nic.br cgi.br | cert.br

Latinoware 2016

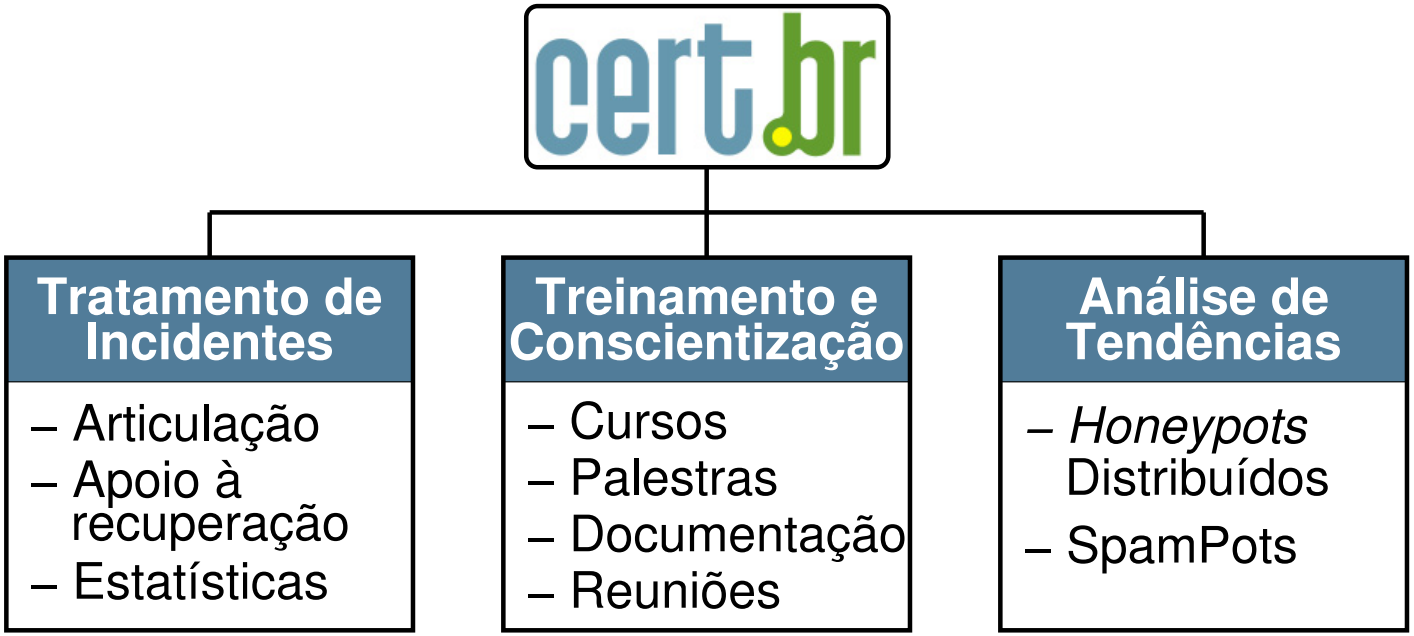
Foz do Iguaçu, PR

20 de outubro de 2016

Segurança em IoT: Novos desafios, velhos problemas

Miriam von Zuben
miriam@cert.br

cert.br nic.br cgi.br



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

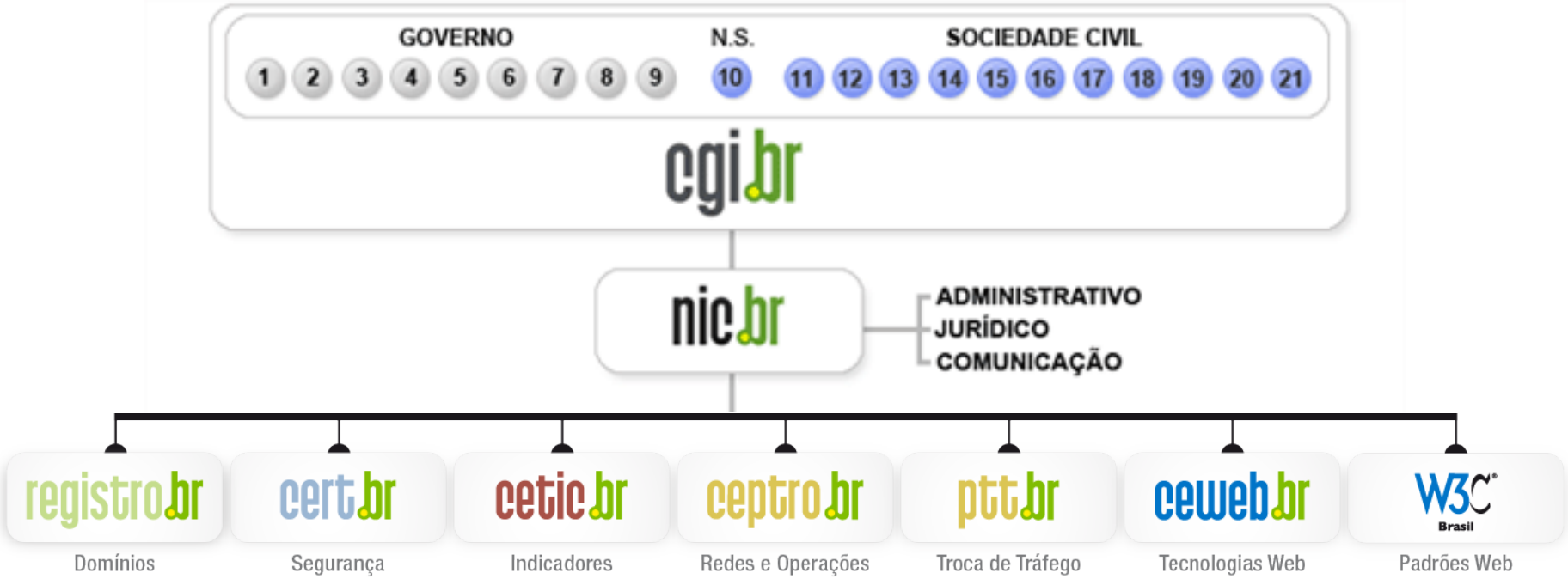
The Honeynet PROJECT

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**

Rumo a Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil
http://www.nic.br/grupo/historico-gts.htm | http://www.cert.br/sobre/

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

Comitê Gestor da Internet no Brasil – CGI.br

Entidade multissetorial, criada em 1995, responsável por coordenar e integrar as iniciativas e serviços da Internet no País.

Dentre as atribuições definidas no Decreto Presidencial nº 4.829, de 03 de setembro de 2003, destacam-se:

- **a proposição de normas e procedimentos relativos à regulamentação das atividades na internet;**
- **a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil;**
- **o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil;**
- **a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país;**
- **a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>;**
- **a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.**
- **ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet;**

http://www.cgi.br/sobre/

Velhos problemas...

cert.br nic.br cgi.br

620Gbps contra o Blog do Brian Krebs

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

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/

Source code of Mirai botnet responsible for Krebs On Security DDoS released online

Now anyone can use the IoT-based botnet for their own destructive purposes.

By Charlie Osborne for Zero Day | October 3, 2016 -- 08:43 GMT (01:43 PDT) | Topic: Security

The source code for the botnet which disrupted Krebs On Security has been published online, leading to fears that the botnet will soon be used by practically anyone to flood the internet with powerful -- and expensive -- attacks.

This month, security expert Brian Krebs' blog, Krebs On Security, was struck with one of the largest distributed denial-of-service (DDoS) attacks on record.

Europol

At 620 Gbps, Akamai engineers were able to repel the attack, but the company -- which gave Krebs a home pro-bono -- was forced to let him go as a "business decision" since keeping the blog and weathering more DDoS attacks could have ended up costing the business a fortune.

The botnet responsible is based on malware called Mirai. The malicious code utilizes vulnerable and compromised Internet of Things (IoT) devices to send a flood of traffic against a target.

In this case, the DDoS attack included SYN Floods, GET Floods, ACK Floods, POST Floods, and GRE Protocol Floods.

http://www.zdnet.com/article/source-code-of-mirai-botnet-responsible-for-krebs-on-security-ddos-released-online/

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

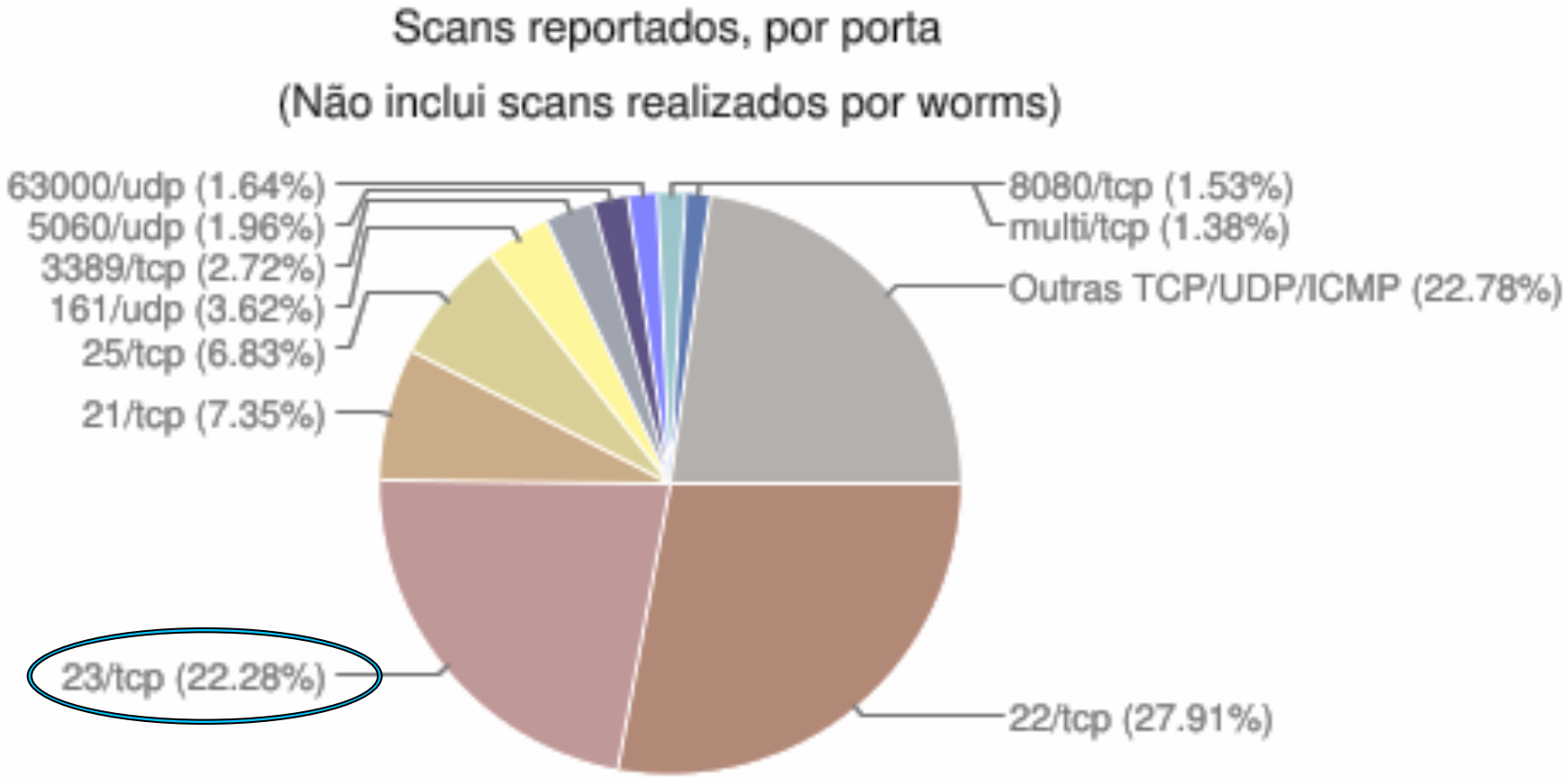
Problema:
telnet e senhas fracas

cert.br nic.br cgi.br

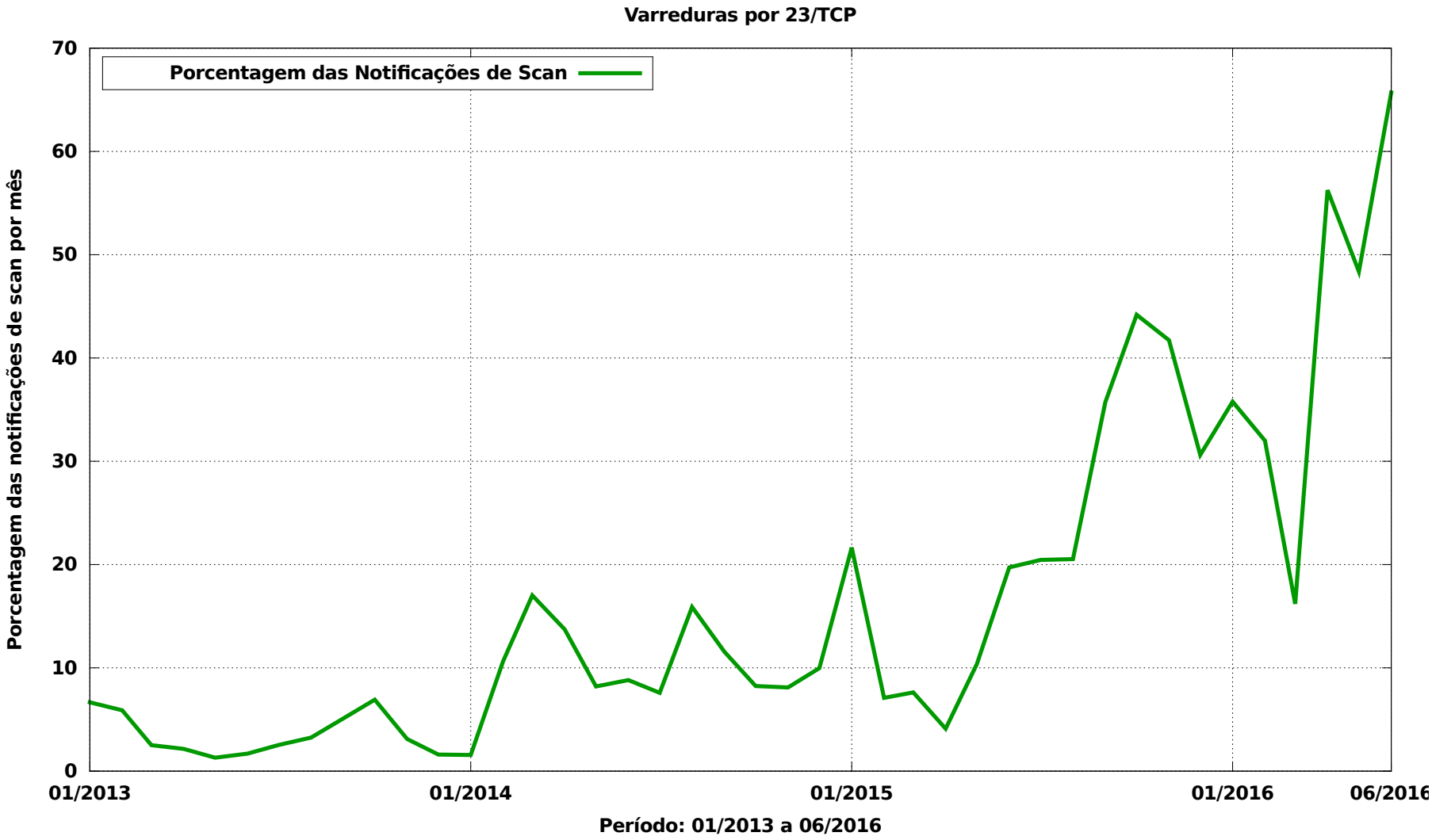
IoT *botnets*

- **CPEs, DVRs, CCTVs, NAS, roteadores domésticos, etc**
- ***Malware* se propaga geralmente via telnet**
- **Explora senhas fracas ou padrão**
  - muitas vezes são "*backdoors*" dos fabricantes
- **Em nossos honeypots**
  - IPs de IoT infectados – 18/10/2016
    - BR: 81.986
    - NOTBR: 470.545

Notificações ao CERT.br:
***Scans* por porta em 2015**



Notificações ao CERT.br:
Scans por 23/TCP – 2013 a jun/2016



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.

cert.br nic.br cgi.br

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.

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

Problema:
dados sensíveis armazenados em texto claro

cert.br nic.br cgi.br

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

Problema: *backdoor* e senhas facilmente descobertas

cert.br nic.br cgi.br

kb.cert.org

CERT | Software Engineering Institute | Carnegie Mellon University

Vulnerability Notes Database

Ad

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

Print Tweet Send Share

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.

Problema:
DRDos e endereços spoofados

cert.br nic.br cgi.br

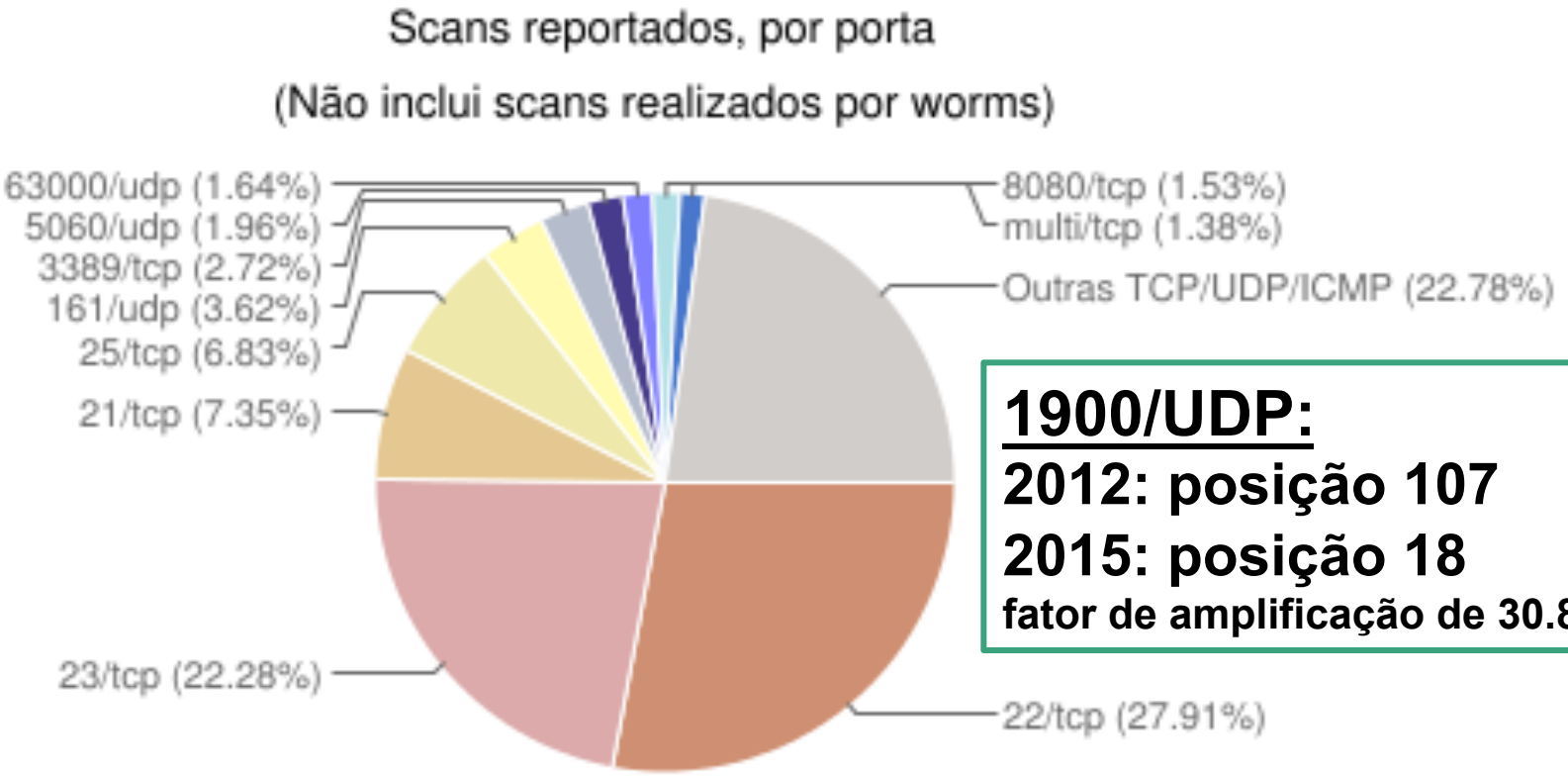
Report: IoT-Connected Devices Leading to Rise in SSDP-based Reflection Attacks

NSFOCUS Report States Online Gaming and Entertainment Sectors Continue to be High on the Target List and Attackers Are Becoming More Sophisticated

SAN FRANCISCO – April 21, 2015 (RSA, Moscone Center, Booth #832) – NSFOCUS released its bi-annual DDoS Threat Report today, revealing new attack findings and rising threats that organizations should be aware of throughout 2015. As the tide of distributed denial-of-service (DDoS) attacks continues to expand, the rise of the Internet of Things (IoT) and the influx of network connected devices, such as webcams and routers, are leading to the growth of Simple Service Discovery Protocol (SSDP)-based amplification attacks. To download the entire report, visit http://www.nsfocus.com/2015/SecurityReport_0416/196.html

http://www.darkreading.com/attacks-breaches/report-iot-connected-devices-leading-to-rise-in-ssdp-based-reflection-attacks-/d/d-id/1320149

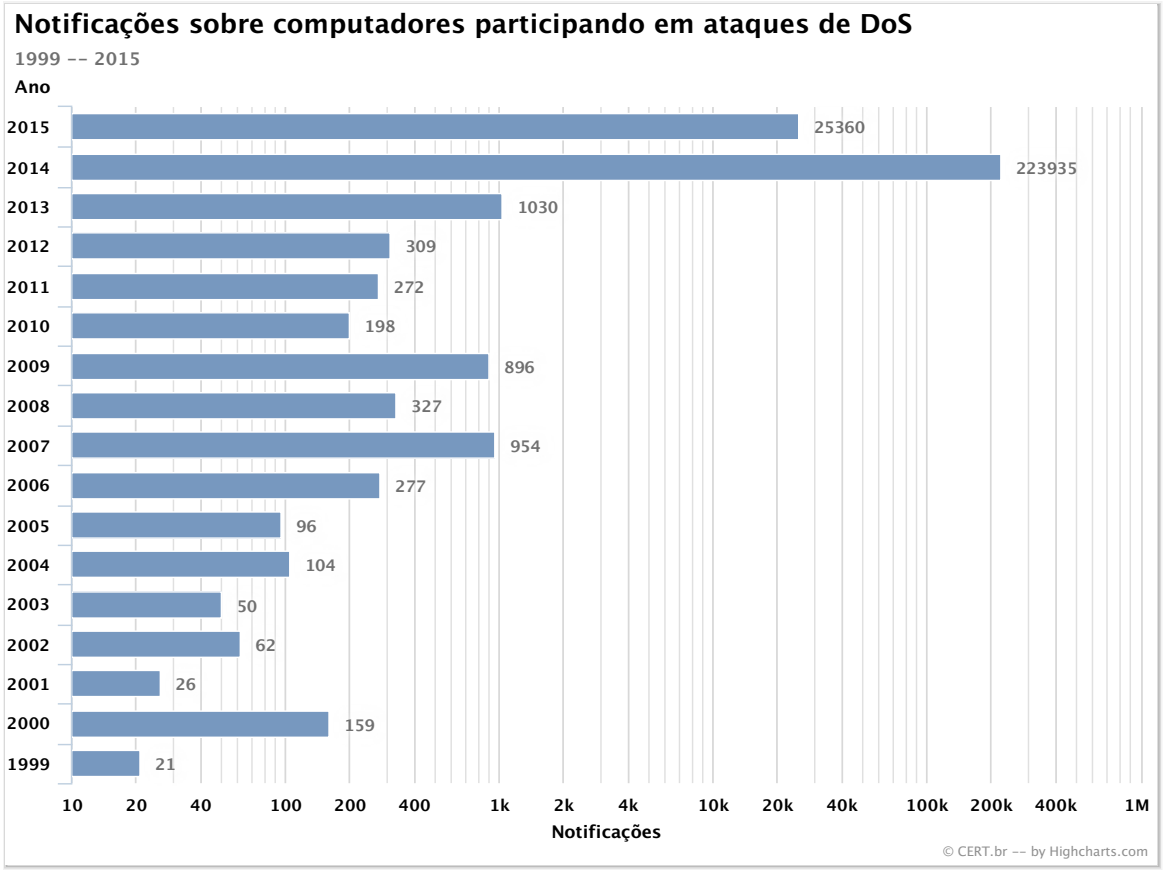
Estatísticas CERT.br – 2015



1900/UDP:
2012: posição 107
2015: posição 18
fator de amplificação de 30.8

Tipos de ataques DDoS
Volumétrico – DRDoS

- **Serviços UDP permitindo abuso**
  - SNMP, SSDP, DNS recursivo aberto, entre outros



Problema:
malware

cert.br nic.br cgi.br

Hackers Make the First-Ever Ransomware for Smart Thermostats

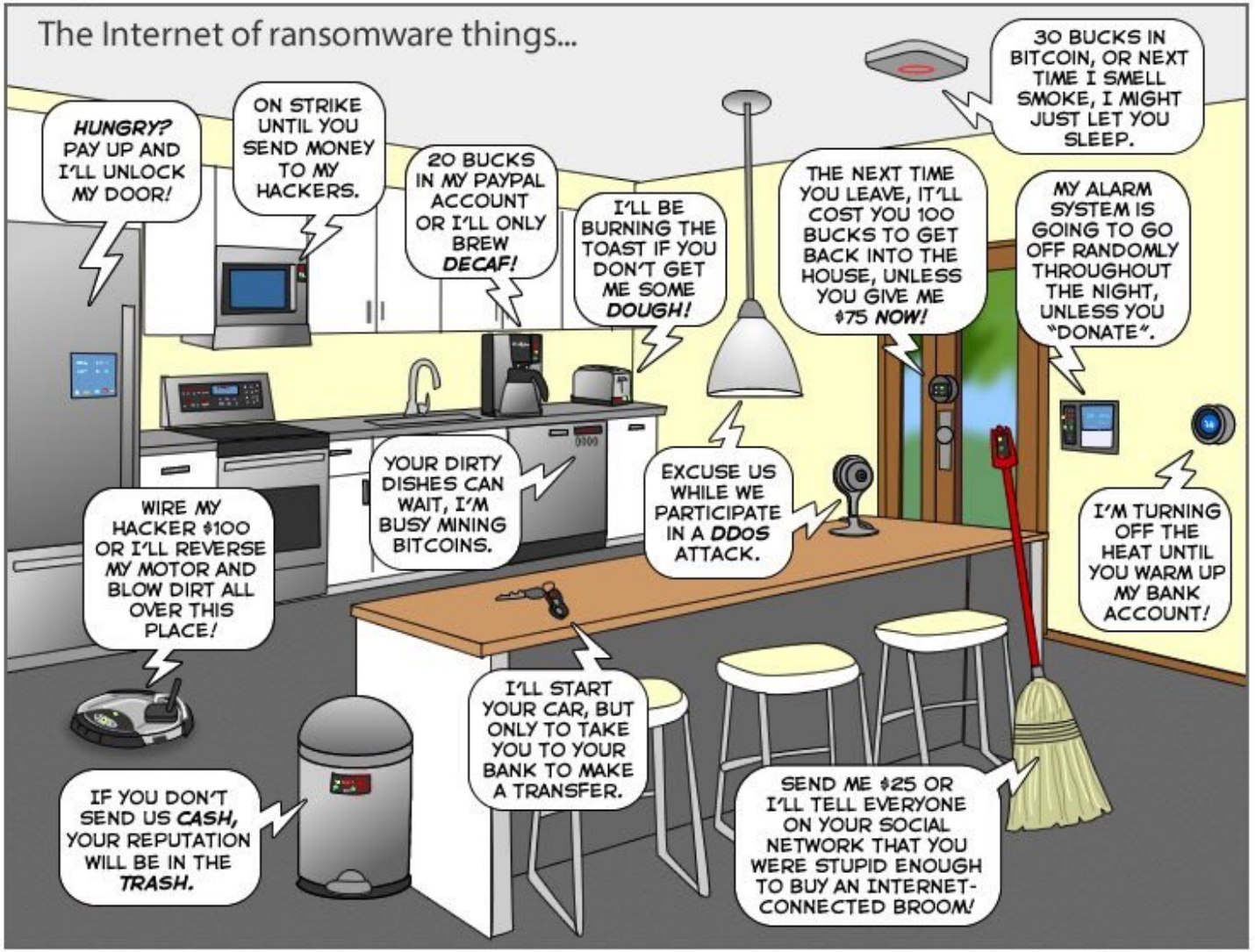
August 7, 2016 // 10:00 AM EST

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

Desafios

cert.br nic.br cgi.br

Como melhorar o cenário

- **Solução depende de diversas camadas**
  - usuários
  - desenvolvedores
  - administradores
  - fabricantes

Usuários (1/2)

- **Assumir que os dispositivos virão com sérios problemas**
  - necessário fazer *hardening*
  - testar em ambiente controlado
  - assumir que terá um "*backdoor*" do fabricante

- **Considerar uma rede de gerência**
  - isolar os dispositivos completamente

- **Antes de comprar**
  - verificar se o fabricante possui política de atualização de *firmware*

Usuários (2/2)

- **Ao fazer a implantação, planejar**
  - se haverá algum esquema de gerência remota
  - como atualizar remotamente
- **Ser criterioso ao escolher o fornecedor**
  - fazer testes, identificar qual o *chipset*, verificar histórico de tratamento de vulnerabilidades do fabricante do *chipset*, etc
- **Dificuldades de fazer análise / perícia**

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
- **Deve ser incluída na analise de risco das empresas**
  - danos à imagem
  - danos aos usuários
- **Como implementar segurança em larga escala**
- **Ter grupo de resposta a incidentes preparado para lidar com os problemas**

Obrigada

www.cert.br

miriam@cert.br

@certbr

20 de outubro de 2016

nic.br cgi.br

www.nic.br | www.cgi.br