nic.br cgi.br | cert.br

# 9º Fórum Brasileiro de CSIRTs

10 de setembro de 2020

Evento *Online*

# Onde Investir para Reduzir o Risco: um Retrato a partir dos dados do CERT.br

**Dra. Cristine Hoepers**
**Gerente Geral**
**cristine@cert.br**

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

cert.br nic.br cgi.br

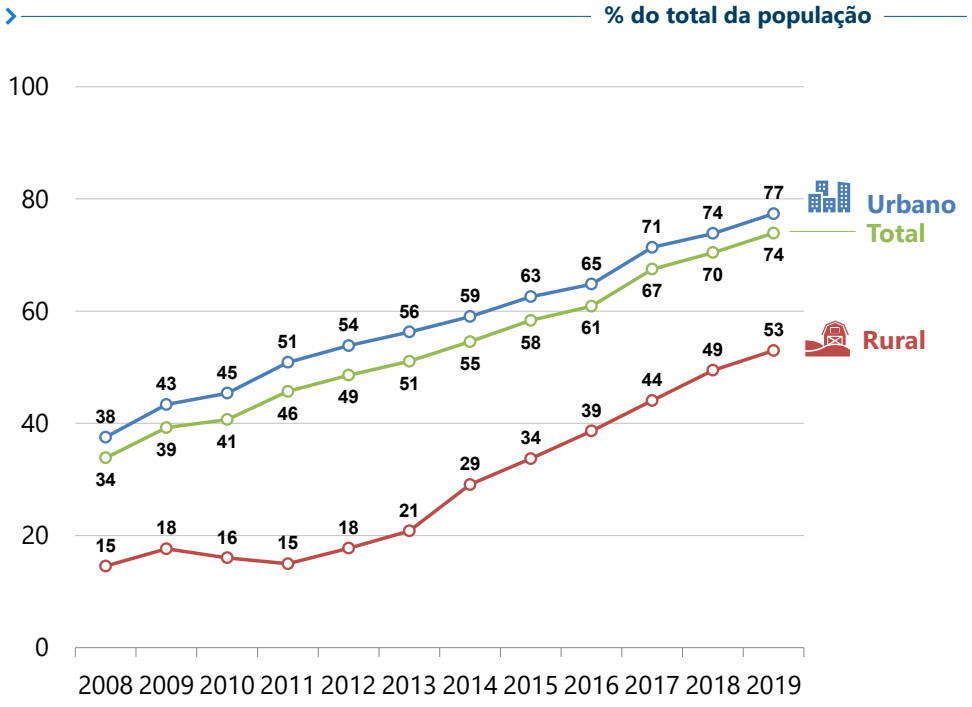
# Internet no Brasil em Números

cert.br nic.br cgi.br

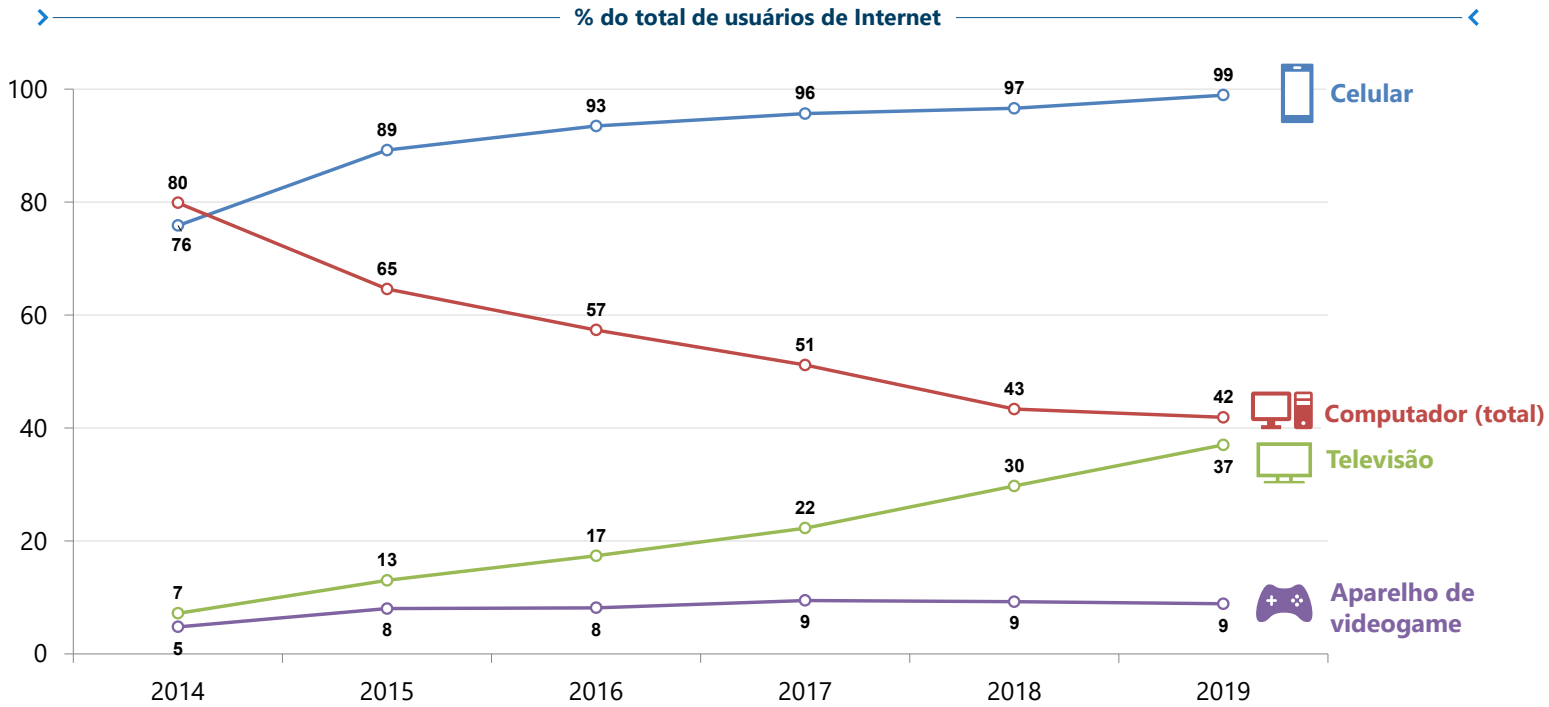
TLP:WHITE

# Internet no Brasil em Números:
# **Usuários e Dispositivos Utilizados**

## Usuários de Internet




## Dispositivo Utilizado para Acesso Individual




**133,8** milhões de usuários de Internet

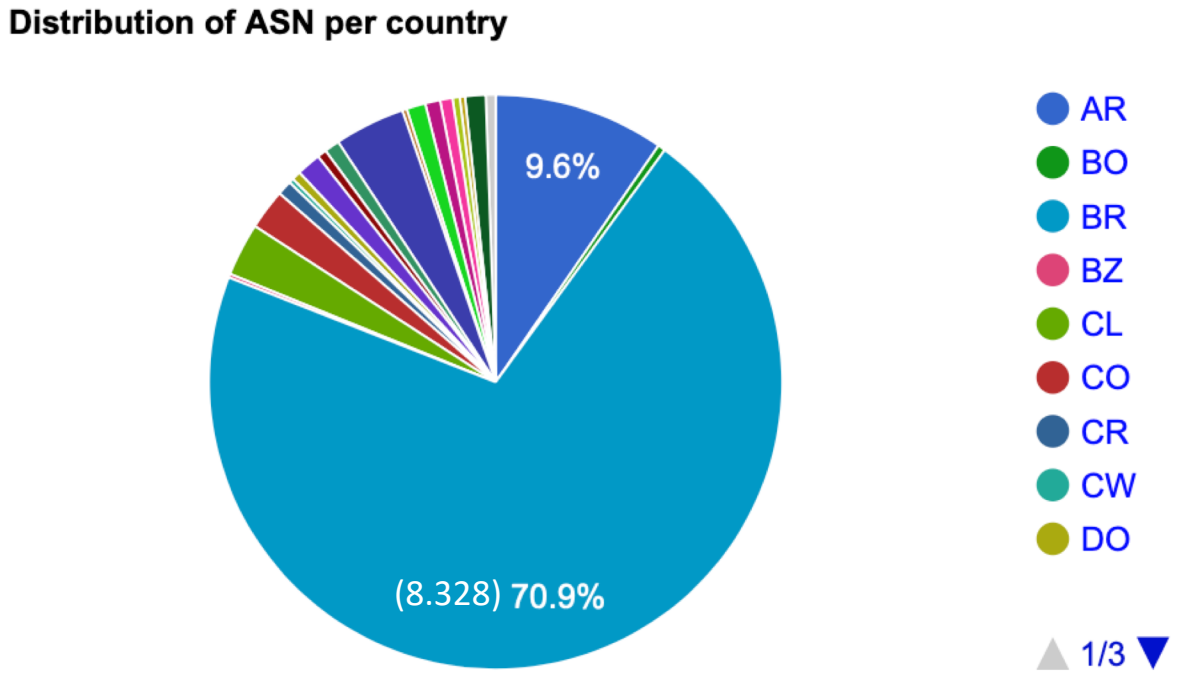
(utilizaram a Internet há menos de 3 meses)

**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 2019.**
https://www.cetic.br/pesquisa/domicilios/indicadores

TLP:WHITE

# Internet no Brasil em Números:
# ASNs, Provedores e Interconexão de Tráfego

## Alocação de Sistemas Autônomos na América Latina e Caribe




Fonte: https://www.lacnic.net/en/web/lacnic/estadisticas-asignacion

Dados atualizados em 07 de setembro de 2020

## 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 (2.000)
- nº 2 em pico de tráfego (10.5Tbps)
- nº 3 em média de tráfego (4.78Tbps)

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

# Incidentes Mais Comuns
# Visão Global

cert.br nic.br cgi.br

TLP:WHITE

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

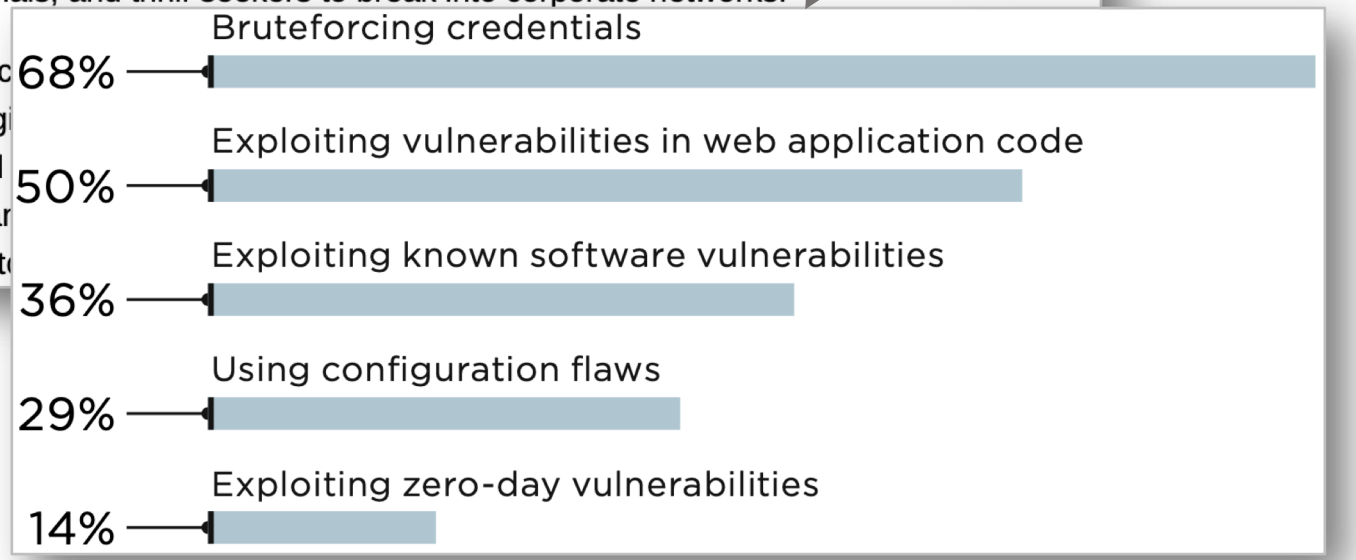
## Three little words: Patches, passwords, policies

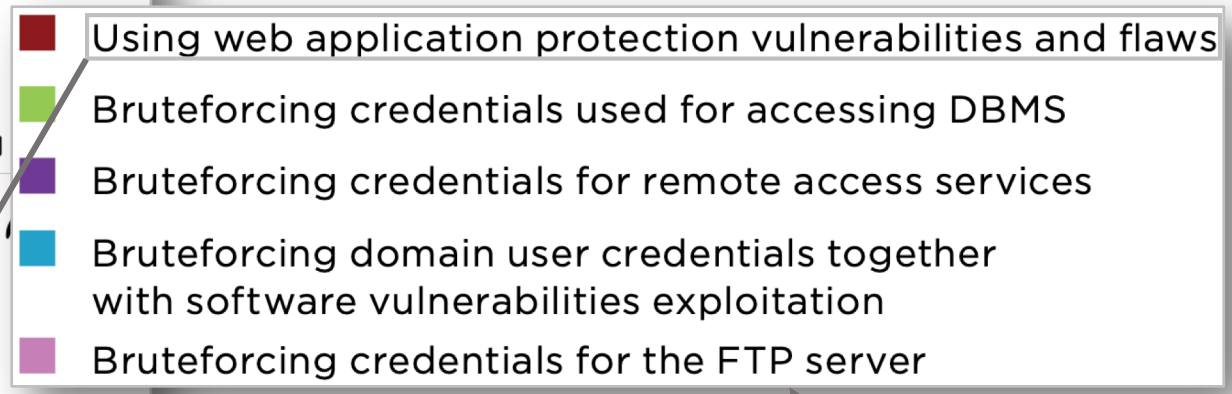
Thu 13 Aug 2020 // 07:06 UTC 31

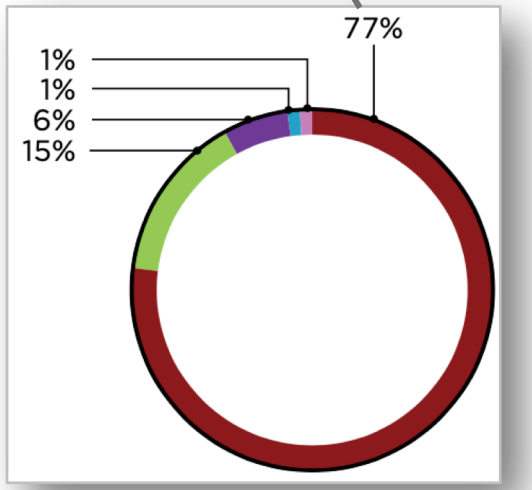
**Shaun Nichols in San Francisco** BIO EMAIL TWITTER

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.

This is acc
Technologi
and found
its red tear
available t




https://www.theregister.com/2020/08/13/pentest_networks_fail/
https://www.ptsecurity.com/upload/corporate/ww-en/analytics/external-pentests-2020-eng.pdf

TLP:WHITE

Cybersecurity
INSIDERS

# Insider Threat Awareness Month Reminds Us That the Biggest Threats Can Arise from Within

Posted By **cyberinsiders**

Insider Threat Awareness Month offers a great opportunity to make organizations realize that today's modern cyberattack is no longer carried out by a dark cyber-assassin with sophisticated hacking techniques. The reality is that they no longer hack in at all, they log in using weak, stolen, or otherwise compromised passwords. And a shocking amount of the time, it is actually an insider doing the "hacking."

https://www.cybersecurity-insiders.com/insider-threat-awareness-month-reminds-us-that-the-biggest-threats-can-arise-from-within/

TLP:WHITE

SC MEDIA

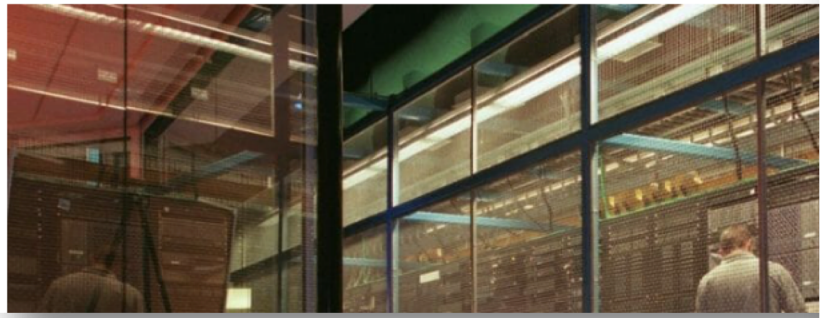
NEWS REVIEWS IN DEPTH EVENTS RESOURCE LIBRARY SC SECURITY OPS CENTER SC UK

THE CYBERSECURITY SOURCE SINCE 1989

August 6, 2020

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

Teri Robinson
Follow @TeriRnNY



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.scmagazine.com/home/security-news/patch-fail-led-to-password-leak-of-900-vpn-enterprise-servers/

TLP:WHITE

## 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.

## 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.

## s Exploited in 2020

10 vulnerabilities from 2016 to 2019 listed above, the U.S.
orted that the following vulnerabilities are being routinely
cated foreign cyber actors in 2020:

- 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*"


https://www.rapid7.com/research/report/nicer-2020/

# Rapid7 NICER Report 2020:
# **Most Exposed Countries**

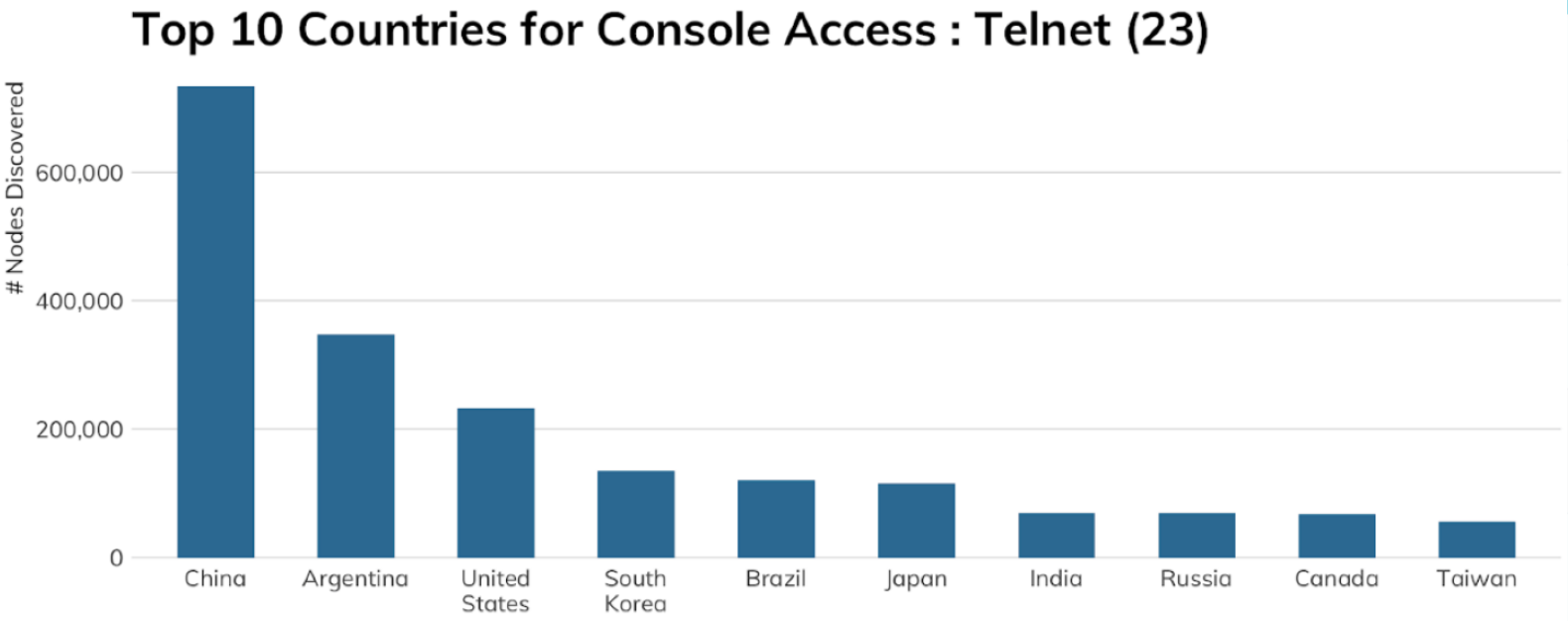
TLP:WHITE

- **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:
# **TELNET (23/TCP)**

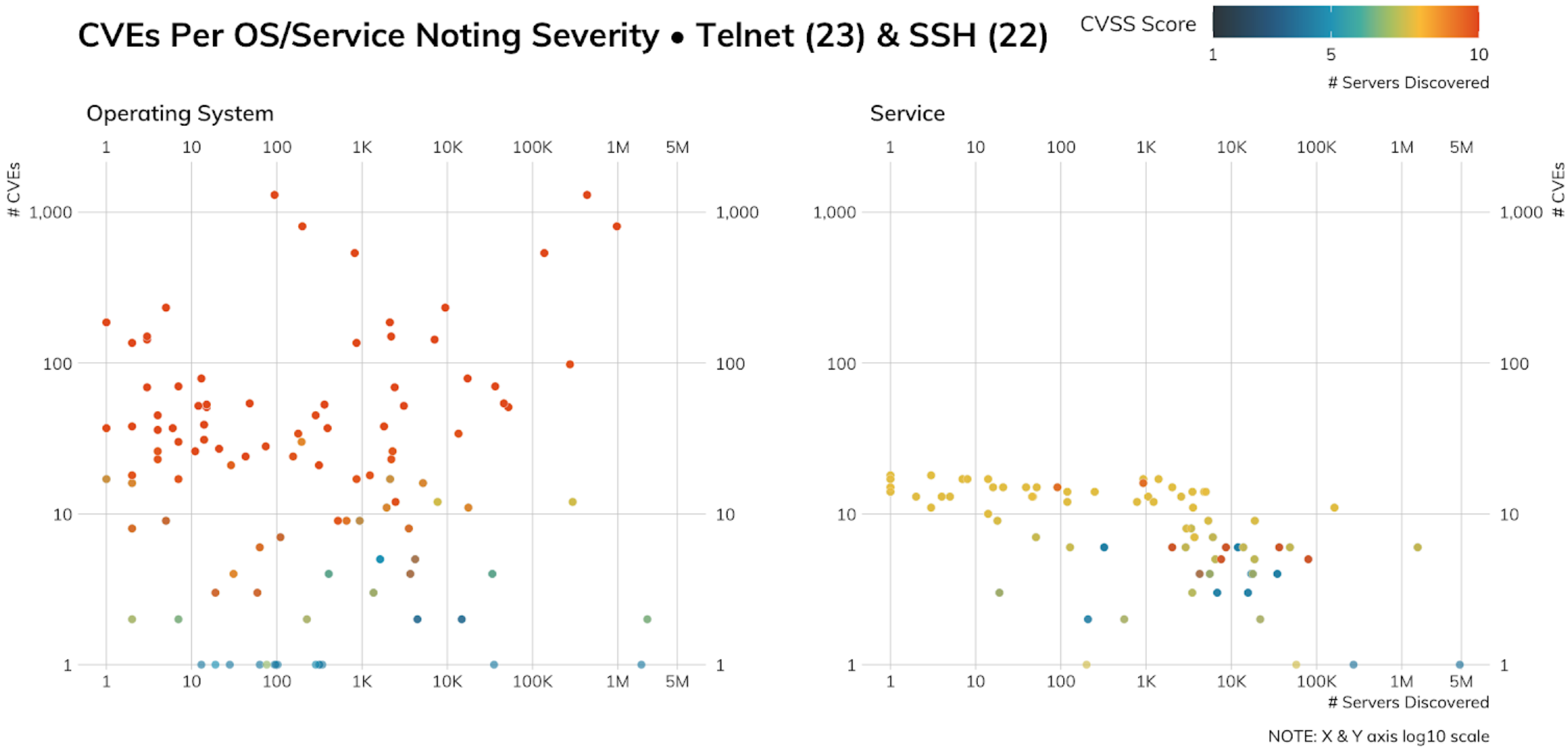
TLP:WHITE




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

# Rapid7 NICER Report 2020:
# CVEs por Sistema Operacional e Serviço

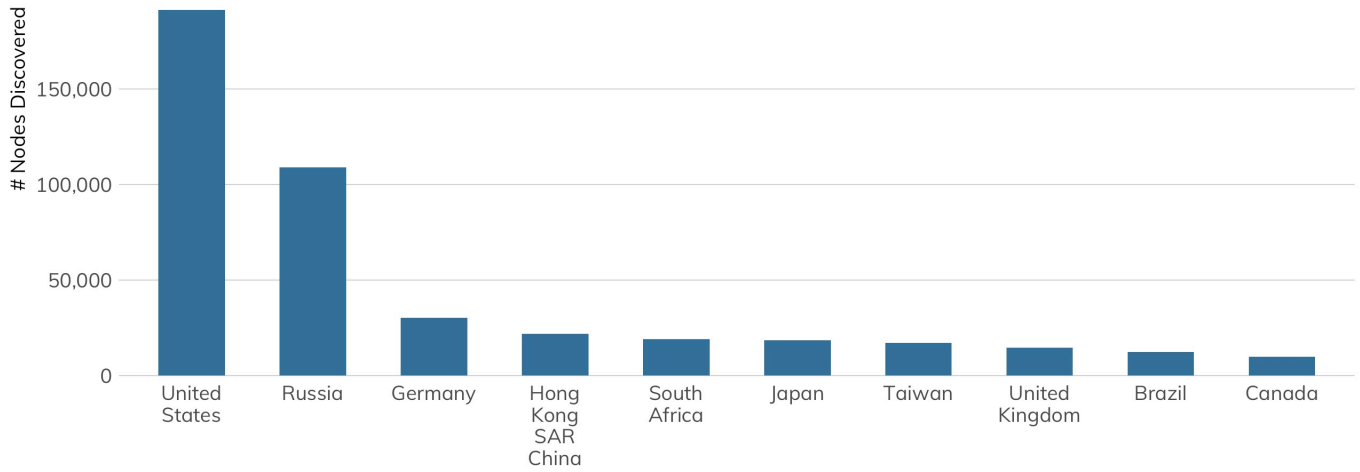
TLP:WHITE



# Rapid7 NICER Report 2020:
# **SMB (445/TCP)**

TLP:WHITE

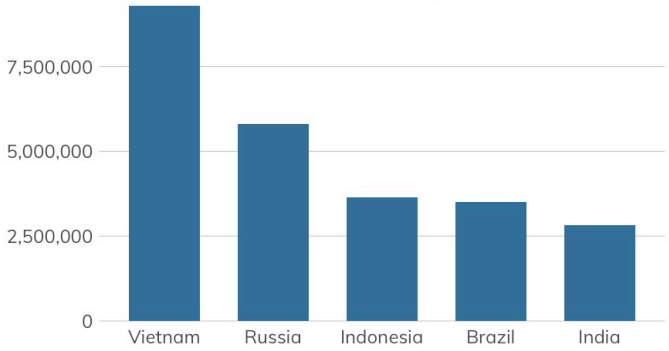
## Top 10 Countries for File Sharing : SMB (445)



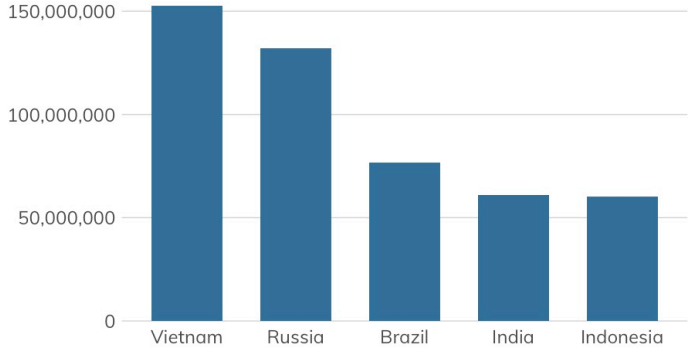

## Project Heisenberg Malicious SMB Activity by Source Country (April 2020)

Note free Y scales

**EternalBlue-based SMB Exploit Attempts**




**Full SMB Protocol Connections**

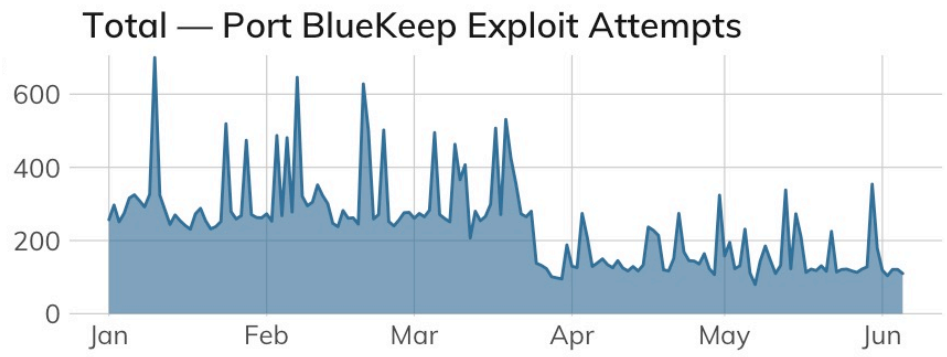


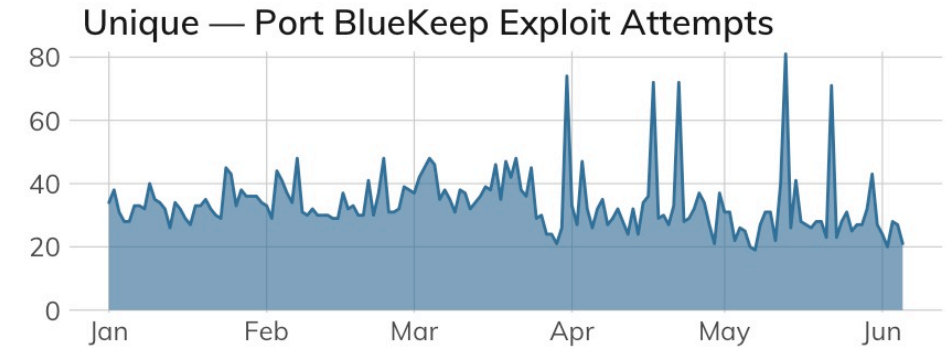

| SMB Server Kind | Count |
|---|---|
| Windows (Server) | 298,296 |
| Linux/Unix/BSD/SunOS (Samba) | 170,095 |
| Windows (Desktop) | 110,340 |
| QNAP NAS Device | 10,164 |
| Other/Honeypot | 1,914 |
| Apple Time Capsule or macOS | 1,465 |
| Windows (Embedded) | 703 |
| Keenetic NAS | 647 |
| Printer | 386 |

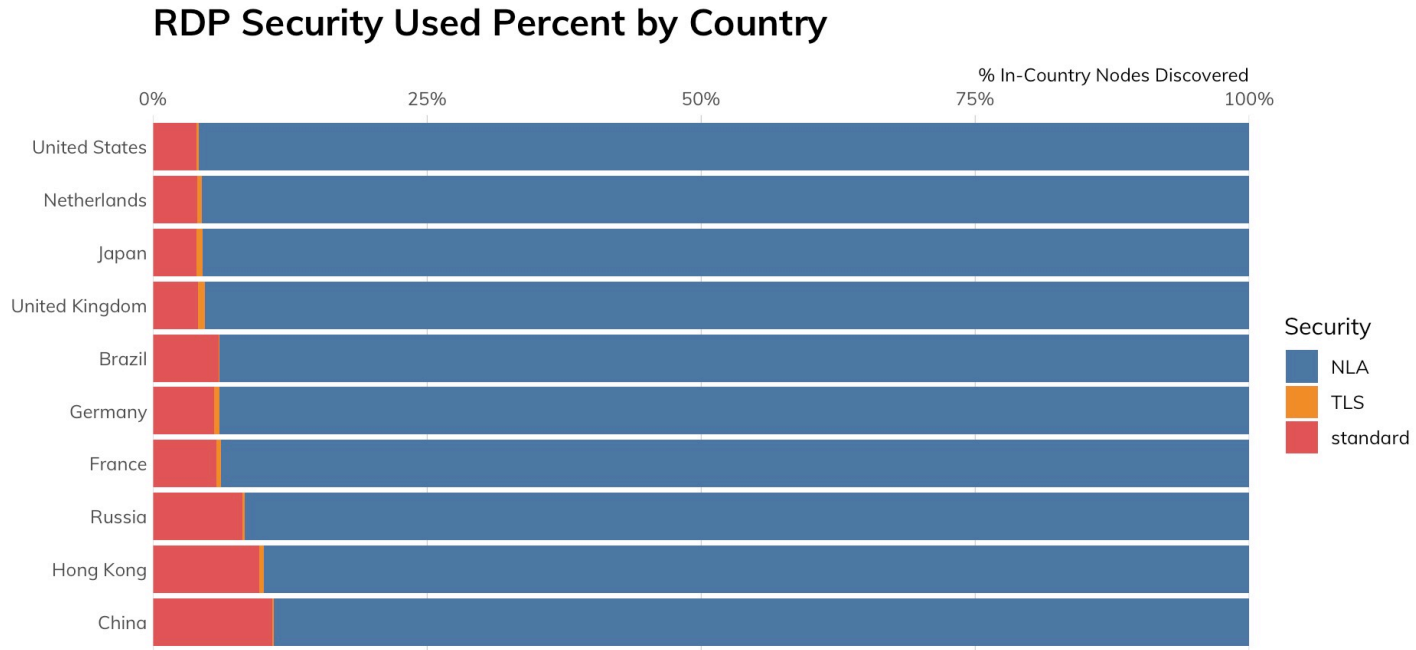
TLP:WHITE

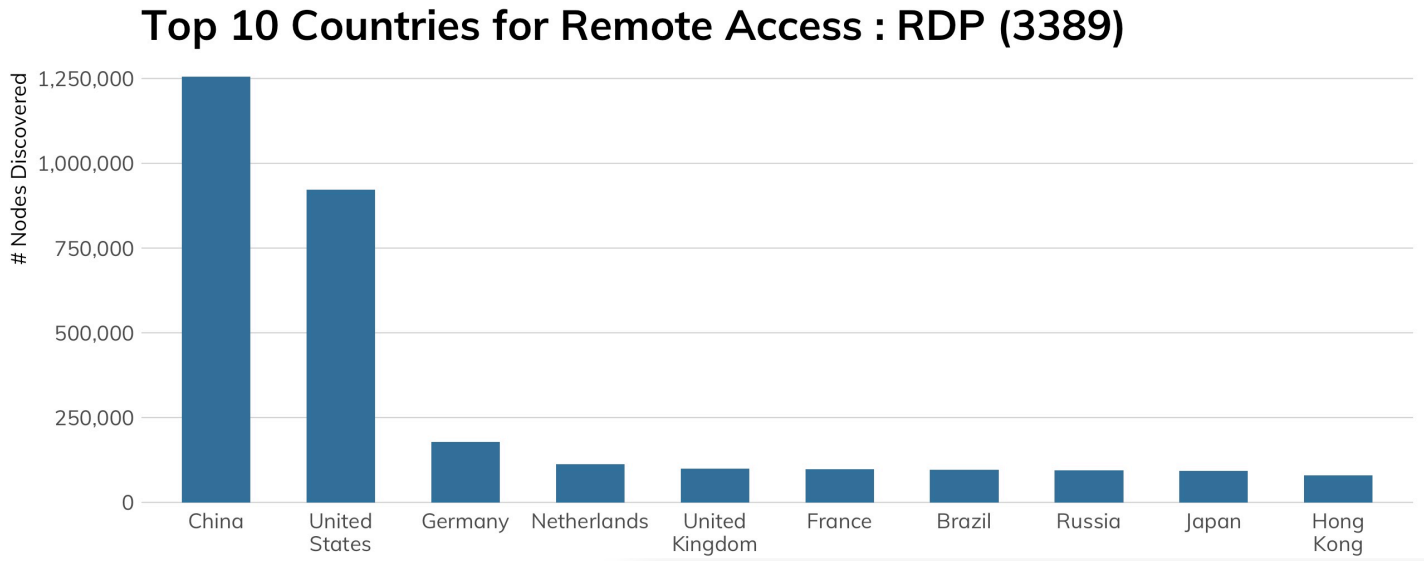
# Rapid7 NICER Report 2020·
# RDP (3389/TCP)

## Project Heisenberg RDP Activity



# Dados do CERT.br

cert.br nic.br cgi.br

cert.br

TLP:WHITE

| Tratamento de Incidentes | Treinamento e Conscientização | Análise de Tendências |
|---|---|---|
| ▶ Articulação | ▶ Cursos | ▶ *Honeypots* Distribuídos |
| ▶ Análise Técnica | ▶ Palestras | ▶ SpamPots |
| ▶ Apoio à recuperação | ▶ Boas Práticas | ▶ Processamento de *threat feeds* |
| | ▶ Reuniões | |

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

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

[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

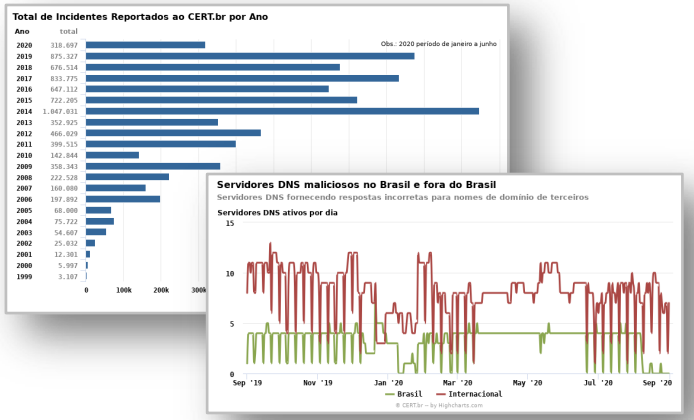
- Ponto de contato nacional
- Trabalho colaborativo com outras entidades
- Auxiliar na análise técnica e compreensão de ataques e ameaças
- Aumentar a detecção, correlação de eventos e determinação de tendências
- Transferir o conhecimento através de cursos, boas práticas e conscientização

# Tratamento de Incidentes:
# **Fontes dos Dados, Métricas e Compartilhamento**

TLP:WHITE

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



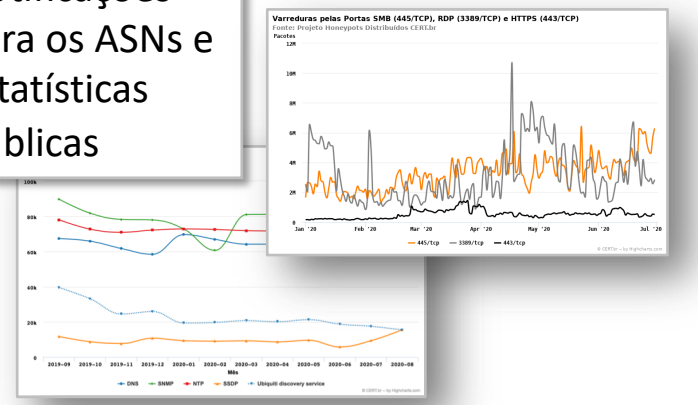

Compartilhamento via MISP

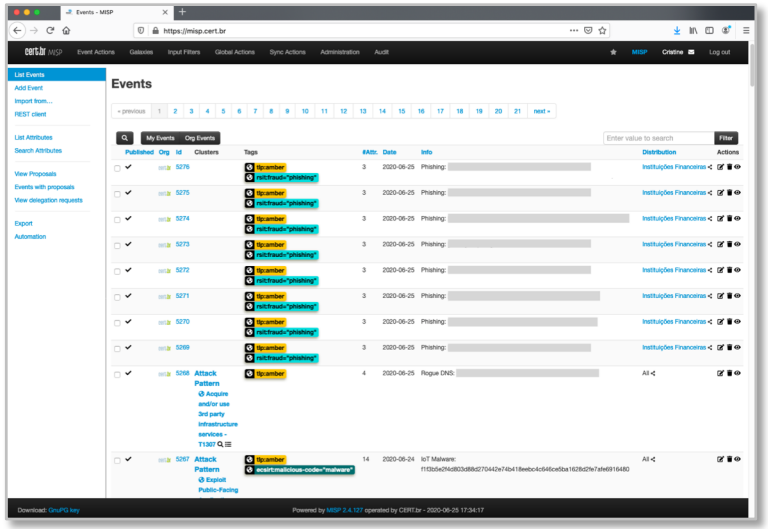
- Indicadores selecionados são compartilhados com parceiros
  - Servidores DNS maliciosos
  - *Phishing*
  - Binários e Comando e Controle de *botnets* IoT
  - Amplificadores usados em ataques DDoS

*Threat feeds*

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

Notificações para os ASNs e estatísticas públicas



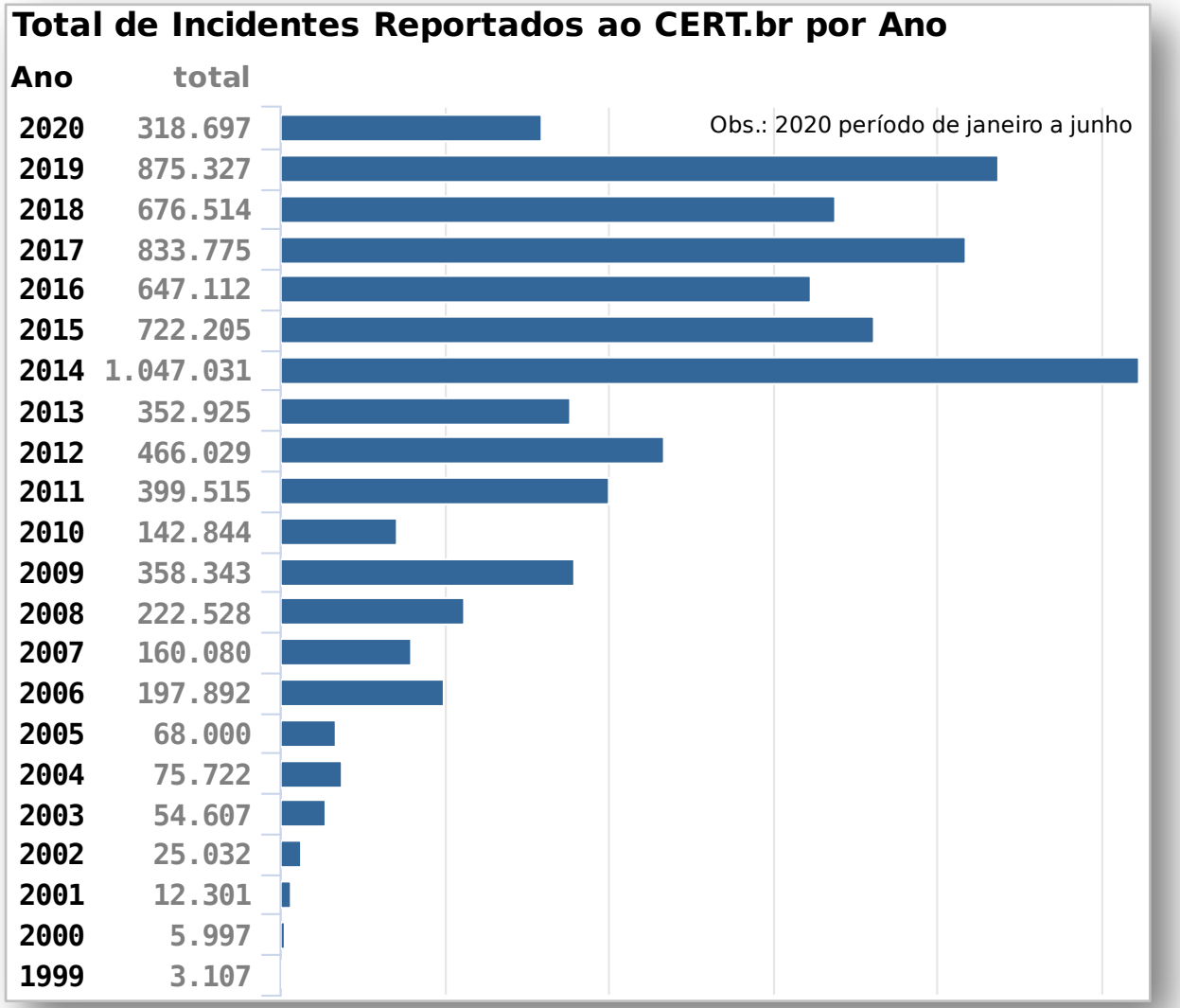

https://cert.br/stats/

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**



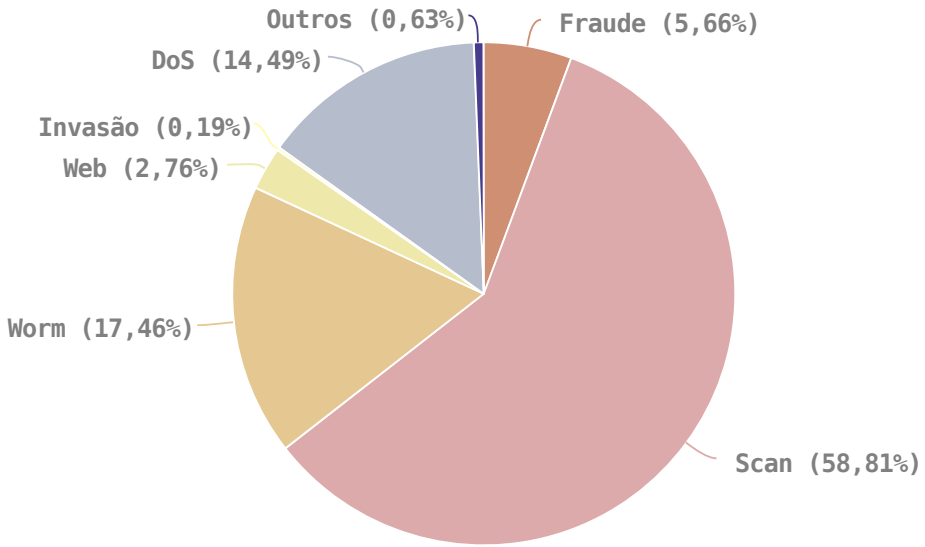

**Fonte:** https://cert.br/stats/incidentes/

## 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

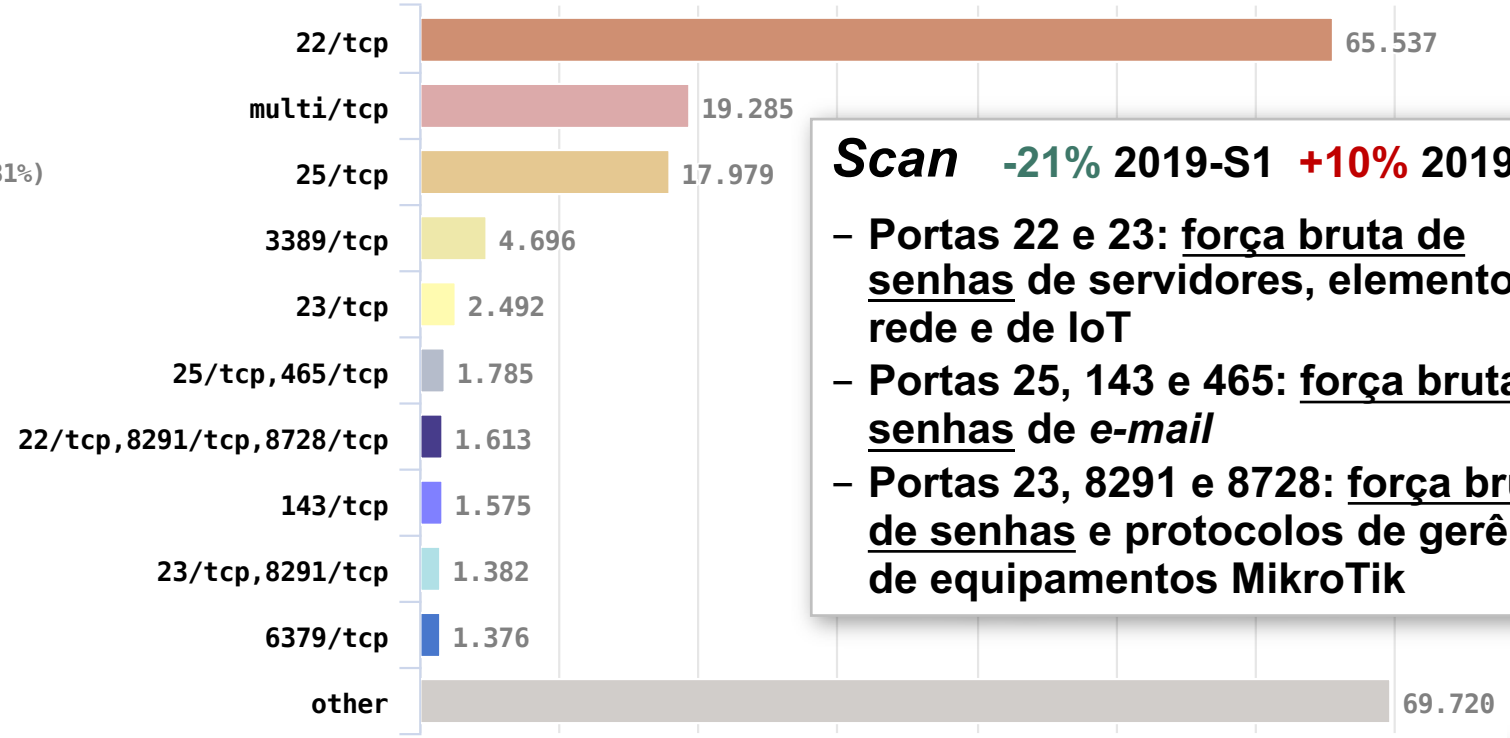
TLP:WHITE

# 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

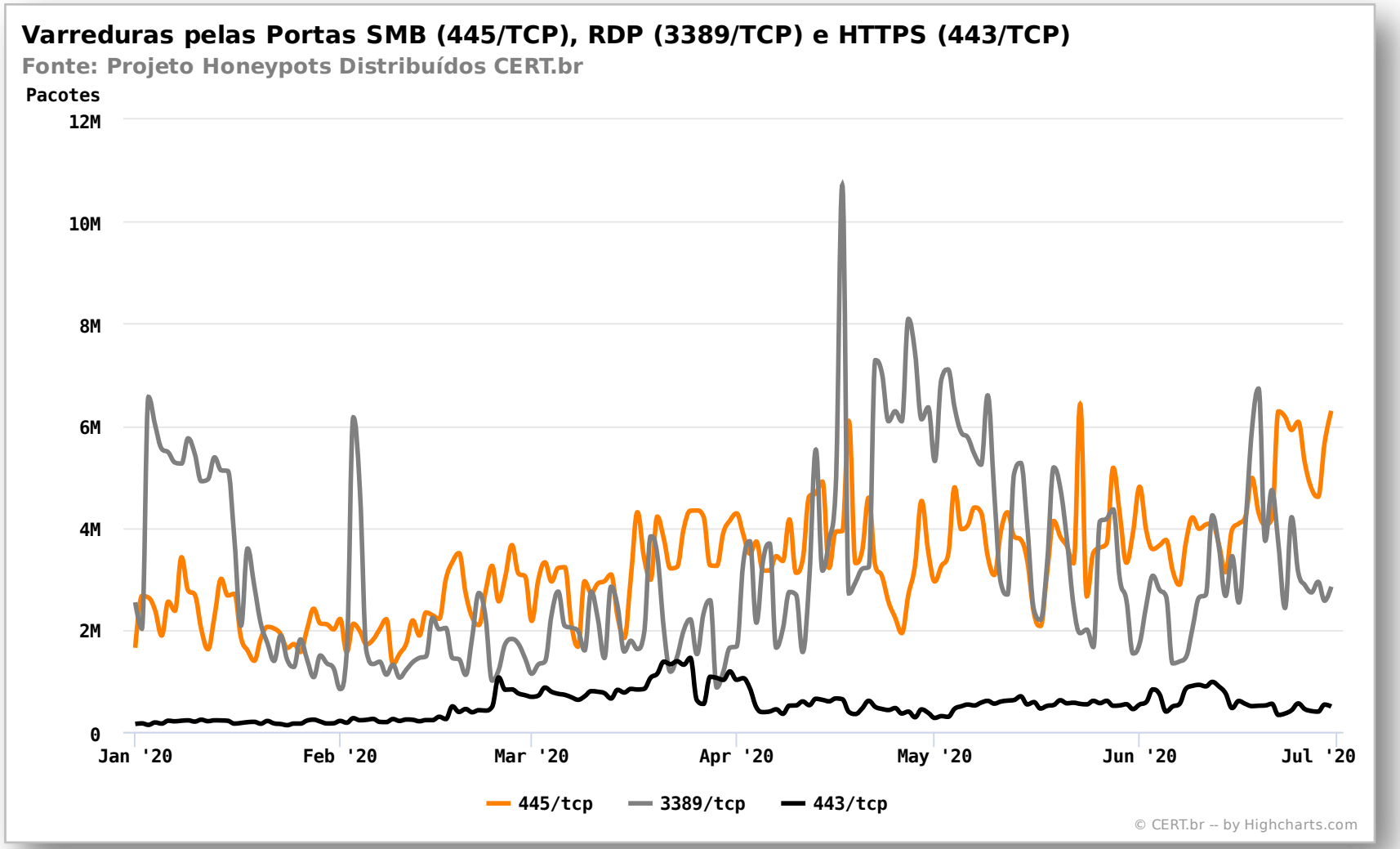
- Aumentou de patamar em 2014
- Maior número em 2019
- Tipos mais frequentes
  - *botnets* IoT
  - amplificação de tráfego

***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

TLP:WHITE

# Projeto *Honeypots* Distribuídos do CERT.br: **Top Portas TCP – 1º semestre de 2020**

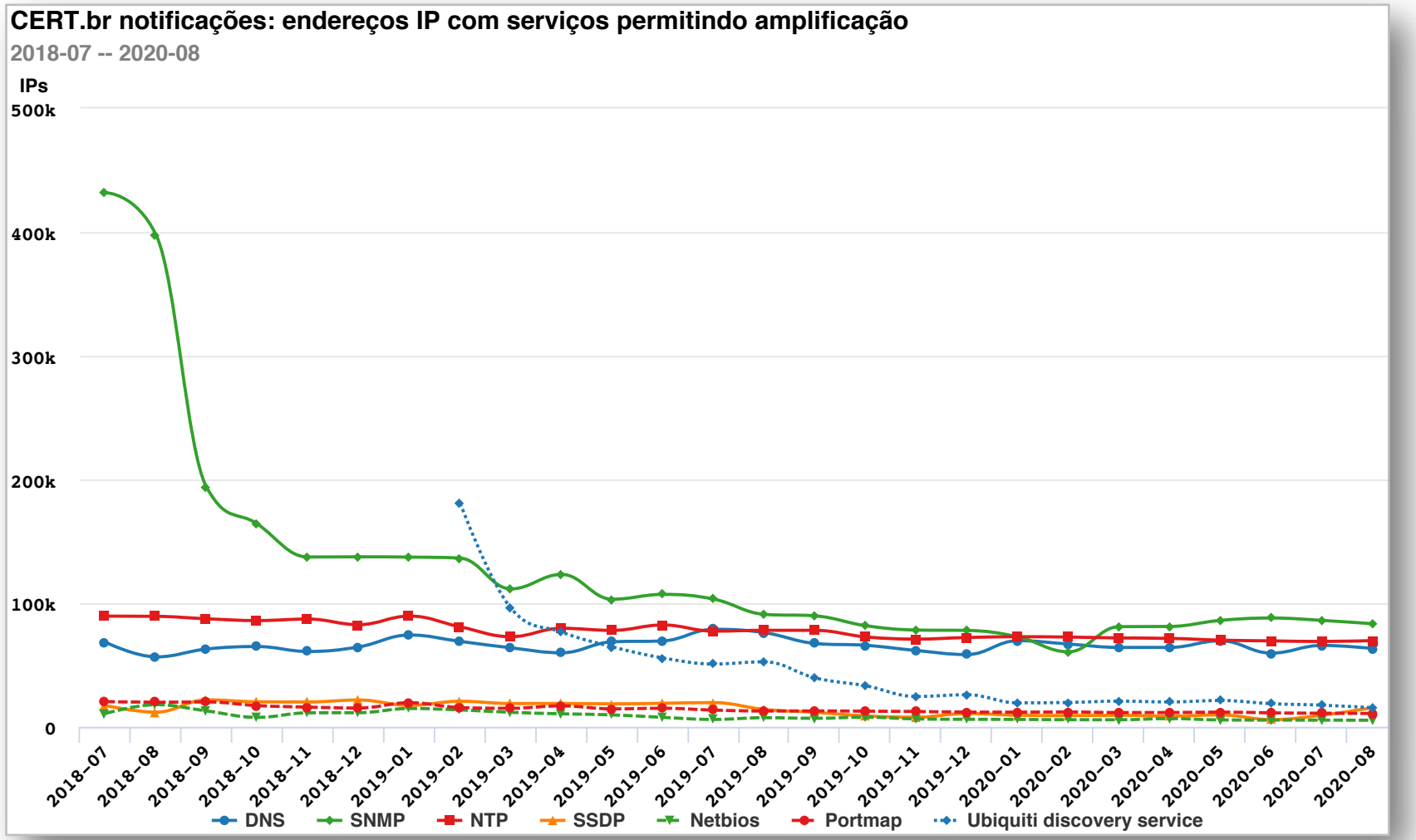



| # | Porta TCP | Pacotes | Bytes | Flows |
|---|---|---|---|---|
| 01 | 23/tcp | 30,1 G | 1,5 TB | 452,8 M |
| 02 | 22/tcp | 1,2 G | 99,0 GB | 250,2 M |
| 03 | 445/tcp | 595,2 M | 43,5 GB | 362,3 M |
| 04 | 3389/tcp | 574,4 M | 28,0 GB | 172,8 M |
| 05 | 80/tcp | 280,0 M | 14,6 GB | 200,6 M |
| 06 | 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 |
| 16 | 8000/tcp | 28,3 M | 1,5 GB | 17,8 M |
| 17 | 465/tcp | 23,7 M | 1018,1 MB | 18,6 M |
| 18 | 139/tcp | 20,3 M | 1,0 GB | 10,5 M |
| 19 | 5038/tcp | 20,2 M | 777,4 MB | 13,8 M |
| 20 | 3390/tcp | 19,5 M | 761,4 MB | 14,6 M |

**Fonte:** https://cert.br/stats/honeypots/

TLP:WHITE

# Estatísticas de Amplificação:
# **Notificações do CERT.br vs. *Honeypots***




| # | Porta UDP | Pacotes | Bytes | Flows |
|---|---|---|---|---|
| 01 | 5060/udp | 637,5 M | 361,9 GB | 396,7 M |
| 02 | 1900/udp | 16,3 M | 1,9 GB | 16,3 M |
| 03 | 123/udp | 15,4 M | 1,6 GB | 15,2 M |
| 04 | 161/udp | 11,6 M | 828,3 MB | 7,3 M |
| 05 | 389/udp | 9,0 M | 694,1 MB | 9,0 M |
| 06 | 53/udp | 8,6 M | 541,5 MB | 8,5 M |
| 07 | 1324/udp | 7,8 M | 816,9 MB | 1,7 M |
| 08 | 11211/udp | 5,9 M | 354,9 MB | 5,8 M |
| 09 | 53413/udp | 4,9 M | 716,5 MB | 4,9 M |
| 10 | 137/udp | 4,9 M | 361,0 MB | 4,7 M |
| 11 | 5353/udp | 3,5 M | 281,5 MB | 3,5 M |
| 12 | 1434/udp | 3,5 M | 104,6 MB | 3,4 M |
| 13 | 111/udp | 3,4 M | 232,9 MB | 3,4 M |
| 14 | 3283/udp | 3,3 M | 106,9 MB | 3,3 M |
| 15 | 19/udp | 3,2 M | 101,4 MB | 3,2 M |
| 16 | 3702/udp | 3,1 M | 1021,3 MB | 3,1 M |
| 17 | 5683/udp | 3,0 M | 148,7 MB | 3,0 M |
| 18 | 1194/udp | 2,9 M | 121,0 MB | 2,9 M |
| 19 | 17/udp | 2,9 M | 112,4 MB | 2,9 M |
| 20 | 623/udp | 2,8 M | 150,4 MB | 2,8 M |

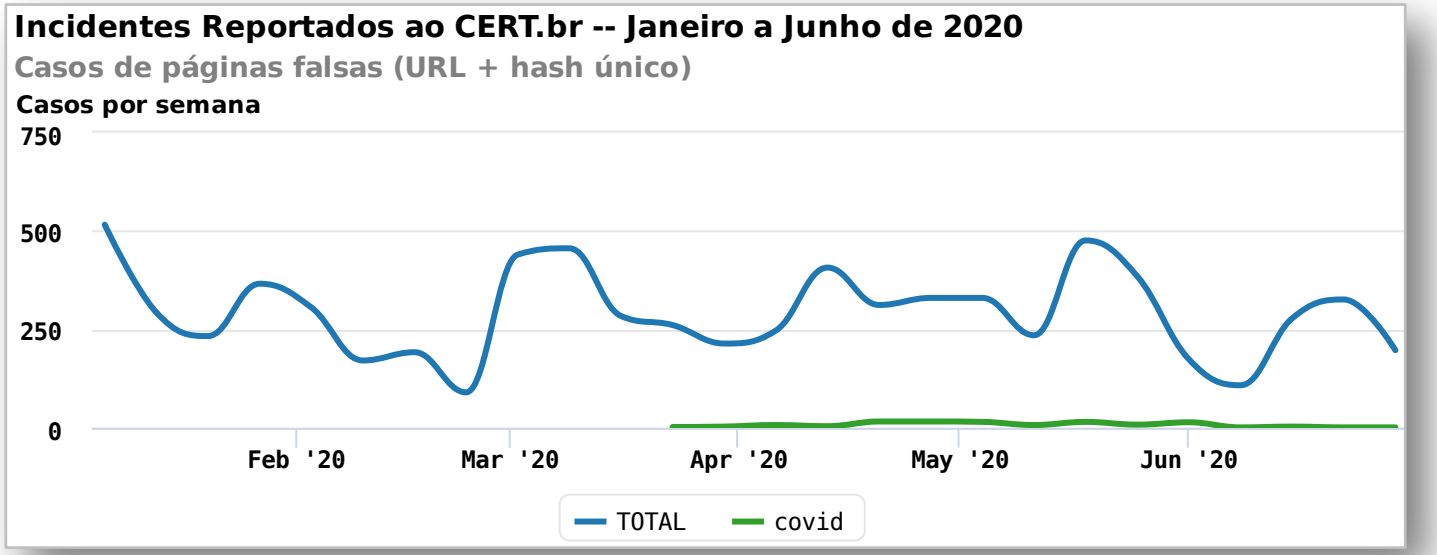
**Fontes:** https://cert.br/stats/amplificadores/ | https://cert.br/stats/honeypots/

# Incidentes Reportados Voluntariamente para o CERT.br: **Tentativas de Fraude – 1º semestre de 2020**

TLP:WHITE

## Variações entre os semestres

| | | |
|---|---|---|
| **Total:** | **+54% 2019-S1** | **-35% 2019-S2** |
| ***Phishing* financeiro:** | **+58% 2019-S1** | **-38% 2019-S2** |
| ***Phishing* outras instituições:** | **+140% 2019-S1** | **+12% 2019-S2** |
| ***Trojans*:** | **-43% 2019-S1** | **-34% 2019-S2** |




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

## Alguns fatos de interesse

- *Phishing* com temas de COVID-19
  - 1ª notificação em 23 de março
  - 165 no total
- Cada vez mais comum
  - *phishings* direcionados para *smartphones*
  - hospedagem em *cloud* e CDN

**Sobre a divisão de *phishing*:**

- *Phishing* financeiro:
  - bancos, cartões, boletos e *sites* de comércio eletrônico
- *Phishing* de outras instituições:
  - para furto de credenciais de: serviços de documentos em nuvem, *streaming* de vídeo, *webmail*, redes sociais, etc

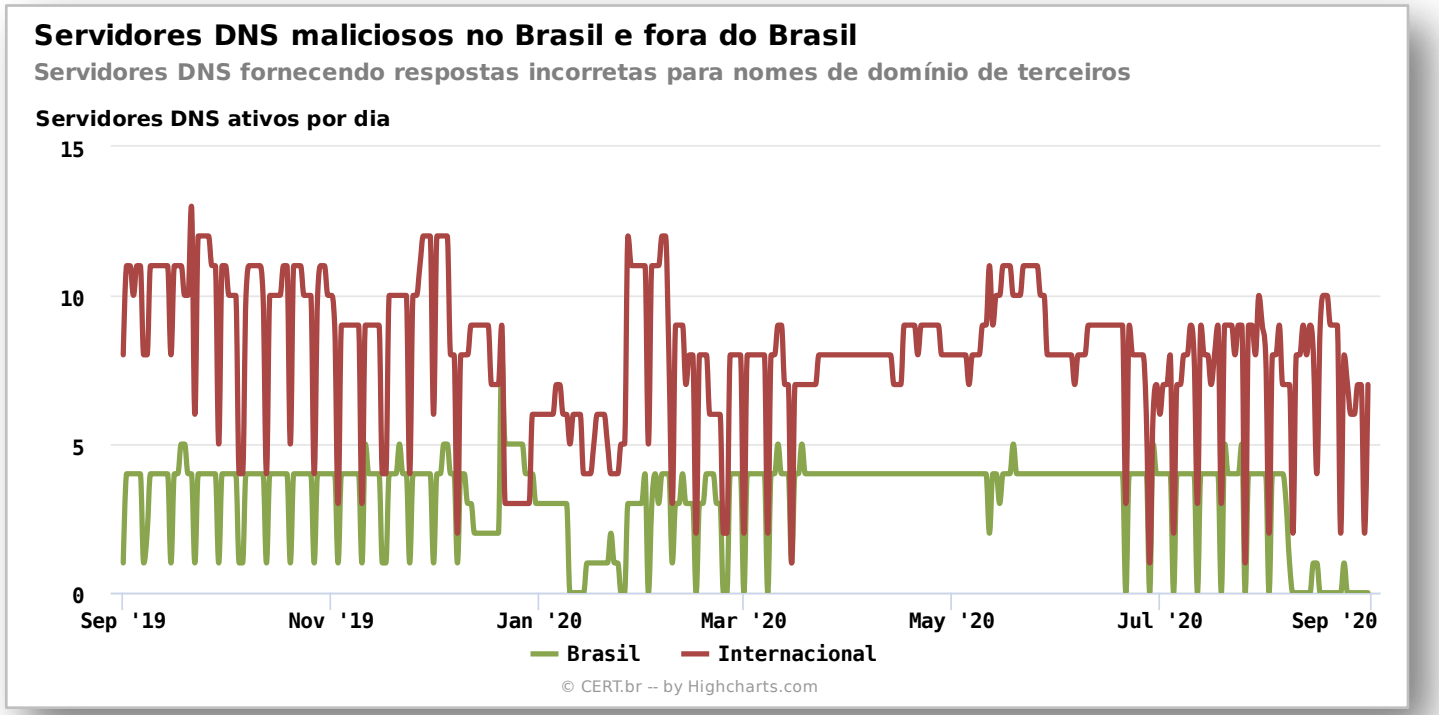
# Servidores DNS Maliciosos Usados nos CPEs Invadidos: **Fornecem Respostas Autoritativas Erradas**

TLP:WHITE

**Hospedagem em serviços de *cloud* e CDN**

**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**

# Incidentes Reportados para o CERT.br:
# **Considerações sobre notificações de fraudes**

TLP:WHITE

## Pontos Cegos

Fraudes subnotificadas ou em ecossistemas fechados

- Lojas de aplicativos
- Redes sociais
- WhatsApp
- SMS

## Serviços de *Cloud* e CDN

Políticas defasadas

- não preveem serviços sendo simplesmente contratados por atacantes
- assumem que repassar a reclamação para o "cliente" é fechar o *ticket*

Não adotam boas práticas de tratamento de incidentes e abusos

- cada uma desenvolvendo sua própria API
- criando um ecossistema fechado

# O que Priorizar

TLP:WHITE

## 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)

## Receber e Tratar Notificações

Acompanhar todas as notificações enviadas para

- *E-mail* do contato `abuse-c` do ASN no serviço `whois`
- *E-mail* de abuse ou do grupo de tratamento de incidentes

Considere que:

- Outras organizações e CSIRTs tem dados relevantes a passar
- Geralmente informações que podem utilizadas gratuitamente

# Onde Investir Primeiro, Além do Básico

cert.br nic.br cgi.br

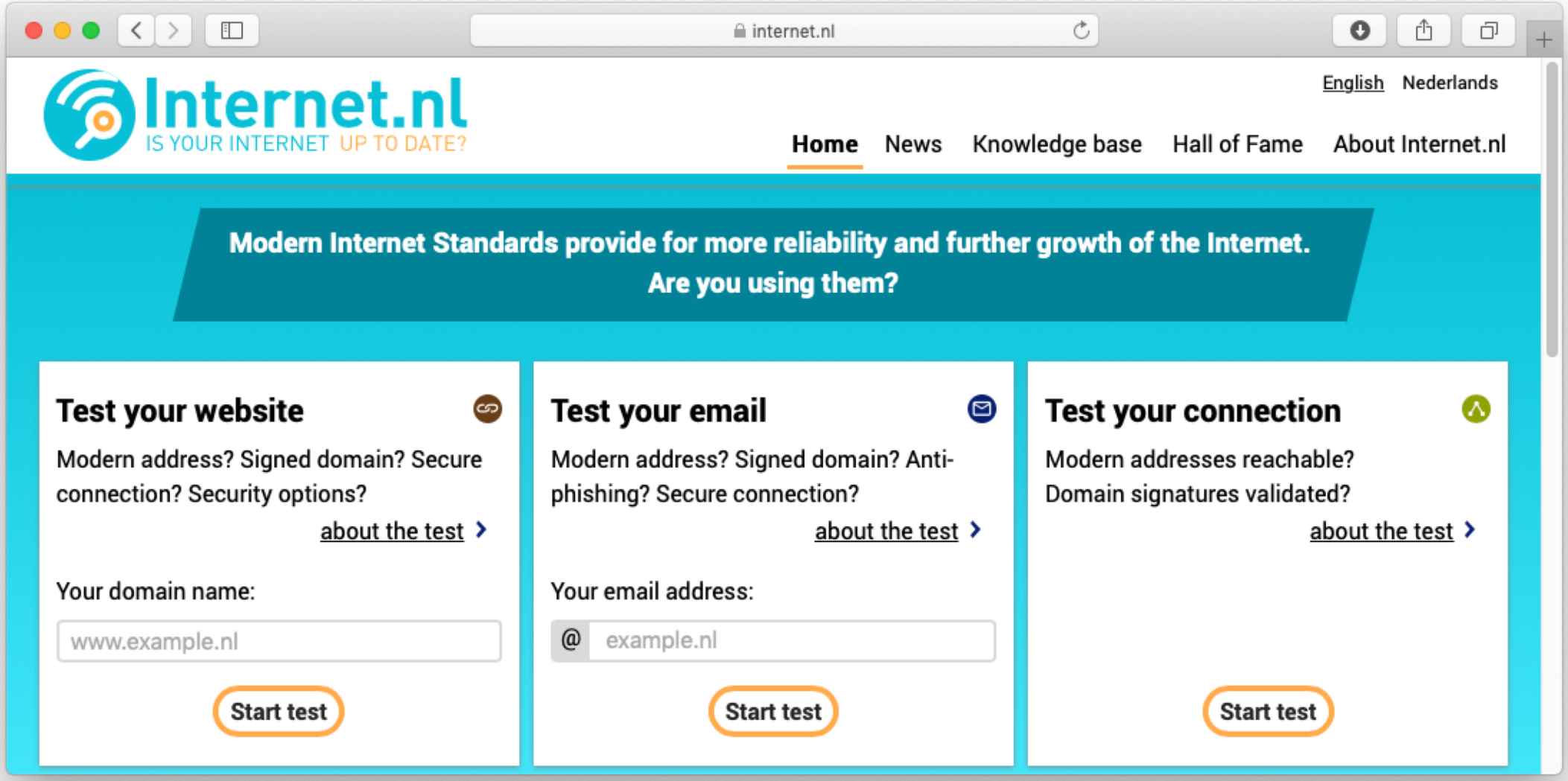
TLP:WHITE

# Adotar Protocolos Mais Modernos

| | Padrões | Vantagens da Adoção |
|---|---|---|
| Criptografia forte | HTTPS mandatório e HSTS<br>Versões atuais de TLS<br>*Forward Secrecy* | Garantia das transações e da proteção de dados<br>Reduz a chance de quebra da criptografia<br>Impede quebra de cripto de tráfego antigo capturado |
| Segurança de DNS | DNSSEC | Proteção contra envenenamento de *cache*<br>Habilitar o uso de outras tecnologias como o DANE |
| Segurança de *e-mail* | STARTTLS<br>• idealmente c/ DANE<br>DMARC, DKIM e SPF | Proteção contra *sniffing* (“espionagem”)<br>Aumento da reputação da mensagem legítima (ajuda a prevenir *phishing* da sua marca) |
| Protocolo IP | IPv6 é o atual<br>IPv4 é legado – e já acabou<br>• novas redes só terão IPv6 | Mais estabilidade<br>• Não depender de CGN ou tradução v6 → v4<br>• Redes móveis tendem a ter IPv6 nativo no futuro<br>Facilita o processo investigativo e de tratamento de incidentes |
| Segurança de roteamento | RPKI | Certificação de recursos<br>Validação de origem no BGP |

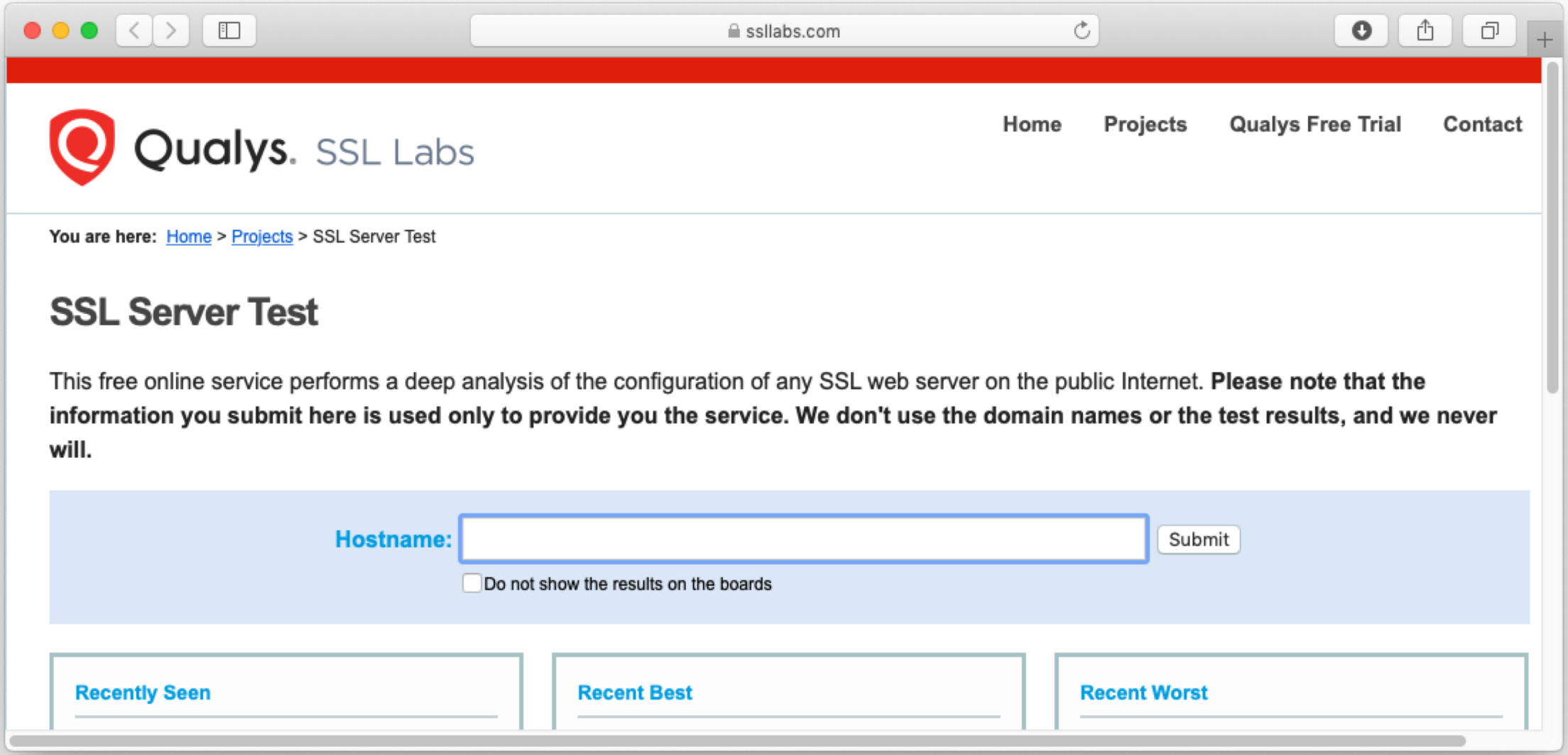
# Is your Internet up to date?
# **https://internet.nl**

TLP:WHITE



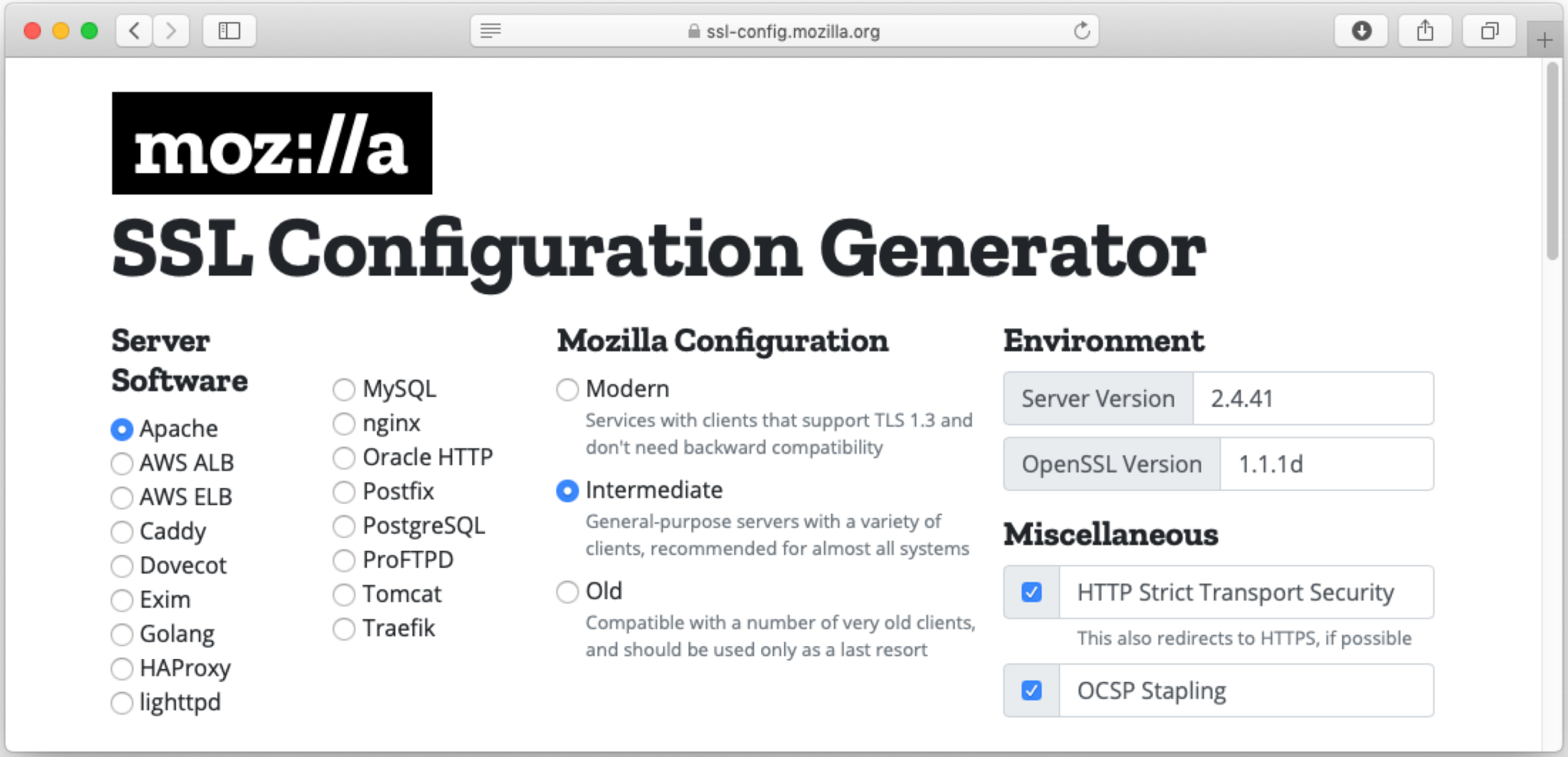
# SSL Server Test
# https://www.ssllabs.com/ssltest/

TLP:WHITE



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

TLP:WHITE



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

# Outras Referências de Interesse para Uma Internet Melhor

cert.br nic.br cgi.br

TLP:WHITE

# Precisamos um Ecossistema mais Saudável: **Programa por uma Internet mais 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

PROGRAMA INTERNET +SEGURA


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

# Conscientização:
# **Portal InternetSegura.br**

TLP:WHITE

# Conscientização:
# Materiais sob Licença Creative Commons

TLP:WHITE

## 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/

nic.br cgi.br

www.nic.br | www.cgi.br