nic.br cgi.br | cert.br

WTRio 2022 - Workshop de Tecnologias de Redes POP-RJ/RNP

22 de setembro de 2022

Rio de Janeiro - RJ

TLP:CLEAR

cert.br

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

CERT Nacional de Último Recurso

Serviços Prestados à Comunidade

Gestão de Incidentes

- Coordenação
- Análise Técnica
- Suporte à Mitigação e Recuperação

Consciência Situacional

- Aquisição de Dados
  - *Honeypots* Distribuídos
  - SpamPots
  - *Threat feeds*
- Compartilhamento das Informações

Transferência de Conhecimento

- Conscientização
  - Desenvolvimento de Boas Práticas
  - Cooperação, Eventos e Reuniões (*Outreach*)
- Treinamento
- Aconselhamento Técnico e de Políticas

Filiações e Parcerias:

FIRST Improving Security Together MEMBER

ACCREDITED BY TI TRUSTED INTRODUCER

APWG RESEARCH PARTNER www.antiphishing.org

CARNEGIE MELLON UNIVERSITY SOFTWARE ENGINEERING INSTITUTE

SEI Partner Network

HN/P

Criação:

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

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

[1] https://cert.br/sobre/estudo-cgibr-1996.html | [2] https://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.

Público Alvo (*Constituency*)

Redes que utilizam recursos administrados pelo NIC.br

- endereços IP ou ASNs alocados ao Brasil
- domínios sob o ccTLD .br

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, coordenada pelo MCTI
- responsável por coordenar e integrar as iniciativas e serviços da Internet no País

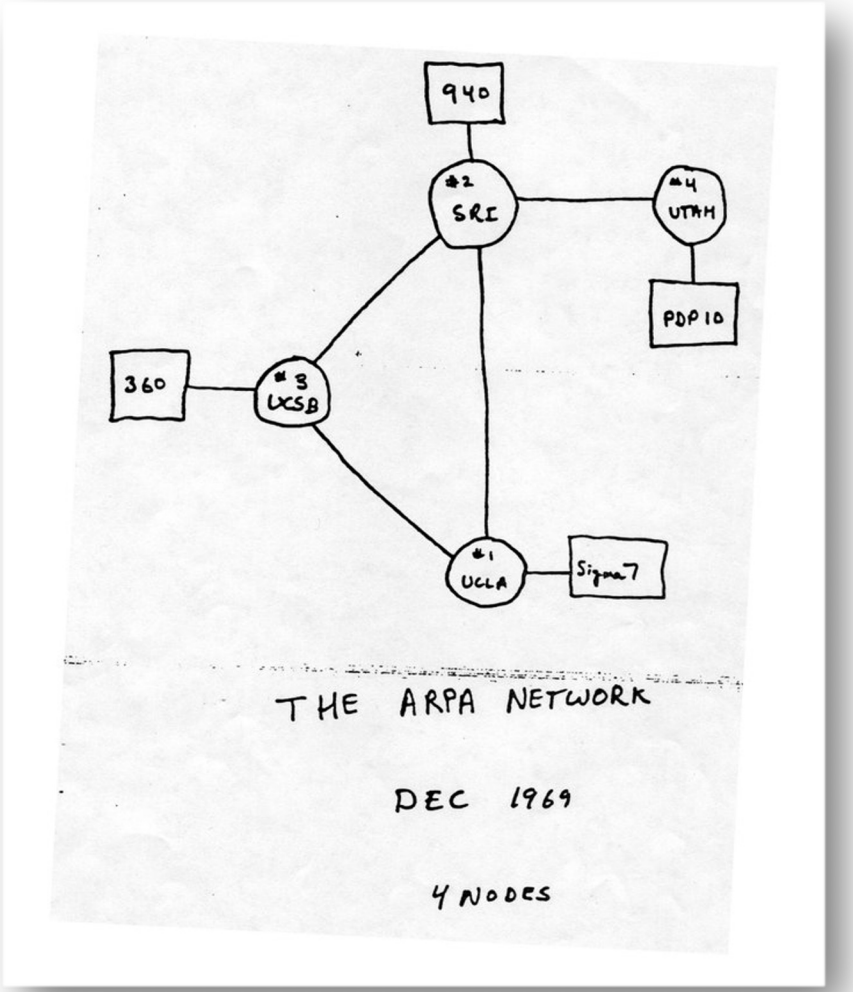
https://cert.br/sobre/
https://cert.br/sobre/filiacoes/
https://cert.br/about/rfc2350/

Importância de Padrões Modernos para a Segurança e Proteção de Dados

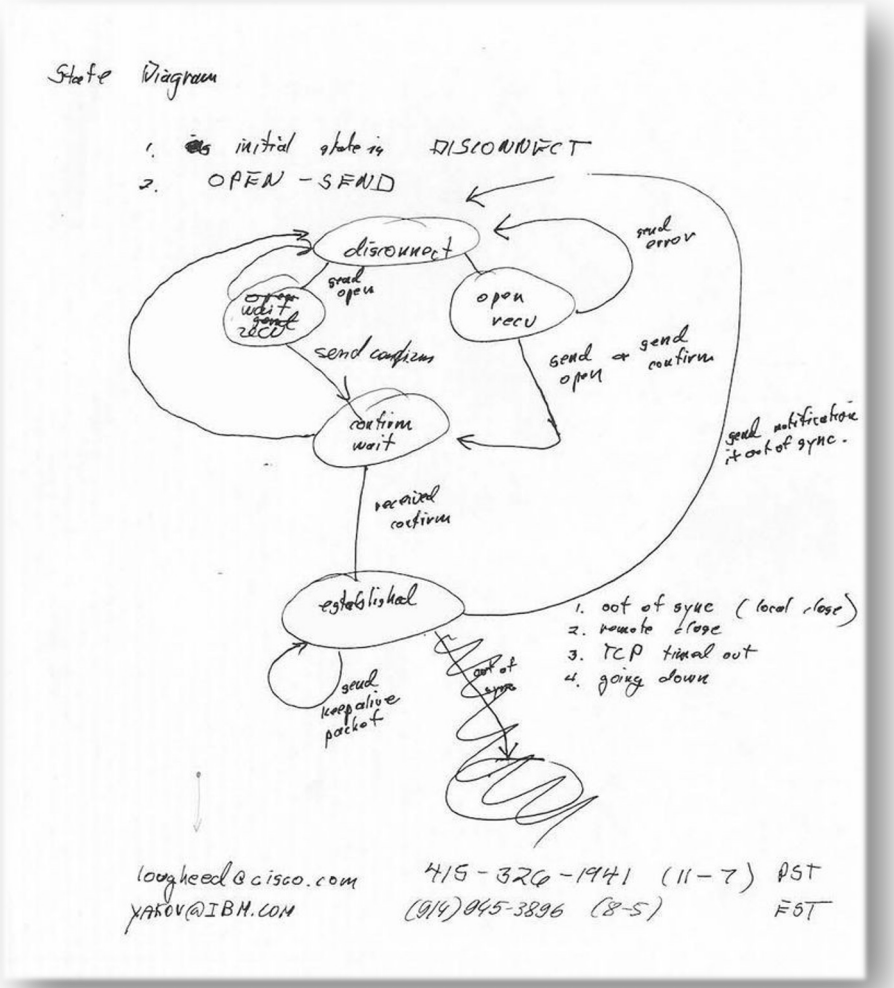
Dra. Cristine Hoepers
Gerente CERT.br/NIC.br
cristine@cert.br

cert.br nic.br cgi.br

Segurança Não Era Parte do Projeto



https://twitter.com/darpa/status/1013047020326739969



https://computerhistory.org/blog/the-two-napkin-protocol/

TLP:CLEAR

olhardigital.com.br

MENU

OLHAR DIGITAL

STJ se restabelece após ransomware; PF investiga cópia de dados

Renato Santino | 13/11/2020 21h45, atualizada em 13/11/2020 21h50

Os estra
Superio
totalme
investig
extensã
arquivo

infomoney.com.br

InfoMoney

O "lado B" da digitalização

Fleury é o mais recente episódio de ransomware; veja como os ataques cibernéticos têm afetado os mercados

Vistos como algumas das maiores ameaças da era atual, sequestros de dados, ou ransomware, viram novo risco a ser monitorado no mercado

Por Lara Riz
24 jun 2021 08h4

www1.folha.uol.com.br

JBS pagou US$ 11 mi em resposta a ataque ransomware em operações na América do Norte

Empresa cancelou turnos em fábricas nos EUA e Canadá na semana passada, após ser afetada por ciberataque

9.jun.2021 às 21h26

Ouvir o texto A- A+

REUTERS A JBS USA, subsidiária da brasileira JBS nos Estados Unidos, confirmou em comunicado divulgado nesta quarta-feira (9) que pagou o equivalente a US$ 11 milhões (R$ 55,5 milhões) em resposta a um ataque hacker contra suas operações

poder360.com.br

PODER 360 Diretor Fernando Rodrigues

Renner diz não ter pago resgate de dados depois de ataque hacker

A varejista sofreu uma invasão na última 5ª feira (19.ago.2021), mas informou que principais bancos de dados estão preservados

Compartilhe

TLP:CLEAR

bloomberg.com

Menu Search **Bloomberg** Sign In **Subscribe**

Bloomberg Cybersecurity

Photographer: Samuel Corum/Bloomberg

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

By William Turton and Kartikay Mehrotra
June 4, 2021, 4:58 PM GMT-3

- Investigators suspect hackers got password from dark web leak
- Colonial CEO hopes U.S. goes after criminal hackers abroad

https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

SolarWinds – Ataque atribuído à Russia pelos EUA

TLP:CLEAR

Causas: senha vazada + exploração de vulnerabilidades

SolarWinds FTP credentials were leaking on GitHub in November 2019 Featured

3 Shares | Share | Tweet 3

By Sam Varghese

More details are emerging about poor security at SolarWinds, following the compromise of its Orion network management software that was then used to effect attacks on many companies in a number of regions around the globe.

A researcher from India had advised SolarWinds in November 2019 that he had found a public GitHub repository which was leaking the company's FTP credentials.

Downloads Url: http://downloads.solarwinds.com
FTP Url: ftp://solarwinds.upload.akamai.com
Username:
Password:
POC: http://downloads.solarwinds.com/test.txt

I was able to upload a test POC.
Via this any hacker could upload malicious exe and update it with release SolarWinds product.

bounty hunter, said in a tweet: "Was
raging SolarWinds. Hmmm, how that
d was *****123 Rolling on the floor

https://www.itwire.com/security/solarwinds-ftp-credentials-were-leaking-on-github-in-november-2019.html
https://threatpost.com/solarwinds-default-password-access-sales/162327/
https://us-cert.cisa.gov/remediating-apt-compromised-networks

TLP:CLEAR

Alert (AA22-117A)

More Alerts

2021 Top Routinely Exploited Vulnerabilities

Original release date: April 27, 2022

Print | Tweet | Send | Share

Summary

This joint Cybersecurity Advisory (CSA) was coauthored by cybersec
Canada, New Zealand, and the United Kingdom: the Cybersecurity a
Security Agency (NSA), Federal Bureau of Investigation (FBI), Austral
Centre for Cyber Security (CCCS), New Zealand National Cyber Sec
National Cyber Security Centre (NCSC-UK). This advisory provides d
Exposures (CVEs) routinely exploited by malicious cyber actors in 20

Table 1: Top 15 Routinely Exploited Vulnerabilities in 2021

CVE	Vulnerability Name	Vendor and Product	Type
CVE-2021-44228	Log4Shell	Apache Log4j	Remote code execution (RCE)
CVE-2021-40539		Zoho ManageEngine AD SelfService Plus	RCE
CVE-2021-34523	ProxyShell	Microsoft Exchange Server	Elevation of privilege
CVE-2021-34473	ProxyShell	Microsoft Exchange Server	RCE
CVE-2021-31207	ProxyShell	Microsoft Exchange Server	Security feature bypass
CVE-2021-27065	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26858	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26857	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26855	ProxyLogon	Microsoft Exchange Server	RCE
CVE-2021-26084		Atlassian Confluence Server and Data Center	Arbitrary code execution
CVE-2021-21972		VMware vSphere Client	RCE
CVE-2020-1472	ZeroLogon	Microsoft Netlogon Remote Protocol (MS-NRPC)	Elevation of privilege
CVE-2020-0688		Microsoft Exchange Server	RCE
CVE-2019-11510		Pulse Secure Pulse Connect Secure	Arbitrary file reading
CVE-2018-13379		Fortinet FortiOS and FortiProxy	Path traversal

https://www.cisa.gov/uscert/ncas/alerts/aa22-117a

Infraestruturas Críticas e Órgãos Governamentais
Alvos de Ataques

TLP:CLEAR

DigiNotar Certificate Authority Breach Crashes e-Government in the Netherlands

›A taste of what is to routinely come?

BY ROBERT N. CHARETTE | 09 SEP 2011 | 7 MIN READ |

Inside 'Operation Black Tulip': DigiNotar hack analysed

CA systems falsely told Iranians they were secure

John Leyden — Tue 6 Sep 2011

28

The Google webmail of as many as 300,000 Iranians may have been intercepted using fraudulently issued security certificates made after a hack against Dutch certificate authority outfit DigiNotar, according to the preliminary findings of an official report into the megahack.

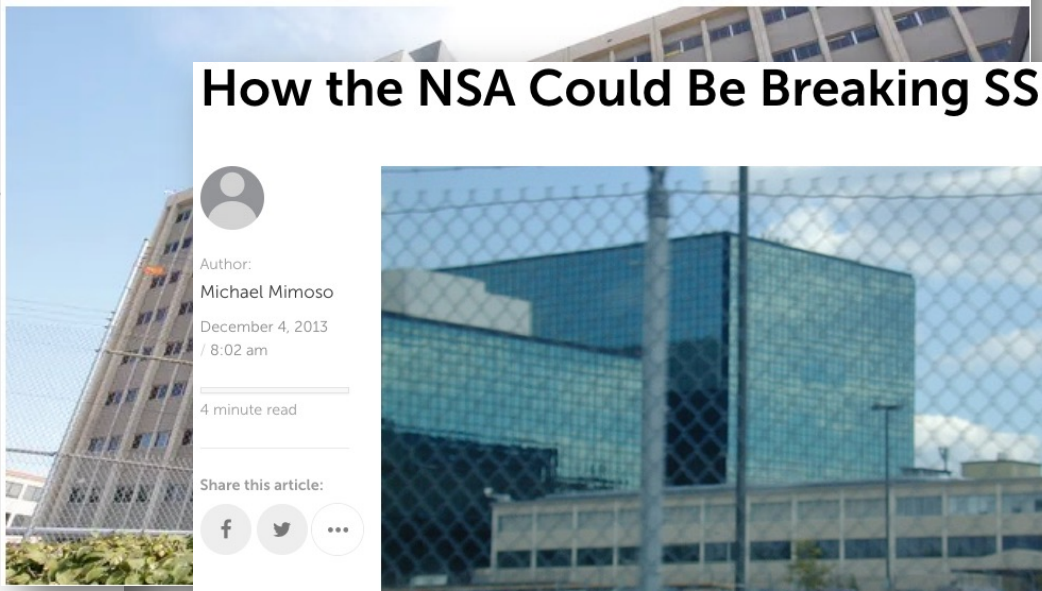
Fox-IT, the security consultancy hired to examine the breach against DigiNotar, reveals that DigiNotar was hacked on or around 6 June – a month before hackers begun publishing rogue certificates.

Between 10 July and 20 July hackers used compromised access to DigiNotar's systems to issue rogue 531 SSL certificate for Google and other domains, including Skype, Mozilla add-ons, Microsoft update and others. DigiNotar only began revoking

Brazil expresses concern at report of NSA spying

AP

Published 5:17 p.m. ET July 7, 2013 | Updated 7:19 p.m. ET July 7, 2013



How the NSA Could Be Breaking SSL

Author: Michael Mimoso

December 4, 2013 / 8:02 am

4 minute read

Share this article:

How is the NSA beating or breaking SSL? Cryptographer Matthew Green lays out a number of possibilities.

https://spectrum.ieee.org/diginotar-certificate-authority-breach-crashes-egovernment-in-the-netherlands
https://www.theregister.com/2011/09/06/diginotar_audit_damning_fail/
https://www.usatoday.com/story/news/world/2013/07/07/brazil-concern-nsa-spying-snowden/2497161/
https://threatpost.com/how-the-nsa-could-be-breaking-ssl/103091/

TLP:CLEAR

Precisamos Cuidar da Base Primeiro:
Causas Mais Comuns de Invasões e Vazamentos de Dados

Ataques mais reportados e mais observados em sensores do CERT.br:

- Tentativas de fraudes financeiras e de comércio eletrônico
  - via e-mails falsos (***phishings***)
  - via infecção de roteadores de banda larga (CPEs) para **DNS *hijacking***
  - via infecção de computadores e de celulares
- Invasão por meio de **senhas comprometidas**, vazadas ou fracas
  - via ***phishing***
  - via força bruta
  - senhas expostas no Github/Pastebin pelos próprios donos/desenvolvedores dos sistemas

  Exemplos de serviços afetados:
  - *e-mails* e serviços em nuvem
  - acesso remoto (VPN, SSH, RDP, Winbox, etc)
  - gestão remota de ativos de rede e servidores
- Exploração de vulnerabilidades para invasão e/ou movimentação lateral
  - falta de aplicação de correções
  - **erros de configuração**
  - **falta / falha de processos**

Veja também: Principais Ataques na Internet: Dados do CERT.br
https://youtu.be/nHh8hHaomFE?t=714
https://cert.br/stats/

Mais de 80% dos incidentes seriam evitados se

- todas as correções (*patches*) fossem aplicadas
- houvesse **mais atenção a erros e configurações**
- todos os serviços tivessem 2FA / MFA

Estudo Setorial Segurança digital: uma análise de gestão de risco em empresas brasileiras
https://cetic.br/pt/publicacao/seguranca-digital-uma-analise-de-gestao-de-risco-em-empresas-brasileiras/

TLP:CLEAR

Padrões Modernos que Aumentam a Segurança

	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	Proteção contra envenenamento de *cache* Habilitar o uso de outras tecnologias como o DANE
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 • redes móveis já tem IPv6 nativo	Mais estabilidade e menor complexidade • Não depender de CGN ou tradução v6 → v4 • Não depender de transição, reduz superfície de ataques Facilita o processo investigativo e de tratamento de incidentes
Segurança de roteamento	RPKI	Certificação de recursos Validação de origem no BGP

TESTE OS PADRÕES

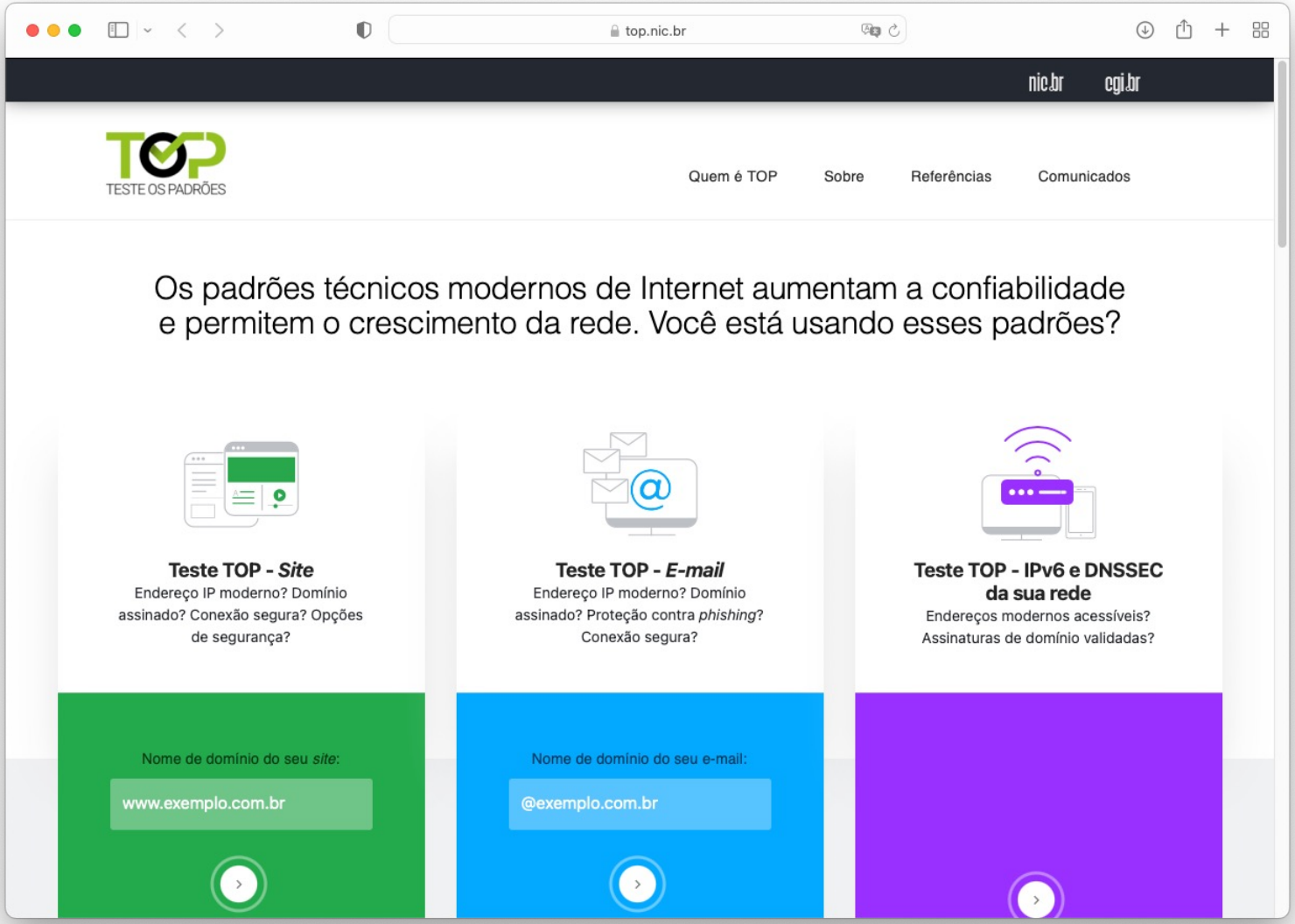
https://top.nic.br/
Padrões Testados

TLP:CLEAR

	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	Proteção contra envenenamento de *cache* Habilitar o uso de outras tecnologias como o DANE
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 • redes móveis já tem IPv6 nativo	Mais estabilidade e menor complexidade • Não depender de CGN ou tradução v6 → v4 • Não depender de transição, reduz superfície de ataques Facilita o processo investigativo e de tratamento de incidentes
Segurança de roteamento	RPKI	Certificação de recursos Validação de origem no BGP

TLP:CLEAR

https://top.nic.br/
Testes para *site*, *e-mail* e conectividade



Testes

- verificam a correta implementação dos padrões
- baseiam-se
  - nas especificações das RFCs
  - em padrões técnicos operacionais recomendados por entidades internacionais

Relatório

- detalhamento de todos os resultados
  - referências detalhadas dos padrões
  - indicações sobre como corrigir possíveis problemas

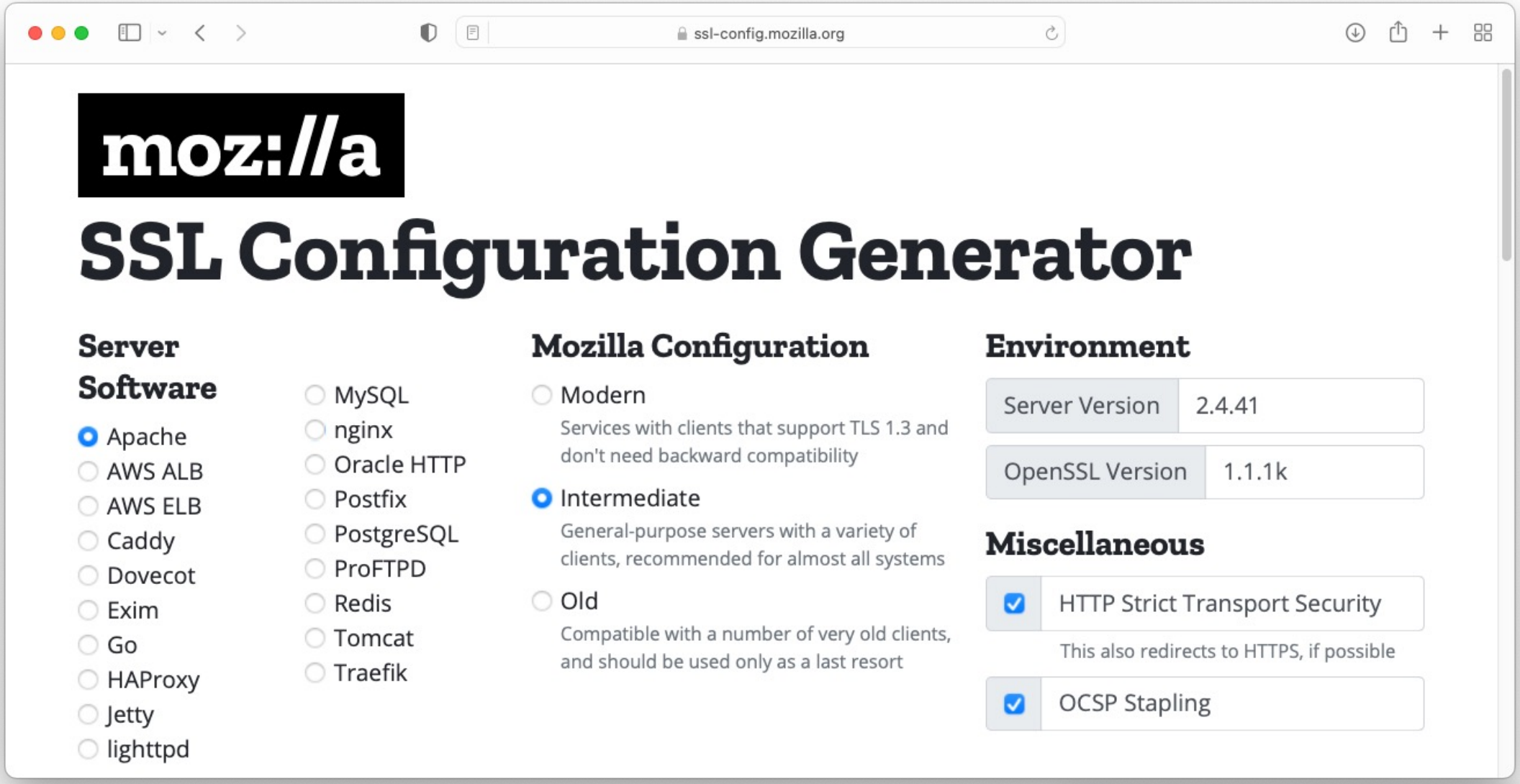
Outros *Sites* para Auxiliar nos Testes e Configurações

cert.br nic.br cgi.br

SSL Configuration Generator

https://ssl-config.mozilla.org/

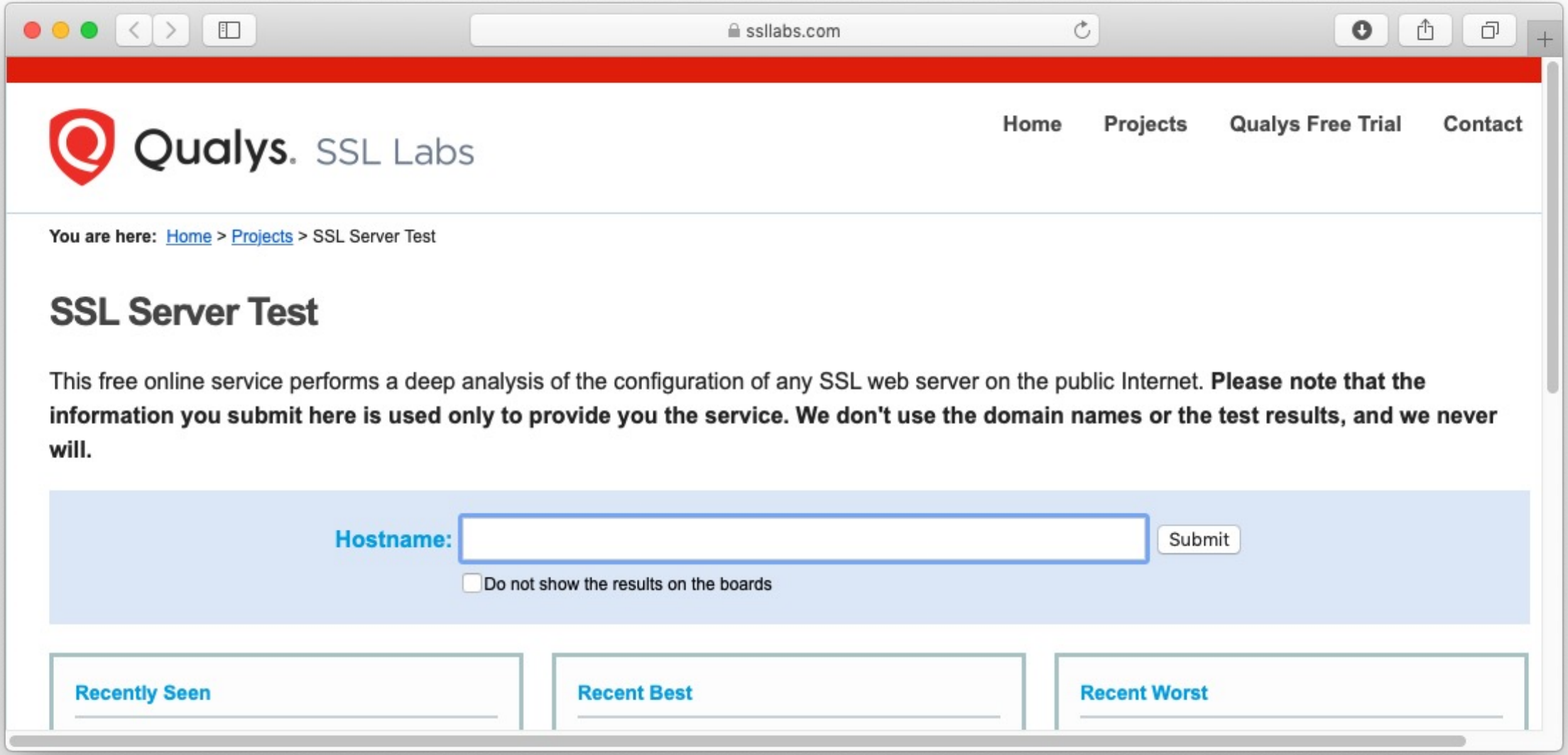
TLP:CLEAR



SSL Server Test

https://www.ssllabs.com/ssltest/

TLP:CLEAR



TLP:CLEAR

Referências dos Padrões Citados

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	https://registro.br/tecnologia/dnssec/dnssec-para-provedores/ https://ftp.registro.br/pub/doc/tutorial-dnssec.pdf 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
RPKI	https://bcp.nic.br/rpki https://sg-pub.ripe.net/jasper/rpki-web-test/

Outras Iniciativas para uma Internet mais Segura

cert.br nic.br cgi.br

TLP:CLEAR

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, Conexis, Abranet, Abrint, InternetSul, RedeTelesul, Telcomp

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

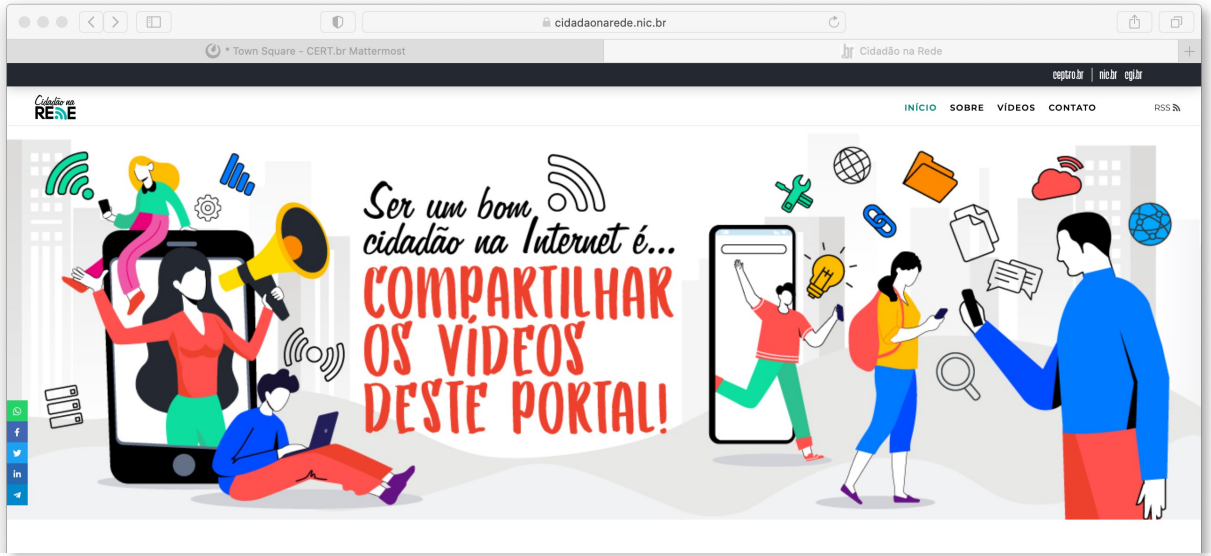
Conscientização:
Portal InternetSegura.br

TLP:CLEAR

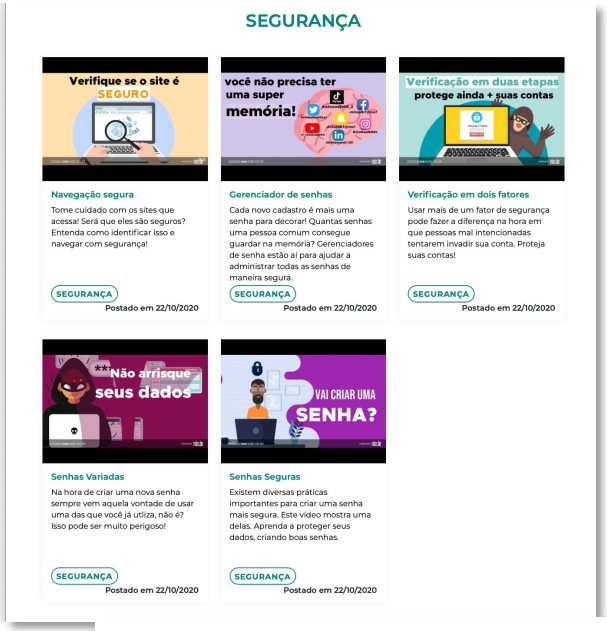
TLP:CLEAR

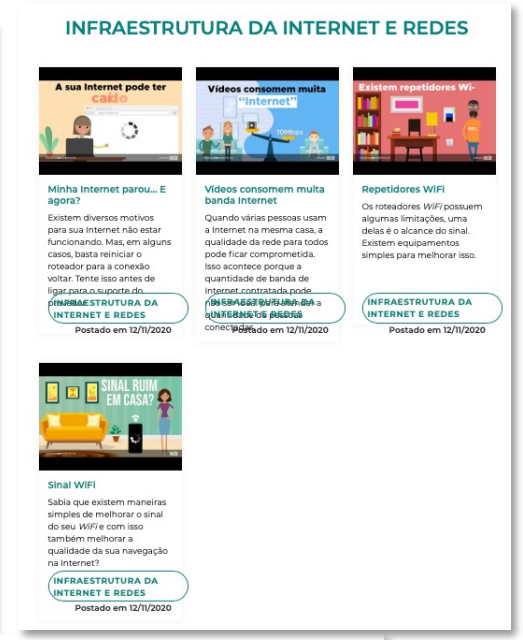
Projeto Cidadão na Rede

- Vídeos curtos sobre diversos temas:
  - Segurança
  - Infraestrutura da Internet e redes
  - Uso responsável e deveres na Internet
- Seja um apoiador
  - Tenha os vídeos com seu logo
  - Todo o processo via o portal



https://cidadaonarede.nic.br/





TLP:CLEAR

Cartilha de Segurança para Internet: **Fascículos e *Slides* para Palestras e Treinamento**

Conteúdo disponível *online* gratuitamente sob Licença *Creative Commons*

- **Fascículos** que cobrem assuntos específicos relacionados com segurança na Internet
- ***Slides*** sobre cada um dos temas, que podem ser utilizados, por exemplo, para dar aulas ou palestras de conscientização
  - Dica do dia no *site*, via *Twitter* e RSS
  - Impressões em pequena escala enviadas a escolas e centros de inclusão digital
  - Possível gerar versões personalizadas com logo da instituição

    Exemplos de parceiros de impressão e distribuição:

    Itaipu, Eletronuclear, ELO, Microsoft, Procergs e Metrô SP

https://cartilha.cert.br/

Novo Material:
Furto de Celular

TLP:CLEAR

SEU CELULAR É SUA CARTEIRA: CUIDE DA SUA VIDA DIGITAL

Toda praticidade que o celular traz pode rapidamente se tornar um pesadelo se ele cair nas mãos erradas.

O Fascículo Furto de Celular mostra como se preparar para reduzir os danos e traz dicas sobre o que fazer se um furto ocorrer.

https://cartilha.cert.br/fasciculos/#furto-de-celular

Obrigada

cristine@cert.br

notificações para: cert@cert.br

@certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br