nic.br cgi.br | cert.br

Workshop de Infraestrutura: “Encontro com o Futuro”

FIESP

21 de outubro de 2019 – São Paulo/SP

Segurança no Contexto da Hiperconectividade

Dra. Cristine Hoepers
Gerente Geral, CERT.br
cristine@cert.br

cert.br nic.br cgi.br

cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Tratamento de Incidentes	Treinamento e Conscientização	Análise de Tendências
▶ Articulação	▶ Cursos	▶ *Honeypots* Distribuídos
▶ Análise Técnica	▶ Palestras	▶ SpamPots
▶ Apoio à recuperação	▶ Boas Práticas	▶ Processamento de *threat feeds*
	▶ Reuniões	

Criação:

Agosto/1996: o relatório "Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil" é publicado pelo CGI.br[1]

Junho/1997: o CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório[2]

[1] https://www.nic.br/grupo/historico-gts.htm | [2] https://www.nic.br/pagina/gts/157

Missão

Aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

Governança

Mantido pelo **NIC.br** – Núcleo de Informação e Coordenação do .br

- todas as atividades são sustentadas pelo registro de domínios .br

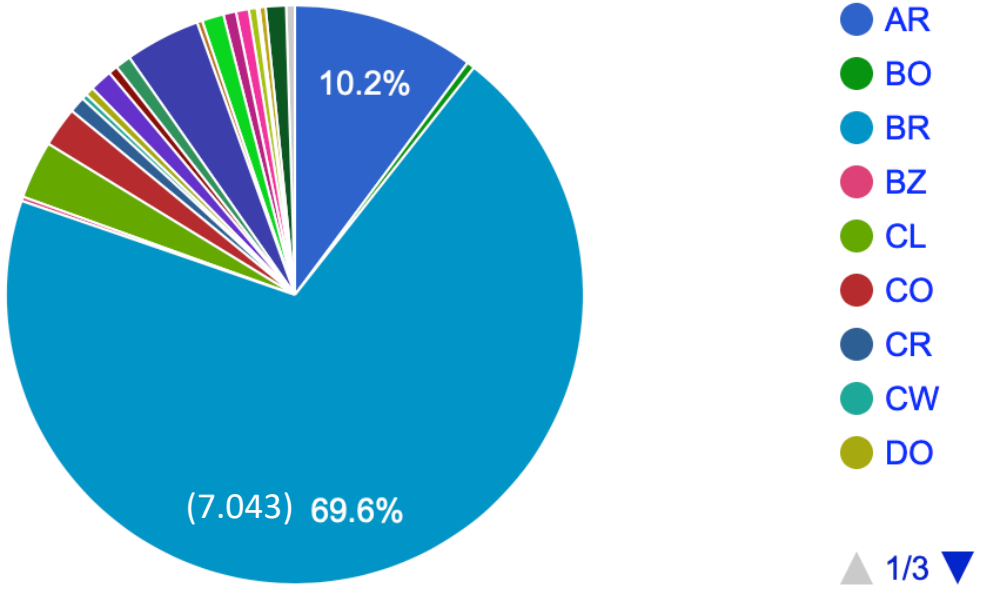
O NIC.br é o **braço executivo do CGI.br** – Comitê Gestor da Internet no Brasil

- entidade multissetorial
  - governo, empresas, terceiro setor e comunidade científica e tecnológica
- **responsável por coordenar e integrar as iniciativas e serviços da Internet no País**

https://cert.br/sobre/

Internet no Brasil em Números:
Redes Autônomas, Provedores e Interconexão de Tráfego

Alocação de Sistemas Autônomos na América Latina e Caribe



Fonte: https://www.lacnic.net/en/web/lacnic/estadisticas-asignacion

Provedores de Acesso

- Total de ISPs (estimado): 6.618
- Respondentes: 2.177
- 75% tem 1.000 clientes ou menos

Fonte: https://www.cetic.br/pesquisa/provedores/

Interconexão de tráfego

IX.br São Paulo - um dos maiores *Internet eXchanges* do mundo

- nº 1 em participantes (1.724)
- nº 3 em tráfego
  - média (4Tbps) e pico (6Tbps)

Fonte: https://www.pch.net/ixp/dir

Internet no Brasil em Números:
Usuários e Dispositivos Utilizados

Organização das Nações Unidas para a Educação, a Ciência e a Cultura

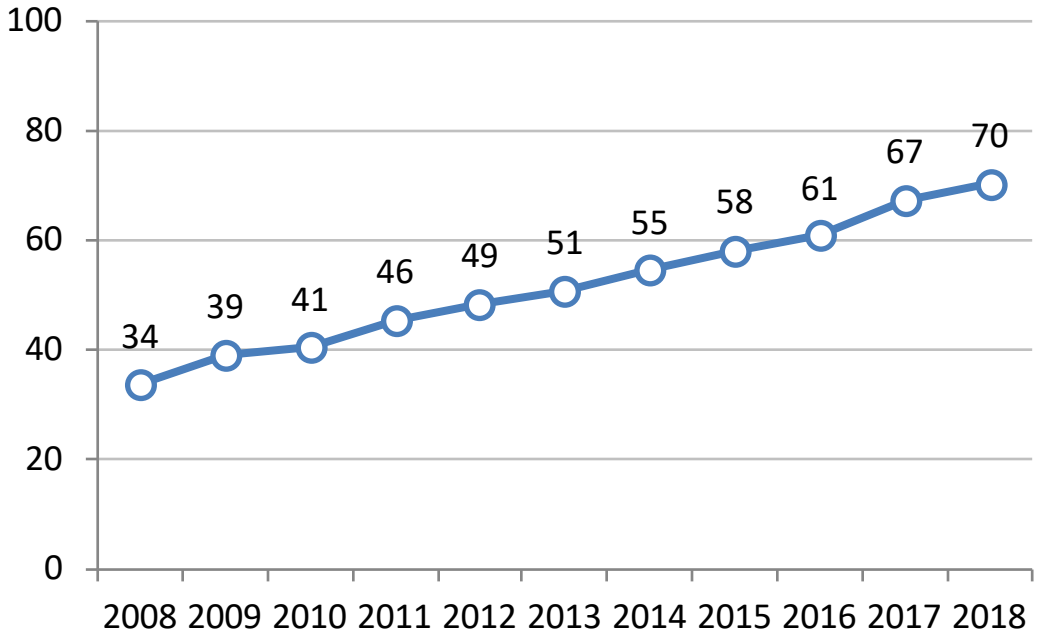
Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação sob os auspícios da UNESCO

Núcleo de Informação e Coordenação do Ponto BR

Comitê Gestor da Internet no Brasil

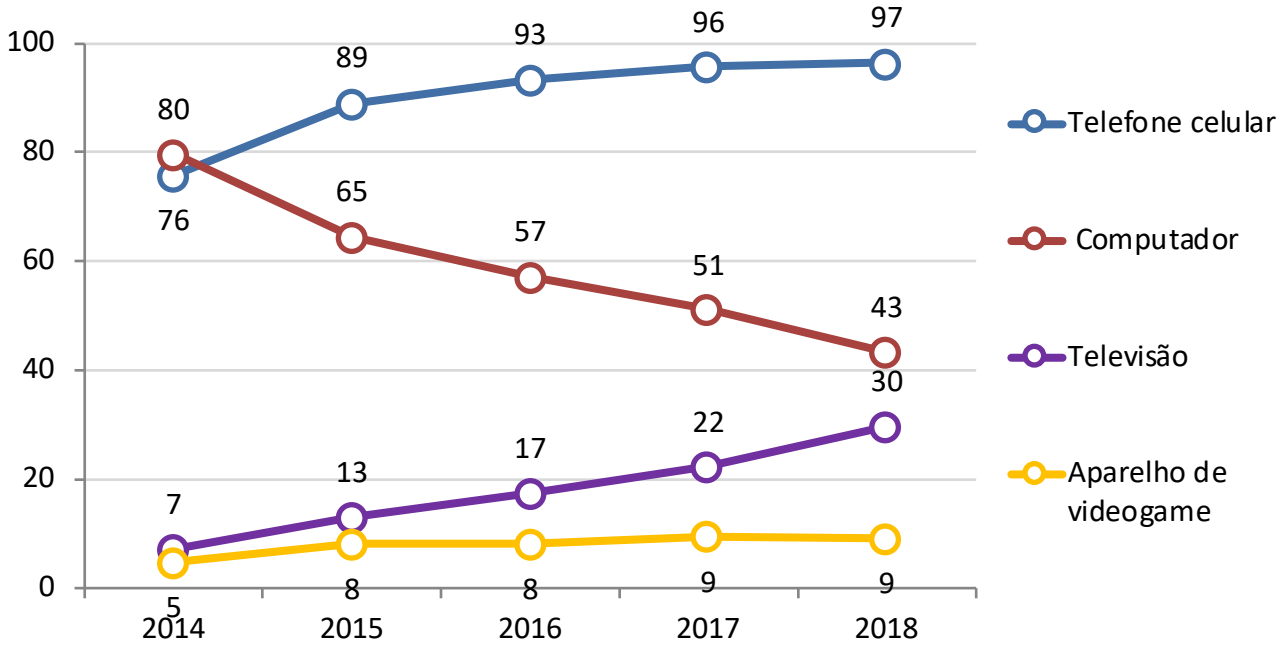
Usuários de Internet

Porcentagem do total da população



Dispositivo Utilizado para Acesso Individual

Porcentagem do total de usuários de Internet

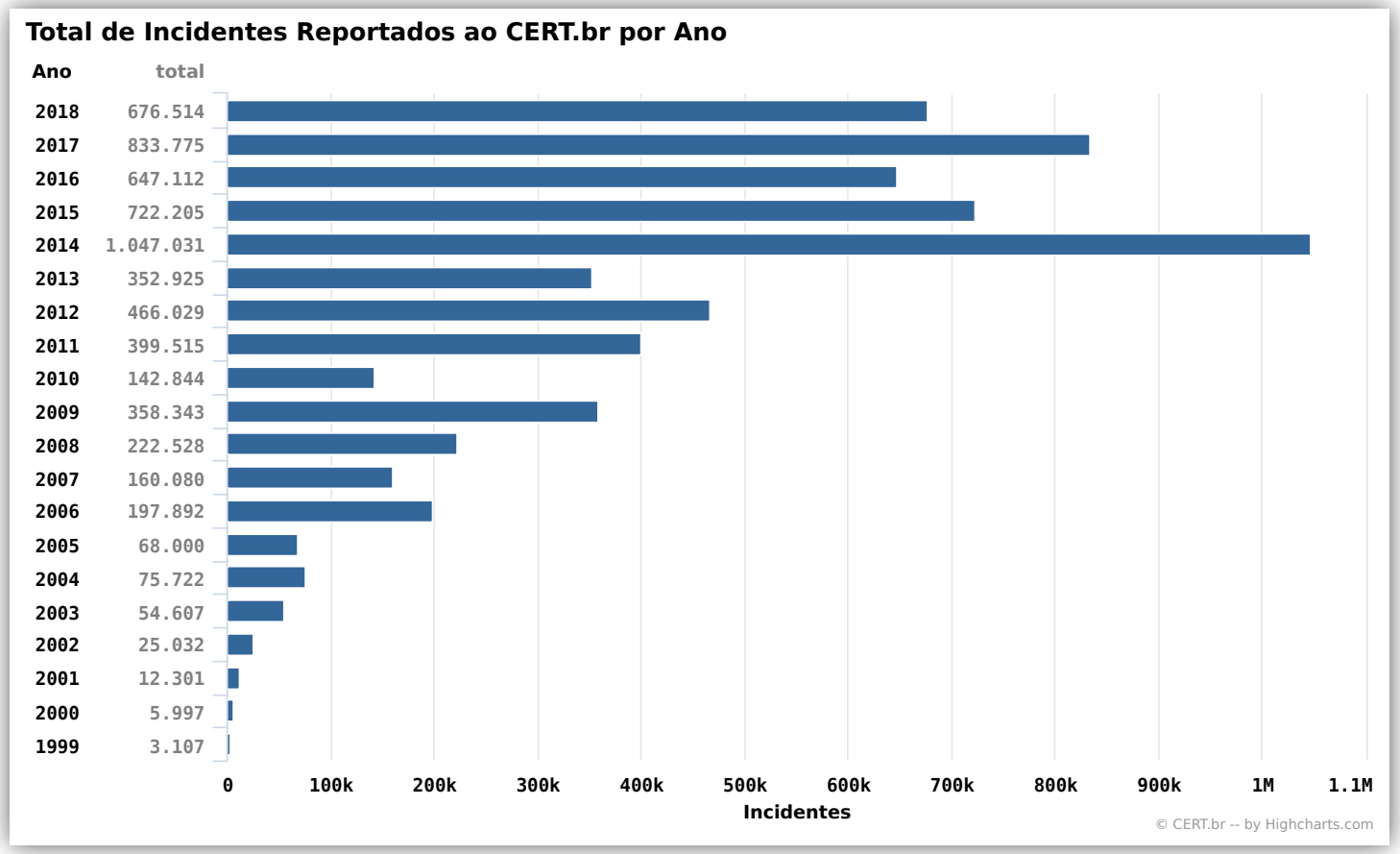


126,9 milhões de usuários de Internet

(utilizaram a Internet há menos de 3 meses)

Fonte: CGI.br/NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nos Domicílios Brasileiros – TIC Domicílios 2018.
https://www.cetic.br/pesquisa/domicilios/indicadores

Incidentes Reportados Voluntariamente para o CERT.br: **Dados Totais de 1999 a 2018**



Ataques mais comuns contra os cidadãos no último ano

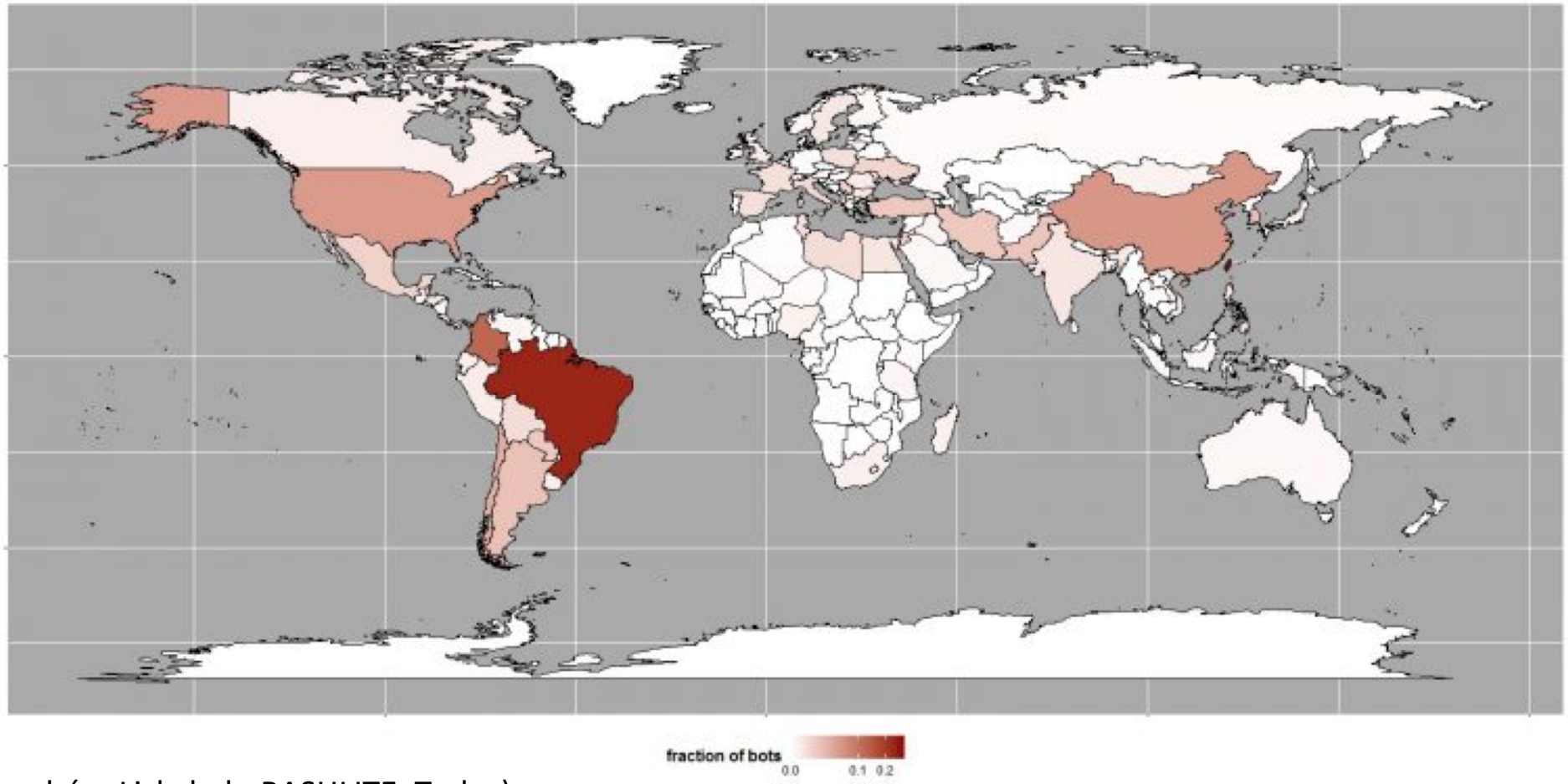
- Internet das coisas
  - Câmeras, *Smartphones*, Roteadores e *Modems* de banda larga/Wi-Fi, TVs
  - Infectados e sendo usados para
    - minerar criptomoedas
    - atacar terceiros
    - fazer fraudes contra os usuários
- Tentativas de fraude
  - Financeira e de comércio eletrônico
    - via *e-mails* falsos
    - via infecção de computadores, celulares e roteadores de banda larga

Fonte: https://www.cert.br/stats/incidentes/

"Those who don't study history are doomed to repeat it. Yet those who *do* study history are doomed to stand by helplessly while everyone else repeats it."

Fonte:
http://imgc-cn.artprintimages.com/images/P-473-488-90/90/9031/84KB500Z/posters/tom-toro-those-who-don-t-study-history-are-doomed-to-repeat-it-yet-those-who-do-s-cartoon.jpg

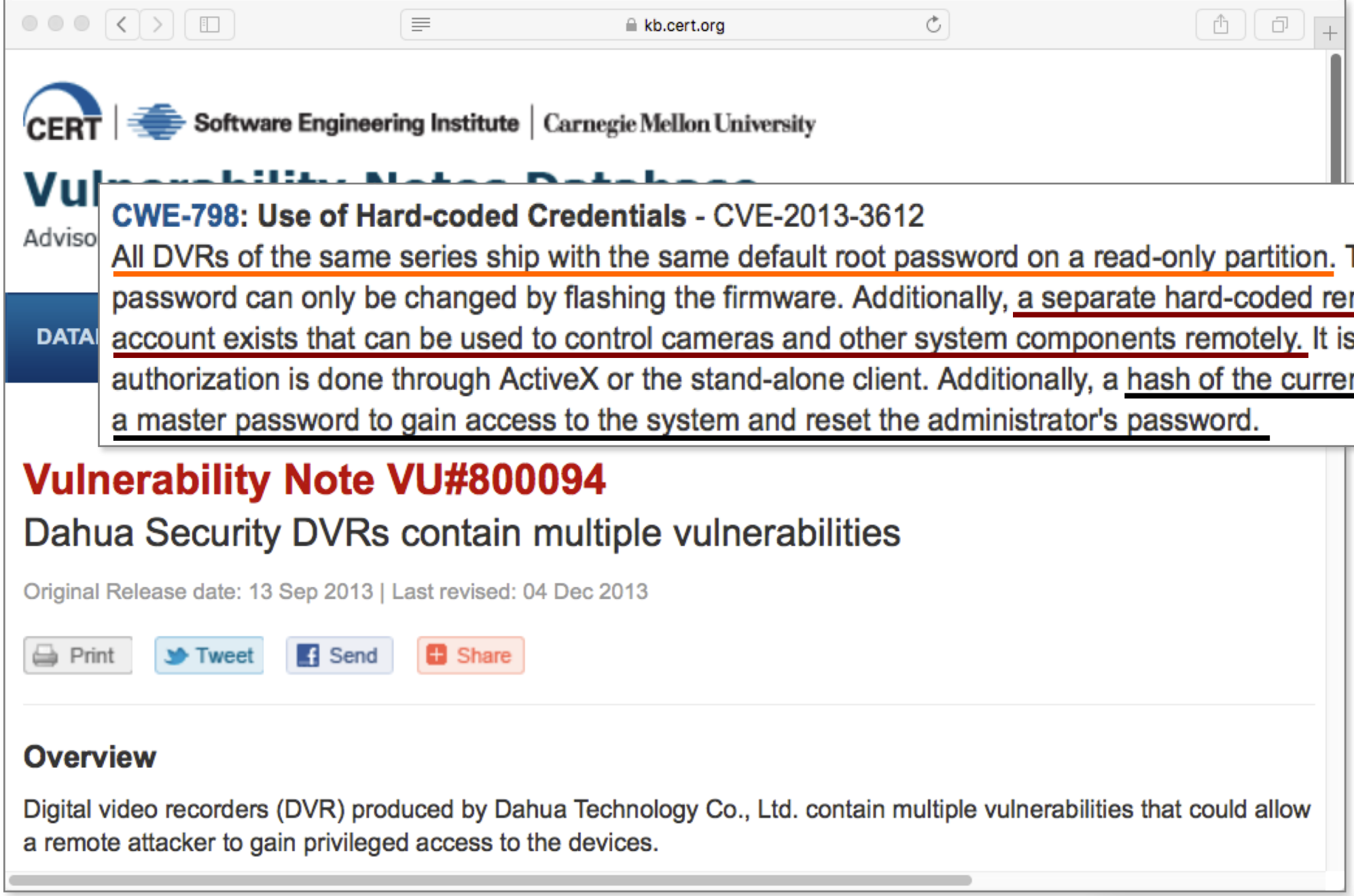
Distribuição Global da botnet IoT mais antiga sendo monitorada **Afeta DVRs e Câmeras de Segurança**



Botnet gafgyt (ou também Lizkebab, BASHLITE, Torlus)

Fonte: Level3 – Estatísticas da distribuição global de origem de ataques DDoS a partir de câmeras infectadas, 25 de agosto de 2016

http://blog.level3.com/security/attack-of-things/


kb.cert.org
CERT | Software Engineering Institute | Carnegie Mellon University
Vul
Adviso
DATA
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.

Setembro/2016, **Mirai** é identificada e também infecta DVRs e Câmeras: **Usada contra Blog do Brian Krebs e Maiores Serviços Online**

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

The sound of silence.

BBC NEWS

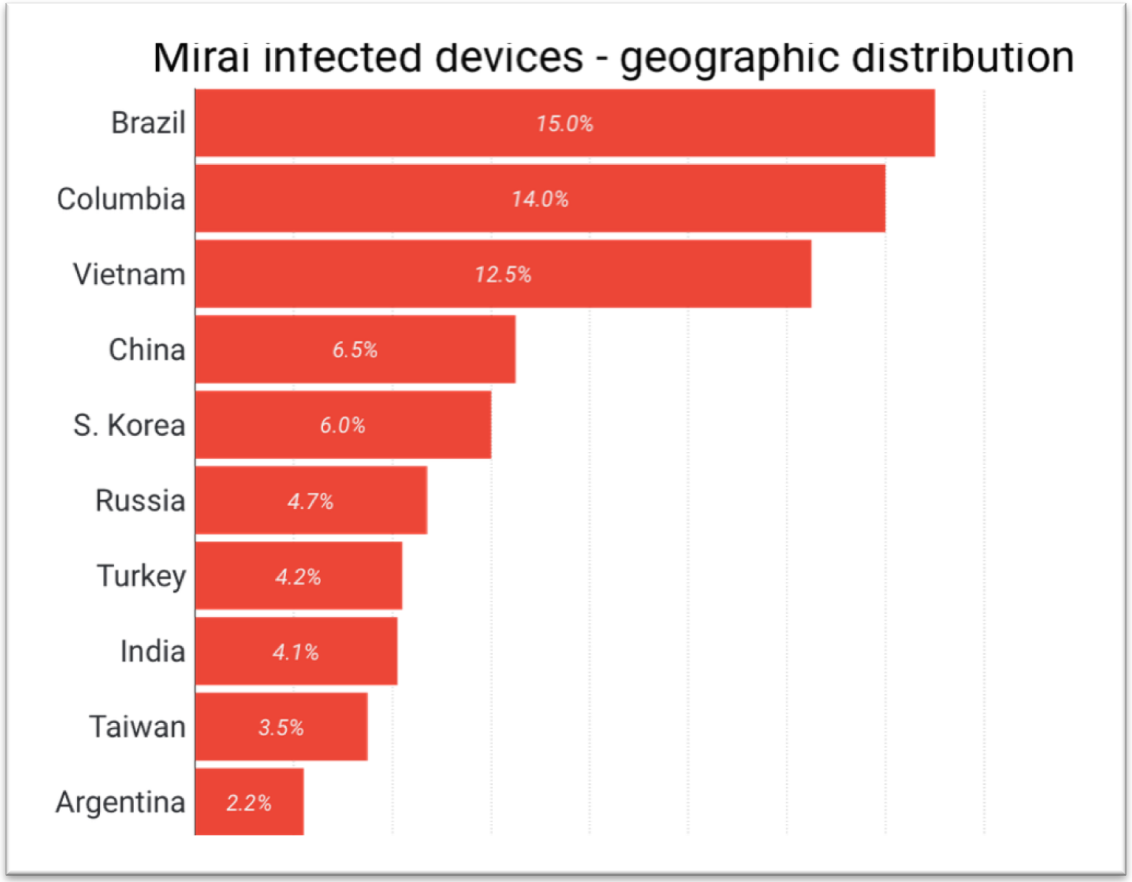
Massive web attack hits security blogger

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.

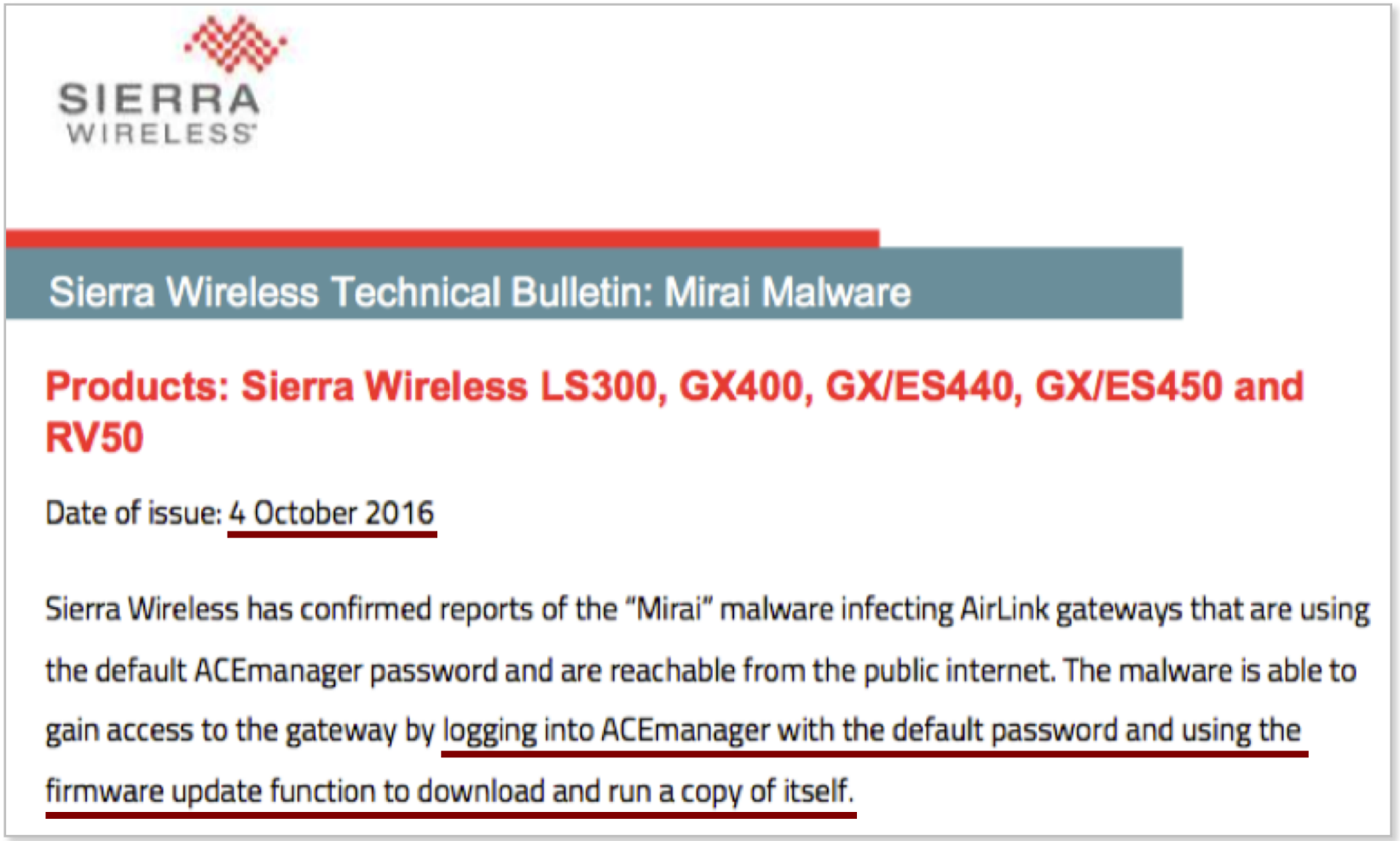


http://www.bbc.co.uk/news/amp/37439513
http://www.pcworld.com/article/3133847/internet/ddos-attack-on-dyn-knocks-spotify-twitter-github-etsy-and-more-offline.html
https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/

Sierra Wireless:
Seus Roteadores 4G-WiFi também são afetados pela Mirai

Utilizados em:

- gasodutos
- oleodutos
- semáforos
- iluminação pública
- *smart grids*
- carros de polícia
- ambulâncias



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/

OUR BRANDS

EPOCH TIMES

International

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

The YouTube video ISIS was spreading alongside the online camera feeds shows how to take control of security cameras by using a basic cyberattack. The attack lets the terrorists change a camera's password, and gain deeper access to its system controls. Using this method, they can then control the cameras remotely.

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

DC police surveillance cameras were infected with ransomware before inauguration

Malware seized 70 percent of DC police DVRs a week before Trump's inauguration.

SEAN GALLAGHER - 1/30/2017, 5:12 PM

system just one week before Inauguration Day. *The Washington Post* reports that 70 percent of the DVR systems used by the surveillance network were infected with ransomware, rendering them inoperable for four days and crippling the city's ability to monitor public spaces.

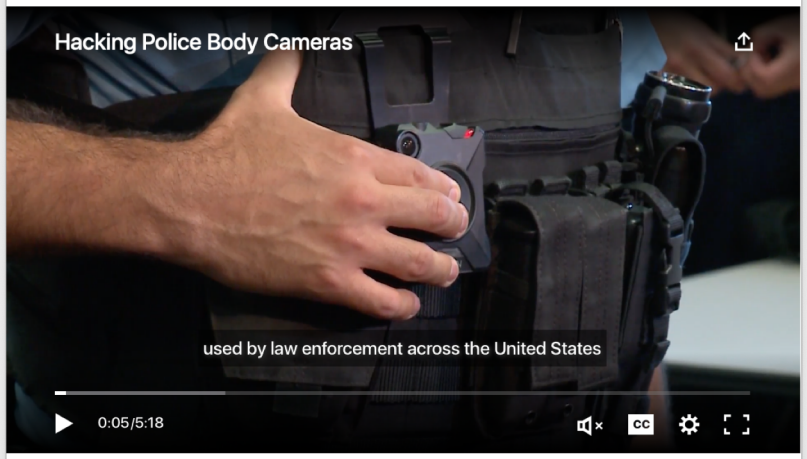
wired.com

WIRED BUSINESS CULTURE GEAR MORE SUBSCRIBE

LILY HAY NEWMAN SECURITY 08.11.2018 03:00 PM

Police Bodycams Can Be Hacked to Doctor Footage

Analysis of five body camera models marketed to police departments details vulnerabilities could let a hacker manipulate footage.



As they proliferate, police body cameras have courted controversy because of the contentious nature of the footage they capture and questions about how accessible those recordings should be.

But when it comes to the devices themselves, the most crucial function they

3 FREE ARTICLES LEFT THIS MONTH Subscribe

https://arstechnica.com/security/2017/01/dc-police-surveillance-cameras-were-infected-with-ransomware-before-inauguration/
https://www.wired.com/story/police-body-camera-vulnerabilities/

Vulnerabilidades em IoT:
O que chama mais atenção

Todos repetem os erros do passado – leia-se dos anos 80/90

- falta de autenticação
  - quando tem, são senhas fracas
- protocolos sem criptografia
- "*backdoors*" dos fabricantes são a norma
  - usualmente senhas padrão, que não podem ser alteradas (*hardcoded*), nem as contas desabilitadas

Segurança não é prioridade

- mesmo em dispositivos de segurança!

Raríssimos fabricantes consideram ciclo de atualizações de segurança (*patches*/*updates*)

- o que inclui maior parte dos fabricantes de *smartphones, que* não fornecem *updates*, ou restringem a disponibilidade para o mercado da América Latina

Desenvolvedores / Fabricantes Precisam Priorizar Segurança

Atualização precisa fazer parte do ciclo de vida

- deve ser possível atualizar dispositivos IoT
- necessário prever algum mecanismo de autenticação

Necessário ter grupo de resposta a incidentes com produtos (PSIRT) preparado para lidar com os problemas

Planejar atualizações de segurança em larga escala

Desafio adicional em IoT: Um *chipset* ➔ diversos "fabricantes"

- Ex.: Dentre os fabricantes nacionais de câmeras, temos encontrando somente *chipsets* Dahua e Xiongmai
- Como atualizar? *Recall* consegue ser efetivo? (vide caso Xiongmai)

Exemplo do Impacto da Falta de Atualização:
Entrada de Smartphones no Horário de Verão Ontem

Mesmo sem horário de verão, celulares adiantam relógio em uma hora

Redes de telefone atualizaram dispositivos automaticamente; horário de verão foi suspenso por um decreto presidencial em abril

Redação, O Estado de S.Paulo
20 de outubro de 2019 | 07h39
Atualizado 20 de outubro de 2019 | 08h26

Na manhã deste domingo, 20, parte da população foi surpreendida pela atualização errônea do **horário de verão** em celulares e outros dispositivos. O horário foi atualizado automaticamente pelas operadoras de telefonia, já que o horário de verão começava tradicionalmente no terceiro final de semana de outubro, na madrugada entre sábado e domingo.

https://brasil.estadao.com.br/noticias/geral,mesmo-sem-horario-de-verao-celulares-adiantam-relogio-em-uma-hora,70003056921

O que provavelmente ocorreu foi falta de atualização: **Arquivo de Fusos Horários é Essencial – Nota do Google**

Trabalhando para a melhor experiência em seu Android

sexta-feira, outubro 18, 2019

Nos últimos dois anos, o governo brasileiro realizou alterações no horário de verão. Inicialmente, a data de início passou do terceiro domingo de outubro para o primeiro domingo de novembro e, recentemente, foi assinado um decreto que determinou o fim da mudança.

Todas essas modificações impactam diretamente no Banco de Dados Global da IANA (em português, Autoridade para Atribuição de Números de Internet), que é utilizado por smartphones e dispositivos eletrônicos para garantir que você esteja sempre na hora certa, onde quer que esteja.

Na prática, isso significa que alguns celulares possivelmente não tenham a informação necessária para evitar que o relógio dos aparelhos seja alterado automaticamente como se o horário de verão ainda estivesse valendo.

Para não correr o risco de perder compromissos, você pode definir a hora manualmente antes da meia noite do domingo, dia 20 de outubro, data em que começaria o horário de verão.

https://brasil.googleblog.com/2019/10/trabalhando-para-melhor-experiencia-em.html

```
Release 2019b - 2019-07-01 00:09:53 -0700

  Briefly:
    Brazil no longer observes DST.
    'zic -b slim' outputs smaller TZif files; please try it out.
    Palestine's 2019 spring-forward transition was on 03-29, not 03-30.

  Changes to future timestamps

    Brazil has canceled DST and will stay on standard time indefinitely.
    (Thanks to Steffen Thorsen, Marcus Diniz, and Daniel Soares de
    Oliveira.)
```

https://data.iana.org/time-zones/tzdb/NEWS

Para os aparelhos que não forem impactados no dia 20 de outubro, existe a possibilidade de que a mudança automática aconteça no dia 3 de novembro, já que a regra mudou em 2018. Nesse caso, valem as mesmas recomendações dadas acima, ou seja, na noite anterior, você pode definir manualmente a hora do seu smartphone.

Caso seu telefone não sofra nenhuma alteração de horário em nenhuma das duas datas, isso significa que o aparelho já foi atualizado pelos fabricantes ou, então, está seguindo as regras de rede da sua operadora (elas usam as antenas para enviar informações como a hora certa, por exemplo).

Atualização de Dispositivos:
Regulações e "Regras de Mercado" vs Segurança

hello android

I've had an iPhone for many years, and an iPad
should switch to Android. I thought they were
know they are crazy. Some notes on recent exp

moto g6

I was looking to get Google Fi's phone service
should work with several phones, the website s
model, so that's the one I got. If Google recom

After turning on, it starts applying security updates. Good. One month at a time. There are many months. This is bad. Why can't it install all the updates? Finally it stops, with January's update. It is no longer January. I'm stuck at Android 8.0 January 2019 Security Patch. I manually check for updates again, and again, but my phone insists it is up to date. I do not like Android. Android is a liar.

Somehow it seems this is related to my phone being set to the retla channel and not the retus channel. I'm not in Latin America, I barely even know Latin, so surely I can switch to the US channel? Haha, of course not. We can't let the poors get access to the good updates.

I suppose this is really my fault for not spending enough time, not doing enough research, not reading enough forums to buy the correct phone. Maybe some people are just too stupid to deserve a good phone.

On the whole, not impressed.

Update: after several months of lying to me about being up to date, I took my phone to Miami. No sooner did I disable airplane mode, I had a notification telling me a system update was available. Apparently Miami is closer enough to Latin America I'm allowed to get updates there.

Posted 01 Jun 2019 18:21 by tedu Updated: 05 Sep 2019 11:28 – https://flak.tedunangst.com/post/hello-android

Segurança é Papel de Todos:
Ecossistema é Complexo e Interdependente

Quase tudo é *software* e está conectado à Internet

- Empresas “tradicionais” agora são empresas de *software*

Ataques são constantes

- Motivações diversas
- Volume crescente
  - ferramentas facilitam a perpetração por atacantes não especializados

Organizações precisam

- Operar mesmo sob ataque
- Estar preparadas para lidar com estes ataques

Melhora do cenário depende de cada ator fazer sua parte

Construindo um Ecossistema mais Saudável:
Programa por uma Internet mais Segura

PROGRAMA INTERNET +SEGURA

Iniciativa conjunta: NIC.br/CGI.br, ISOC, SindiTelebrasil, Abranet, Abrint e Abinee

https://bcp.nic.br/i+seg

Construindo um Ecossistema mais Saudável: **Portal InternetSegura.br**

Materiais educativos de uso livre, sob licença *Creative Commons*

https://internetsegura.br

Obrigada

cristine@cert.br

Notificações para: cert@cert.br

@certbr

www.cert.br

21 de outubro de 2019

nic.br cgi.br

www.nic.br | www.cgi.br