nic.br cgi.br | cert.br

Workshop – Semana da Internet Segura

10 de fevereiro de 2020

São Paulo / SP

O Ano é 2020!

Hora de Modernizar a sua Presença na Internet

Dra. Cristine Hoepers
Gerente Geral
cristine@cert.br

Dr. Klaus Steding-Jessen
Gerente Técnico
jessen@cert.br

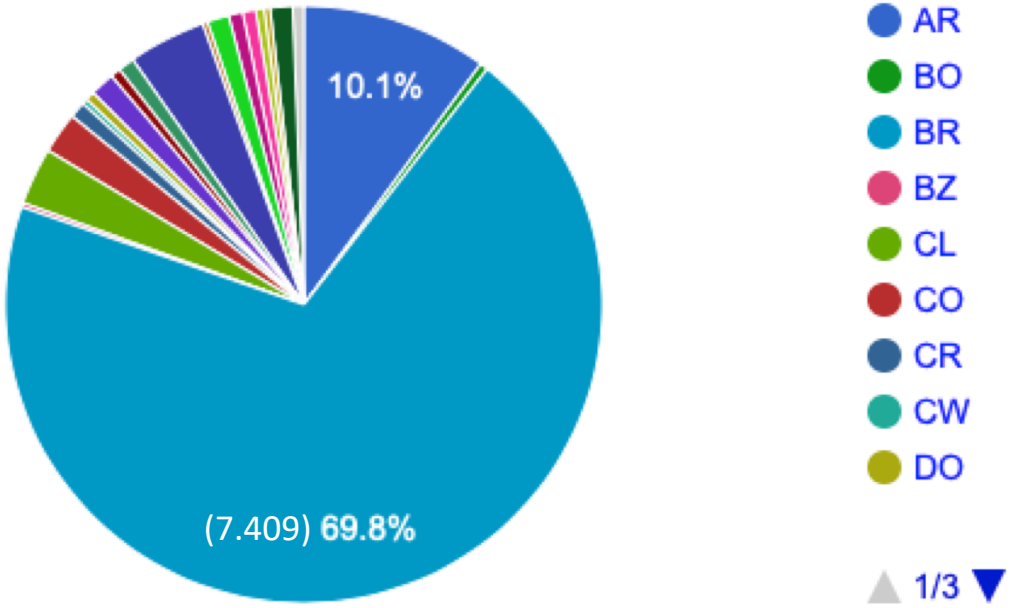
cert.br nic.br cgi.br

Antes de falar de segurança: em qual ecossistema estamos conectados?

cert.br nic.br cgi.br

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 2 em pico de tráfego (7.1Tbps)
- nº 3 em média de tráfego (4.8Tbps)

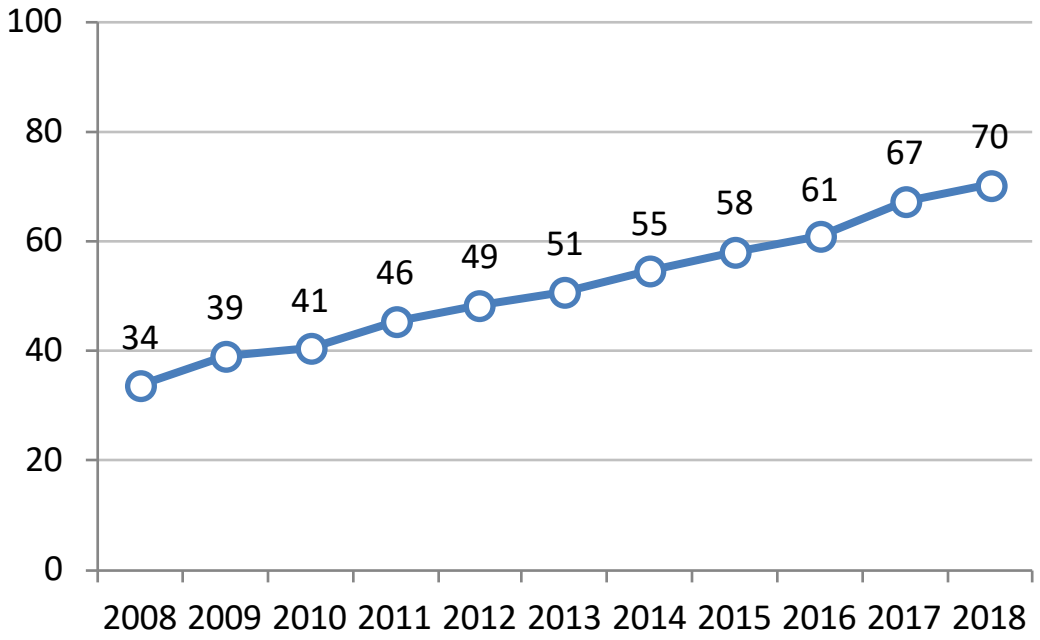
Fonte: https://www.pch.net/ixp/dir

Dados atualizados em 06 de fevereiro de 2020

Internet no Brasil em Números:
Usuários e Dispositivos Utilizados

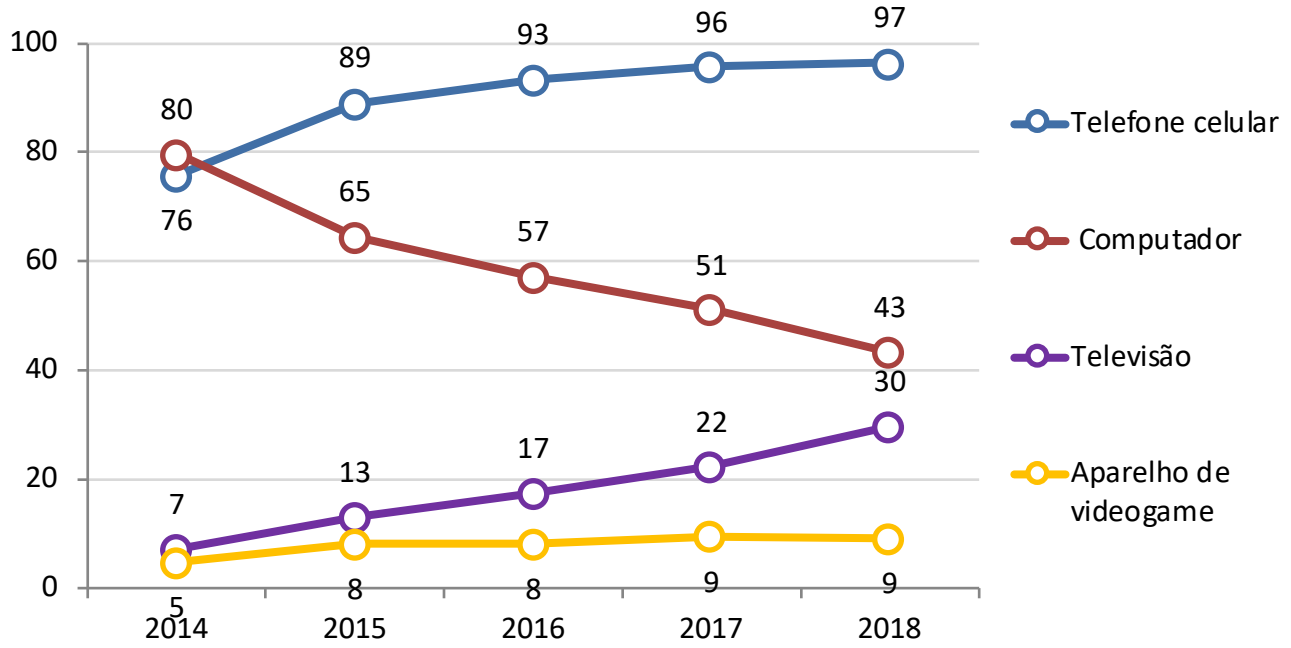
Usuários de Internet

Porcentagem do total da população



Dispositivo Utilizado para Acesso Individual

Porcentagem do total de usuários de Internet

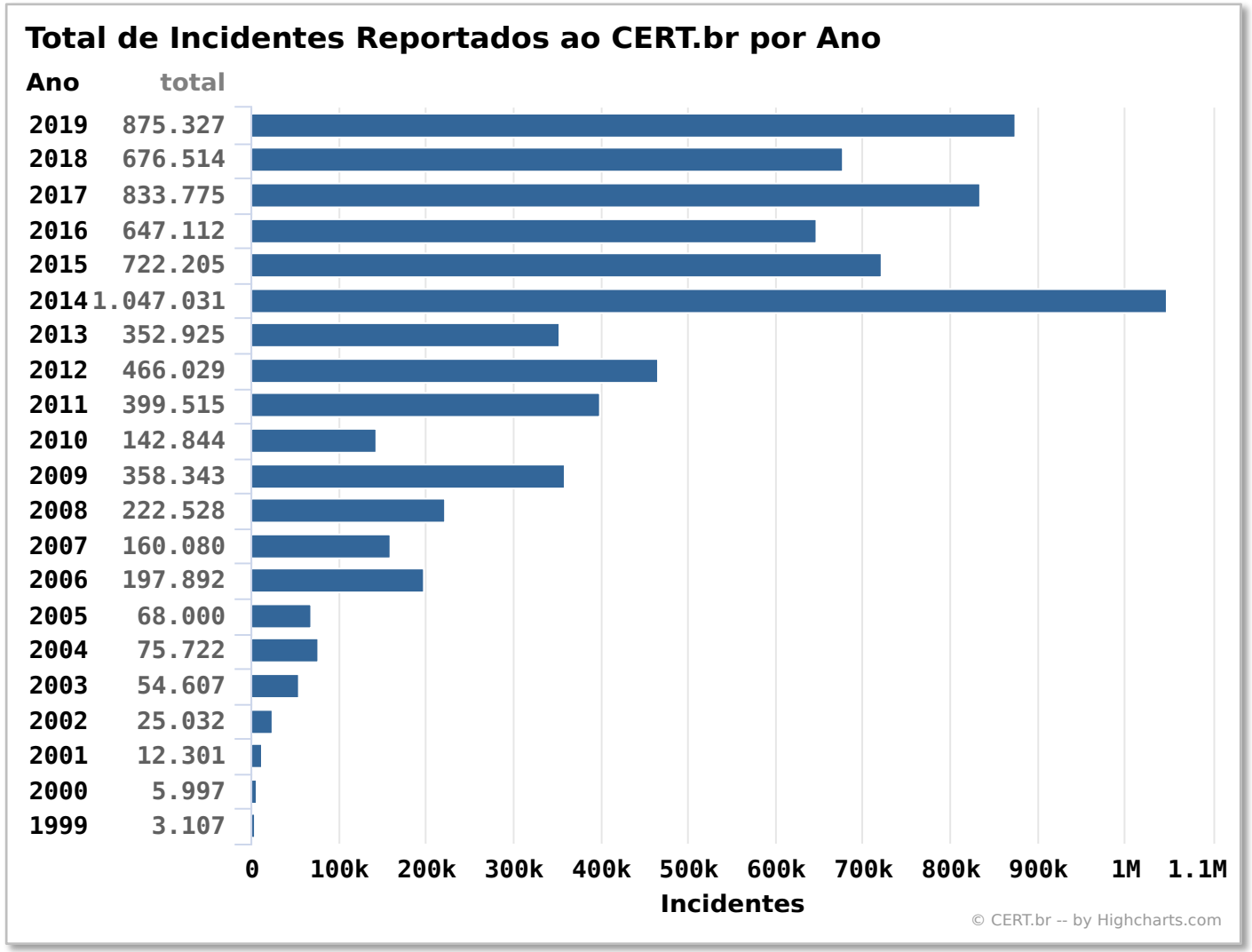


126,9 milhões de usuários de Internet

(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 2019**

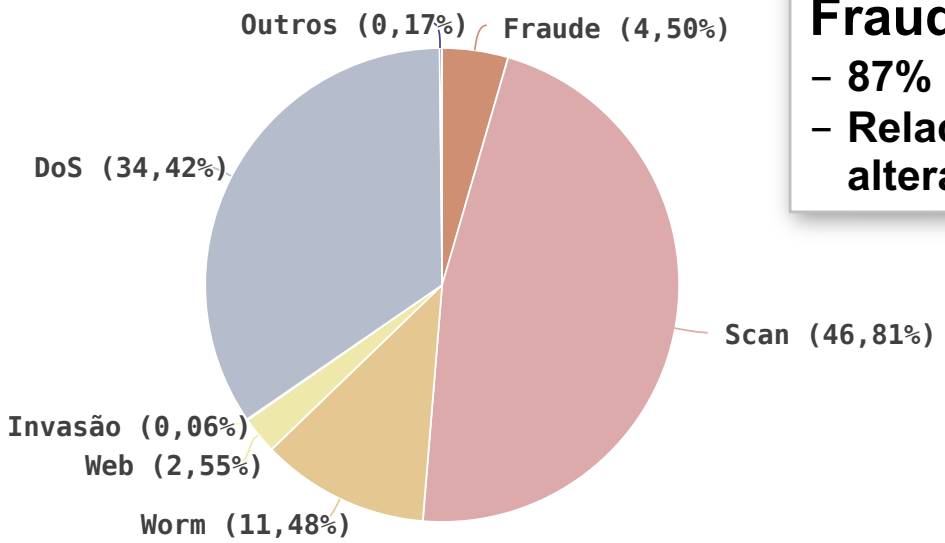


Fonte: https://www.cert.br/stats/incidentes/

Ataques mais comuns no último ano

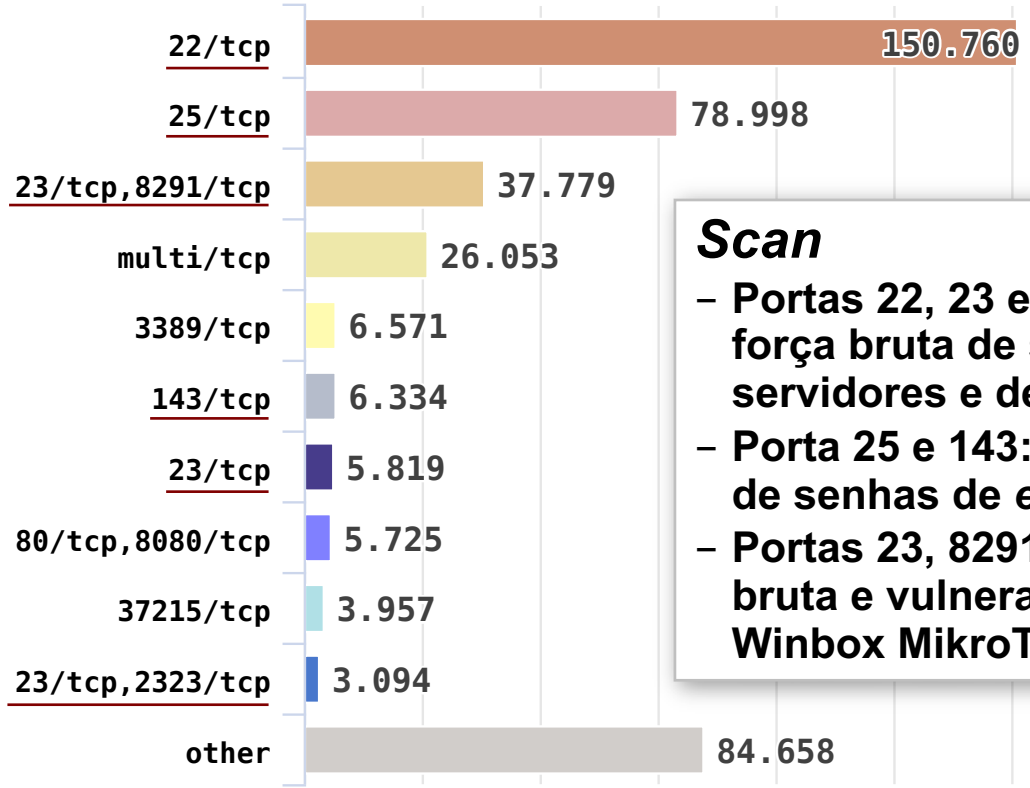
- DDoS a partir de Internet das coisas
  - Câmeras, *Smartphones*, Roteadores e *Modems* de banda larga/Wi-Fi, TVs
  - Infectados e sendo usados para DDoS e também para:
    - minerar criptomoedas
    - fazer fraudes contra os usuários
- Comprometimento de credenciais
  - Principalmente *e-mails*
    - via ataques de força bruta contra Webmail, POP, IMAP e SMTP
    - via infecção de computadores, celulares e roteadores de banda larga

Incidentes Reportados para o CERT.br :
Detalhes sobre os tipos de incidentes vistos em 2019



Fraude
- 87% são páginas falsas (*phishing*)
- Relacionadas com invasão de CPEs para alterar o DNS

DDoS
- Aumentou de patamar em 2014
- Maior número em 2019
- 300Gbps é o “normal”
- Tipos mais frequentes
  - *botnets* IoT
  - amplificação de tráfego

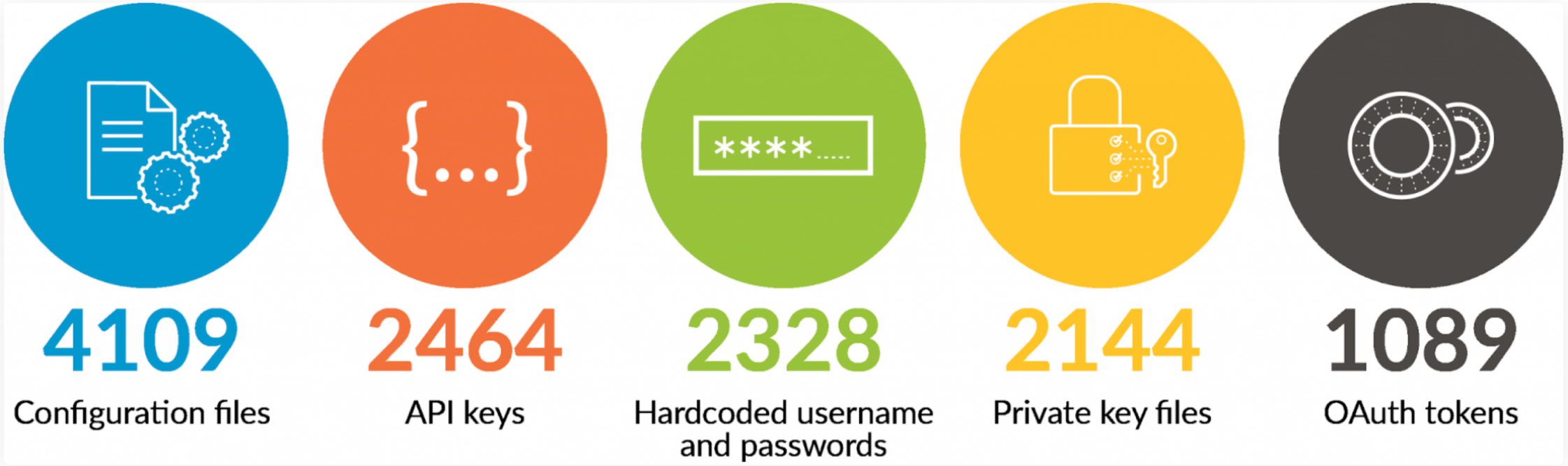


Scan
- Portas 22, 23 e 23, 2323: força bruta de senhas de servidores e de IoT
- Porta 25 e 143: força bruta de senhas de *e-mail*
- Portas 23, 8291: força bruta e vulnerabilidade Winbox MikroTik

Credenciais também são usadas em aplicativos e aplicações: **Estudo da Palo Alto em Dados Públicos no GitHub**

Key Findings

Unit 42 researchers analyzed more than 24,000 public GitHub data uploads via the GitHubs Event API and found thousands of files containing potentially sensitive information, which included:

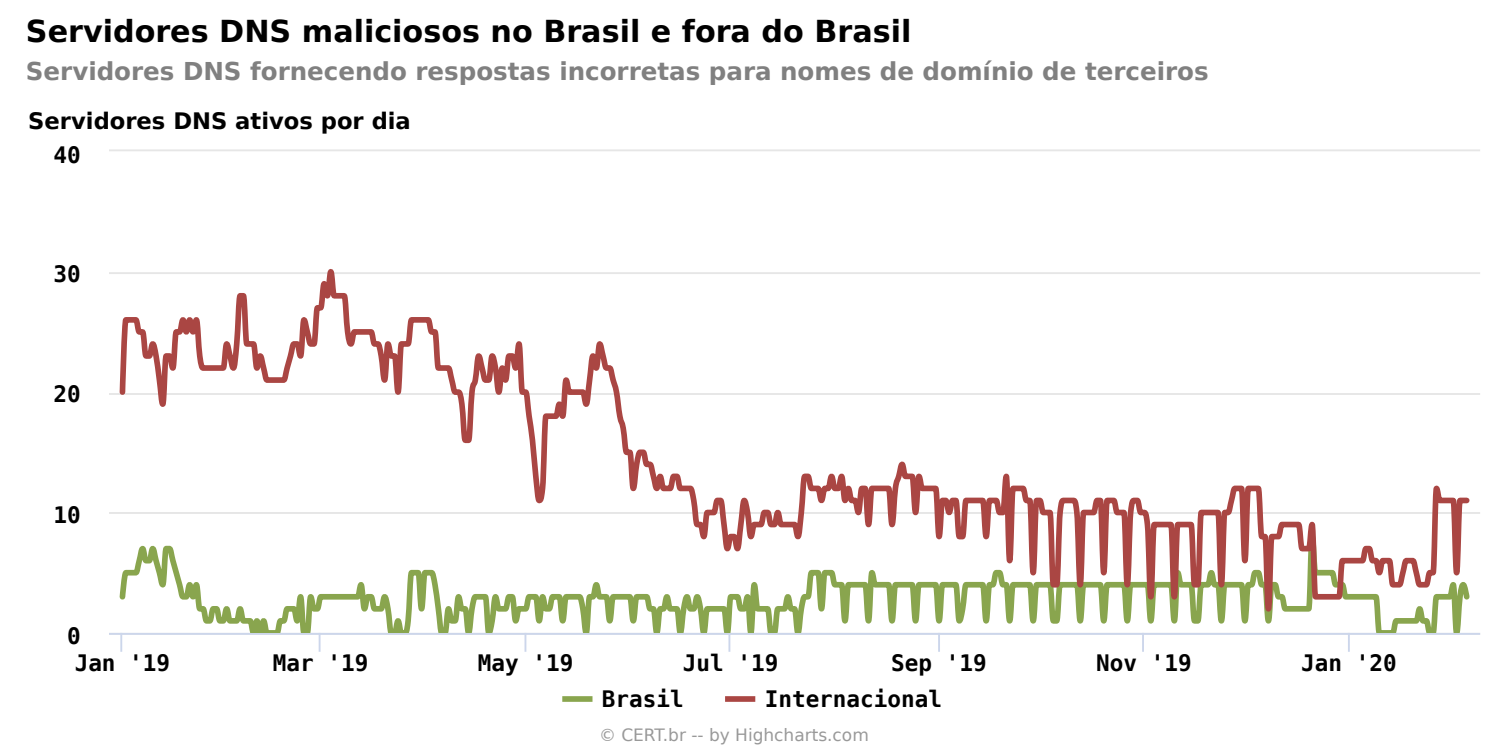


Fonte: https://unit42.paloaltonetworks.com/github-data-exposed/

Servidores DNS Maliciosos Usados nos CPEs Invadidos: **Fornecem Respostas Autoritativas Erradas**

Domínios afetados dos seguintes setores:

- Bancos, Serviços de Pagamento, Serviços de *Streaming*, Mobilidade, Redes Sociais, *Webmail*, Comércio Eletrônico, entre outros



Fonte: https://cert.br/stats/dns-malicioso/

Semântica é importante ao reportar incidentes ou pedir takedown!

- **Isto não é um DNS invadido**
- **Isto não é envenenamento (*cache poisoning*)**
- **Isto não é sequestro de domínio (*domain hijacking*)**

Isto é um servidor DNS malicioso (*rogue*) sendo usado para sequestro de DNS (*DNS hijacking*)

- **autoritativo para os domínios das vítimas**
- **recursivo aberto respondendo ao restante das consultas**

Invasão de Roteadores de Banda Larga (CPEs): **Anatomia do Ataque**

Atacantes compram serviços de *cloud*/*hosting*

Configuram o IP **`x.y.z.1`** como um DNS malicioso

- responde com autoridade para os domínios das organizações vítima
  - Registro DNS do tipo **"A"** para o domínio da vítima aponta para o IP **`x.y.z.2`**
- para outras consultas é recursivo

Hospedam a página de *phishing* no IP **`x.y.z.2`**

Usa o IP **`x.y.z.3`** para varrer a Internet em busca de CPEs vulneráveis

Explora vulnerabilidades nos CPEs de diversos Provedores

- muda a configuração de DNS para que seja usado o servidor **`x.y.z.1`**

Invasão de Roteadores de Banda Larga (CPEs): **Exemplo de ataque contra o domínio `gmail.com`**

IP **`52.211.x.x`** é um DNS malicioso

- responde com autoridade para o domínio **`gmail.com`**
  - Registro DNS do tipo **"A"** aponta para o IP **`35.163.x.x`**

```
$ dig +short @52.211.x.x gmail.com A
35.163.x.x
```

- para outras consultas é recursivo

Resposta correta:

```
$ dig +short gmail.com A
172.217.29.165
```

A página de *phishing* está no IP **`35.163.x.x`**

```
$ curl -s -H 'Host: gmail.com' http://35.163.x.x/
<!DOCTYPE html>
<html lang="en">
[...]
<body>
[...]
<a id="link-forgot-passwd" class="need-help"
   href="#/signin/recovery?hl=en"> Esqueceu a senha? </a>
</div>
</div>
<span id="inge" style="display: none" role="alert" class="error-msg">
  Desculpe, Goole não reconhece esse email. <a href="#">Criar
    conta</a> usando esse endereço? </span>
<span id="timeoutError" style="display: none" role="alert"
      class="error-msg"> Algo deu errado. Verifique sua conexão e
      tente novamente.</span>
</form>
[...]
```

Modernizar a presença na Internet?

O que isso tem a ver com a minha empresa? E com segurança?

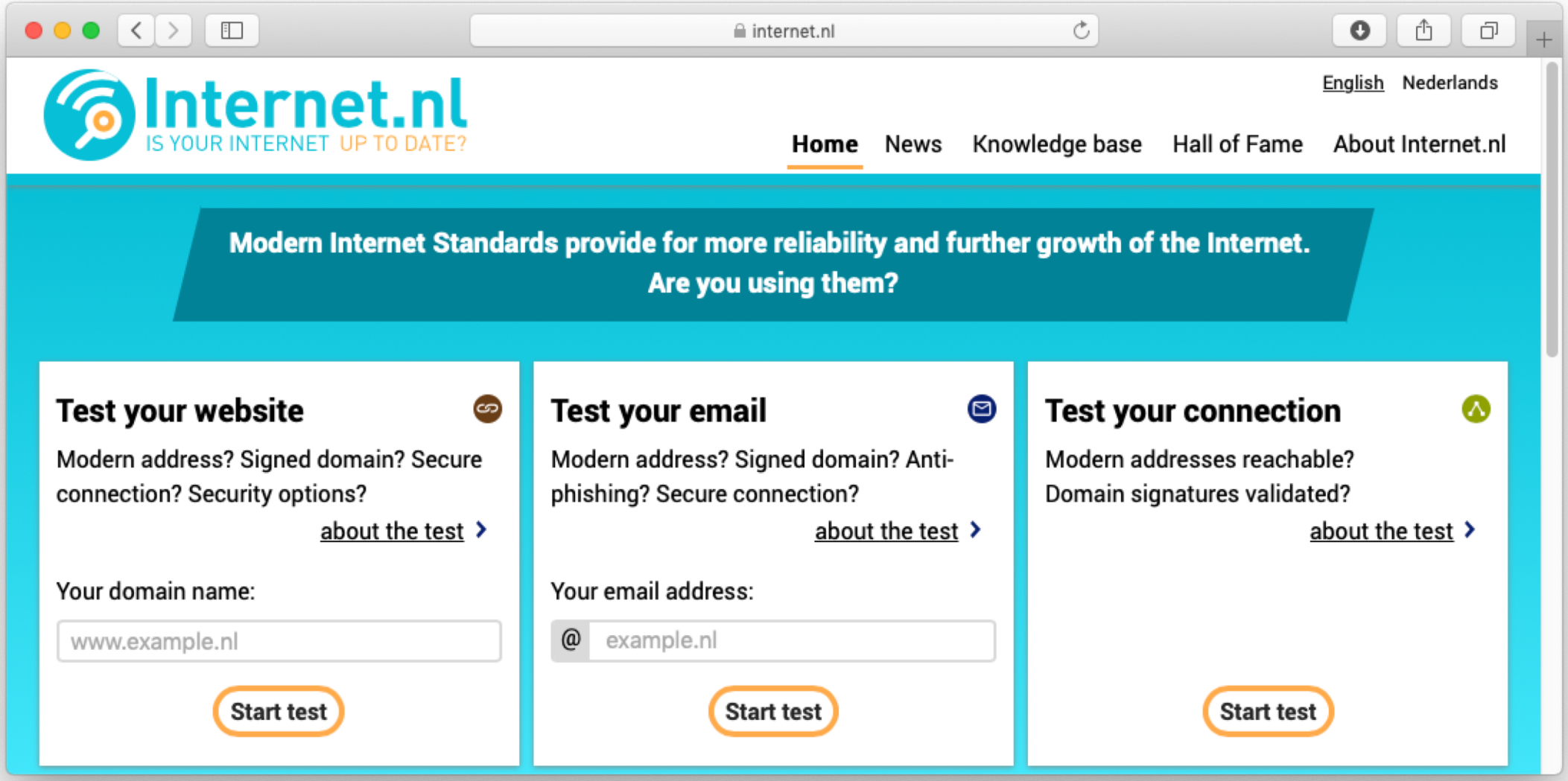
cert.br nic.br cgi.br

	Padrões	Vantagens da Adoção
Autenticação com Múltiplos Fatores	Tokens • em *hardware* (FIDO2/U2F) • em *software* (HOTP/TOTP)	Impede sucesso de força bruta de senhas Reduz impacto do comprometimento de credenciais
Criptografia forte	HTTPS mandatório e HSTS Versões atuais de TLS *Forward Secrecy*	Garantia das transações e da proteção de dados Reduz a chance de quebra da criptografia Impede quebra de cripto de tráfego antigo capturado
Segurança de DNS	DNSSEC DoH/DoT	Proteção contra envenenamento de *cache* Controle do servidor utilizado e checagem de certificados – se for embutido na Aplicação
Segurança de *e-mail*	STARTTLS [idealmente c/ DANE] DMARC, DKIM e SPF	Proteção contra *sniffing* (“espionagem”) Aumento da reputação da mensagem legítima (ajuda a prevenir *phishing* da sua marca)
Protocolo IP	IPv6 é o atual IPv4 é legado – e já acabou • novas redes só terão IPv6	Mais estabilidade • Não depender de CGN ou tradução v6 → v4 • Redes móveis tendem a ter IPv6 nativo Facilita o processo investigativo e de tratamento de incidentes

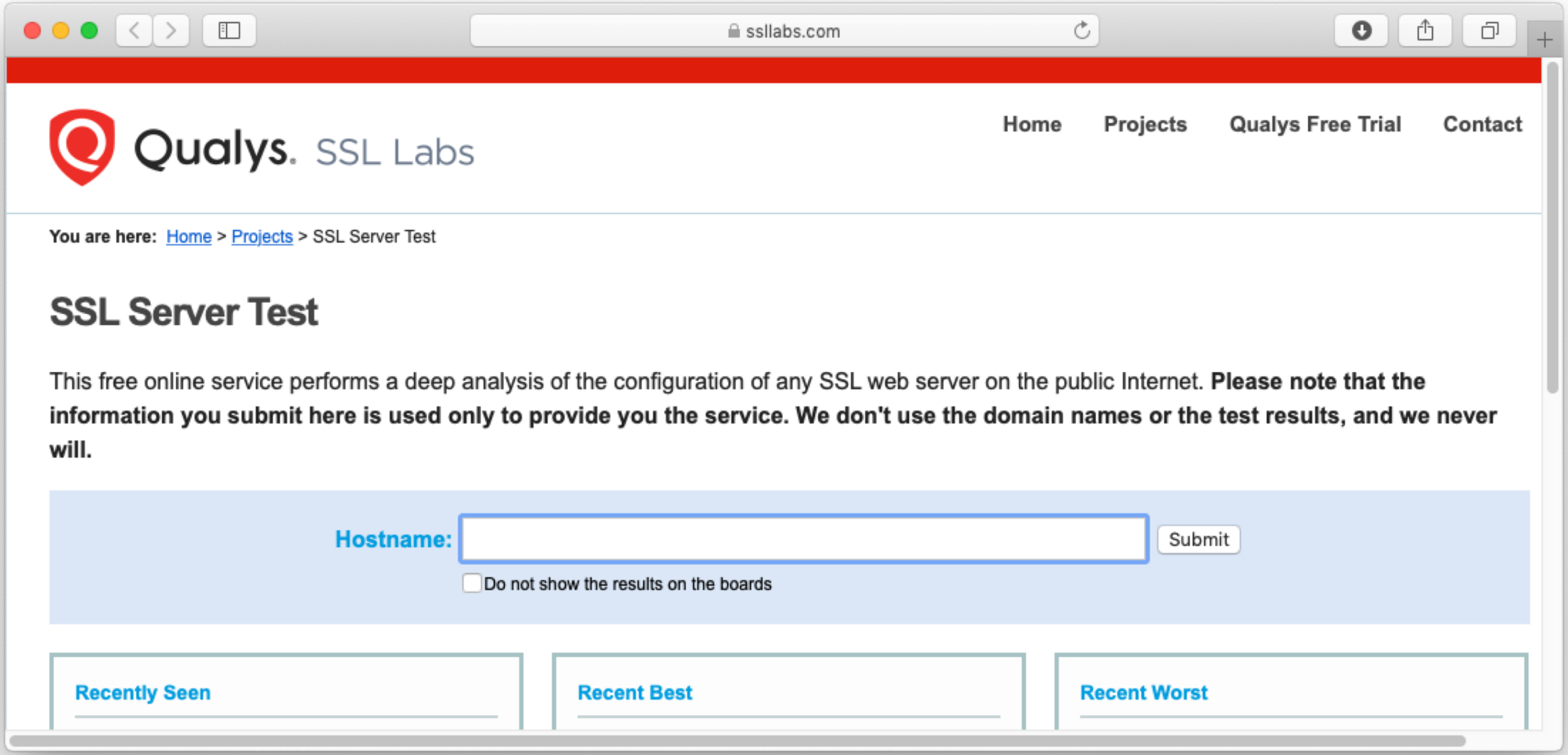
Como Testar e Onde Procurar Referências

cert.br nic.br cgi.br

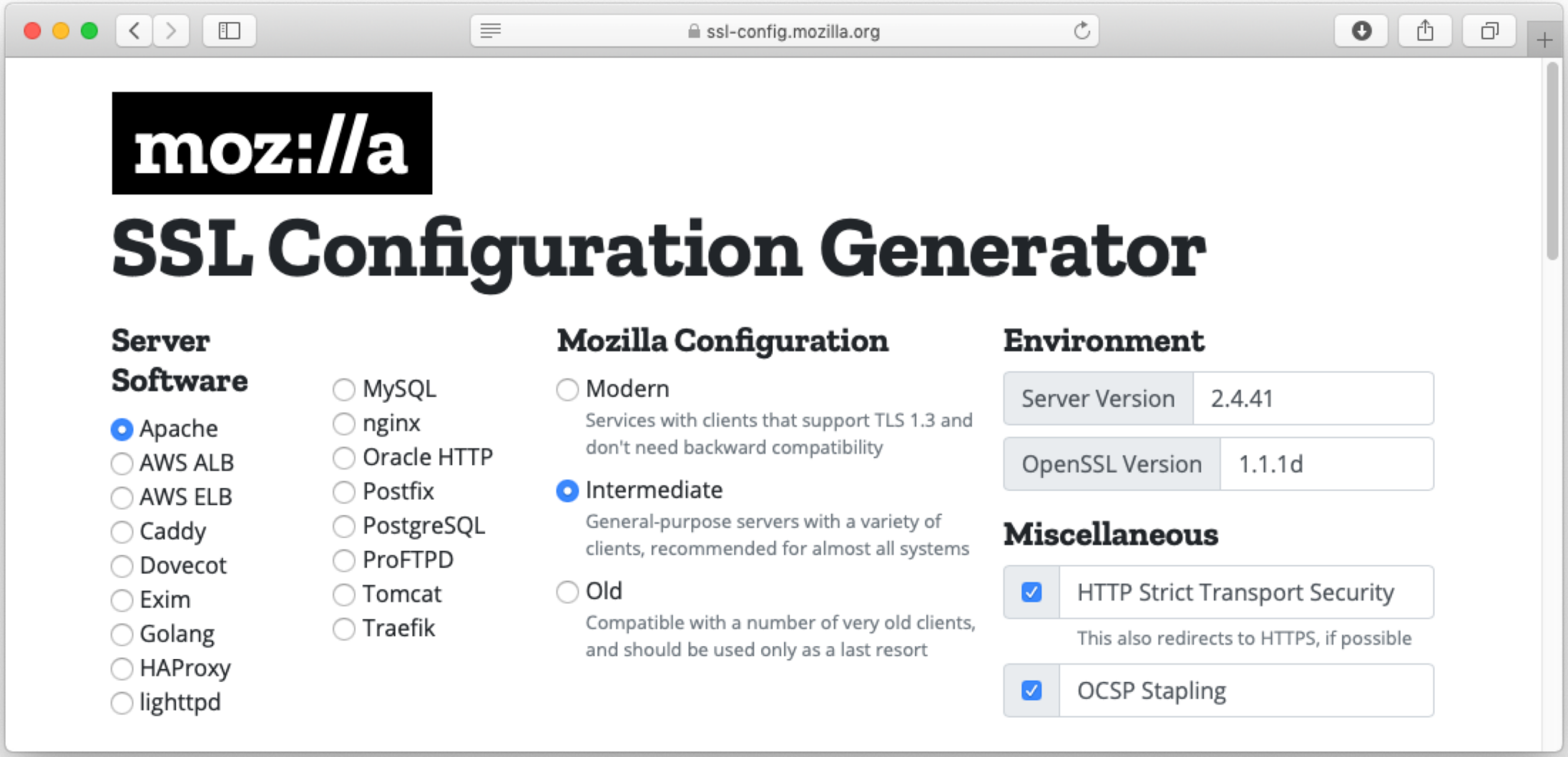
Is your Internet up to date?
https://internet.nl



SSL Server Test
https://www.ssllabs.com/ssltest/



SSL Configuration Generator
https://ssl-config.mozilla.org/



Padrões	Referências
Tokens em *hardware* (FIDO2/U2F)	https://fidoalliance.org/specifications/
Tokens em *software* (HOTP/TOTP)	https://tools.ietf.org/html/rfc4226 https://tools.ietf.org/html/rfc6238
HTTPS mandatório e HSTS Versões atuais de TLS *Forward Secrecy*	https://www.ssllabs.com/ssltest/ https://ssl-config.mozilla.org https://observatory.mozilla.org
DNSSEC DoH/DoT	https://registro.br/tecnologia/dnssec/dnssec-para-provedores/ ftp://ftp.registro.br/pub/doc/tutorial-dnssec.pdf https://english.ncsc.nl/latest/news/2019/oktober/2/prepare-for-dot-and-doh-factsheet-available https://dnsviz.net
STARTTLS [idealmente c/ DANE] DMARC, DKIM e SPF	https://starttls-everywhere.org https://english.ncsc.nl/publications/factsheets/2019/juni/01/factsheet-secure-the-connections-of-mail-servers https://mecsa.jrc.ec.europa.eu/en/technical#starttls https://havedane.net https://dmarc.org https://dmarc.globalcyberalliance.org
IPv6	https://ipv6.br https://test-ipv6.com

Outras Referências de Interesse para Uma Internet Melhor

cert.br nic.br cgi.br

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

PROGRAMA INTERNET +SEGURA

Objetivo principal:

- Reduzir o número de sistemas que possam ser abusados para gerar ataques DDoS

Incentivo à adoção de boas práticas:

- *Hardening*
- Segurança de roteamento (MANRS)
- *Anti-spoofing* (BCP 38)
- Reduzir serviços abertos que permitam amplificação

Iniciativa conjunta:

- ISOC, NIC.br, SindiTelebrasil, Abranet, Abrint, Abinee

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

Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition

Requisitos mínimos de segurança

- Aplicáveis a IoT em geral

Trabalho desenvolvido no LAC-AAWG – *Latin American and Caribbean Anti-Abuse Working Group*

- Editora: Lucimara, Chair LAC-AAWG / CERT.br

Publicação conjunta

- **M³AAWG** - *Messaging, Malware and Mobile Anti-Abuse Working Group*
- **LACNOG** - *Latin American and Caribbean Network Operators Group*

Disponível em

- **Português**, Inglês, Japonês e Koreano

www.m3aawg.org/CPESecurityBP-Portuguese
www.lacnog.net/docs/lac-bcop-1
www.m3aawg.org/CPESecurityBP

Conscientização:
Portal InternetSegura.br

Conscientização:
Materiais sob Licença Creative Commons

Segurança na INTERNET

Faça sua parte e todos teremos uma Internet mais segura!

Já há muito tempo que segurança na Internet não é um assunto somente de interesse de um público especializado. Com a iniciativa InternetSegura.br, o NIC.br produz e disponibiliza gratuitamente uma série de materiais, em diversos formatos, que orientam diferentes públicos sobre o uso seguro da Internet.
www.internetsegura.br

Catálogo de materiais e iniciativas do NIC.br

Formato impresso, colorido e permite inclusão de logo de parceiros de impressão

para Crianças

Guia Internet Segura
Apresenta conceitos de segurança na Internet de forma lúdica, com atividades para colorir, palavras cruzadas, desafios cifrados, dicas, complete a frase, caça-palavras, entre outros.

Desafios
Contém tanto os desafios do guia Internet Segura como materiais adicionais, atualizados periodicamente.
internetsegura.br/desafios

para Adolescentes

Encarte #FikDik
Encarte do guia #Internet com Responsa - Cuidados e Responsabilidades no Uso da Internet, que apresenta os principais cuidados, riscos e consequências do uso inadequado da Internet de forma resumida.

para Pais e Educadores

Guia Internet Segura para seus filhos
Informações para pais e responsáveis sobre como proteger os filhos, seja zelando pela privacidade das crianças, ou utilizando tecnologias de controle parental.

Guia #Internet com Responsa - Cuidados e responsabilidades no uso da Internet
Orienta pais, responsáveis e educadores de adolescentes em temas sensíveis, como exposição excessiva na Internet, liberdade de expressão e danos à imagem e reputação, *cyberbullying*, danos e riscos da prática de nude, *selfie*, entre outros. Acompanha o encarte #FikDik

Guia #Internet com Responsa na sua Sala de Aula
Explica os desafios do uso da Internet a partir da exposição excessiva, dos direitos e possíveis danos à imagem dos professores e alunos, e dos limites da liberdade de expressão.

Slides: Fascículos da Cartilha de Segurança para Internet
Slides para a divulgação de boas práticas sobre o uso seguro da Internet. Há versões de apoio para professores, com notas explicativas.
Disponíveis em formatos PowerPoint (.ppt), LibreOffice (.odp), PDF sem notas explicativas e PDF com notas explicativas.
cartilha.cert.br/downloads

VEJA TAMBÉM

Curso de Formação de Professores Multiplicadores para o Uso Consciente e Responsável da Internet:
cursointernetcomresponsa.nic.br

Materiais de referência:

TIC Kids Online Brasil
Indicadores com mapeamento de possíveis riscos e oportunidades *on-line* a partir dos usos que crianças e adolescentes de 9 a 17 anos fazem da Internet. Contém dados distintos para "crianças e adolescentes" e "pais e responsáveis".
cetic.br/pesquisa/kids-online

TIC Educação
A pesquisa entrevista alunos, professores, coordenadores pedagógicos e diretores para mapear o acesso, o uso e a apropriação das tecnologias de informação e comunicação (TIC) em escolas públicas e privadas de educação básica.
cetic.br/pesquisa/educacao

Para quem tem 60 anos ou mais

#Internet com Responsa 60+: Cuidados e responsabilidades no uso da Internet
Apresenta cuidados específicos para essa faixa etária, pois esse ambiente repleto de informações e oportunidades também oferece alguns riscos para quem ingressou no uso das novas tecnologias recentemente.

para Técnicos

Portal BCP e Programa Por uma Internet Mais Segura
Reúne um conjunto de boas práticas operacionais para Sistemas Autônomos (ASs) conectados à Internet. São destacadas algumas práticas que, embora extremamente importantes, ainda não são adotadas amplamente pelos ASs brasileiros.
O portal também disponibiliza conteúdos e iniciativas direcionadas à comunidade de operadores de redes e serviços que formam a Internet por meio do **Programa por uma Internet Mais Segura.**
bcp.nic.br

VEJA TAMBÉM

Curso de Boas Práticas Operacionais para Sistemas Autônomos – Presencial:
bcp.nic.br/curso-bcop

Curso "*Fundamentals of Incident Handling*"
cert.br/cursos/fih/

Curso "*Advanced Topics in Incident Handling*"
cert.br/cursos/atih/

Interesse geral

Cartilha de Segurança para Internet
Documento com recomendações e dicas sobre como o usuário de Internet deve se comportar para aumentar a sua segurança e se proteger de possíveis ameaças. Apresenta o significado de diversos termos e conceitos utilizados na Internet, aborda os riscos de uso desta tecnologia e fornece uma série de dicas e cuidados a serem tomados pelos usuários.
Também disponível em **cartilha.cert.br** e em espanhol em cartilla.cert.br

Fascículos da Cartilha de Segurança para Internet
Aborda tópicos específicos contidos na Cartilha de Segurança para Internet e complementa conteúdos que não estavam disponíveis à época da última edição da Cartilha, como Boatos, cuidados atualizados para Redes Sociais e Códigos Maliciosos. Também disponíveis em **cartilha.cert.br/fasciculos** e em espanhol em cartilla.cert.br/fasciculos.

Guia #Internet com Responsa Vai às Compras
Detalha os cuidados necessários para realizar compras na Internet de forma responsável, além de enfatizar a importância de exercer direitos previstos no Código de Defesa do Consumidor.

Portal Antispam.br
Fonte de referência imparcial e embasada tecnicamente sobre o *spam*. Contém desde informações para administradores de redes e usuários finais, incluindo vídeos que abordam de forma simples e divertida os perigos aos quais os usuários estão expostos, explicam o que é *spam* e dão dicas de como navegar com mais segurança na rede.
antispam.br

VEJA TAMBÉM

Materiais de referência:

Caderno CGI.br "Combate ao spam na Internet no Brasil"
Histórico e reflexões sobre o combate ao spam e a gerencia da porta 25 coordenados pelo Comitê Gestor da Internet no Brasil.
cgi.br/publicacao/combate-ao-spam-na-internet-no-brasil

DISTRIBUIÇÃO DOS MATERIAIS
O NIC.br tem o compromisso de atender todos os interessados em seus materiais, da forma mais racional possível. Para que o máximo de interessados sejam atendidos, sem desperdício, limitamos o envio de materiais a lotes de 100 unidades. Caso sua instituição tenha interesse em distribuir uma quantidade maior, teremos o prazer em disponibilizar o conteúdo para que a impressão, com seu logotipo, seja realizada de acordo com sua capacidade.

SEJA UM PARCEIRO PARA A IMPRESSÃO DOS MATERIAIS!
Escreva para **info@nic.br** solicitando a inclusão do seu logotipo e especifique quais materiais você gostaria de imprimir.

LICENCIAMENTO
O objetivo primordial da produção dos nossos materiais é o compartilhamento de conteúdo, portanto a maioria deles está disponível gratuitamente para *download* e uso sob licenças *Creative Commons*. Sua instituição pode utilizá-los livremente, sem necessidade de autorização prévia, desde que a fonte seja mencionada, o uso do material não seja comercial (venda do material) e que o conteúdo não seja alterado. Para usos específicos fora do escopo da licença, escreva para **info@nic.br**.

Confira todas as nossas publicações e atividades em nic.br.

nic.br cgi.br

Obrigado

cristine@cert.br jessen@cert.br

notificações para: cert@cert.br @certbr

https://cert.br

10 de fevereiro de 2020

nic.br cgi.br

www.nic.br | www.cgi.br