nic.br cgi.br | cert.br

Segurança Cibernética Hoje em Dia
26 de Outubro de 2016
Consulado Geral dos EUA /FAAP, São Paulo

Resposta a incidentes no Brasil: Um pouco de história e novos desafios

Lucimara Desiderá
lucimara@cert.br

cert.br nic.br cgi.br

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 03/09/2003, 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/

cgi.br

1 2 3 4 5 6 7 8 9 — GOVERNO e 10 11 12 13 14 15 16 17 18 19 20 21 — SOCIEDADE CIVIL

Representantes do Governo:

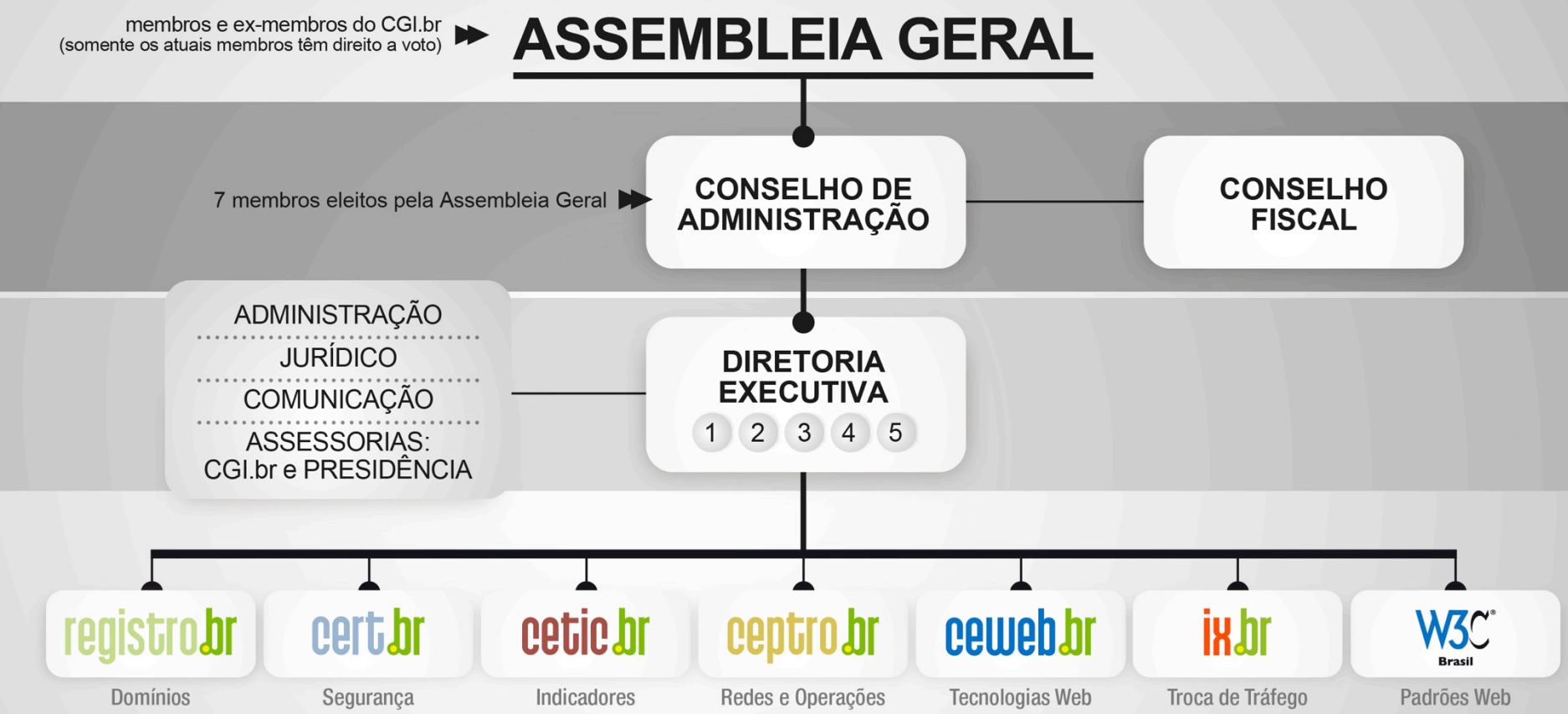
1 Ministério da Ciência, Tecnologia e Inovação (coordenador)
2 Casa Civil da Presidência da República
3 Ministério das Comunicações
4 Ministério da Defesa
5 Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 Ministério do Planejamento, Orçamento e Gestão
7 Agência Nacional de Telecomunicações
8 Conselho Nacional de Desenvolvimento Científico e Tecnológico
9 Conselho Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia

Representantes da Sociedade Civil:

10 Notório saber em assunto da Internet
11 a 14 Representantes do setor empresarial
- provedores de acesso e conteúdo da Internet
- provedores de infra-estrutura de telecomunicações
- indústria de bens de informática, de bens de telecomunicações e de software
- setor empresarial usuário

15 a 18 Representantes do terceiro setor
19 a 21 Representantes da comunidade científica e tecnológica

Estrutura do NIC.br



1 Diretor presidente
2 Diretor administrativo e financeiro
3 Diretor de serviços e de tecnologia
4 Diretor de projetos especiais e de desenvolvimento
5 Diretor de assessoria às atividades do CGI.br

Um pouco de conceitos e de história

cert.br nic.br cgi.br

Conceitos

Incidente de Segurança em Computadores – qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores

Tratamento de Incidentes – processo de identificar e mitigar os incidentes de segurança; também envolve a prevenção

CSIRT – acrônimo internacional para designar um Grupo de Resposta a Incidentes de Segurança, responsável por tratar incidentes de segurança para um público alvo específico

Outros acrônimos: IRT, CIRC, CIRT, SERT, SIRT, CERT®

Como nasceu o CERT.br

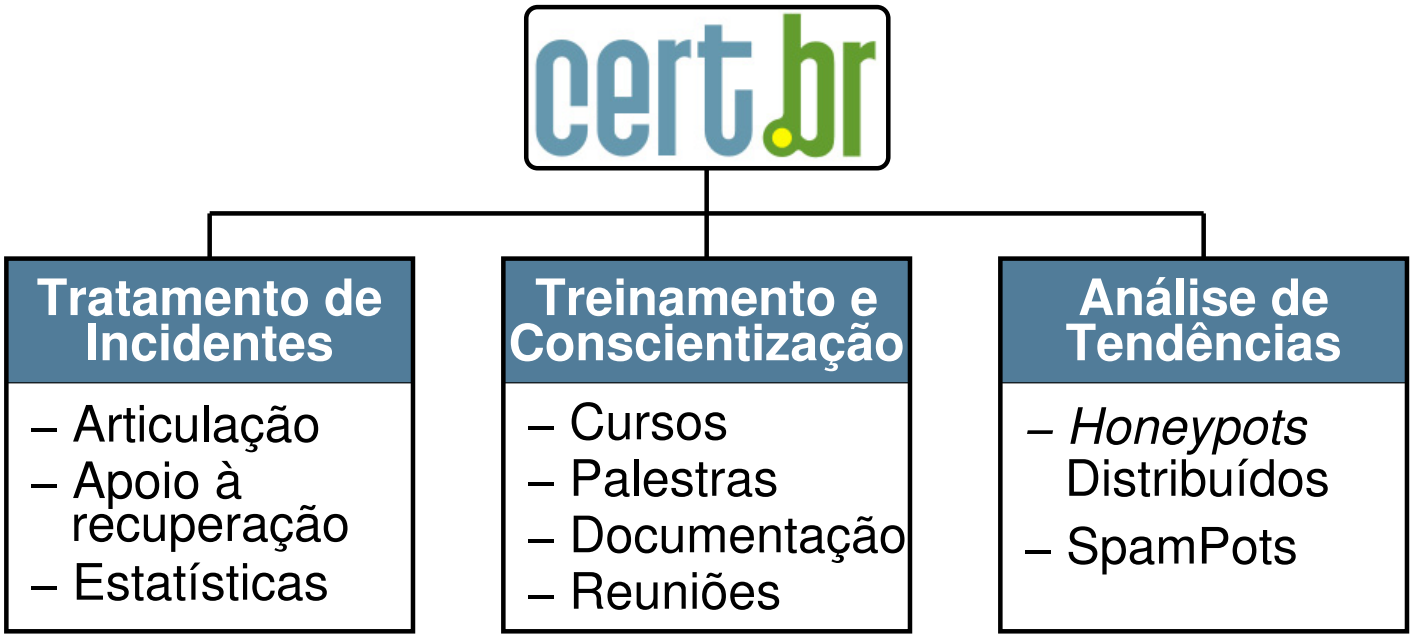
Agosto/1996: o relatório "Rumo à Criação de uma Coordenadoria de Seguraça de Redes na Internet Brasil" é publicado pelo **CGI.br**[1]

- Levantamento da situação no País
- Definição de prioridades
- Levantamento do melhor modelo para agir como facilitador para o tratamento de incidentes de segurança
  - grupo autônomo e neutro, que atue como ponto de contato nacional
  - que possa orientar tecnicamente sobre prevenção e resposta a incidentes
  - que fomente treinamento, atualização e cooperação
  - que fomente a criação de novos CSIRTs no País

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

[1] http://www.nic.br/grupo/historico-gts.htm

[2] http://www.nic.br/grupo/gts.htm



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet PROJECT

Principais atividades:

- **Tratamento de Incidentes**
  - Ponto de contato nacional para notificação de incidentes
  - Atua facilitando o processo de resposta a incidentes das várias organizações
  - Trabalha em colaboração com outras entidades
  - Auxilia novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades
- **Formação de profissionais para atuar em Tratamento de Incidentes**
- **Produção de boas práticas e material para conscientização sobre a necessidade de segurança na Internet para diversas audiências**

Atividades de Tratamento de Incidentes

O CERT.br recebe notificações de incidentes de segurança envolvendo redes conectadas à Internet no Brasil

- feitas voluntariamente por administradores de redes e usuários de Internet, sejam eles do Brasil ou do exterior
- ponto de entrada: e-mail cert@cert.br

  (1.597.148 mensagens tratadas em 2015)

Modo de atuação:

- provê suporte, dicas e recomendações técnicas para mitigação e recuperação de incidentes, como invasões
- foco na redução no número de vítimas
- agrega dados de organismos internacionais (*data feeds*) e repassa para as redes nacionais, para identificação e erradicação de problemas
- cooperação com organizações no combate a *botnets*

APWG RESEARCH PARTNER www.antiphishing.org

FIRST Improving Security Together MEMBER

The Honeynet PROJECT

Segurança em IoT:
Velhos problemas e novos desafios

cert.br nic.br cgi.br

Botnets de Dispositivos IoT

- **CPEs, DVRs, CCTVs, NAS, roteadores domésticos, etc**
- **Foco em dispositivos com versões "enxutas" de Linux**
  - **para sistemas embarcados**
  - **arquiteturas ARM, MIPS, PowerPC, etc**
- ***Malware* se propaga geralmente via Telnet**
- **Explora Senhas Fracas ou Padrão**
  - **muitas vezes são "*backdoors*" dos fabricantes**
- **Em nossos *honeypots***
  - **IPs únicos de IoT infectados com Mirai – dados de 25/10/2016:**
    - **Brasil: 87.711**
    - **Resto do Mundo: 504.481**

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

KrebsonSecurity

In-depth security news and investigation

21 Hacked Cameras, DVRs Powered To Massive Internet Outage

OCT 16

A massive and sustained Internet attack that has caused ou congestion today for a large number of Web sites was launched with "Internet of Things" (IoT) devices, such as CCTV video cameras and di new data suggests.

Earlier today cyber criminals began training their attack cannons o infrastructure company that provides critical technology services to sc top destinations. The attack began creating problems for Internet users sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.

> *"The issue with these particular devices is that a user cannot feasibly change this password," Flashpoint's* ***Zach Wikholm*** *told KrebsOnSecurity. "The password is hardcoded into the firmware, and the tools necessary to disable it are not present.*

https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

ZDNet MENU US

Mirai DDoS botnet powers up, infects Sierra Wireless gateways

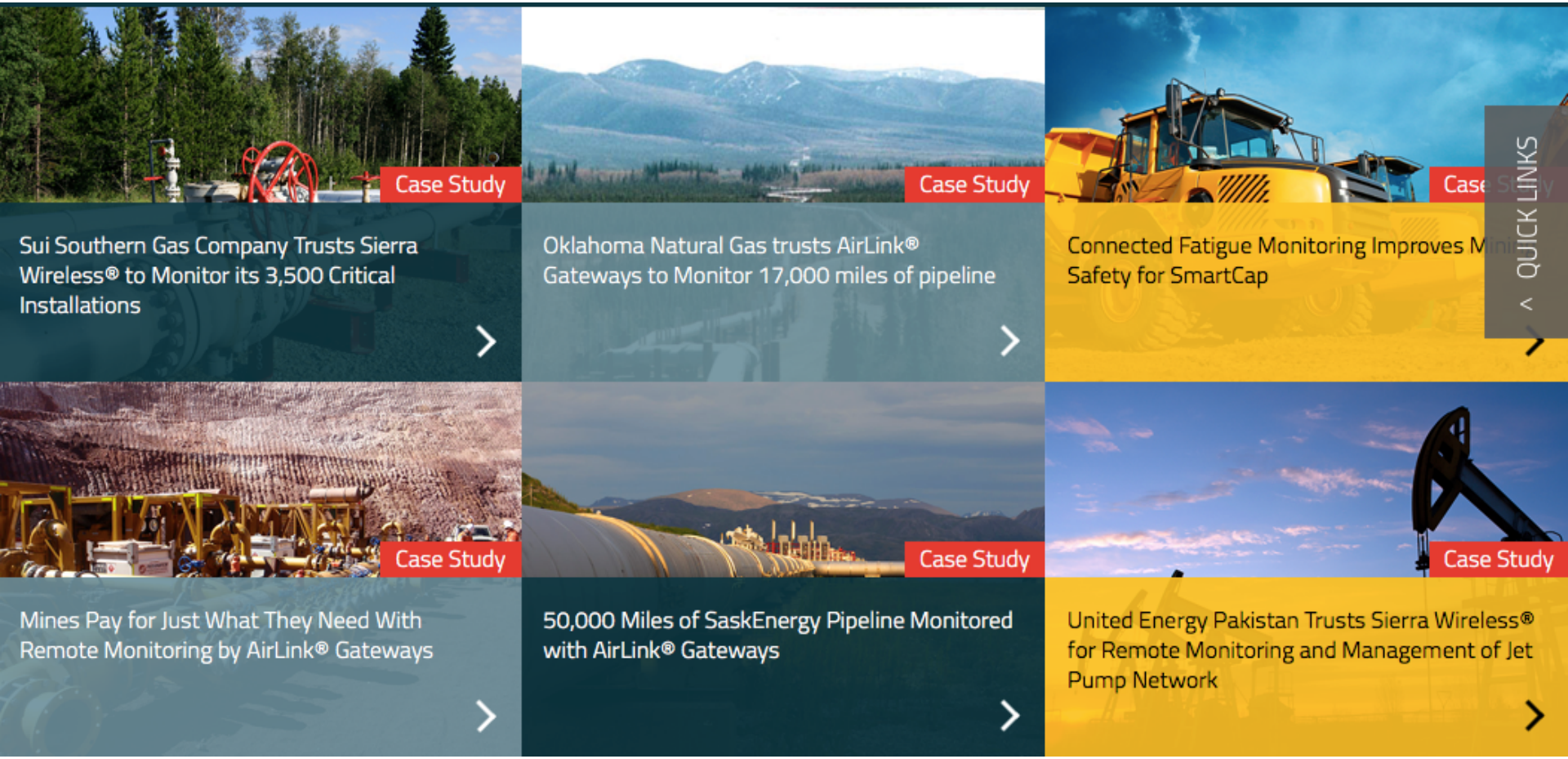
Sierra Wireless AirLink Gateways are vulnerable to the debilitating botnet, of which source code has been made public.

By Charlie Osborne for Zero Day | October 17, 2016 -- 08:14 GMT (01:14 PDT) | Topic: Security

"ICS-CERT would like to emphasize that there is no software or hardware vulnerability being exploited in the Sierra Wireless devices by the Mirai malware," the advisory reads. "The issue is configuration management of the device upon deployment."

http://www.zdnet.com/article/mirai-ddos-botnet-powers-up-infects-sierra-wireless-gateways/

Potenciais clientes afetados...

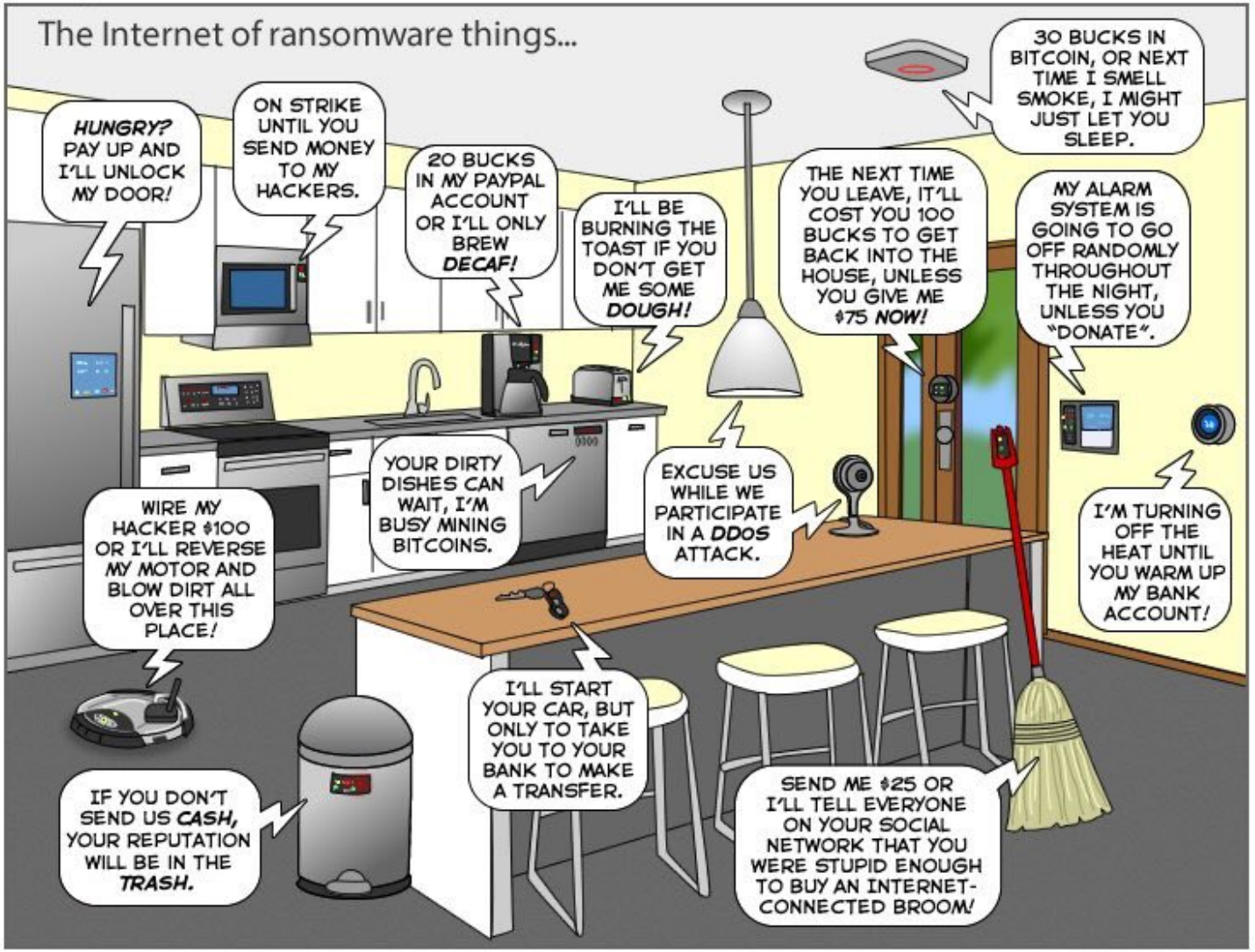


https://www.sierrawireless.com/resources/#/q=Case%20Study|Oil%20&%20Gas,%20Mining

O que mais nos aguarda?

cert.br nic.br cgi.br

The Joy of Tech™ by Nitrozac & Snaggy



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

joyoftech.com

Obrigada

www.cert.br

lucimara@cert.br @certbr

26 de Outubro de 2016

nic.br cgi.br

www.nic.br | www.cgi.br