nic.br cgi.br | 20 anos cert.br

Jornada IESCAMP de Tecnologia da Informação

Campinas, SP

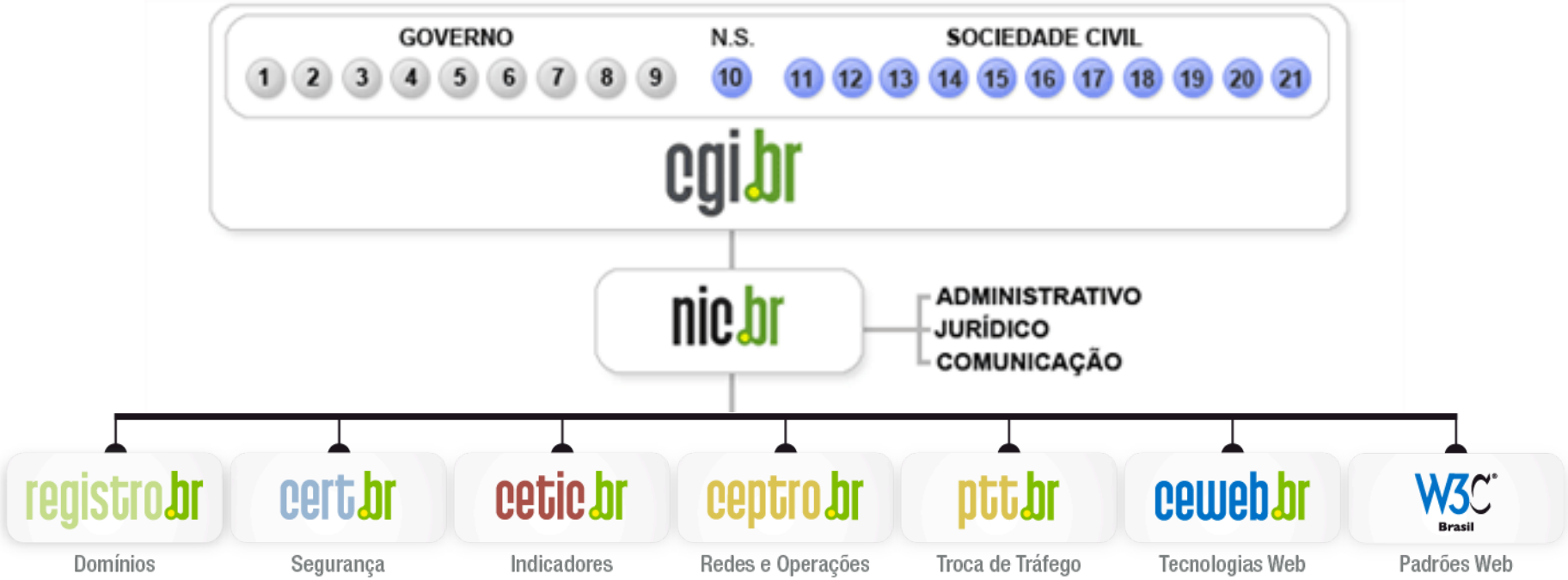
18/10/17

Segurança e IoT
Desafios e Expectativas

Miriam von Zuben
miriam@cert.br

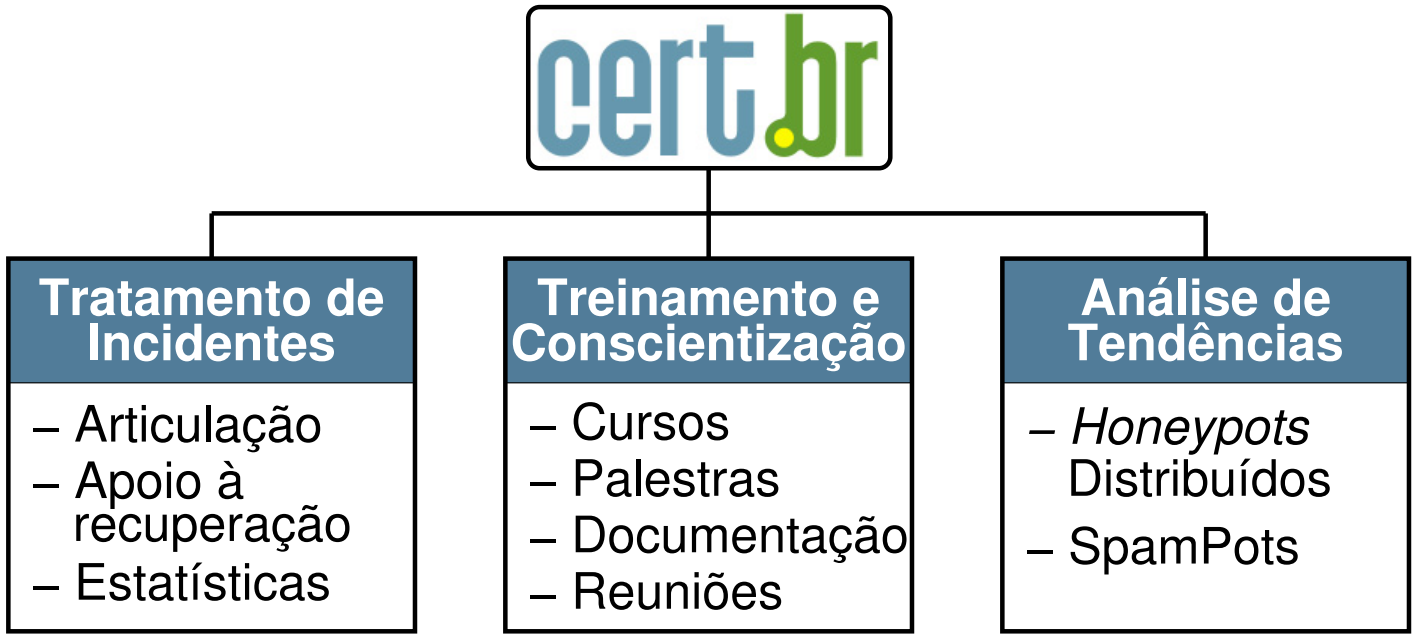
cert.br nic.br cgi.br

Estrutura do CGI.br e NIC.br



1 – Ministério da Ciência e Tecnologia (Coordenação)
2 – Ministério das Comunicações
3 – Casa Civil da Presidência da República
4 – Ministério da Defesa
5 – Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 – Ministério do Planejamento, Orçamento e Gestão
7 – Agência Nacional de Telecomunicações (Anatel)
8 – Cons. Nacional de Desenvolvimento Científico e Tecnológico
9 – Fórum Nac. de Secretários Estaduais para Assuntos de C&T
10 – Representante de Notório Saber em assuntos de Internet

11 – provedores de acesso e conteúdo
12 – provedores de infra-estrutura de telecomunicações
13 – indústria de bens de informática, telecomunicações e software
14 – segmento das empresas usuárias de Internet
15-18 – representantes do terceiro setor
19-21 – representantes da comunidade científica e tecnológica



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet PROJECT

Criado em 1997 para:

- **Ser um ponto de contato nacional para notificação de incidentes**
- **Prover a facilitação e o apoio necessários no processo de resposta a incidentes**
- **Estabelecer um trabalho colaborativo com outras entidades**
- **Aumentar a conscientização sobre a necessidade de segurança na Internet**
- **Auxiliar novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades**

IoT

Computação Ubíqua

- **Mark Weiser, em 1988**
- **Oposto da “realidade virtual”**
  - pessoas colocadas em realidade gerada por computadores
- **Computador se integra a 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 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

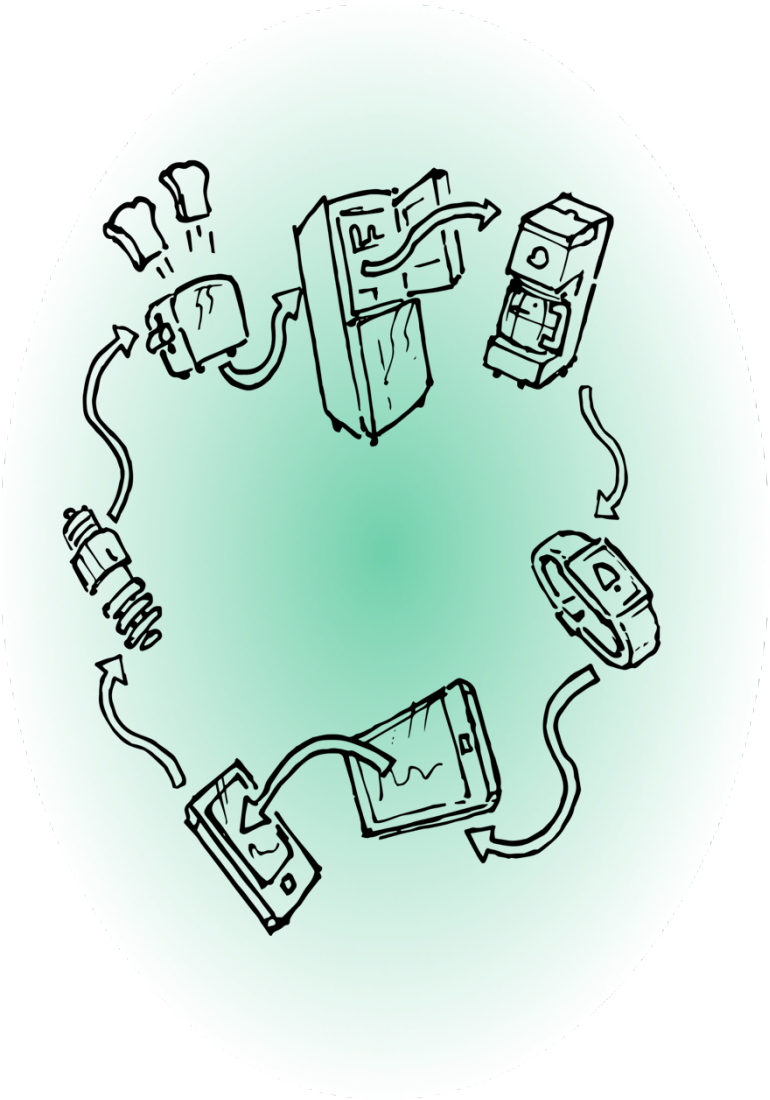
In the real world, things matter more than ideas

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

Definição IoT

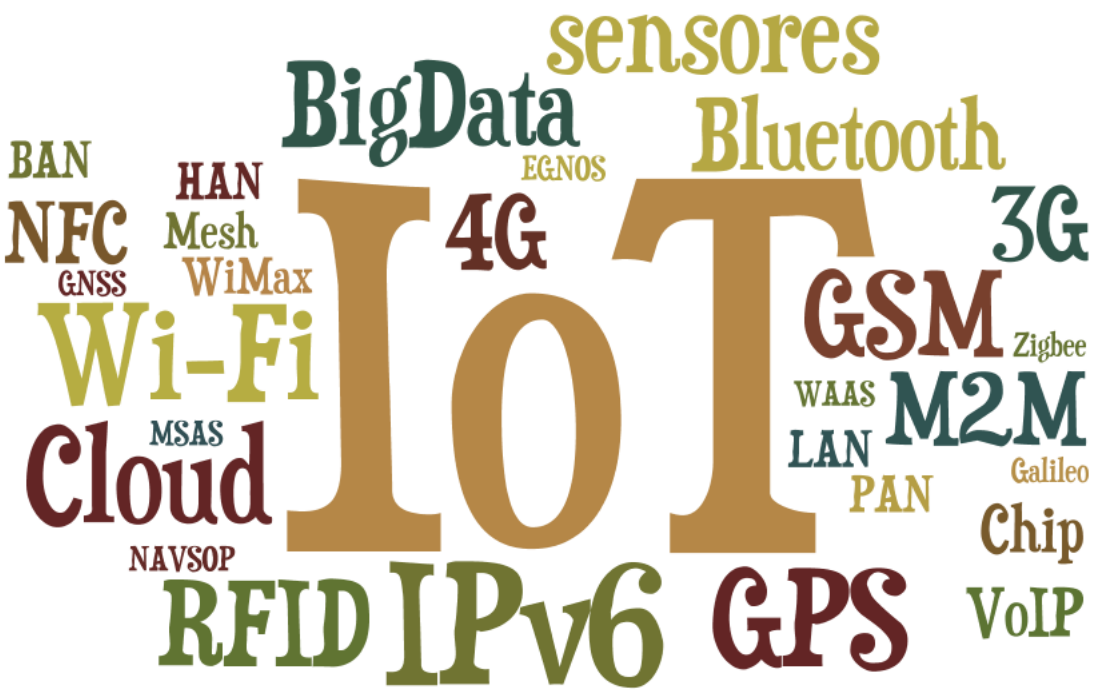
“... é uma rede de objetos físicos, veículos, prédios e outros que possuem tecnologia embarcada, sensores e conexão com rede capaz de coletar e transmitir dados.”

Wikipedia



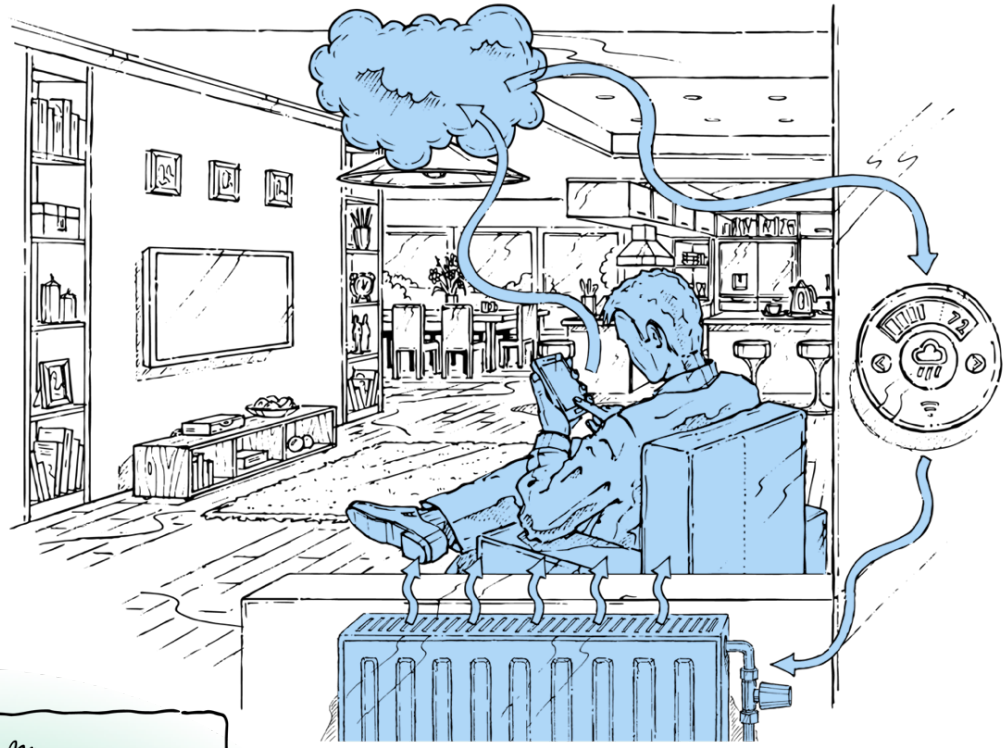
Atualmente

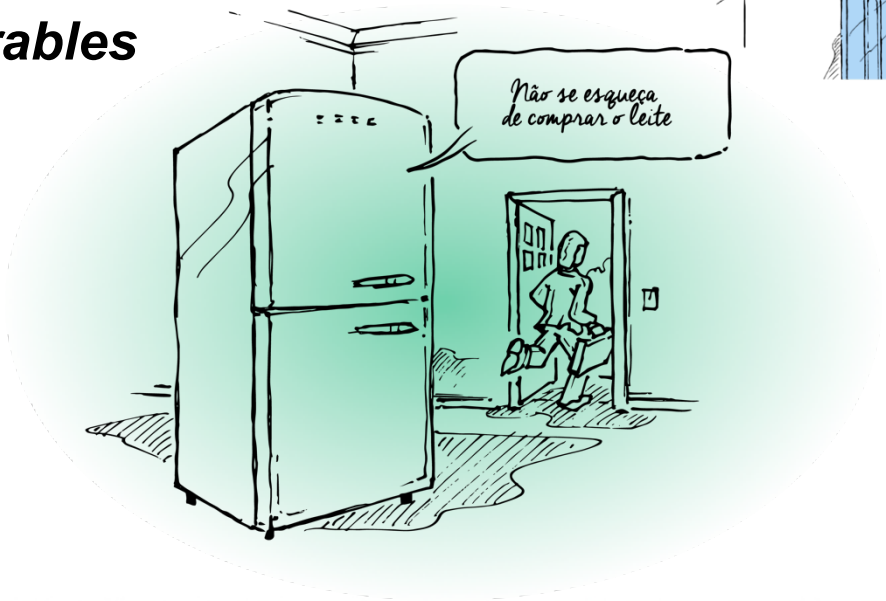
- **As coisas já estão conectadas**
  - sistemas complexos e completos
    - sistema operacional, aplicações Web, permitem acesso remoto, etc
    - múltiplas tecnologias



Usos

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



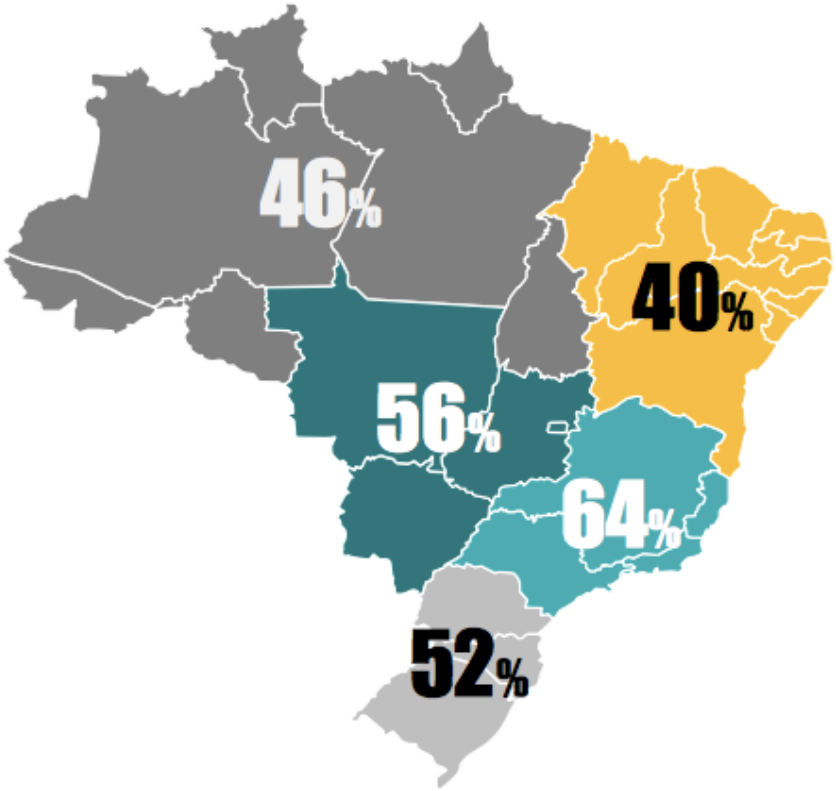


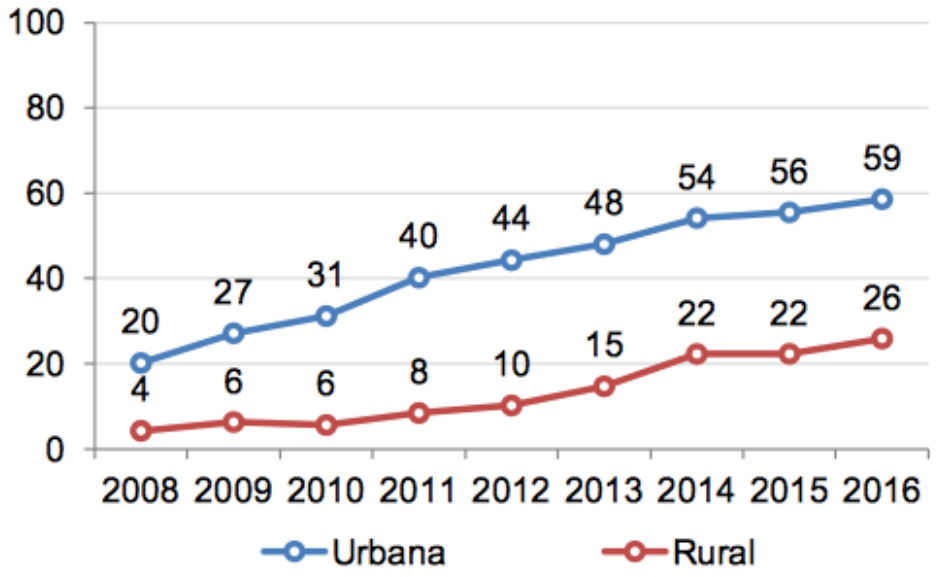
Desafios

Principais Desafios

- **Infraestrutura**
- **Privacidade**
- **Segurança**

Infraestrutura - TIC Domicílios 2016
Domicílios com acesso à Internet





http://cetic.br/pesquisa/domicilios/

Privacidade

- **Proteção de dados**
  - responsabilidades
  - assimetria de acesso entre empresas e consumidores
    - planos de saúde
    - seguradoras de veículos
    - compras em geral
- **Difícil adquirir equipamentos sem essas tecnologias**
  - tudo tem que estar conectado
  - porque é possível conectar não significa que tem que estar

Privacidade

News > Technology News

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

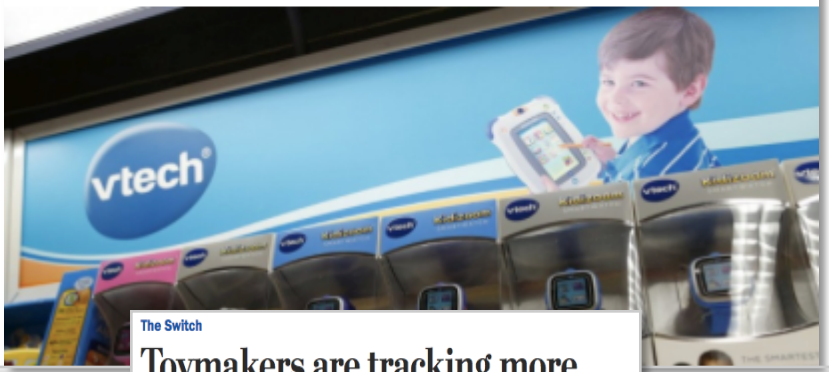
Consumer groups say the doll, which has a microphone and uses Bluetooth to transmit audio recordings via the Internet, poses both a security and a privacy threat.

By David Emery Feb 24th, 2017

The Switch

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

yley 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

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

Share 1355 Tweet

SHARE THIS URL

nydn.us/1rwYG2C

Wake Up, baby

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

Shodan: The IoT search engine for watching sleeping kids and bedroom antics

"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.

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/

Segurança

Falhas em IoT

- **Sendo exploradas por:**
  - criminosos
  - espionagem industrial
  - governos
  - vândalos
  - pessoas que querem diversão

- **Dificuldade de explicar e de entender o problema**
  - o que temos ouvido no dia-a-dia:
    - “Isto é apenas um(a) [_____]”
    - “Não, a gente não tem Internet aqui...”
    - “Esse dispositivo não é minha responsabilidade...”

Principais vulnerabilidades

- **Projetos sem levar em conta segurança**
- **Sistemas desatualizados**
  - defasagem de tempo entre ser “fabricado” e chegar ao cliente
- **Defeitos de *software* / *firmware***
- **Falhas de configuração**
- **Falta de proteção de dados**
- **Contas:**
  - sem senhas
  - com senhas fracas ou *default*
  - de serviço (*backdoors*)
  - com acesso remoto

Segurança

- **Mesmos velhos problemas**
  - telnet, senha *default*, falta de atualização, erros de programação, etc
- **Definição e normatização de responsabilidades**
  - quem lança as correções?
  - quem aplica as correções?
  - quem e como os clientes contatam as empresas?
- **Políticas de atualização inexistentes**
  - a política em geral é “comprar outro”
  - vale a pena atualizar equipamentos muito baratos?
  - tempo de suporte X tempo de vida útil do equipamento

Segurança

- **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

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)

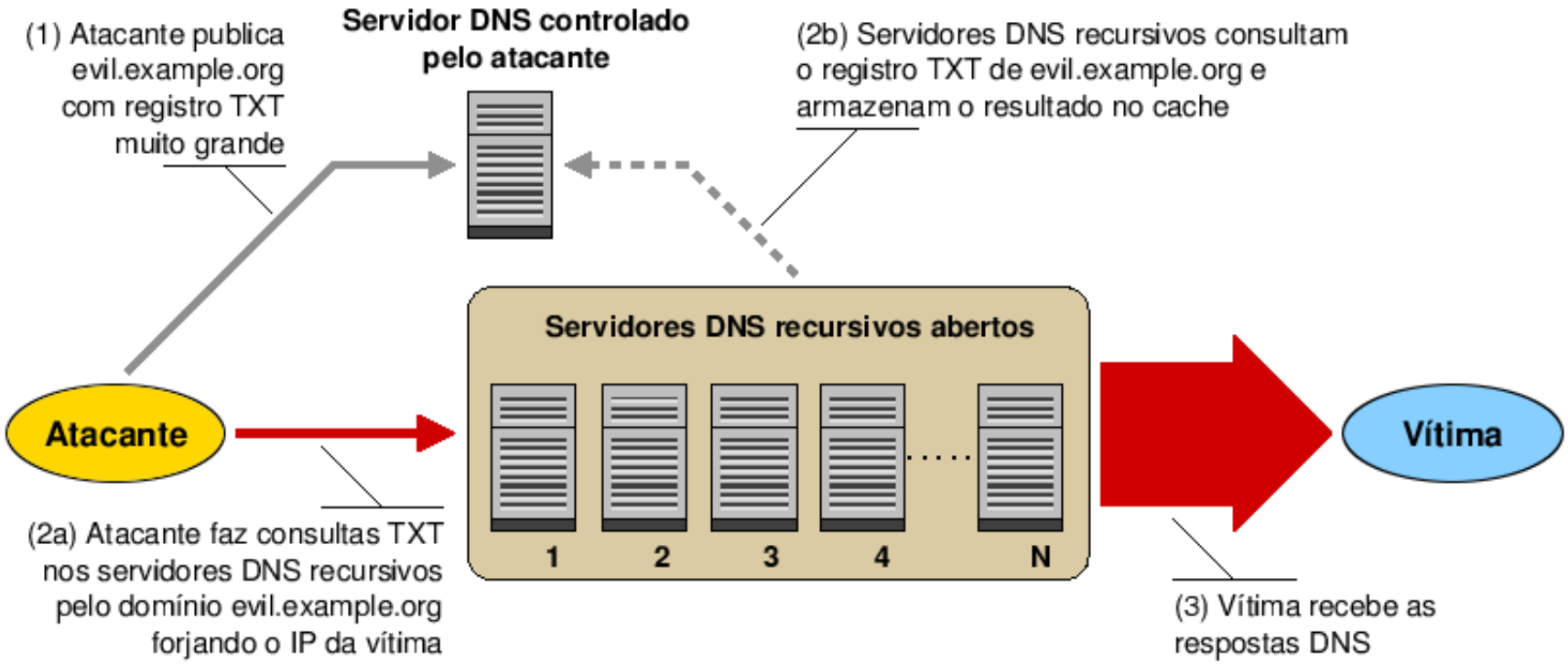
Ataques DRDoS

- ***Distributed Reflective Denial of Service***
- **Usa infraestrutura pública da Internet para amplificação**
- **Tem grande "poder de fogo"**

Protocolo	Fator de amplificação	Comando Vulnerável
DNS	28 até 54	Ver: TA13-088A
NTP	556.9	Ver: TA14-013A
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request

https://www.us-cert.gov/ncas/alerts/TA14-017A
http://www.internetsociety.org/sites/default/files/01_5.pdf

Ataques DRDoS
Exemplo de funcionamento abusando DNS



Fonte: CERT.br

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

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/

NEWS

Hackers create more IoT botnets with Mirai source code

The total number of IoT devices infected with the Mirai malware has reached 493,000

By Michael Kan FOLLOW

IDG News Service | Oct 18, 2016 2:04 PM PT

RELATED TOPICS

Security

Internet of Things

Malware & Vulnerabilities

3 COMMENTS

Malware that can build botnets out of IoT products has gone on to infect twice as many devices after its source code was publicly released.

The total number of IoT devices infected with the Mirai malware has reached 493,000, up from 213,000 bots before the source code was disclosed around Oct. 1, according to internet backbone provider Level 3 Communications.

http://www.computerworld.com/article/3132359/security/hackers-create-more-iot-botnets-with-mirai-source-code.html

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

Infusion Pumps

www.hospira.com/en/products_and_services/infusion_pumps

Reader

SMART OPTIONS FOR RELIABLE MEDICATION DELIVERY

Hospira high-performance infusion pumps make it easy for you to deliver exceptional patient safety and care. Our focused portfolio features proven, innovative smart pump and pain management technology designed to help meet your clinical safety and workflow goals. The powerful Hospira MedNet™ safety software helps to reduce medication errors and raise the bar for your medication management system. And, with an eye to the future, our Plum™ family of smart pumps with Hospira MedNet are designed to integrate with your electronic medical record (EMR) systems through our IV Clinical Integration solution.

Contact Hospira

Our focused line of infusion systems includes general infusion and pain management pumps:

PLUM 360™ INFUSION SYSTEM

Your direct connection to clinical excellence with integrated safety and efficiency at every step.

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 pur
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

Hackers Make the First-Ever Ransomware for Smart Thermostats

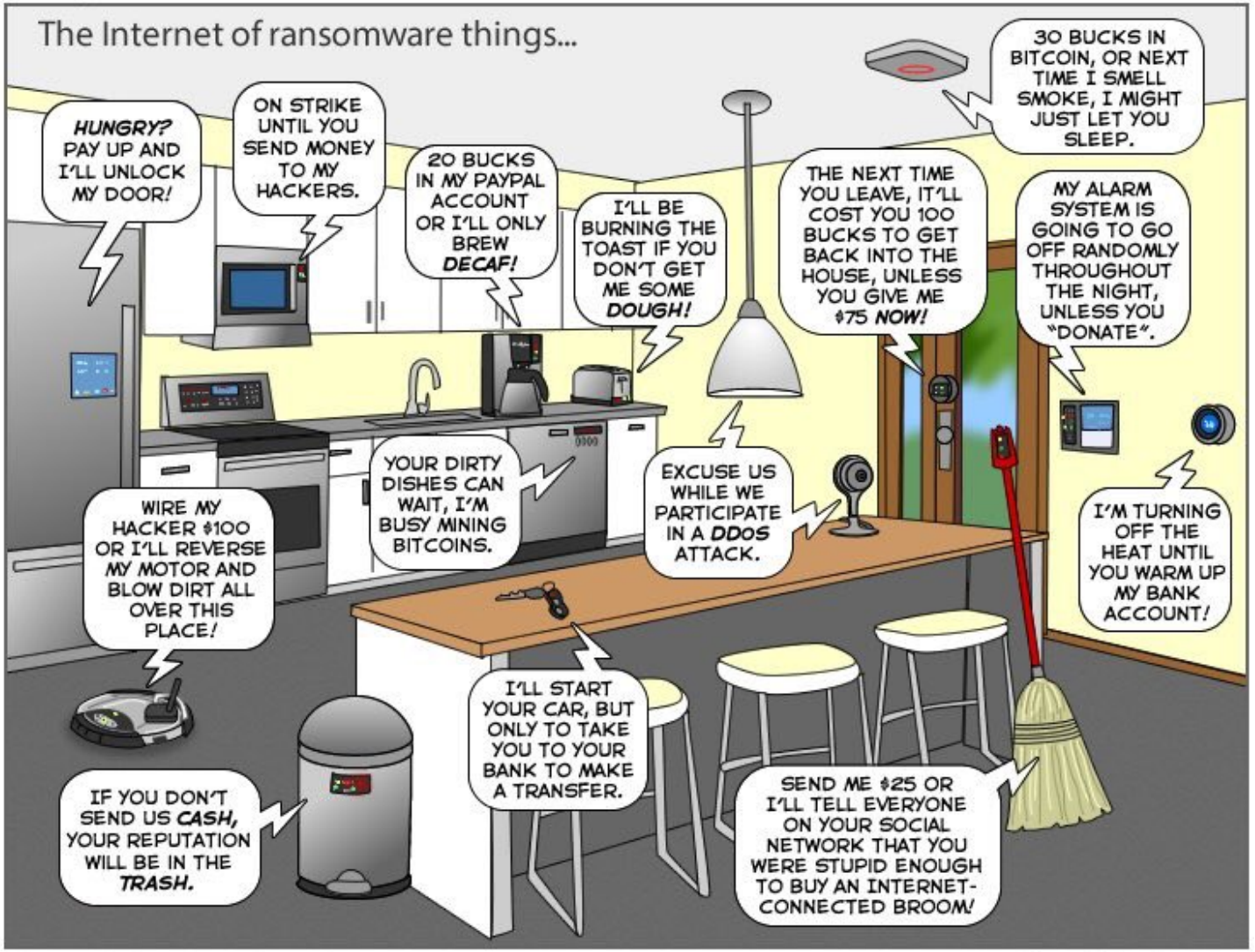
August 7, 2016 // 10:00 AM EST

One day, your thermostat will get hacked by some cybercriminal hundreds of miles away who will lock it with malware and demand a ransom to get it back to normal, leaving you literally in the cold until you pay up a few hundred dollars.

This has been a scenario that security experts have touted as one of the theoretical dangers of the rise of the Internet of Things, internet-connected devices that are often 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



You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech

joyoftech.com

Security researchers
forever altered the au
safety" in July when t
could remotely hack a
transmission and bral
issue an unprecedente
mailing out USB drive
infotainment systems
network that connect

CNNMoney
@CNNMoney

Follow

Recall Alert: Fiat Chrysler is recalling 1.4 million hackable vehicles. Check affected cars: cnnmon.ie/1OrrqGv

9:59 PM - Jul 24, 2015

48 22

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Innovations

How a fish tank helped hack a casino

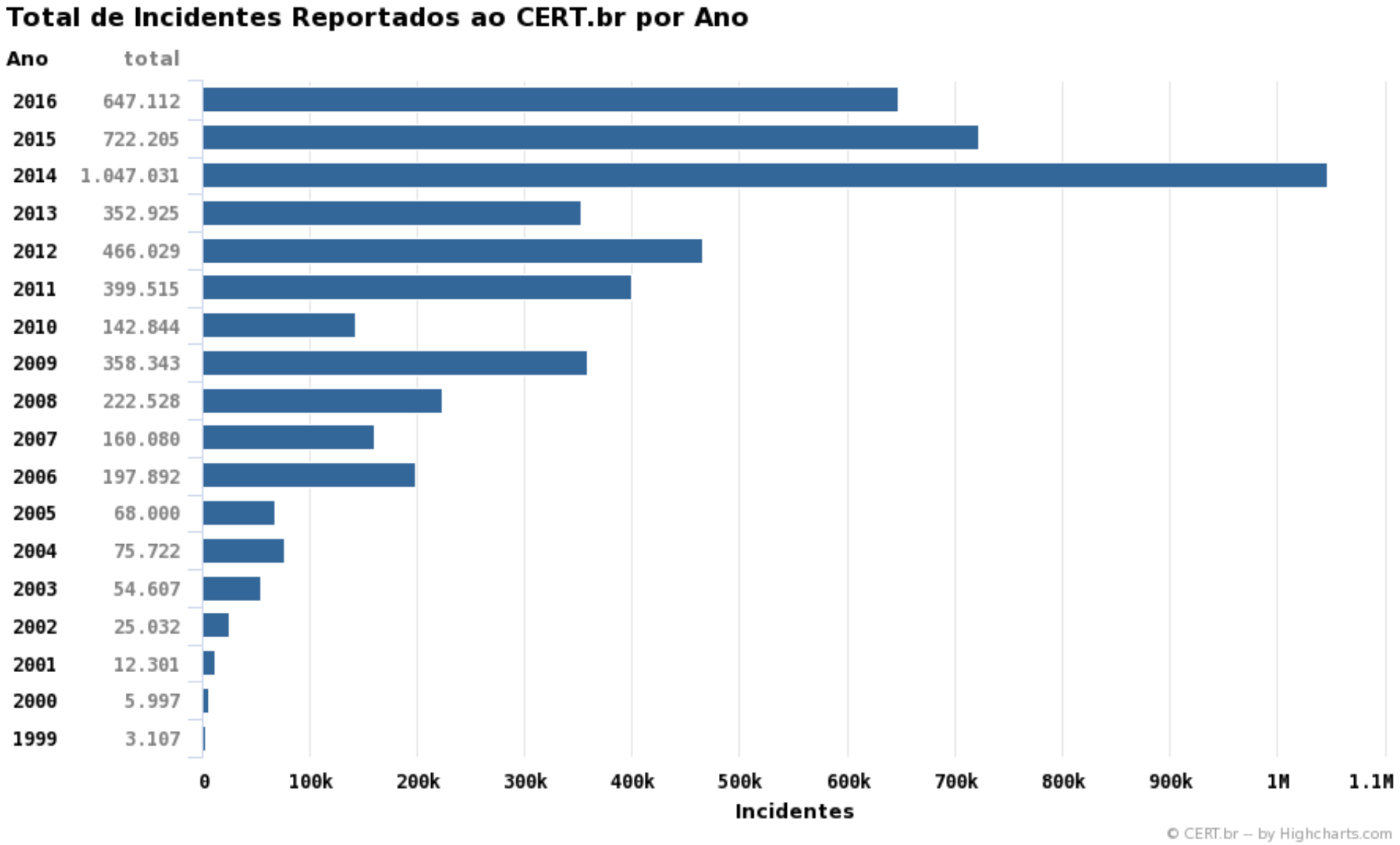
By Alex Schiffer July 21

Hackers stole data from a casino by hacking into an Internet-connected fish tank, according to a new report. (iStock)

https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/?utm_term=.5eac99bf1092

Estatísticas CERT.br

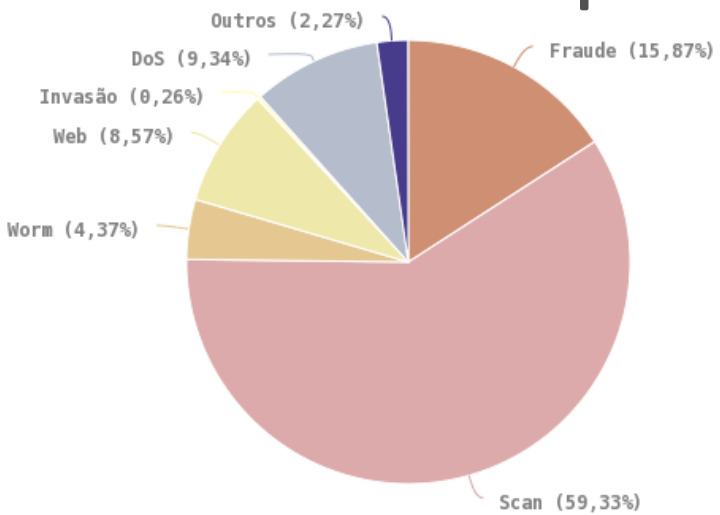
cert.br nic.br cgi.br

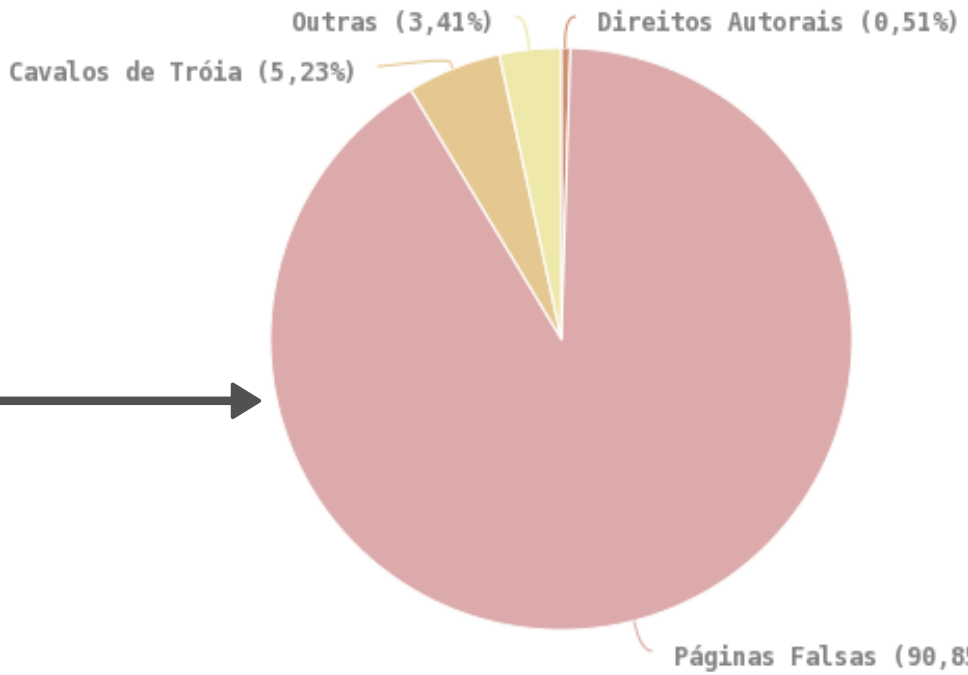


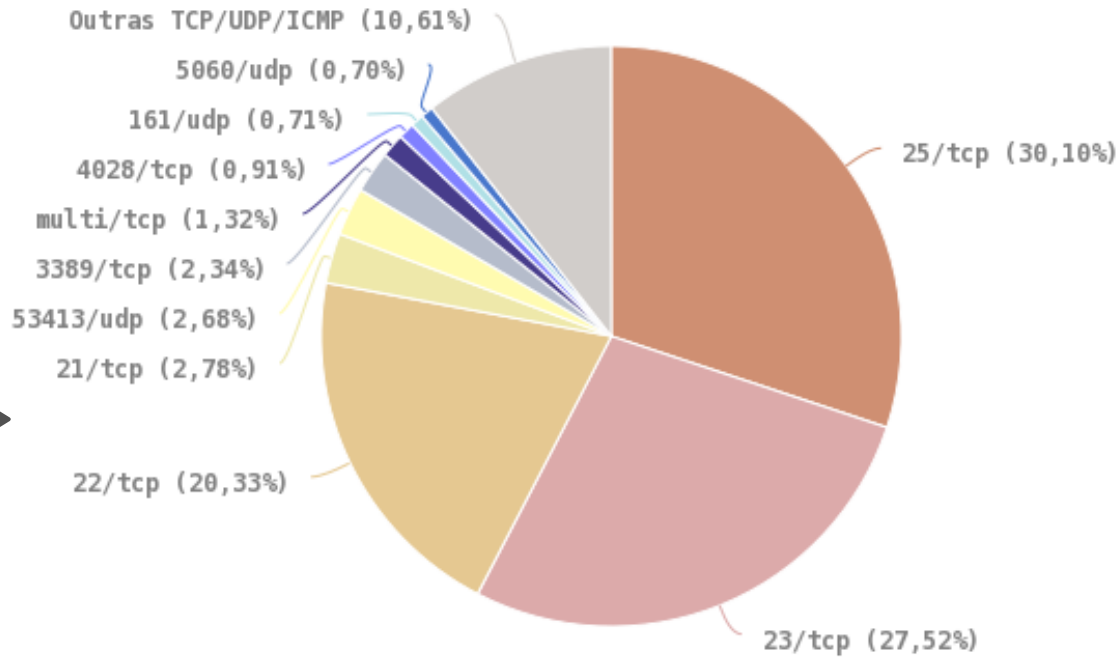
Estatísticas de notificações enviadas voluntariamente por administradores de sistemas e usuários finais para o *e-mail* cert@cert.br.

https://cert.br/stats/

Estatísticas 2016



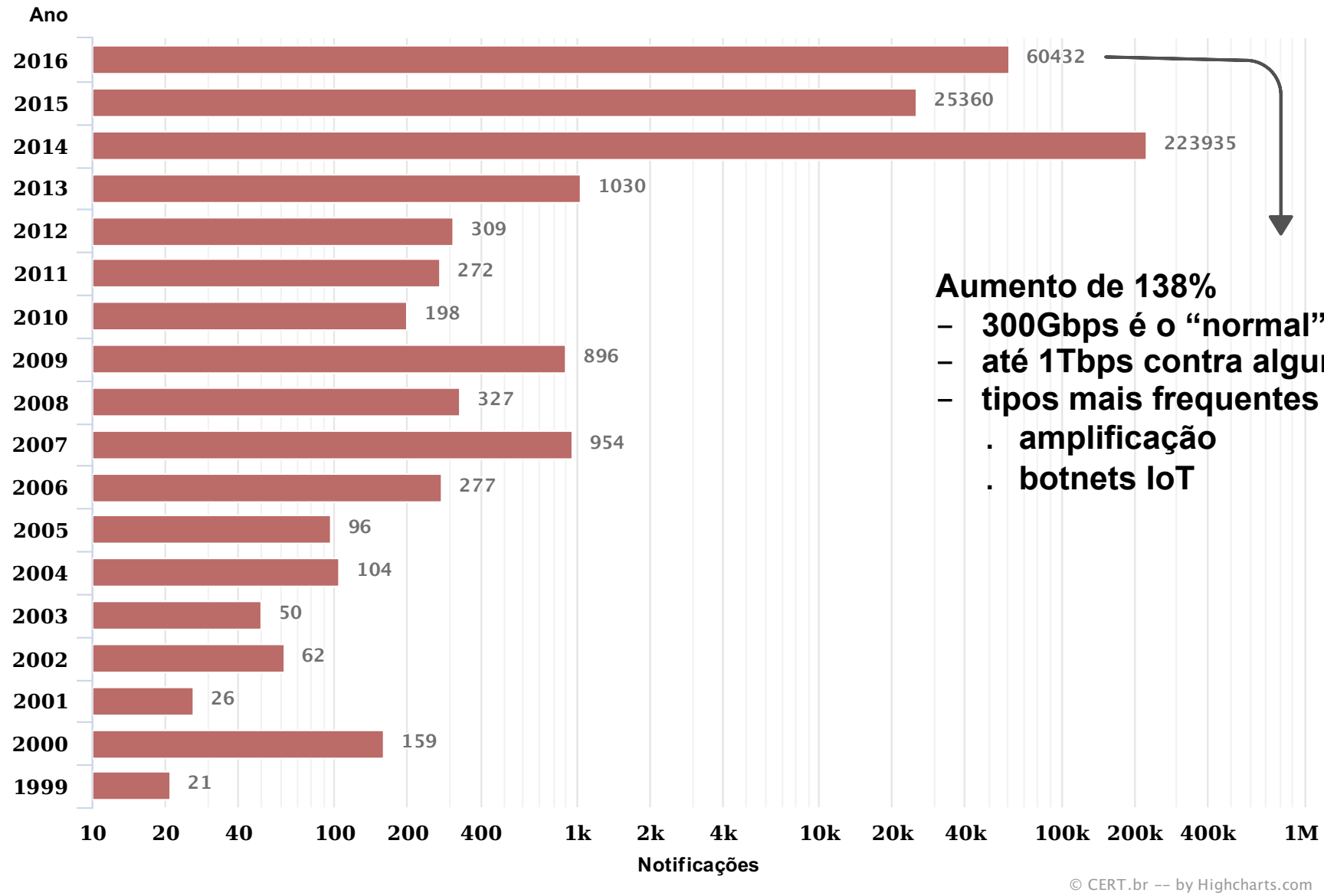




Fonte: CERT.br

Notificações sobre computadores participando em ataques de DoS

1999 -- 2016



Aumento de 138%

- 300Gbps é o “normal”
- até 1Tbps contra alguns alvos
- tipos mais frequentes
  - amplificação
  - botnets IoT

Fonte: CERT.br

Como melhorar o cenário

Solução depende de diversas camadas

- **Usuários**
- **Desenvolvedores**
- **Administradores**
- **Fabricantes**
- **Pesquisadores**

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

- **Não usar protocolos obsoletos**
- **Usar criptografia e autenticação forte**
- **Não ter senha do dia, senha padrão não documentada, *reset* de configuração via rede, etc**
- ***Defaults* seguros**
- **Atualização**
  - precisa ser possível
  - necessário prever algum mecanismo de autenticação
- **Usar práticas de desenvolvimento seguro**

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:**
  - BCP38/BCP84
  - filtrar pacotes com endereços “spoofados”
  - 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

Fabricantes

- **Segurança deve ser nativa**
  - não deve ser opcional
  - 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**
- **Um equipamento -> diversos fabricantes**
- **Ter grupo de resposta a incidentes preparado para lidar com os problemas (PSIRT)**

Obrigada

www.cert.br

miriam@cert.br

@certbr

18 de outubro de 2017

nic.br cgi.br

www.nic.br | www.cgi.br