

nic.br egi.br

cert.br

X Encontro de Segurança em Informática do CERT.Bahia
05 a 09 de Outubro de 2020
Evento *Online*

Onde Investir para Reduzir o Risco: o que dizem os dados?

Lucimara Desiderá, M.Sc
Analista de Segurança
lucimara@cert.br

cert.br nic.br egi.br

Incidentes Mais Comuns

Visão Global

cert.br nic.br egi.br

You weren't hacked because you lacked space-age network defenses. Nor because cyber-gurus picked on you. It's far simpler than that

Three little words: Patches, passwords, policies

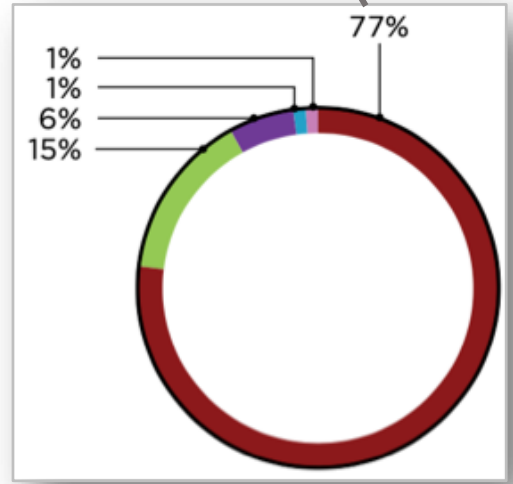
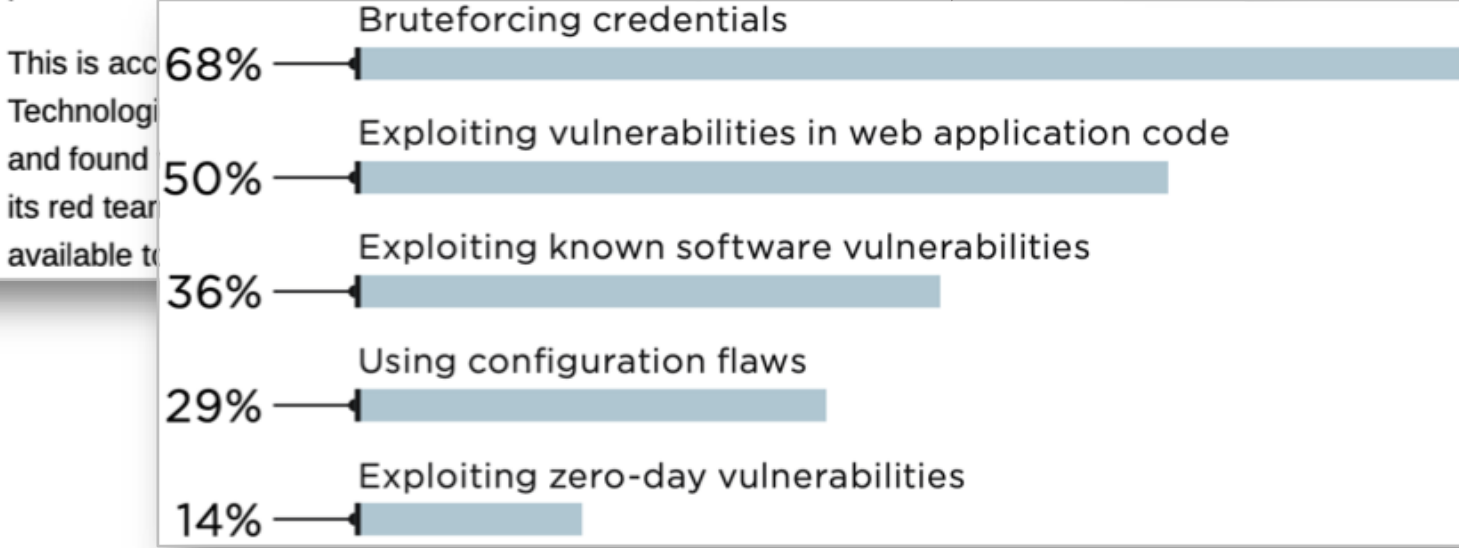
Thu 13 Aug 2020 // 07:06 UTC

Shaun Nichols in San Francisco [BIO](#) [EMAIL](#) [TWITTER](#)

The continued inability of organizations to patch security vulnerabilities in a timely manner, combined with guessable passwords and the spread of automated hacking tools, is making it pretty easy for miscreants, professionals, and thrill-seekers to break into corporate networks.

31

- Using web application protection vulnerabilities and flaws
- Bruteforcing credentials used for accessing DBMS
- Bruteforcing credentials for remote access services
- Bruteforcing domain user credentials together with software vulnerabilities exploitation
- Bruteforcing credentials for the FTP server



https://www.theregister.com/2020/08/13/pentest_networks_fail/

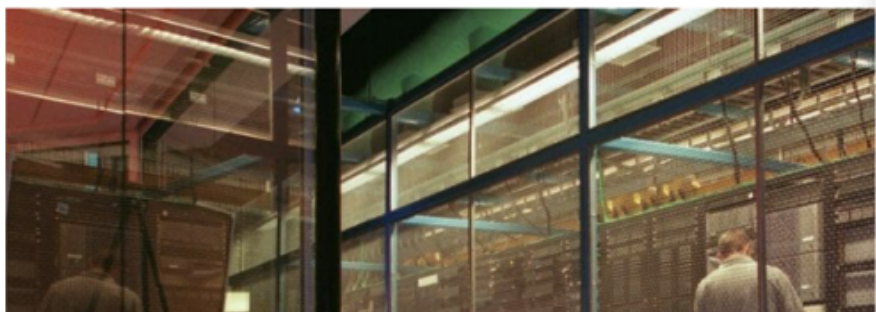
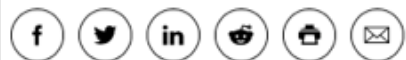
<https://www.ptsecurity.com/upload/corporate/ww-en/analytics/external-pentests-2020-eng.pdf>

August 6, 2020

Lesson learned: Failure to patch led to password leak of 900 VPN enterprise servers

Teri Robinson

Follow @TeriRnNY



The [CVE-2019-11510](#) has a CVSS score of 10.

Applying a security update to a CVE released more than a year ago could have prevented a hacker from publishing plaintext usernames and passwords, as well as IP addresses, for more than 900 Pulse Secure VPN enterprise servers.

“The lesson here? Patch, patch, patch,” said Laurence Pitt, global security strategy director at Juniper Networks. “The fact that this vulnerability allowed for username/cleartext password combinations to be exposed is bad enough, but what makes it unacceptable is that this was reported in a CVE, released over a year ago and fixed in a later version of the product.”

<https://www.kb.cert.org/vuls/id/927237/>

<https://www.scmagazine.com/home/security-news/patch-fail-led-to-password-leak-of-900-vpn-enterprise-servers/>

Top 10 Most Exploited Vulnerabilities 2016–2019

U.S. Government reporting has identified the top 10 most exploited vulnerabilities by state, nonstate, and unattributed cyber actors from 2016 to 2019 as follows: CVE-2017-11882, CVE-2017-0199, CVE-2017-5638, CVE-2012-0158, CVE-2019-0604, CVE-2017-0143, CVE-2018-4878, CVE-2017-8759, CVE-2015-1641, and CVE-2018-7600.

Top 10 Most Exploited in 2020

Of the top 10 vulnerabilities from 2016 to 2019 listed above, the U.S. Government reported that the following vulnerabilities are being routinely exploited by sophisticated foreign cyber actors in 2020:

Alert (AA20-133A)

Top 10 Routinely Exploited Vulnerabilities

Original release date: May 12, 2020

Print Tweet Send Share

Summary

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the broader U.S. Government are providing this technical guidance to advise IT security professionals at public and private sector organizations to place an increased priority on patching the most commonly known vulnerabilities exploited by sophisticated foreign cyber actors.

- Malicious cyber actors are increasingly targeting unpatched Virtual Private Network vulnerabilities.
 - An arbitrary code execution vulnerability in Citrix VPN appliances, known as CVE-2019-19781, has been detected in exploits in the wild.
 - An arbitrary file reading vulnerability in Pulse Secure VPN servers, known as CVE-2019-11510, continues to be an attractive target for malicious actors.
- March 2020 brought an abrupt shift to work-from-home that necessitated, for many organizations, rapid deployment of cloud collaboration services, such as Microsoft Office 365 (O365). Malicious cyber actors are targeting

<https://us-cert.cisa.gov/ncas/alerts/aa20-133a>

Rapid7 NICER Report 2020

Metodologia de estudo

- “probe against all of IPv4 space to see if there’s something listening at all on a given port using Zmap”
- “then perform a protocol-level request against all nodes that responded to the initial probe”
- “Project Heisenberg is a net of honeypots Rapid7 has deployed across the [...] attacks are aggregated and sent to Rapid7 for enrichment and analysis”

National / Industry / Cloud Exposure Report (NICER) 2020

Rapid7’s National / Industry / Cloud Exposure Report (NICER) for 2020 is the most comprehensive census of the modern internet. In a time of global pandemic and recession, the Rapid7 research team offers this data-backed analysis of the changing internet risk landscape, measuring the prevalence and geographic distribution of commonly known exposures in the interconnected technologies that shape our world.



Rapid7 NICER Report 2020: Most Exposed Countries

- **Total attack surface** (i.e., number of total IPv4s in use exposing something during the study period). Rationale: More stuff = more stuff to attack.
- **Total exposure of selected services.** Specifically SMB, SQL Server, and Telnet. Rationale: These should never be exposed. Ever.
- **Distinct number of CVEs present across all services.** Rationale: More known vulnerabilities = more exposure.
- **The center of the distribution of vulnerability rates.** Vulnerability rate is defined as the number of exposed services with vulnerabilities/exposed services. Rationale: Higher vulnerability concentration across all exposed services should contribute more to the rank penalty.
- **Maximum vulnerability rate.** Rationale: To break any ties that remain after the previous steps, penalize a nation state with the highest vulnerability rate.

Rank	Country
1	United States
2	China
3	South Korea
4	United Kingdom
5	Germany
6	Brazil
7	Russia
8	Japan
9	Canada
10	Iran

Rapid7 NICER Report 2020: Internet Security – Key Findings

Acesso/console

- **Key finding:** We have discovered nearly 3 million Telnet servers still active and available on the internet, and many of those are associated with core routing and switching gear. This is 3 million too many. While remote console access is a fundamental design goal of the internet, there is no reason to rely on this ancient technology on the routers and switches that are most responsible for keeping the internet humming.

Patches

- **Key finding:** Patch and update adoption continues to be slow, even for modern services with reports of active exploitation. This is particularly true in the areas of email handling and remote console access where, for example, 3.6 million SSH servers are sporting vulnerable versions between five and 14 years old. More

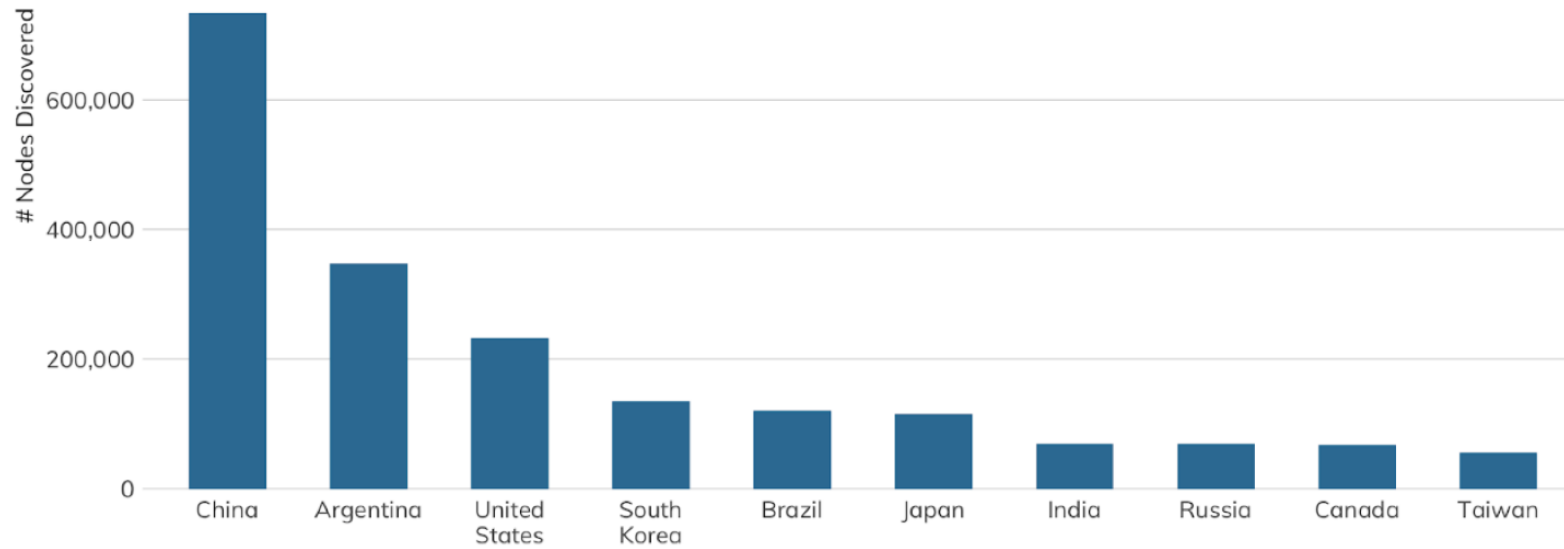
Criptografia

- **Key finding:** A technical assessment of the 24 service protocols surveyed finds that, on the whole, unencrypted, cleartext protocols are still the rule, rather than the exception, on how information flows around the world, with 42% more plaintext HTTP servers than HTTPS, 3 million databases awaiting insecure queries, and 2.9 million routers, switches, and servers accepting Telnet connections.

Rapid7 NICER Report 2020: TELNET (23/TCP)

TLP:WHITE

Top 10 Countries for Console Access : Telnet (23)



Vendor	Count
Cisco	278,472
Huawei	108,065
MikroTik	73,511
HP	70,821
Ruijie	17,565
ZTE	15,558

Dados do CERT.br

cert.br nic.br egi.br

Tratamento de Incidentes

- ▶ Articulação
- ▶ Análise Técnica
- ▶ Apoio à recuperação

Treinamento e Conscientização

- ▶ Cursos
- ▶ Palestras
- ▶ Boas Práticas
- ▶ Reuniões

Análise de Tendências

- ▶ *Honeypots* Distribuídos
- ▶ SpamPots
- ▶ Processamento de *threat feeds*

Filiações e Parcerias:



SEI
Partner
Network



Criação:

Agosto/1996: o relatório “Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil” é publicado pelo CGI.br¹

Junho/1997: o CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório²

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.

Público Alvo (*Constituency*)

Redes que utilizam recursos alocados pelo NIC.br (endereços IP ou ASNs alocados ao Brasil e domínios sob o ccTLD .br).

Foco das Atividades

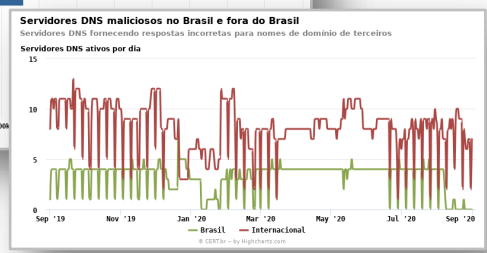
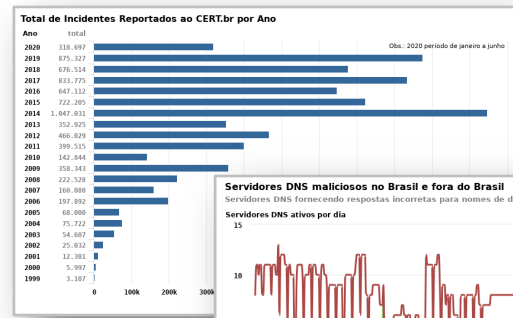
- Ponto de contato nacional
- Trabalho colaborativo com outras entidades
- Auxiliar na análise técnica e compreensão de ataques e ameaças
- Aumentar a detecção, correlação de eventos e determinação de tendências
- Transferir o conhecimento através de cursos, boas práticas e conscientização

Tratamento de Incidentes: Fontes dos Dados, Métricas e Compartilhamento

Notificações voluntárias de incidentes enviadas para:

cert@cert.br

- 2019: 4.086.406 de e-mails tratados, relativos a 875.327 incidentes notificados ao CERT.br



Compartilhamento via MISP

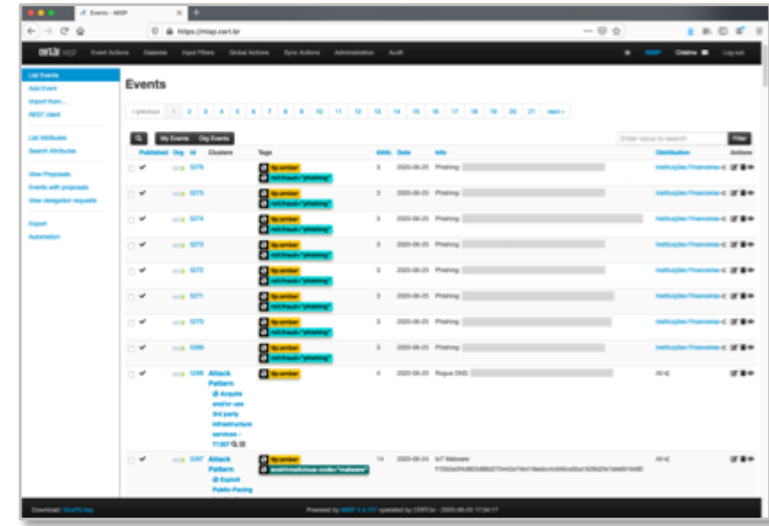
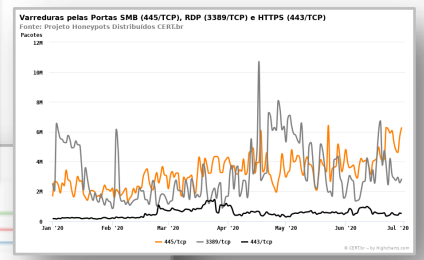
- Indicadores selecionados são compartilhados com parceiros
- Servidores DNS maliciosos
- Phishing
- Binários e Comando e Controle de botnets IoT
- Amplificadores usados em ataques DDoS

Threat feeds

- Honeypots Distribuídos do CERT.br
- Team Cymru
- SpamHaus
- ShadowServer
- Shodan
- Operações Anti-Botnet (Microsoft/FBI)



Notificações para os ASNs e estatísticas públicas



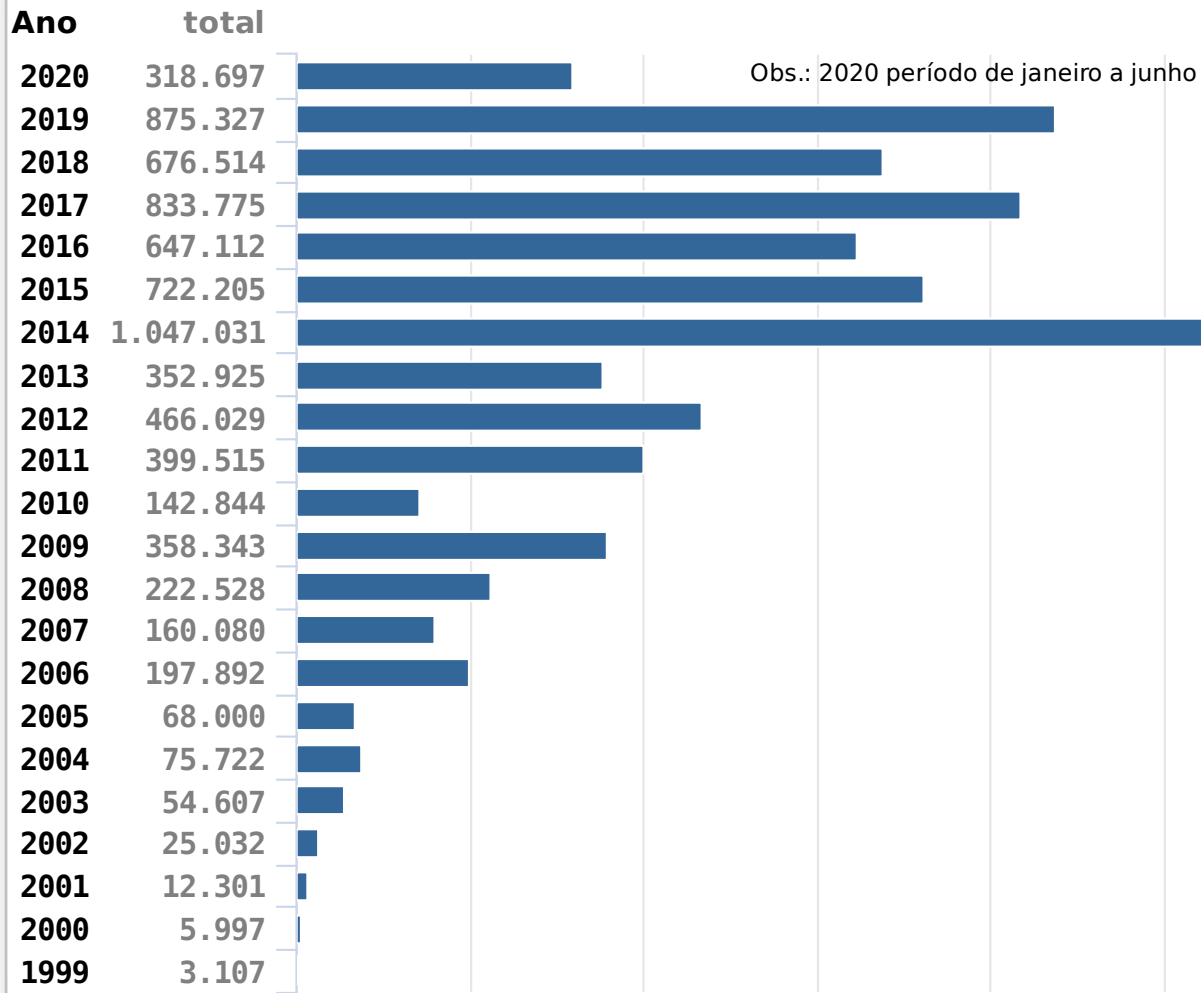
<https://cert.br/stats/>

<https://cert.br/misp/>

Incidentes Reportados Voluntariamente para o CERT.br: Dados Totais de 1999 ao 1º Semestre de 2020

TLP:WHITE

Total de Incidentes Reportados ao CERT.br por Ano

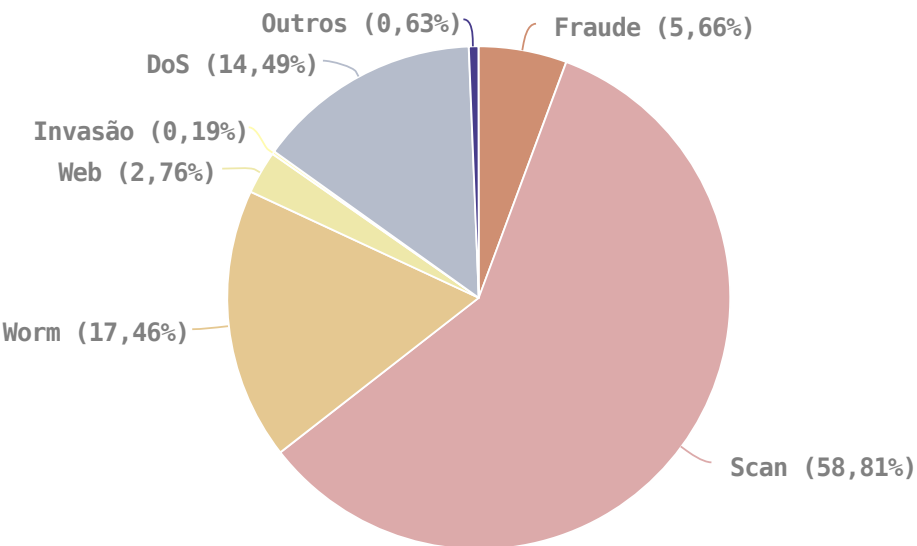


Ataques mais comuns no último semestre

- Busca por serviços com credenciais fáceis e sem MFA
 - *e-mails* (IMAP, SMTP e SMTPS)
 - SSH e TELNET
 - elementos de rede e servidores
 - IoT e roteadores de banda larga
- Internet das coisas
 - Câmeras, *Smartphones*, TVs, Roteadores e *Modems* de banda larga/Wi-Fi
 - DDoS (UDP *flood*)
 - modificar DNS como parte de fraudes
 - minerar criptomoedas

Fonte: <https://cert.br/stats/incidentes/>

Incidentes Reportados para o CERT.br: Tipos de incidentes – 1º semestre de 2020

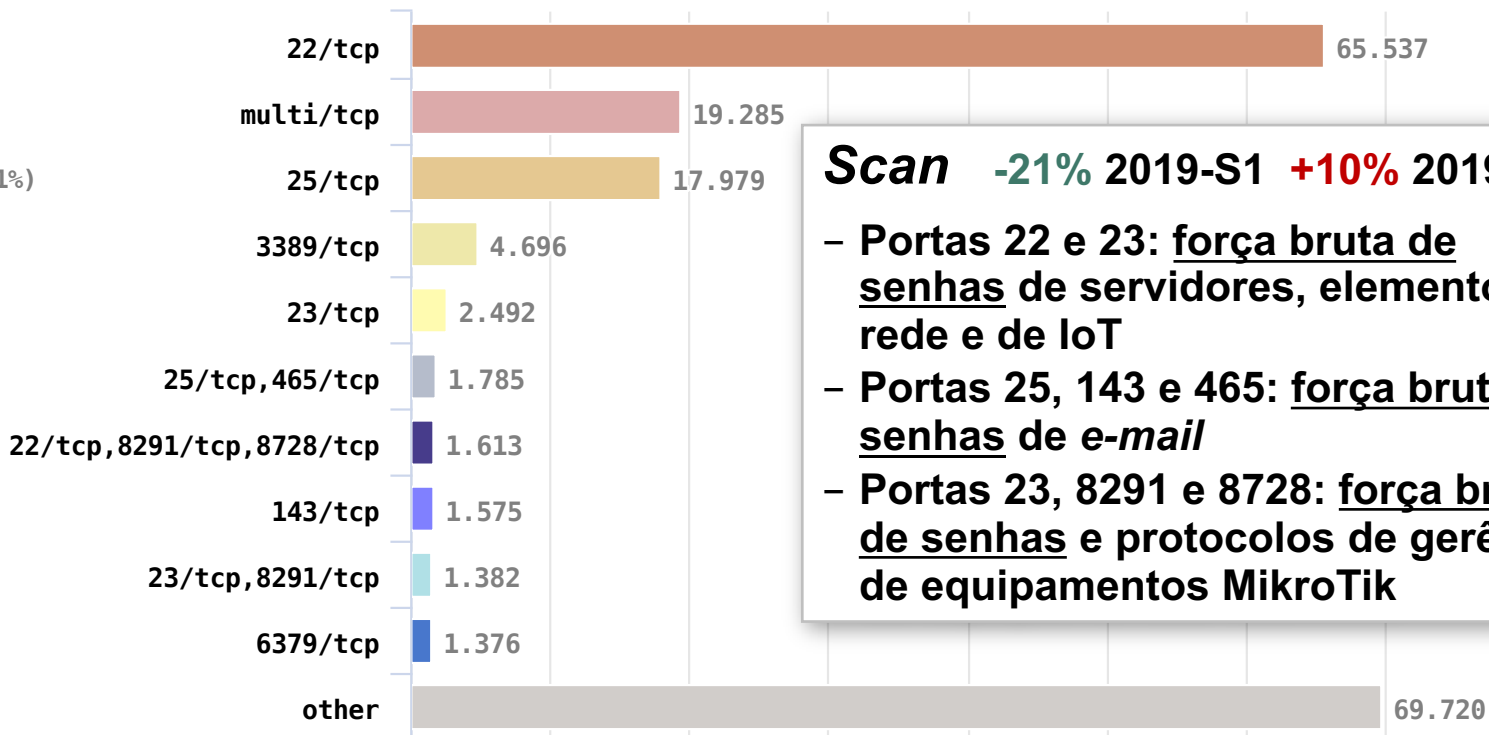


Fraude +54% 2019-S1 -35% 2019-S2

- 96% são páginas falsas (*phishing*)
- Relacionadas com invasão de CPEs para alterar o DNS

DDoS -81% 2019-S1 -17% 2019-S2

- Aumentou de patamar em 2014
- Maior número em 2019
- Tipos mais frequentes
 - . botnets IoT
 - . amplificação de tráfego

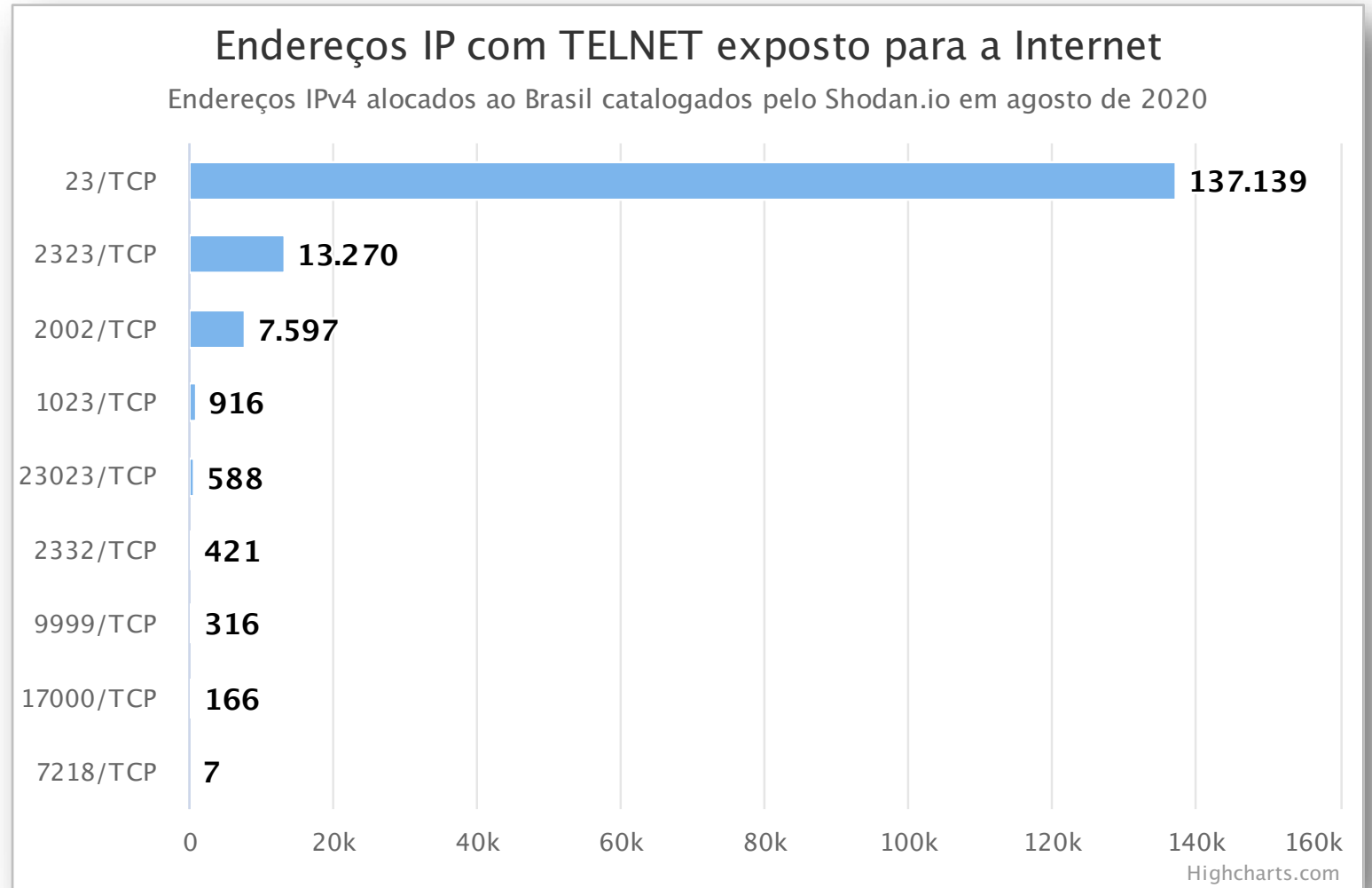


Scan -21% 2019-S1 +10% 2019-S2

- Portas 22 e 23: força bruta de senhas de servidores, elementos de rede e de IoT
- Portas 25, 143 e 465: força bruta de senhas de e-mail
- Portas 23, 8291 e 8728: força bruta de senhas e protocolos de gerência de equipamentos MikroTik

Varreduras TCP: *Honeypots* (2020-S1) e TELNET no Shodan.io

#	Porta TCP	Pacotes	Bytes	Flows
01	23/tcp	30,1 G	1,5 TB	452,8 M
02	22/tcp	1,2 G	99,0 GB	250,2 M
03	445/tcp	595,2 M	43,5 GB	362,3 M
04	3389/tcp	574,4 M	28,0 GB	172,8 M
05	80/tcp	280,0 M	14,6 GB	200,6 M
06	1433/tcp	202,3 M	8,4 GB	174,0 M
07	443/tcp	95,6 M	4,1 GB	74,8 M
08	8080/tcp	77,2 M	3,9 GB	54,1 M
09	110/tcp	54,5 M	2,3 GB	12,0 M
10	81/tcp	47,1 M	1,8 GB	45,4 M
11	5900/tcp	44,7 M	2,1 GB	17,2 M
12	5555/tcp	41,8 M	1,6 GB	39,8 M
13	8545/tcp	37,9 M	1,4 GB	37,7 M
14	8291/tcp	37,6 M	1,6 GB	36,5 M
15	21/tcp	35,2 M	1,4 GB	12,5 M



Fonte: <https://cert.br/stats/honeypots/>

O que Priorizar

cert.br nic.br egi.br

O Básico:

Manter Sistemas Atualizados

- Acompanhe todos os fabricantes do seu parque
- Atualize **TODOS** os sistemas e aplicações
 - mesmo que sejam “só internos”
- Defina regras para priorizar a aplicação de correções de segurança

<https://www.first.org/cvss/>

Múltiplos Fatores de Autenticação

- Impede sucesso de força bruta de senhas
- Reduz impacto do comprometimento de credenciais

Tecnologias:

- Chaves criptográficas / certificados
- *Tokens*
 - em *hardware* (FIDO2/U2F)
 - em *software* (HOTP/TOTP)

Onde Investir Primeiro, Além do Básico

cert.br nic.br egi.br

Depois do Básico: Adotar Protocolos Mais Modernos

	Padrões	Vantagens da Adoção
Criptografia forte	HTTPS mandatório e HSTS Versões atuais de TLS <i>Forward Secrecy</i>	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 <i>cache</i> Habilitar o uso de outras tecnologias como o DANE
Segurança de <i>e-mail</i>	STARTTLS • idealmente c/ DANE DMARC, DKIM e SPF	Proteção contra <i>sniffing</i> (“espionagem”) Aumento da reputação da mensagem legítima (ajuda a prevenir <i>phishing</i> 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 no futuro Facilita o processo investigativo e de tratamento de incidentes

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

TLP:WHITE

The screenshot shows a web browser window with the URL internet.nl. The page features the Internet.nl logo with the tagline "IS YOUR INTERNET UP TO DATE?". Navigation links include Home, News, Knowledge base, Hall of Fame, and About Internet.nl. A teal banner contains the text: "Modern Internet Standards provide for more reliability and further growth of the Internet. Are you using them?". Below this are three test sections:

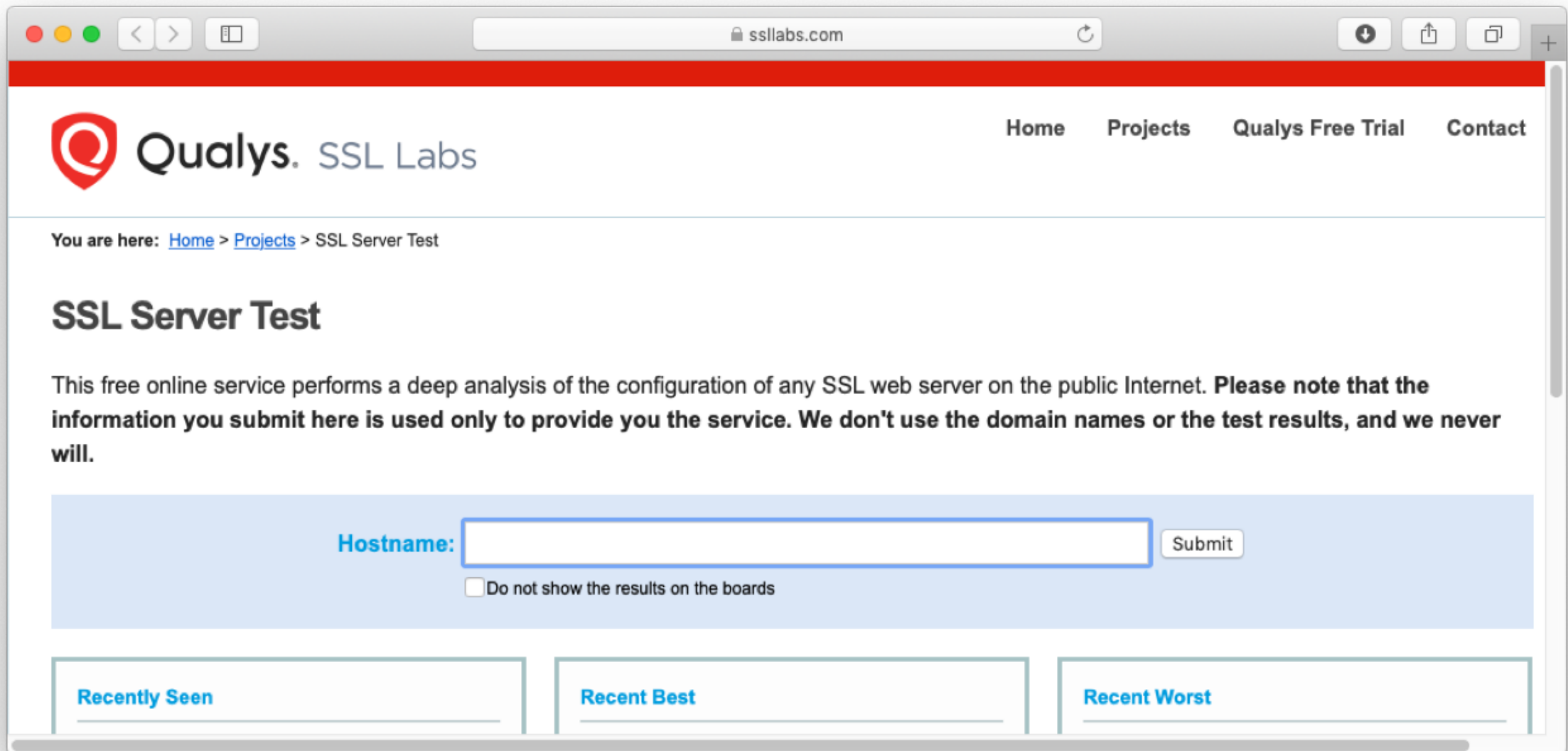
- Test your website** (with a padlock icon): "Modern address? Signed domain? Secure connection? Security options?" with a link to "about the test". The input field contains "www.example.nl".
- Test your email** (with an envelope icon): "Modern address? Signed domain? Anti-phishing? Secure connection?" with a link to "about the test". The input field contains "@ example.nl".
- Test your connection** (with a signal icon): "Modern addresses reachable? Domain signatures validated?" with a link to "about the test".

Each section has a "Start test" button.

SSL Server Test

TLP:WHITE

<https://www.ssllabs.com/sslltest/>



SSL Configuration Generator

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

The screenshot shows the Mozilla SSL Configuration Generator website. The browser address bar displays 'ssl-config.mozilla.org'. The main heading is 'SSL Configuration Generator' with the Mozilla logo 'moz://a' above it. The page is divided into three main sections: 'Server Software', 'Mozilla Configuration', and 'Environment'. Under 'Server Software', 'Apache' is selected. Under 'Mozilla Configuration', 'Intermediate' is selected. Under 'Environment', 'Server Version' is set to '2.4.41' and 'OpenSSL Version' is set to '1.1.1d'. In the 'Miscellaneous' section, 'HTTP Strict Transport Security' and 'OCSP Stapling' are checked.

moz://a

SSL Configuration Generator

Server Software

- Apache
- AWS ALB
- AWS ELB
- Caddy
- Dovecot
- Exim
- Golang
- HAProxy
- lighttpd

MySQL

nginx

Oracle HTTP

Postfix

PostgreSQL

ProFTPD

Tomcat

Traefik

Mozilla Configuration

- Modern
Services with clients that support TLS 1.3 and don't need backward compatibility
- Intermediate
General-purpose servers with a variety of clients, recommended for almost all systems
- Old
Compatible with a number of very old clients, and should be used only as a last resort

Environment

Server Version 2.4.41

OpenSSL Version 1.1.1d

Miscellaneous

- HTTP Strict Transport Security
This also redirects to HTTPS, if possible
- OCSP Stapling

Padrões	Referências
Tokens em <i>hardware</i> (FIDO2/U2F)	https://fidoalliance.org/specifications/
Tokens em <i>software</i> (HOTP/TOTP)	https://tools.ietf.org/html/rfc4226 https://tools.ietf.org/html/rfc6238
HTTPS mandatório e HSTS Versões atuais de TLS <i>Forward Secrecy</i>	https://www.ssllabs.com/ssltest/ https://ssl-config.mozilla.org https://observatory.mozilla.org https://letsencrypt.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

Conscientização: Portal InternetSegura.br

TLP:WHITE



The screenshot shows a web browser window with the URL `internetsegura.br`. The page header includes the `nic.br` logo, the `INTERNET SEGURA BR` logo, and navigation links for `Sobre`, `Outras iniciativas`, and `Como Pedir Ajuda`. The main heading reads: `Internet Segura – Faça sua parte e todos teremos uma Internet mais segura!`

Below the heading, there are six categories of target audiences, each with an illustration and a label:

- `para Crianças`: Illustration of two children.
- `para Adolescentes`: Illustration of two young people.
- `para Pais e Educadores`: Illustration of a woman and a man.
- `para 60+`: Illustration of an elderly couple.
- `para Técnicos`: Illustration of a person in a lab coat next to server racks.
- `para Interesse Geral`: Illustration of a diverse group of people.

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

para Crianças

Guia Internet Segura

Apresenta conceitos de segurança na Internet de forma lúdica, com atividades para colorir, palavras cruzadas, desafios criados, 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.



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

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), Libre-Office (.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". ctic.br/pesquisa/kids-online

TIC Educação
A pesquisa entrevistou 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. ctic.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 cartilha.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 cartilha.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 gerência 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 destes 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

Obrigada!

✉ lucimara@cert.br

✉ Notificações para: cert@cert.br

🌐 @certbr

www.cert.br

8 de outubro de 2020

nic.br **cgi.br**

www.nic.br | www.cgi.br