Live Intra Rede “IoT (Internet das Coisas)”

Lucimara Desiderá, M.Sc. CISSP
Analista de Segurança
CERT.br/NIC.br

03 de setembro de 2025 | Ceptro.br/NIC.br | Evento *Online*

cert.br nic.br cgi.br

The search engine for the Internet of Things

The most shocking of Shodan

SEE FULL GALLERY





"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/

Alerta à População - Câmeras de Segurança

por imprensa — publicado 01/04/2020 15h30, última modificação 02/04/2020 11h21

http://www.pf.gov.br/imprensa/materias_banner/aviso-cameras-de-seguranca

PF descobre invasão de babás eletrônicas e câmeras residenciais

Os investigadores da Unidade de Repressão a Crimes de Ódio e Pornografia Infantil da Polícia Federal já identificaram a invasão de 141 equipamentos na residência de famílias que vivem em 35 municípios do País

Agência Estado
atende.ae@estadao.com

Publicado em 07/04/2020 às 15h15

Uma investigação da Polícia Federal identificou que criminosos estão invadindo dispositivos eletrônicos residenciais em diversas regiões do Brasil. Crédito: Ricardo Medeiros

https://www.agazeta.com.br/brasil/pf-descobre-invasao-de-babas-eletronicas-e-cameras-residenciais-0420

5 March 2025 5 min read

Camera off: Akira deploys ransomware via webcam

CYBER SECURITY

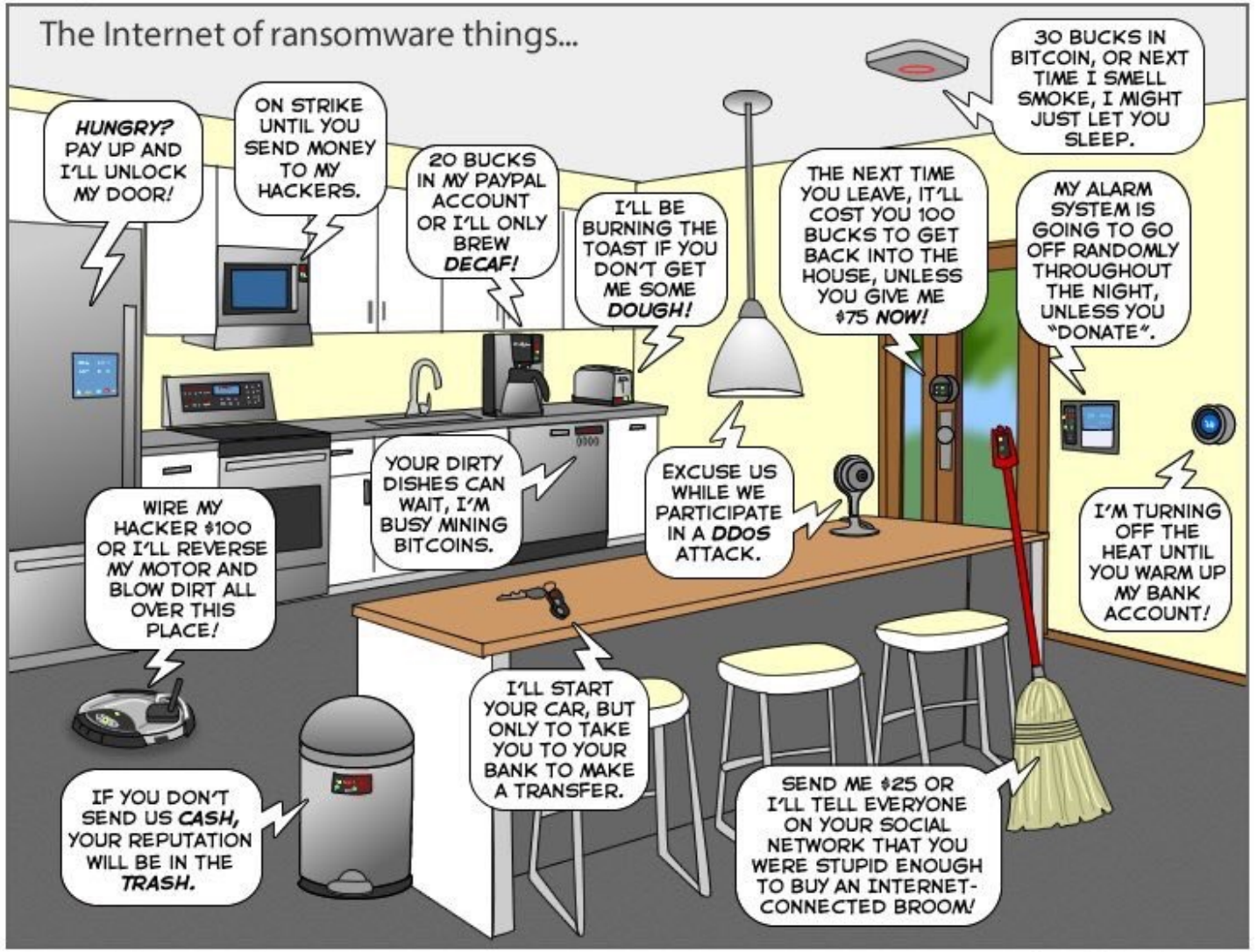
1 The webcam had several critical vulnerabilities, including remote shell capabilities and unauthorised remote viewing of the camera.

2 It was running a lightweight Linux operating system that supported command execution as if it were a standard Linux device, making the device a perfect candidate for Akira's Linux ransomware variant.

3 The device did not have any EDR tools installed on it, leaving it unprotected. In fact, due to the limited storage capacity, it is doubtful that any EDR could be installed at all.

https://www.s-rminform.com/latest-thinking/camera-off-akira-deploys-ransomware-via-webcam

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 Issues Identified in 75% of Infusion Pumps

Posted By Steve Alder on Mar 4, 2022

This week, researchers at Palo Alto's Unit 42 team published a report that shows security gaps and vulnerabilities often exist in smart infusion pumps. These bedside devices automate the delivery of medications and fluids to patients and are connected to networks to allow them to be remotely managed by hospitals.

The researchers used crowdsourced scans from more than 200,000 infusion pumps at hospitals and other healthcare organizations and searched for vulnerabilities and security gaps that could potentially be exploited. The devices were assessed against more than 40 known vulnerabilities and over 70 other IoT vulnerabilities.

75% of the 200,000 infusion pumps were discovered to have security gaps that placed them at an increased risk of being compromised by hackers. Worryingly, 52% of the analyzed devices were found to be vulnerable to two serious infusion pump vulnerabilities dating back to 2019, one of which is a critical flaw with a CVSS severity score of 9.8 out of 10 (Wind River VxWorks CVE-2019-12255), and the other is a high severity flaw with a CVSS score of 7.1 (Wind River VxWorks CVE-2019-12264).

U.S. Food and Drug Administration (FDA) announced **seven recalls for infusion pumps** or their components in 2021, and **nine other recalls in 2020.**

https://www.hipaajournal.com/security-issues-identified-in-75-of-infusion-pumps/
https://unit42.paloaltonetworks.com/infusion-pump-vulnerabilities/

St. Jude Medical drops after Muddy Water findings of 'negligent product design'

PUBLISHED THU, AUG 25 2016•4:43 PM EDT | UPDATED THU, AUG 25 2016•4:43 PM EDT

Richard Washington
@HTTPS://WWW.LINKEDIN.COM/IN/RICHARD-WASHINGTON-58A506100/
@IAMRICHWASH

SHARE

Shares of St. Jude Medical briefly fell more than 8 percent Thursday after Muddy Waters Capital announced the firm is short the stock because it believes St. Jude's cardiac devices are vulnerable to cyberattacks.

In a report published Thursday, the short selling firm suggested the recall and remediation of St. Jude Medical's cardiac devices. Such an event would result in roughly a 50 percent decrease in St. Jude Medical's revenue for the next two years — the estimated period for remediation.

https://www.cnbc.com/2016/08/25/st-jude-medical-drops-after-muddy-water-findings-of-negligent-product-design.html

System Shocks? EV Smart Charging Tech Poses Cyber-Risks

Trend Micro's Salvatore Gariuolo talks with the Black Hat USA 2025 News Desk about how the new ISO 15118 standard for electric vehicle smart charging and vehicle-to-grid communications can be weaponized by threat actors.

by **Rob Wright**, Senior News Director

AUG 21, 2025

https://www.darkreading.com/iot/ev-smart-charging-cyber-risks

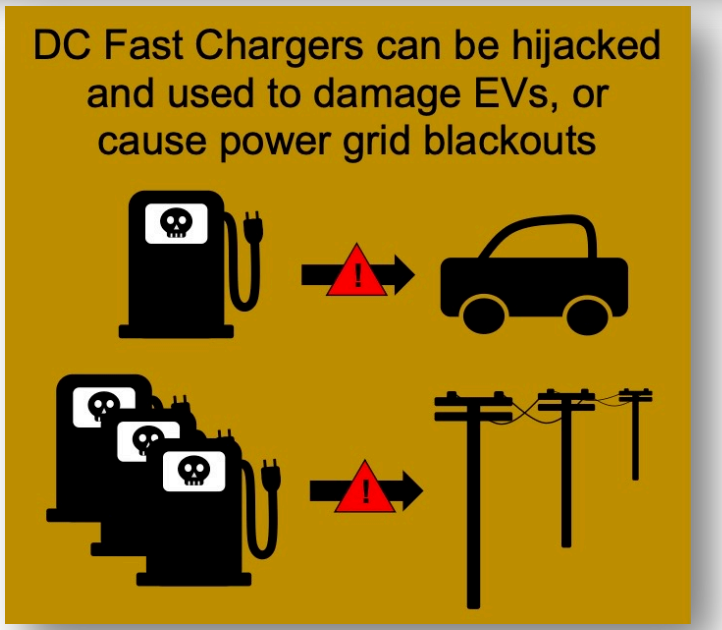
https://nexusconnect.io/podcasts/nexus-podcast-salvatore-gariuolo-on-iso-15118-safe-ev-charging

ISO 15118 Makes a 'Dangerous' Assumption

Gariuolo points out that ISO 15118 does not consider the protection of the charging station.

"The charging station is by design out of the focus of the ISO standard," he said. "The standard makes an assumption and it's a very dangerous assumption, that the charging stations are secure entities. This is an assumption that can backfire."

"The charging station is believed to be trusted, it is not," he said.



https://doi.org/10.1016/j.geits.2025.100262

(In)Segurança em IoT

Segurança é negligenciada

- até mesmo em dispositivos de segurança!
- “é problema da equipe de segurança”

Maioria dos fabricantes ainda repete velhos erros:

- autenticação falha ou inexistente
  - com senhas padrão comum, senhas *hardcoded*, contas ocultas (*backdoors*)
- protocolos obsoletos, sem criptografia (ex: Telnet)
- serviços desnecessários ativos por *default*
- falta de uma visão holística de segurança

Poucos fabricantes possuem ciclo de vida de suporte/*updates*

- mecanismo de *bug report*
- distribuição de *updates*
- políticas claras

Como melhorar o cenário?

cert.br nic.br cgi.br

Solução depende de diversos atores

- Fabricantes
- Desenvolvedores
- Área acadêmica
- Administradores
- Usuários

Desenvolvedores/Fabricantes/Indústria

Segurança deve ser incluída na análise de risco das empresas

- Risco para o negócio e para o usuário

Segurança *by design* e *by default*

- Não opcional
- Considerar requisitos de segurança desde o início projeto
  - pensar também nos “casos de abuso”
- Implementar padrões (versões correntes)
- Usar boas práticas de desenvolvimento seguro
- Configurações padrão de fábrica seguras (restritiva ao invés de permissiva)
- Abrangente (dispositivo, mobile apps, rede, nuvem)

Updates

- Deve ser possível e deve ser seguro (*supply chain attacks*)
- Planejar para fazer em larga escala

Idealmente, ter grupo de resposta a incidentes de segurança em produto (PSIRT)

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

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/

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

Solução depende de diversos atores (cont.)

Área acadêmica

- Incluir segurança já nos primeiros anos
  - como base, não como disciplina optativa

Administradores

- Manter softwares e firmwares atualizados
- 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*

Usuários

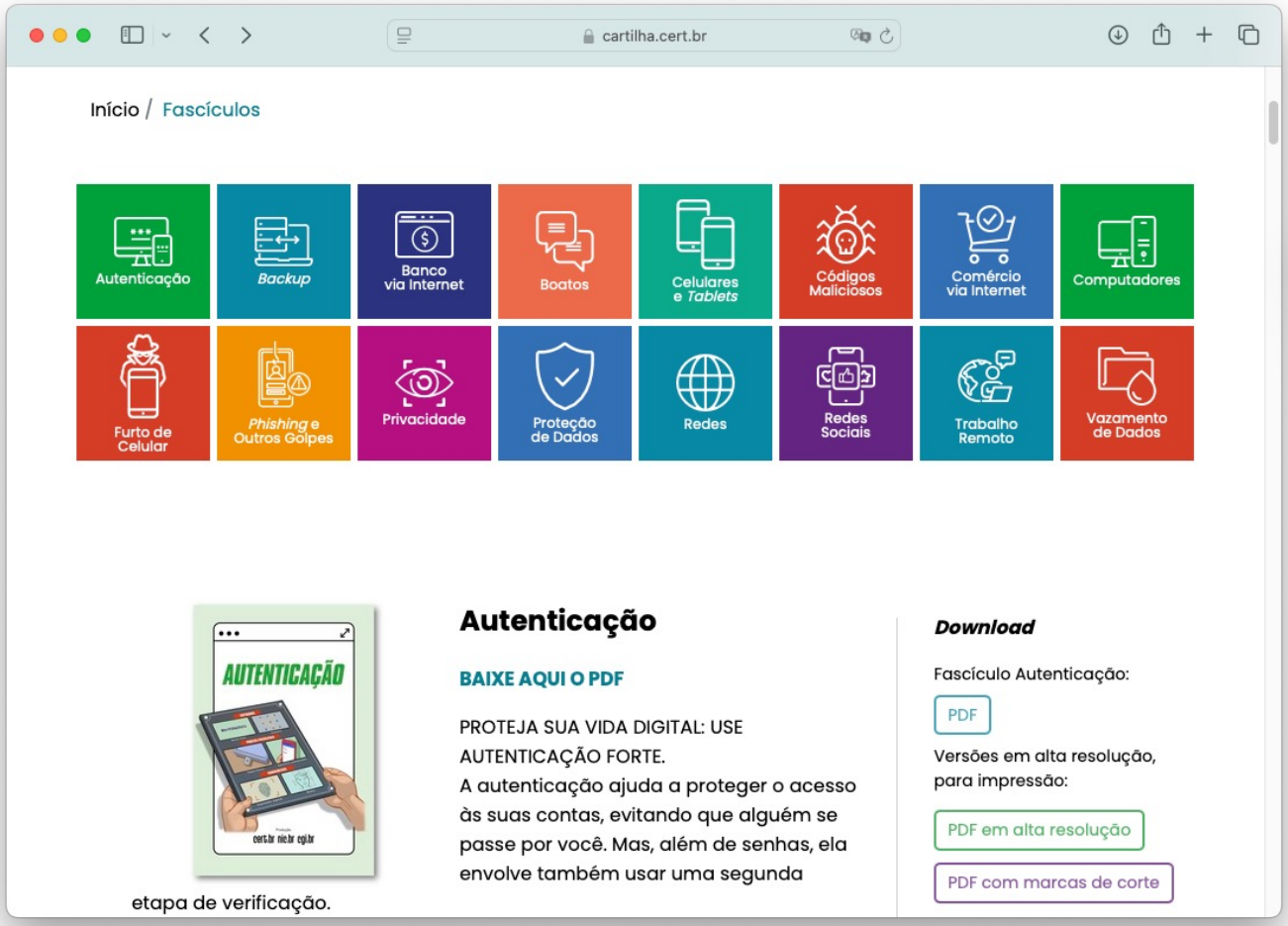
Antes de comprar

- 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

Mantenha-se Informado
Fascículos da Cartilha de Segurança para Internet



https://cartilha.cert.br/

Obrigada!

lucimara@cert.br

para materiais de conscientização: doc@cert.br

notificações para: cert@cert.br

@certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br