nic.br cgi.br | cert.br

SET Expo 2016

São Paulo, SP

01 de setembro de 2016

Segurança na Internet
Tendências e Desafios

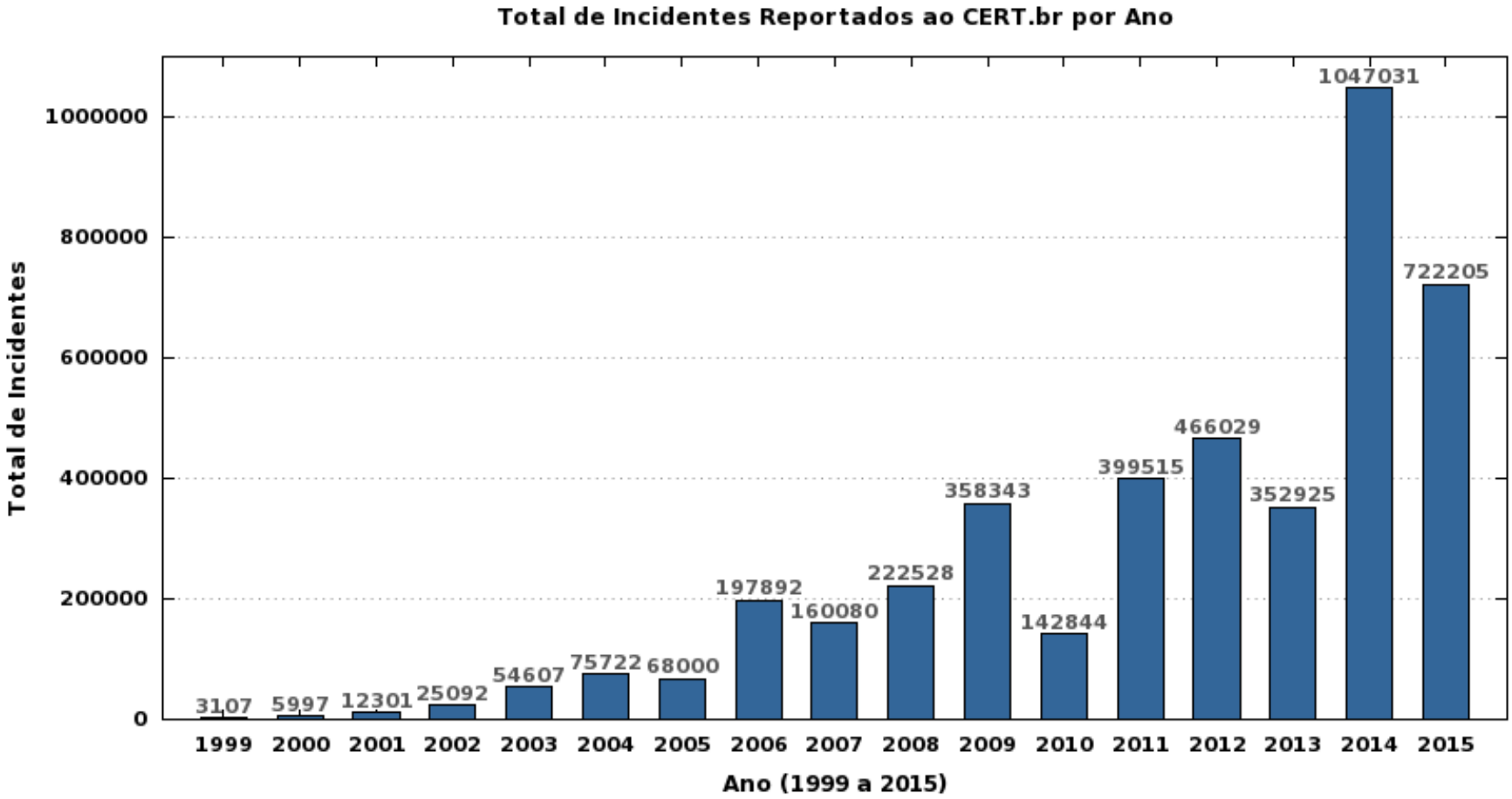
Miriam von Zuben
miriam@cert.br

cert.br nic.br cgi.br

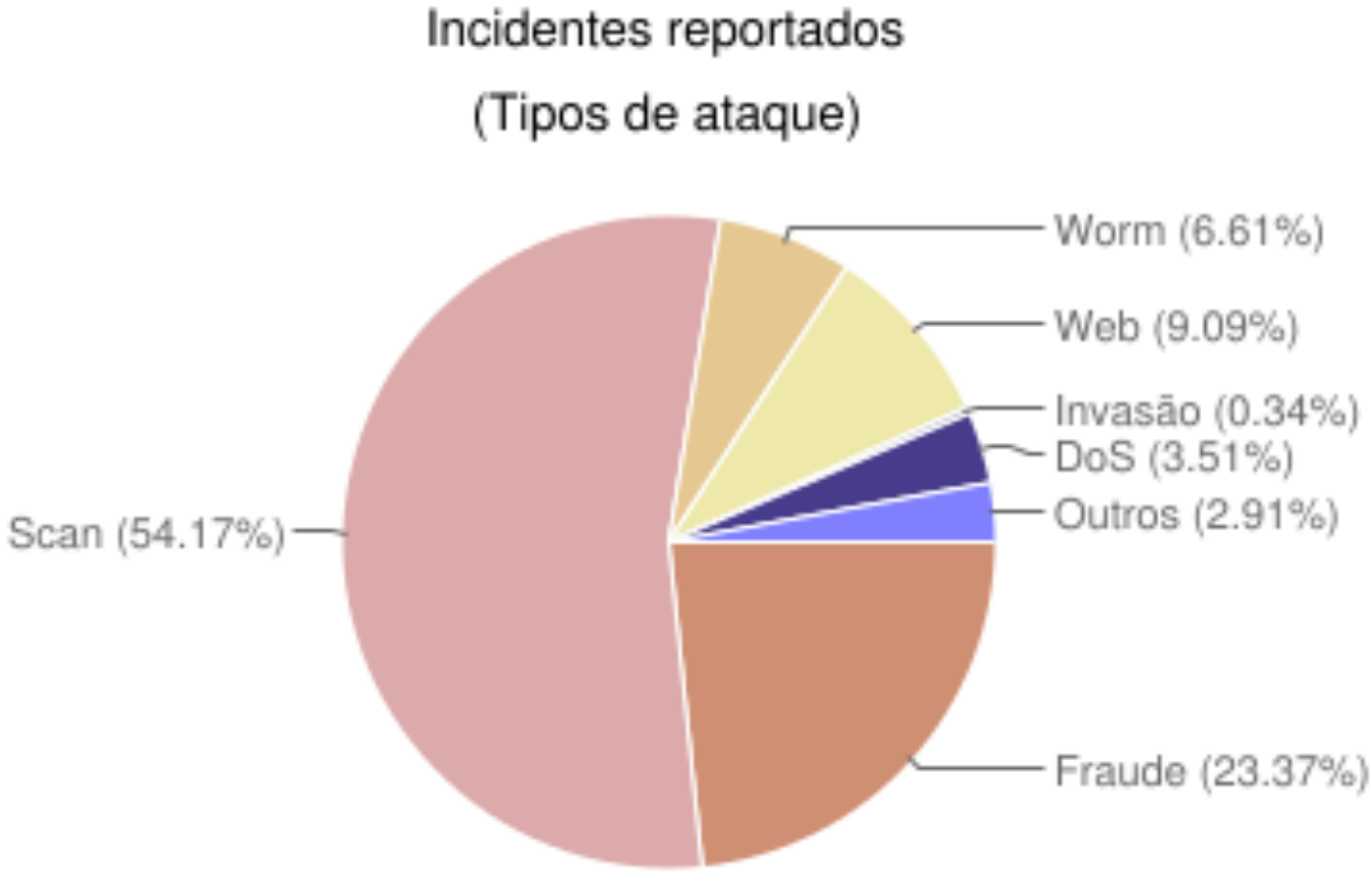
Cenário atual

cert.br nic.br cgi.br

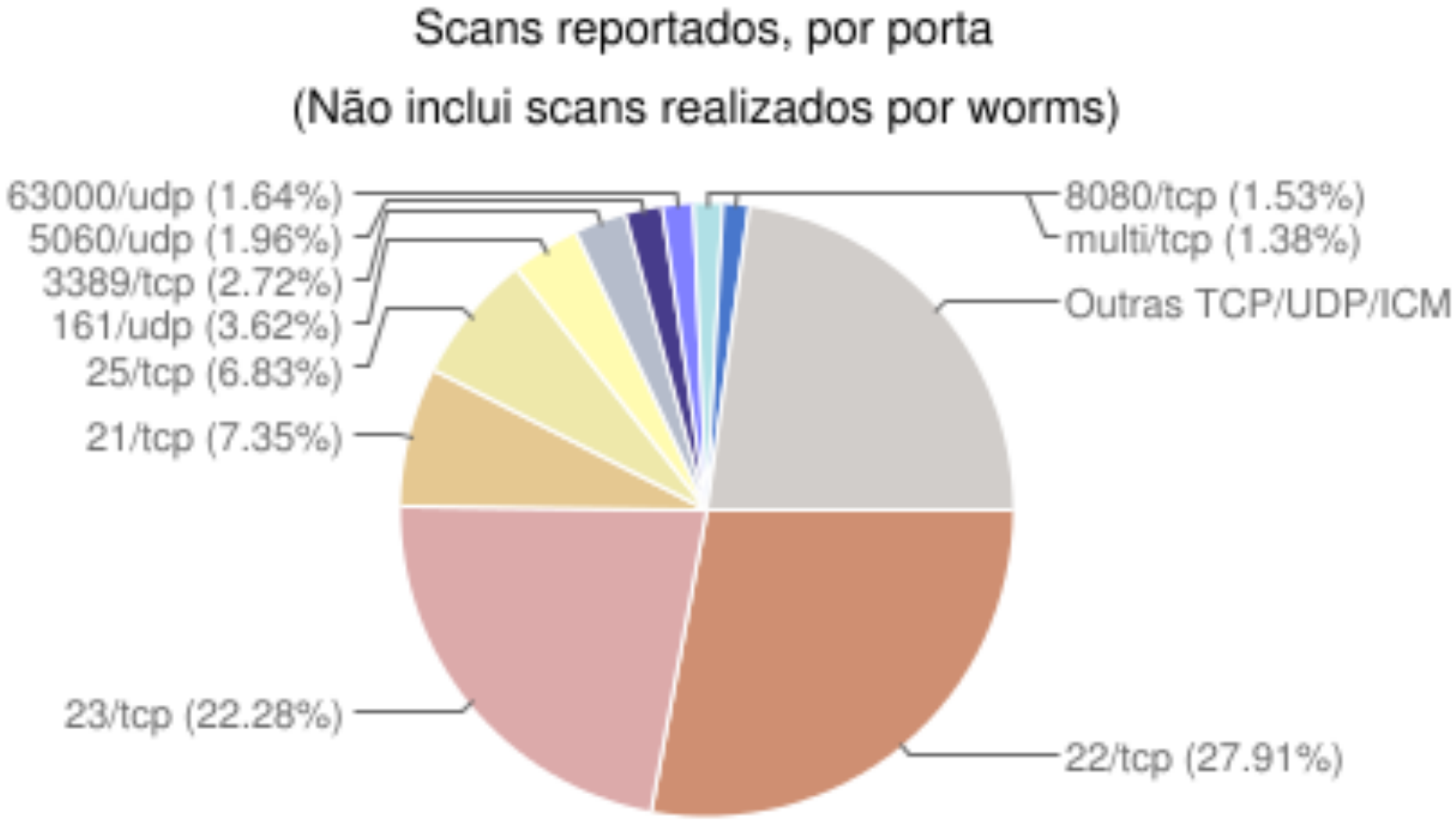
Estatísticas CERT.br – 1999 a 2015



Estatísticas CERT.br – 2015
Incidentes reportados



Estatísticas CERT.br – 2015
Scans reportados

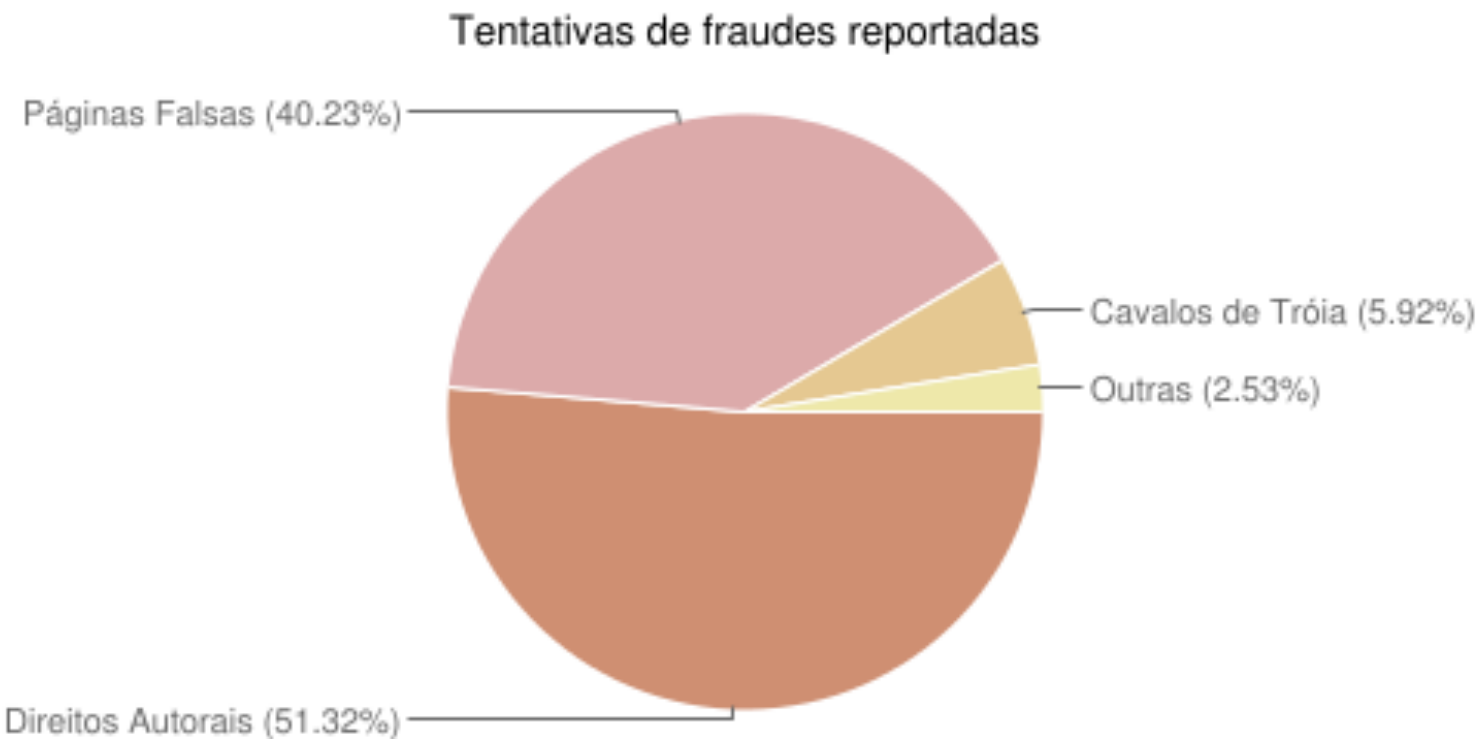


Estatísticas CERT.br
Scans reportados

- **Ataques:**
  - tentam explorar senhas fracas ou padrão
  - foco em dispositivos com versões “enxutas” de Linux
    - para sistemas embarcados
    - arquiteturas ARM, MIPS, PowerPC

Evolução de *scans* porta 23/TCP em % de todos os *scans* reportados	
2013	**3%**
2014	**10%**
2015	**22%**
2016	
01	**34%**
02	**32%**
03	**16%**
04	**56%**
05	**48%**
06	**65%**

Estatísticas CERT.br – 2015
Tentativas de fraudes reportadas



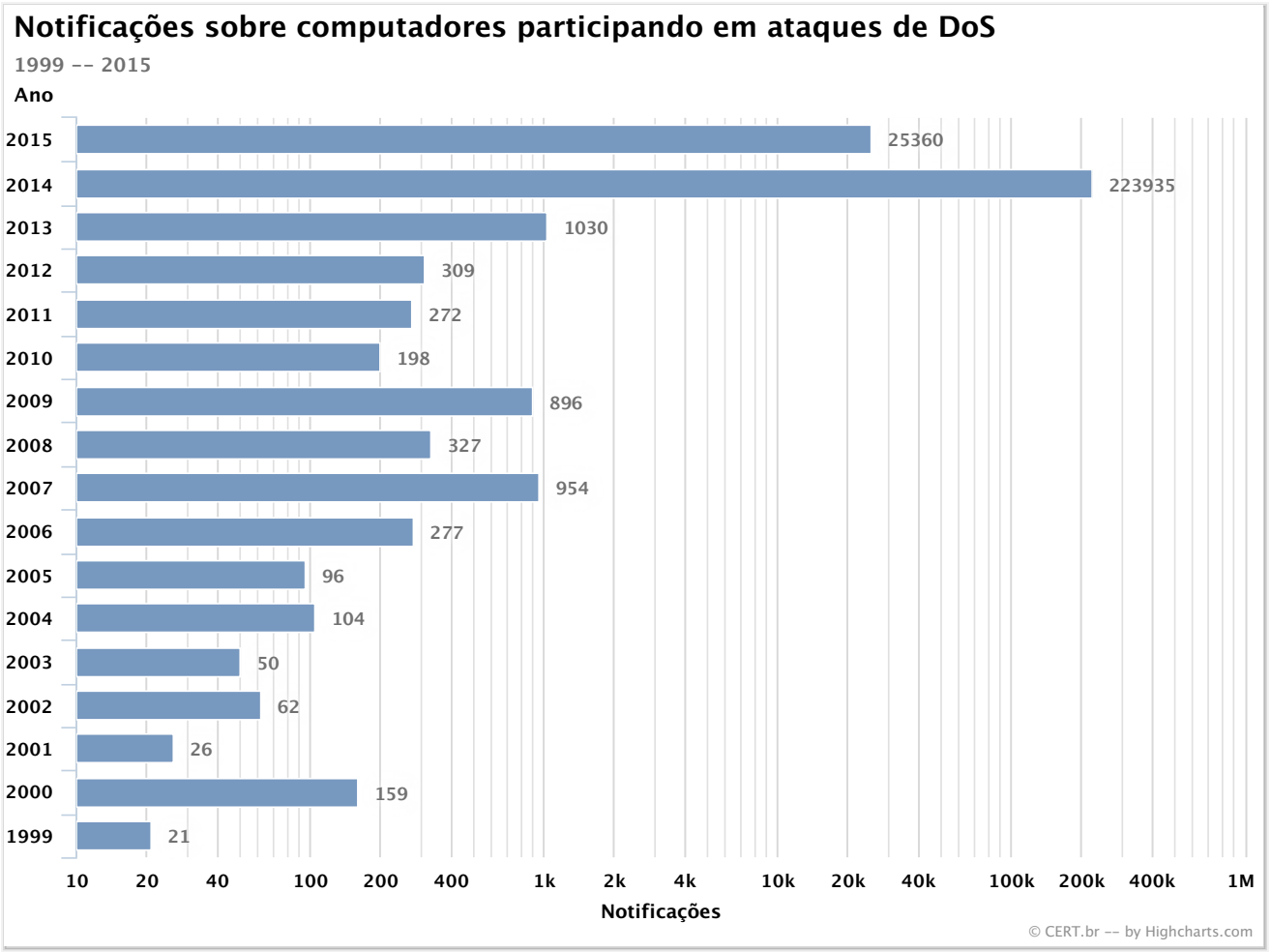
Malware

- **RAT e *ransomware* em amplo uso**
- **"*Government Grade Malware for the Masses*"**
  - vazamento do *Hacking Team*, código fonte disponível para atacantes
  - código multiplataforma: "Windows, Windows Phone, Windows Mobile, Mac OSX, iOS, Linux, Android, BlackBerry OS, and Symbian"
- **Novos *malwares* sendo desenvolvidos**
  - difíceis de serem detectados por antivírus
  - difíceis de serem simulados em *sandboxes*
    - necessitam de condições específicas
- **Grande mercado de *zero-days***

Fantom Ransomware Encrypts your Files while pretending to be Windows Update

http://www.bleepingcomputer.com/news/security/fantom-ransomware-encrypts-your-files-while-pretending-to-be-windows-update/

Estatísticas CERT.br – 1999 a 2015
Ataques DDoS



DDoS

- **Ataques com amplificação são triviais**
  - serviços UDP permitindo abuso
    - SNMP, SSDP, DNS recursivo aberto
- **Ataques dificilmente são menores que 50Gbps**
  - vários ocorrendo no Brasil
  - internacionalmente DD4BC e *Collective Armada* atacando instituições financeiras, realizando extorsão com pagamento via *bitcoin*
- ***Botnets* compostas de:**
  - *desktops*, servidores *Web*, dispositivos móveis, CPEs, CCTVs, raio X, etc.
- **Mitigação é realmente difícil**
  - técnicas de mitigação tem que levar em conta questões de privacidade e possibilidade de descarte de tráfego legítimo

Tendências e desafios

cert.br nic.br cgi.br

IoT

- **Cada vez mais equipamentos/sistemas conectados**
- **Falta de cuidados de segurança**
  - no projeto, implementação e adoção
  - dificuldade de atualização de sistemas
    - lâmpadas Phillips Hue LED:
      - criptografia fraca permite descobrir senha do Wi-Fi
      - vulnerabilidades permitem controlar remotamente
    - TVs Samsung:
      - mandam o som ambiente para a sede
    - TVs LG:
      - enviam nomes de arquivos, filmes e *drives* de rede
    - carros da Fiat Chrysler:
      - controle dos veículos via 3G/4G, explorando vulnerabilidades do Uconnect
    - aviões:
      - potencialmente vulneráveis via sistemas de entretenimento
    - dispositivos médicos

BBC | Sign in | News | Sport | Weather | Shop | Earth | Travel | M

NEWS

Home | Video | World | UK | Business | Tech | Science | Magazine | Entertainment & Arts

Technology

Osram Lightify light bulbs 'vulnerable to hack'

27 July 2016 | T

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

The flaws in the Lightify products could give attackers access to a home wi-fi network, and potentially operate the lights without permission.

Osram said a "majority" of the problems would be fixed in a software update in August, but four remained unpatched.

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

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

Thousands of medical devices are vulnerable to hacking, security researchers say

The security flaws put patients' health at risk

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

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.

Advisory (ICSA-15-161-01)

More Advisories

Hospira Plum A+ and Symbiq Infusion Systems Vulnerabilities

Original release date: June 10, 2015 | Last revised: June 12, 2015

STACK-BASED BUFFER OVERFLOW[b]

The researcher has evaluated the device and asserts that the device contains a buffer overflow vulnerability that could be exploited to allow execution of arbitrary code on the device. This vulnerability has not been validated by Hospira. However, acting out of an abundance of caution, ICS-CERT is including this information to enhance healthcare providers' awareness, so that additional monitoring and controls can be applied.

CVE-2015-3955[c] has been assigned to this vulnerability. A CVSS v2 base score of 7.6 has been assigned; the CVSS vector string is (AV:N/AC:H/Au:N/C:C/I:C/A:C).[d]

IMPROPER AUTHORIZATION[e]

The communication module gives unauthenticated users root privileges on Port 23/TELNET by default. An unauthorized user could issue commands to the pump.

CVE-2015-3954[f] has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).[g]

INSUFFICIENT VERIFICATION OF DATA AUTHENTICITY[h]

The device accepts drug libraries, firmware updates, pump commands, and unauthorized configuration changes from unauthenticated devices on the host network. The device listens on the following ports: Port 20/FTP, Port 23/TELNET, Port 80/HTTP, Port 443/HTTPS, and Port 5000/UPNP. Hospira has not validated claims of firmware updates and pump commands for Plum A+ and Plum A+3 from unauthorized devices on the host network.

Roteadores Domésticos - CPEs

- **CPEs vistos como "Coisas"**
  - ninguém assume responsabilidade por configuração e atualização
- **Enorme base vulnerável**
  - sem instalação de *patches*
  - configurações padrão de fábrica com serviços com senha padrão, serviços como telnet habilitados, etc
- **Usados para todos os tipos de ataque**
  - *botnets* para DDoS e mineração de *bitcoins*
  - comprometimento para alteração de DNS
    - pode levar a ataques: *phishing*, *malware*, falsos boletos
- **Servidores DNS maliciosos hospedados em serviços de *hosting*/*cloud***
  - casos com mais de 30 domínios de redes sociais, serviços de *e-mail*, buscadores, comércio eletrônico, cartões, bancos

NEWS

Update: Malware-infected home routers used to launch DDoS attacks

Researchers found a botnet of more than 40,000 routers being used to launch the attacks

The researchers said they don't believe the routers were hacked through a vulnerability in their firmware, but because they had been deployed in an insecure manner: with their management interfaces exposed to the Internet via SSH and HTTP using default credentials.

In addition to DDoS attacks, compromised routers are used to redirect users to malicious websites, intercept online banking sessions, inject rogue ads into Web traffic, steal credentials for various online accounts and perform other illegal activities.

http://www.computerworld.com/article/2921559/malware-vulnerabilities/malware-infected-home-routers-used-to-launch-ddos-attacks.html

CCTV/DVR

- **Hospedando *phishing***
- **Utilizado para desferir ataques DDoS**
  - porta telnet com senha padrão
- **Dificuldade do usuário em entender o problema**
  - “Mas aqui não tem Internet”
  - “É só uma câmera”
- **Solução adotada pelo usuário**
  - troca de número IP

Imperva, Inc.

CCTV Botnet In Our Own Back Yard | Incapsula.com

IMPERVA INCAPSULA

PRODUCTS ENTERPRISE PARTNERS BLOG

The Incapsula Blog

21 CCTV Botnet In Our Own Back Yard

Attack Details

As noted, this assault consisted of HTTP GET floods that peaked at around 20,000 RPS, with its traffic originating from roughly 900 CCTV cameras spread around the globe. Their target was a rarely-used asset of a large cloud service, catering to millions of users worldwide.

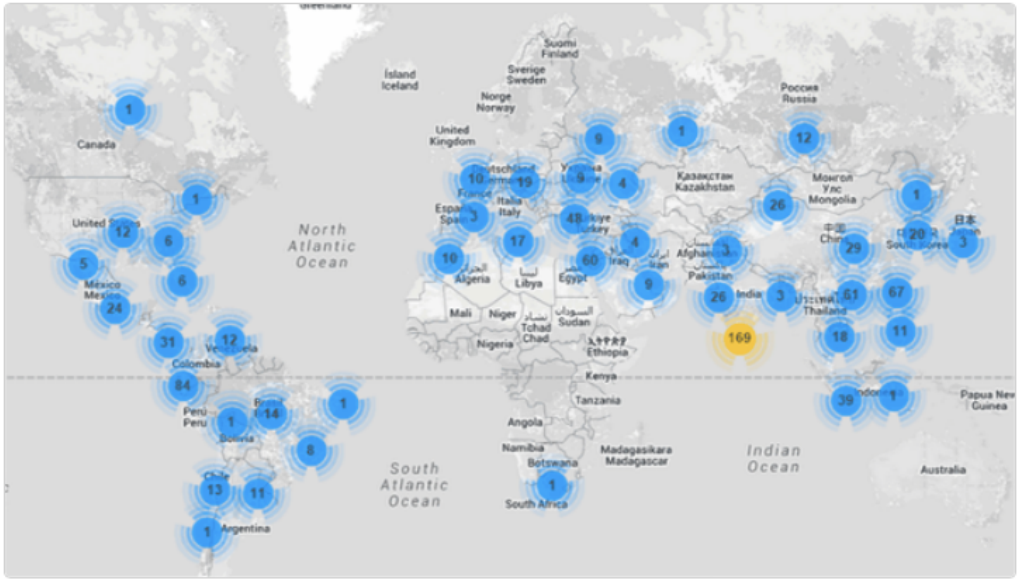


Figure 1: Geo-location of botnet devices

Fonte: https://www.incapsula.com/blog/cctv-ddos-botnet-back-yard.html

Best Buy faces criminal investigation for pornography on display TV

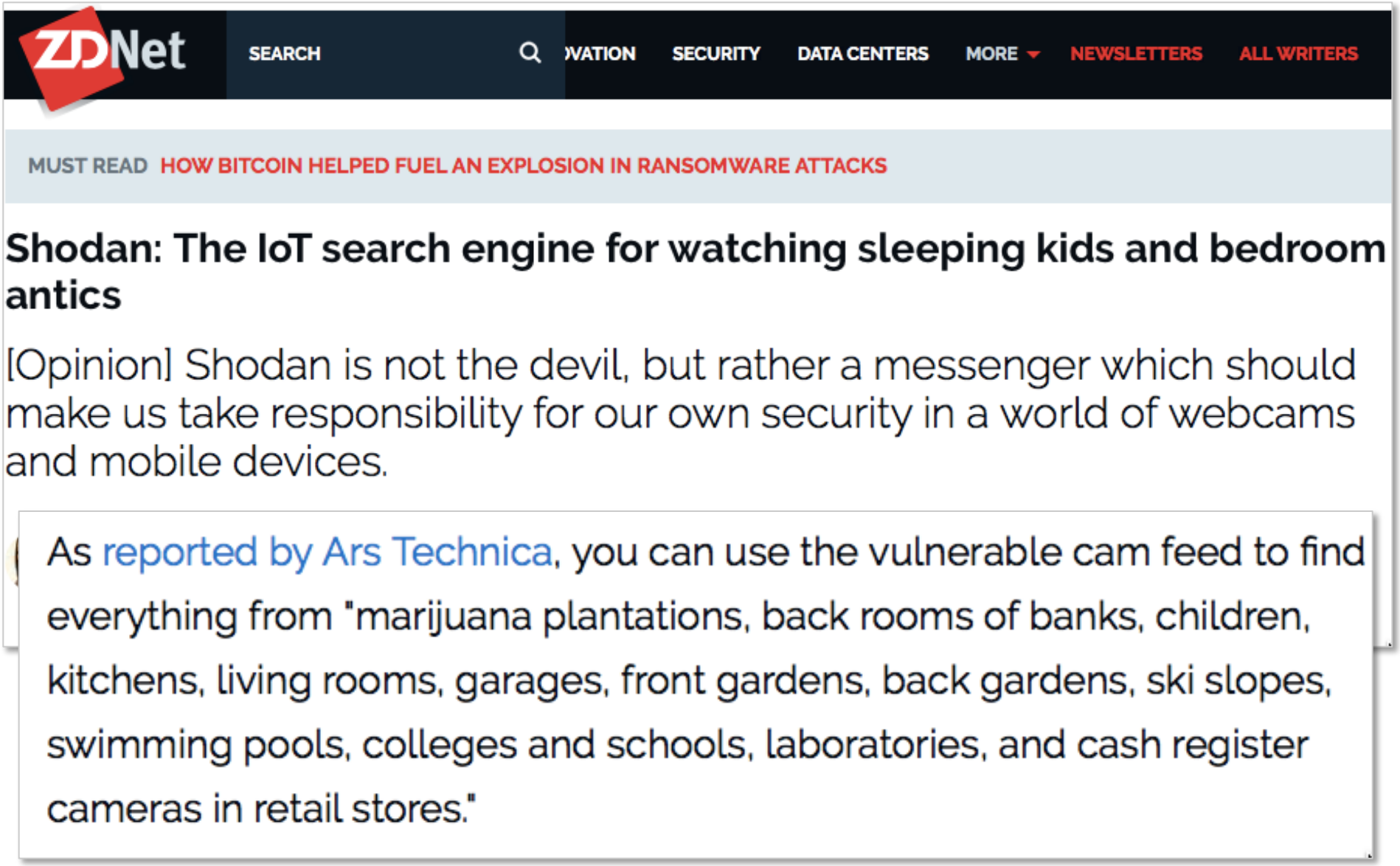
22

Mark Raby - Feb 23, 2012

Twitter | Facebook 30 | Google | Reddit

Best Buy has apologized for the fact that pornography managed to show up on a 55-inch TV in its store two days in a row. The retailer said it did not know who was responsible for the salacious content, but said it was due to someone hacking into the store's Wi-Fi network. One shopper was quoted as describing the images that appeared on the screen as "extremely, extremely pornographic." A police report was even filed by an offended customer.

http://www.slashgear.com/best-buy-faces-criminal-investigation-for-pornography-on-display-tv-23215075/



http://www.zdnet.com/article/shodan-the-iot-search-engine-which-shows-us-sleeping-kids-and-how-we-throw-away-our-privacy/

Tendência de [In]segurança

- **P&D não vai se preocupar com segurança**
- **Prioridade é baixo custo**
  - de *hardware*
  - de contratação de desenvolvedores
- **Politicas de atualização são inexistentes**
  - a politica em geral é “comprar outro”
  - em casos como o das TVs Digitais com Ginga:
    - os desenvolvedores são taxativos: “não dá pra fazer update ‘pelo ar’ ”
  - mas cogita-se ter serviços como *Internet Banking* via o espectro alocado para a TV

Precisamos um ecossistema mais saudável

Nenhum único grupo ou estrutura conseguirá fazer sozinho a segurança

Todos possuem um papel

Precisamos um ecossistema mais saudável

- **Administradores de redes e sistemas**
  - não emanar “sujeira” de suas redes e adotar boas práticas
    - implementar BCP38 (http://bcp.nic.br/) e gerência de porta 25
  - notificar usuários sobre infecções e indícios de comprometimento
  - fazer *hardening* das máquinas
- **Usuários**
  - entender os riscos e seguir as dicas de segurança
  - manter seus dispositivos atualizados e tratar infecções
- **Desenvolvedores**
  - pensar em segurança desde o início
  - pensar nos casos de ABUSO (o ambiente é HOSTIL)
- **Acadêmicos**
  - incluir conceitos de programação segura logo nos primeiros anos

Cabe a vocês demandar segurança

- **Não assuma que "é seguro" só porque uma empresa de segurança (física?) disse que é**
  - Ex: câmeras de segurança, monitores de bebês, etc
- **Assuma que o fabricante/desenvolvedor:**
  - não pensou em ataques pela Internet
  - não pensou em *update* de *firmware*
  - não tem pessoal especializado em segurança
    - Ex: que entenda de autenticação, desenvolvimento seguro, cripto, etc
  - vai reutilizar código vulnerável

Obrigada

www.cert.br

miriam@cert.br

@certbr

01 de setembro de 2016

nic.br cgi.br

www.nic.br | www.cgi.br