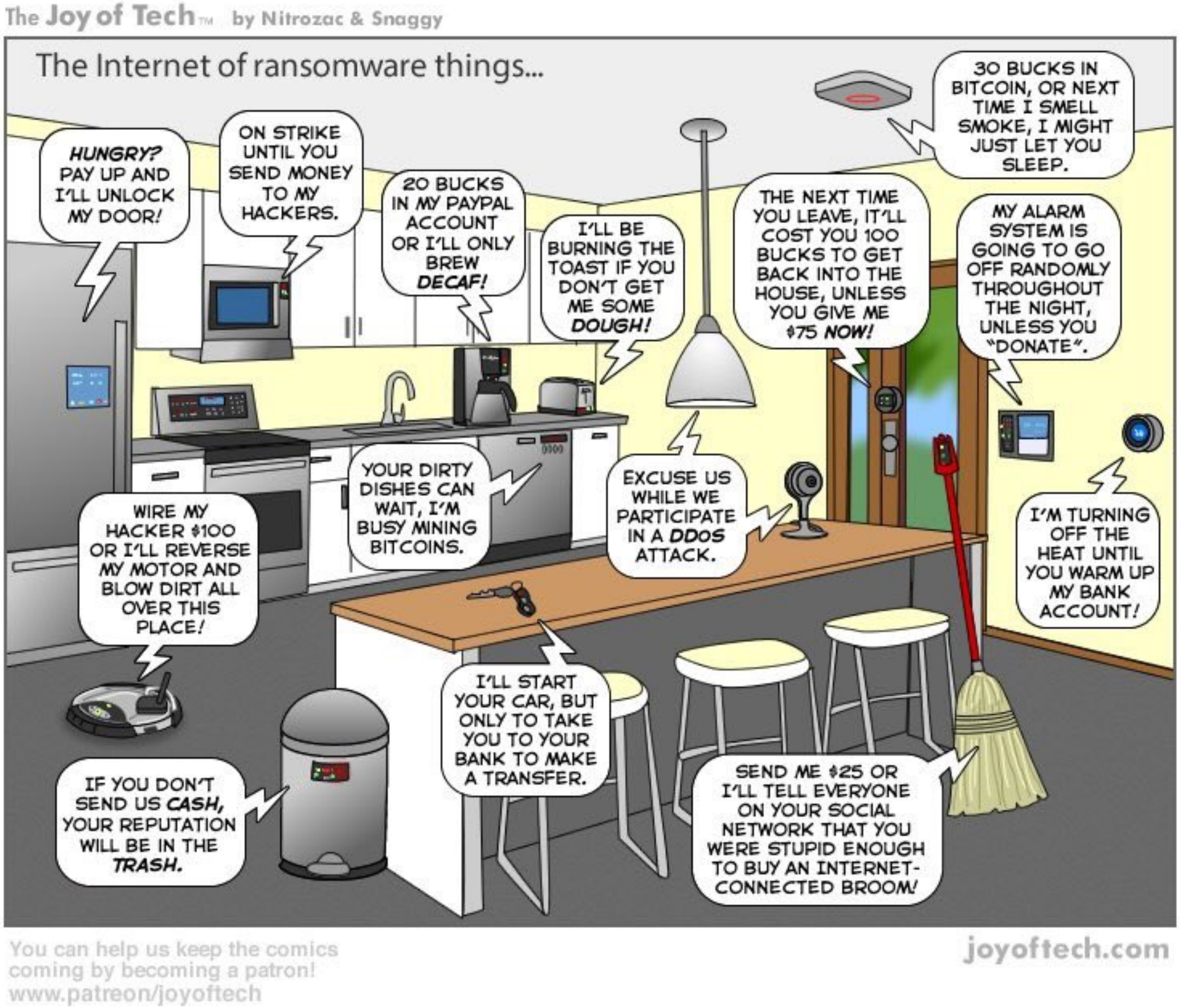
Hackers Make the First-Ever Ransomware for Smart Thermostats

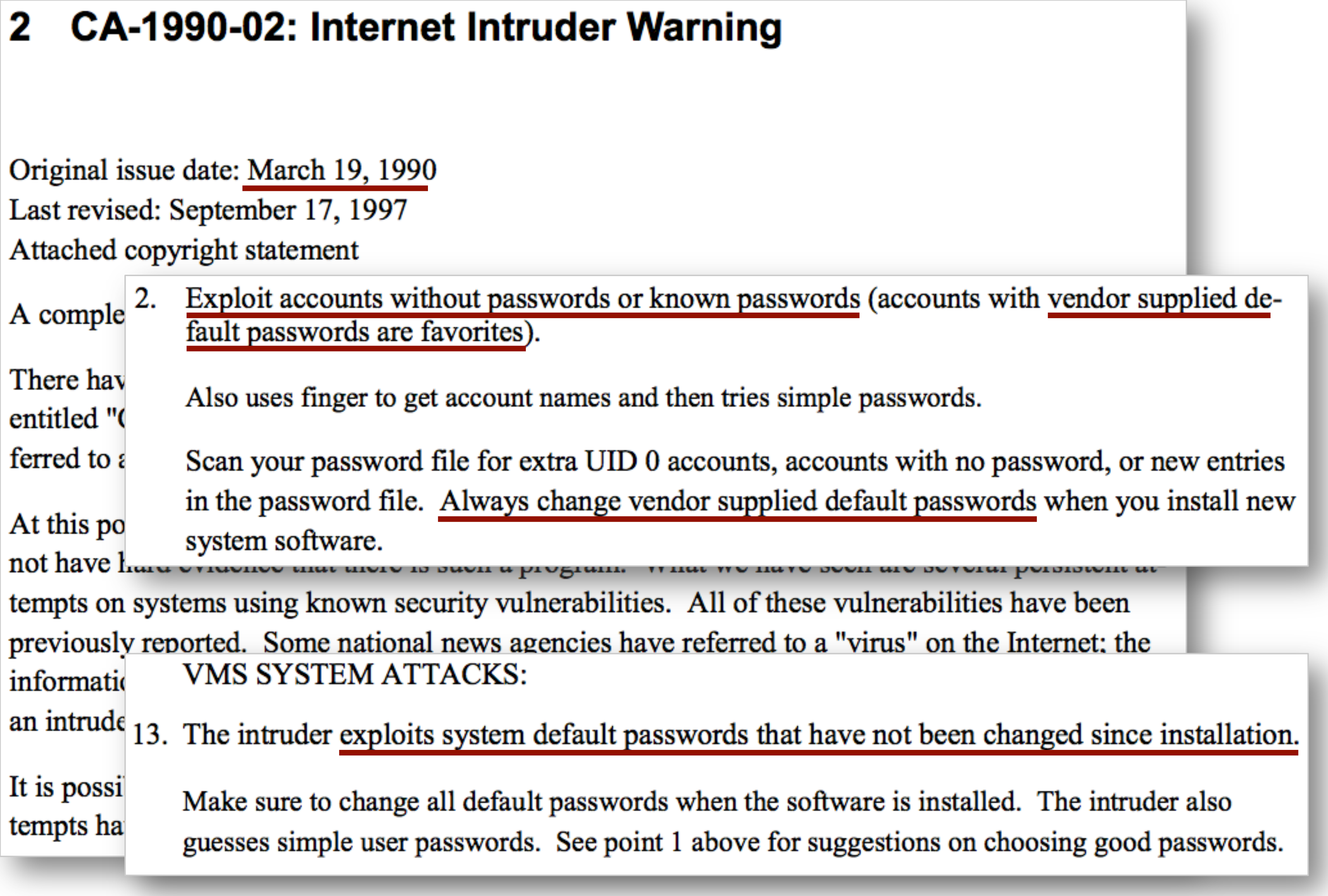
August 7, 2016 // 10:00 AM EST

One day, your thermostat will get hacked by son
away who will lock it with malware and demand
leaving you literally in the cold until you pay up a

This has been a scenario that security experts ha
dangers of the rise of the Internet of Things, inte
insecure. On Saturday, what sounds like a Mr. Robot plot line came one step closer to 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".
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!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
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



2 CA-1990-02: Internet Intruder Warning

Original issue date: March 19, 1990
Last revised: September 17, 1997
Attached copyright statement

A comple

There hav
entitled "(
ferred to a

At this po
not have hard evidence that there is such a program. What we have seen are several persistent attempts on systems using known security vulnerabilities. All of these vulnerabilities have been previously reported. Some national news agencies have referred to a "virus" on the Internet; the
informati
an intrude

It is possi
tempts ha

2. Exploit accounts without passwords or known passwords (accounts with vendor supplied default passwords are favorites).

   Also uses finger to get account names and then tries simple passwords.

   Scan your password file for extra UID 0 accounts, accounts with no password, or new entries in the password file. Always change vendor supplied default passwords when you install new system software.

VMS SYSTEM ATTACKS:

13. The intruder exploits system default passwords that have not been changed since installation.

    Make sure to change all default passwords when the software is installed. The intruder also guesses simple user passwords. See point 1 above for suggestions on choosing good passwords.

https://www.cert.org/historical/advisories/CA-1990-02.cfm

Como melhorar o cenário

Solução depende de diversos atores

- **Usuários**
- **Desenvolvedores**
- **Administradores**
- **Fabricantes**
- **Área acadêmica**

Usuários

- **Antes de comprar**
  - ser criterioso ao escolher o fabricante
    - verificar se possui política de atualização de *firmware*
    - verificar histórico de tratamento de vulnerabilidades
- **Assumir que os dispositivos virão com problemas**
  - mantê-los atualizados
  - desabilitar o acesso remoto se não for necessário
  - alterar as senhas padrão
  - desabilitar serviços desnecessários (*hardening*)

Desenvolvedores

- **Segurança deve ser nativa**
  - não opcional
  - requisitos de segurança desde o início projeto
- **Considerar todos os elementos**
  - *hardware*, *firmware*, app do *mobile*, nuvem, rede
- **Usar criptografia e autenticação forte**
- **Não usar protocolos obsoletos**
- **Abolir práticas ruins**
  - senha do dia, conta não documentada, reset de configuração via rede, etc
- ***Defaults* seguros**
- **Usar práticas de desenvolvimento seguro**
- **Atualização**
  - com autenticação/verificação da atualização

Desenvolvedores - 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

Administradores

- **Implementar boas práticas:**
  - filtros antispoofing
    - http://bcp.nic.br/entenda-o-antispoofing/
- **Manter os equipamentos atualizados**
  - sistema operacional e todos os *serviços nele executados*
  - *serviço Web, SGBD, extensões, módulos e plugins*
- **Desabilitar serviços desnecessários**
- **Ser cuidadoso ao usar e elaborar senhas**
  - se disponível, usar verificação em duas etapas
- **Planejar a implantação antecipadamente**
  - segregar redes
  - como gerenciar remotamente
  - como fazer *updates*

Fabricantes

- **Segurança deve ser nativa**
  - não deve ser opcional / customização
  - requisitos de segurança devem ser considerados desde o projeto
  - investir em programação segura
- **Deve ser incluída na análise de risco das empresas**
  - danos à imagem
  - danos aos usuários
- **Como implementar segurança em larga escala**
  - atualizações / correções
- **Um equipamento ➔ diversos fabricantes**
- **Ter grupo de resposta a incidentes preparado para lidar com os problemas (PSIRT)**

Área acadêmica

- **Área acadêmica**
  - ensinar segurança / programação segura já nos primeiros anos

Obrigada

www.cert.br

@ lucimara@cert.br

@certbr

25 de outubro de 2017

nic.br cgi.br

www.nic.br | www.cgi.br