nic.br cgi.br | cert.br

ITU 2020 Global CyberDrill – Regional Dialog for the America Region

September 15, 2020

Online Event

Incidents and Trends in Brazil

Dr. Cristine Hoepers
General Manager
cristine@cert.br

cert.br nic.br cgi.br

cert.br

TLP:WHITE

Incident Management	Training and Awareness	Trend Analysis
Coordination	Courses	Distributed Honeypots
Technical Analysis	Presentations	SpamPots
Support for recovery	Best Practices	Processing of threat feeds
	Meetings	

Filiations and Partnerships:

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

Creation:

August/1996: a report proposing a model for incident management for the country is published by the Brazilian Internet Steering Committee – CGI.br[1]

June/1997: CGI.br creates CERT.br (at that time called NBSO – *NIC BR Security Office*) based on the report's recommendations[2]

[1]https://www.nic.br/grupo/historico-gts.htm | [2]https://www.nic.br/pagina/gts/157

Mission

To increase the level of security and incident handling capacity of the networks connected to the Internet in Brazil.

Constituency

Networks that use Internet Resources allocated by NIC.br (IPs or ASNs allocated to Brazil, and domains under the ccTLD .br)

Focus of the Activities

- National focal point for incident reports
- Support technical analysis and the understanding of attacks and threats
- Develop collaborative relationships with other entities
- Increase incident detection, event correlation and trend analysis in the country
- Transfer knowledge through courses, best practices and awareness materials

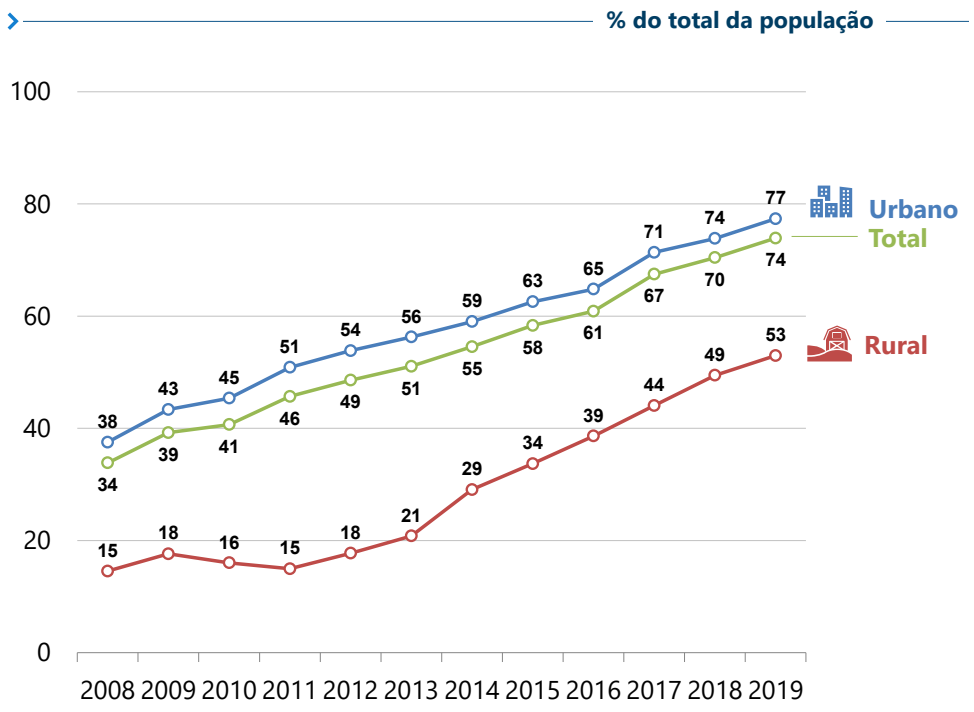
Brazilian Internet in Numbers

cert.br nic.br cgi.br

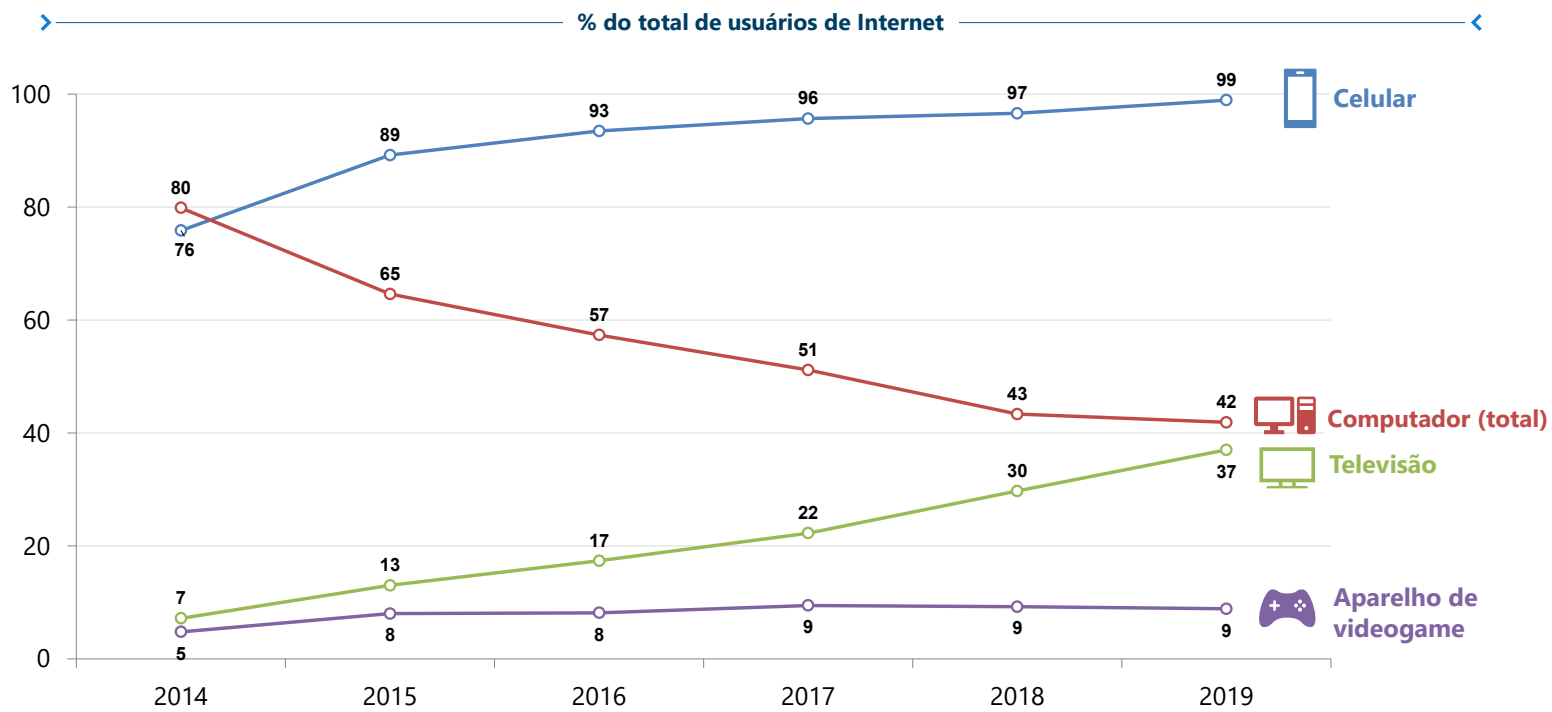
Brazilian Internet in Numbers:
Users and Devices

TLP:WHITE

Internet Users (% of population)



Device Used for Individual Access (% of internet users)



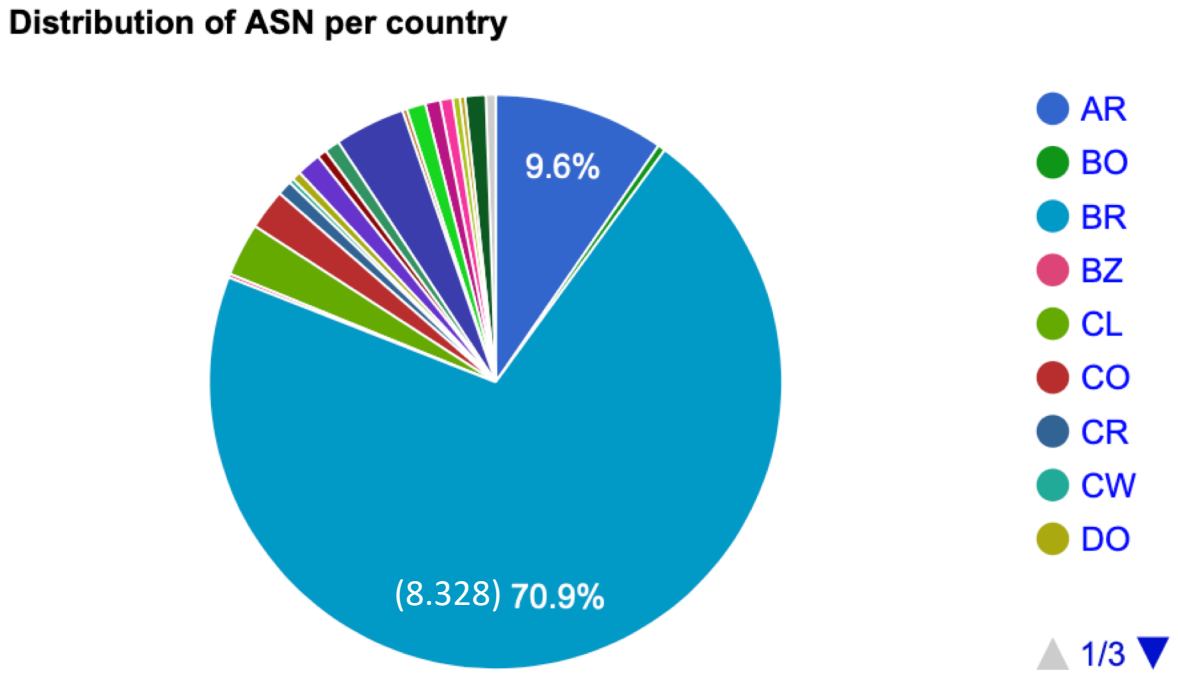
133,8 Million Internet Users

Source: 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

Brazilian Internet in Numbers:
ASNs, ISPs and Traffic eXchange

TLP:WHITE

Autonomous Systems Allocated in the Latin American and Caribbean Region



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

Data updated on September 07, 2020

ISPs in Brazil

- Total (estimated): 6.618
- 75% have 1.000 clients or less

Source: https://www.cetic.br/pesquisa/provedores/

Internet Traffic eXchange

IX.br São Paulo – one of the biggest in the world

- nº 1 in participants (2.000)
- nº 2 in peak traffic (10.5Tbps)
- nº 3 in average traffic (4.78Tbps)

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

CERT.br Data

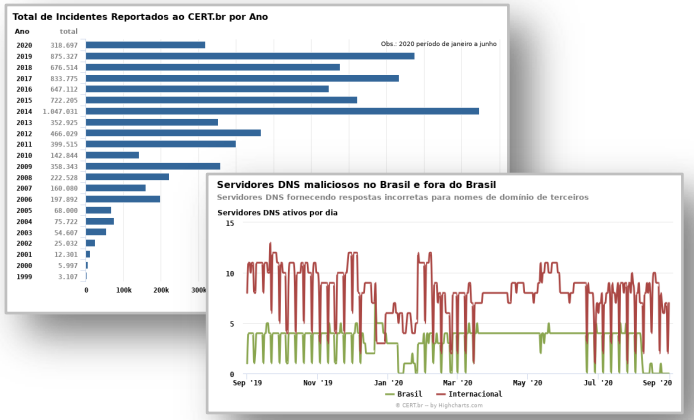
cert.br nic.br cgi.br

TLP:WHITE

CERT.br Data

Voluntary notification of incidentes to: cert@cert.br

- 2019: 4.086.406 *e-mails* handled, related to 875.327 incidents notified to CERT.br



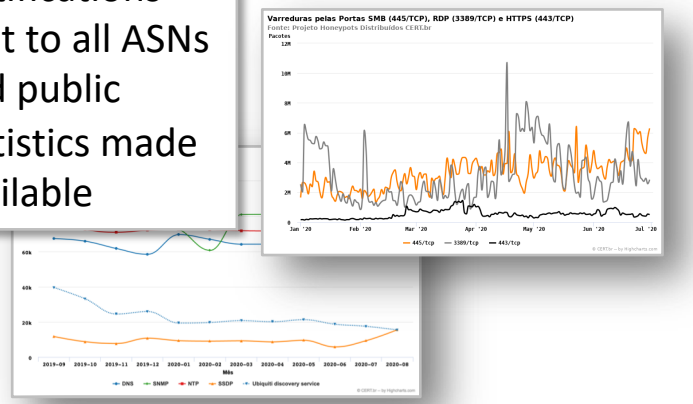
Sharing via MISP

- Selected IoCs are shared with trusted partners
  - Rogue DNS servers
  - Phishing URLs
  - IoT botnet binaries and Command and Control IPs
  - Amplifiers that might be abused for DDoS attacks

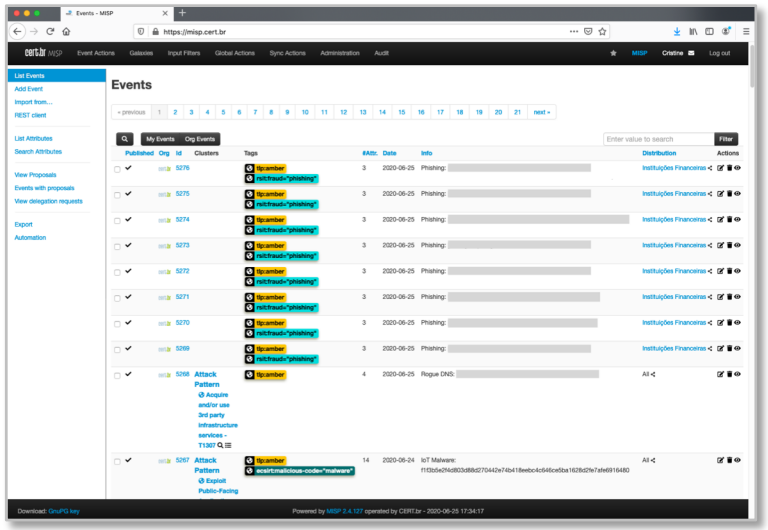
Threat feeds

- CERT.br Distributed Honeypots
- Team Cymru
- SpamHaus
- ShadowServer
- Shodan
- Anti-Botnet operations (Microsoft/FBI)

Notifications sent to all ASNs and public statistics made available



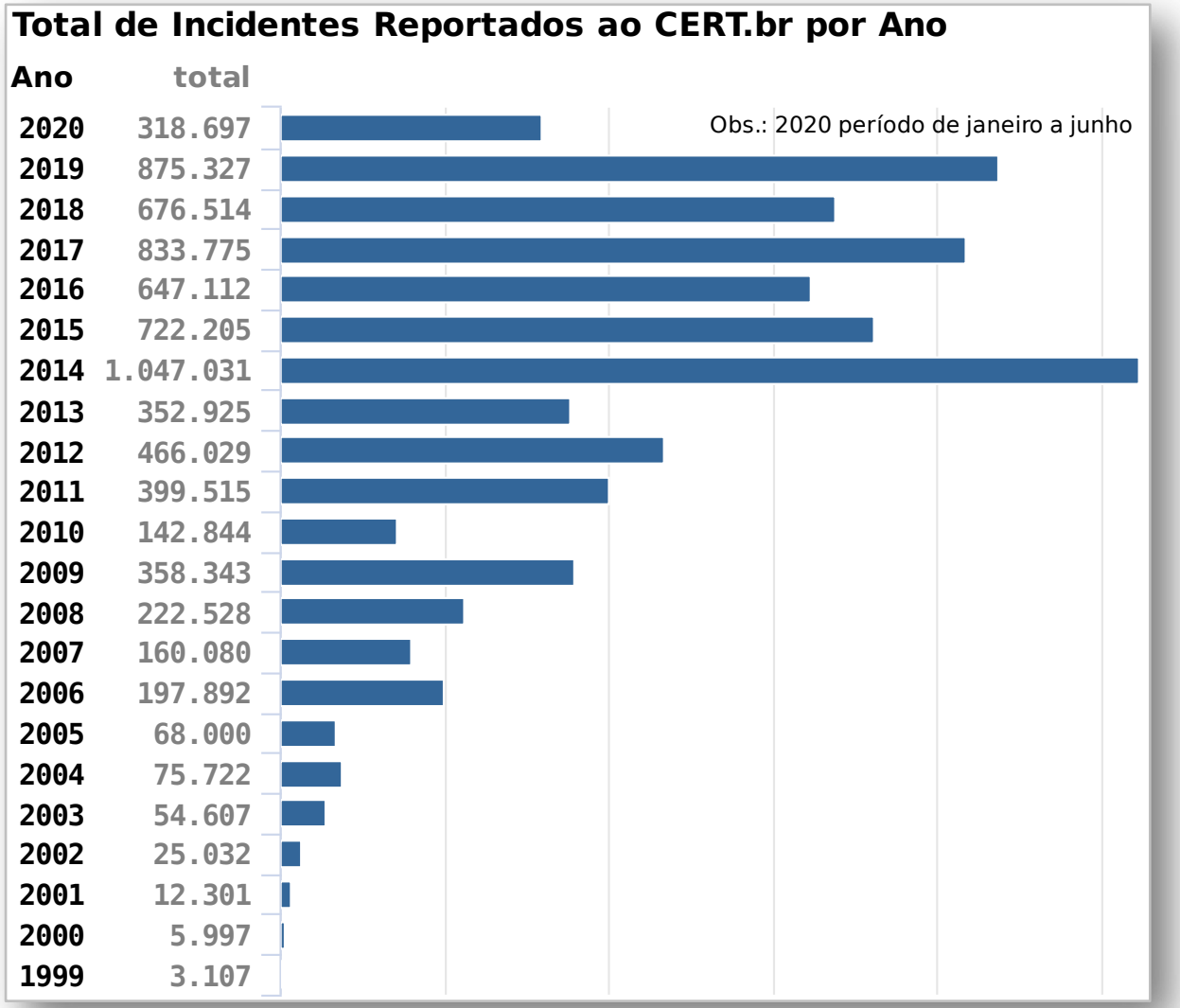
https://cert.br/stats/



https://cert.br/misp/

Incidents Reported to CERT.br: **1999 to 1st Half 2020**

TLP:WHITE



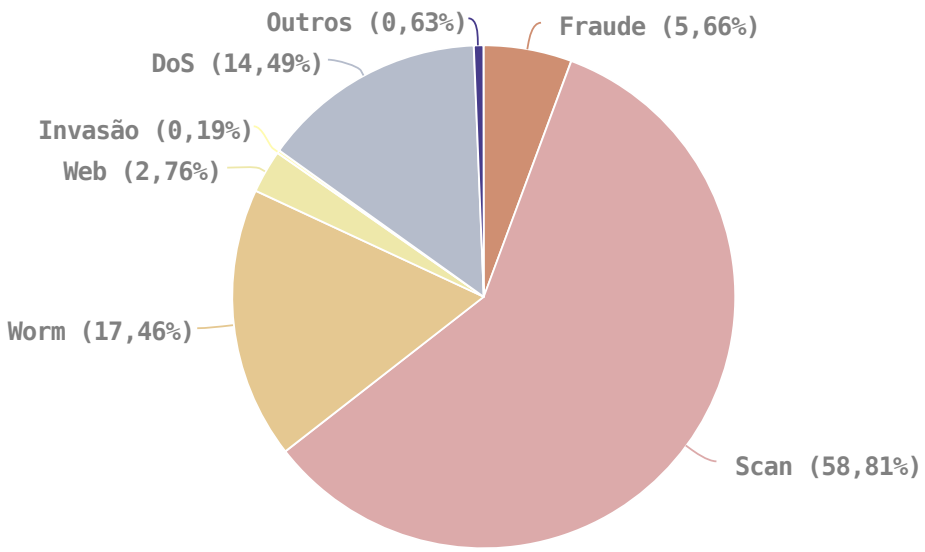
Source: https://cert.br/stats/incidentes/

Most common attacks – 1st half 2020

- Credential brute force attacks
  - *e-mails* (IMAP, SMTP e SMTPS)
  - SSH and TELNET
    - servers and network devices
    - IoT and broadband routers
- IoT abuse
  - Cameras, Smartphones, Smart TVs, Broadband and Wi-Fi routers
    - DDoS (UDP *flood*)
    - change the DNS resolution (to commit fraud)
    - crypto mining

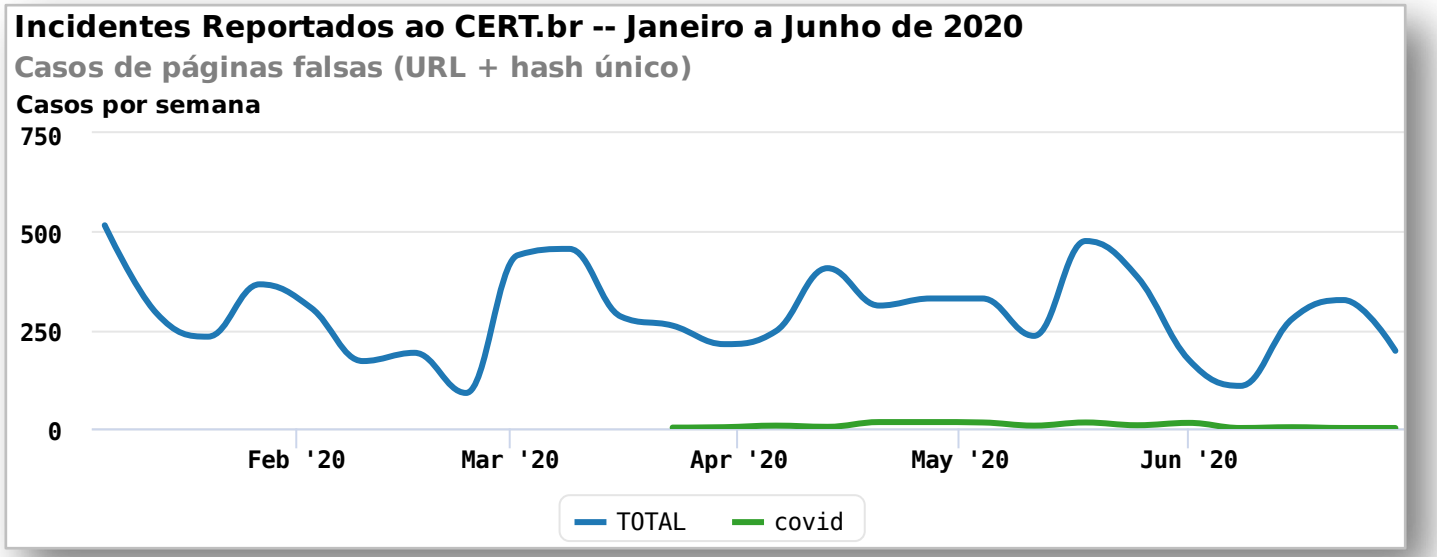
Incidents Reported to CERT.br:
Fraud attempts and DDoS in more detail

TLP:WHITE



Fraud attempts +54% 2019-S1 -35% 2019-S2

- 96% phishing attacks
  - less than 1% is COVID-19 related (see graph below)
  - increase in reports of phishing for credential of cloud document services, video streaming, webmail and social networks



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

- 2019 was the record of reports
- most frequent reports
  - IoT botnets
  - traffic amplification

Lessons Learned

Continue normal operations

- The types of incidents are not likely to change
  - current/extreme events will be used as a lure
  - this has happened before
    - earthquakes, Olympics, tsunamis, etc
- Exposure is likely to change due to unplanned remote working (but nothing really new)
  - internal services exposed
  - less control over desktops/laptops security
  - use of new tools with no training
- Don't panic
  - even if others are panicking
  - don't be too quick to block everything and blacklist everyone

Always be prepared

- to work remotely **securely**
  - equipment and tools
  - multi-factor authentication
- to share information
  - participate in task forces
  - use information sharing platforms
- to provide high level information
  - statistics, briefings, reports, etc
- to educate your constituency!
  - have well known channels
  - enlist the help of others

National Initiatives for a Healthier Internet Ecosystem

cert.br nic.br cgi.br

TLP:WHITE

We need a healthier ecosystem:
National Initiative – A More Secure Internet Program

PROGRAMA INTERNET +SEGURA

Current Goal:

- Reduce the number of systems that can be abused for DDoS attacks

Incentive to adopt best practices:

- Hardening
- Routing Security
- Anti-spoofing (BCP 38)
- Close open services

Joint initiative involving several organizations

- ISOC and ISPs, Hosting and Telco Associations

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

Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition

TLP:WHITE

Work developed by the LAC-AAWG – Latin American and Caribbean Anti-Abuse Working Group

Joint Publication of

- M³AAWG - Messaging, Malware and Mobile Anti-Abuse Working Group
- LACNOG - Latin American and Caribbean Network Operators Group
- Editor: Lucimara, LAC-AAWG Chair / CERT.br

Currently available in:

- English, Portuguese, Korean and Japanese

New translations to be released soon:

- Spanish, French and German

www.lacnog.net/docs/lac-bcop-1

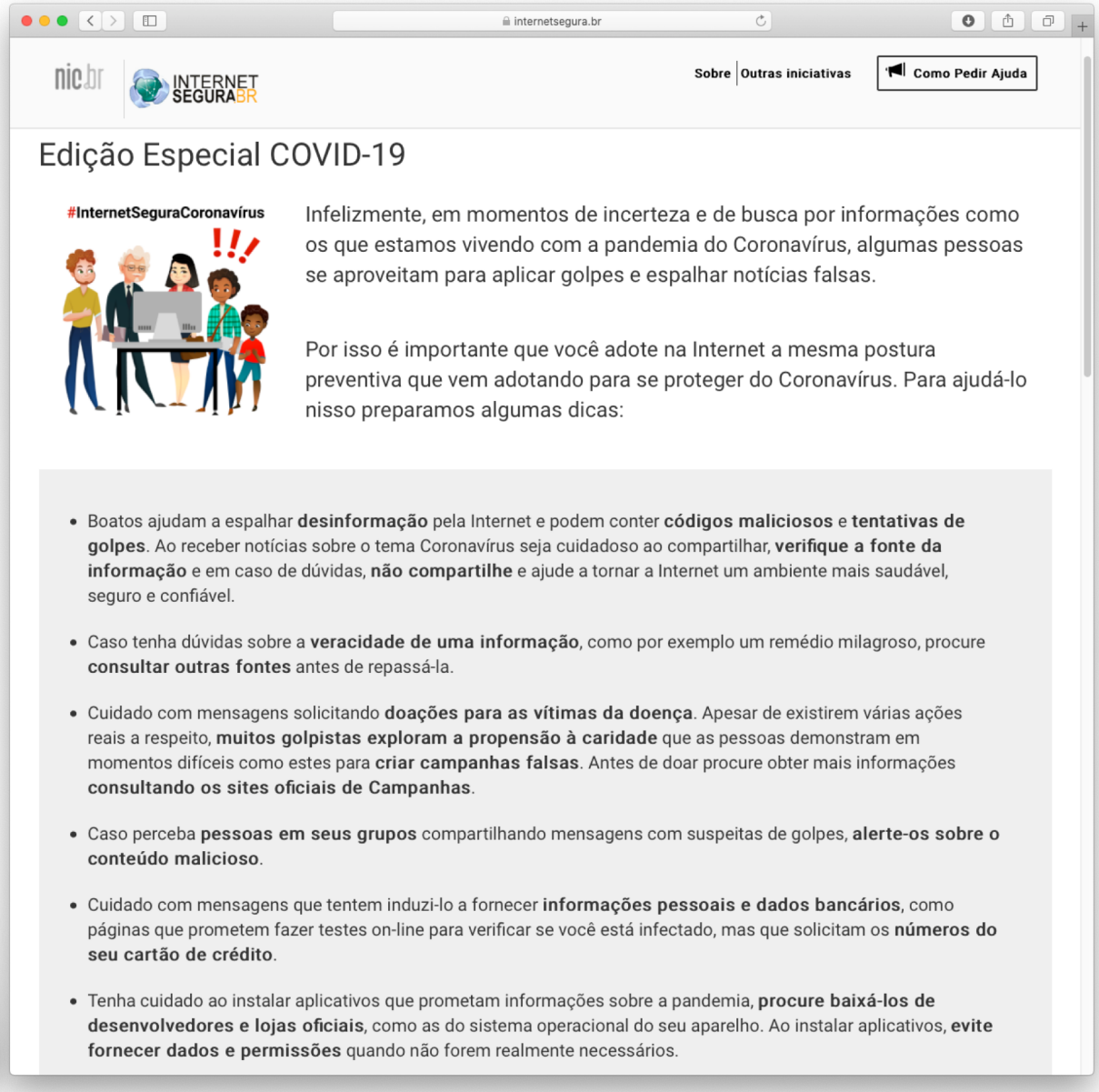
www.m3aawg.org/CPESecurityBP

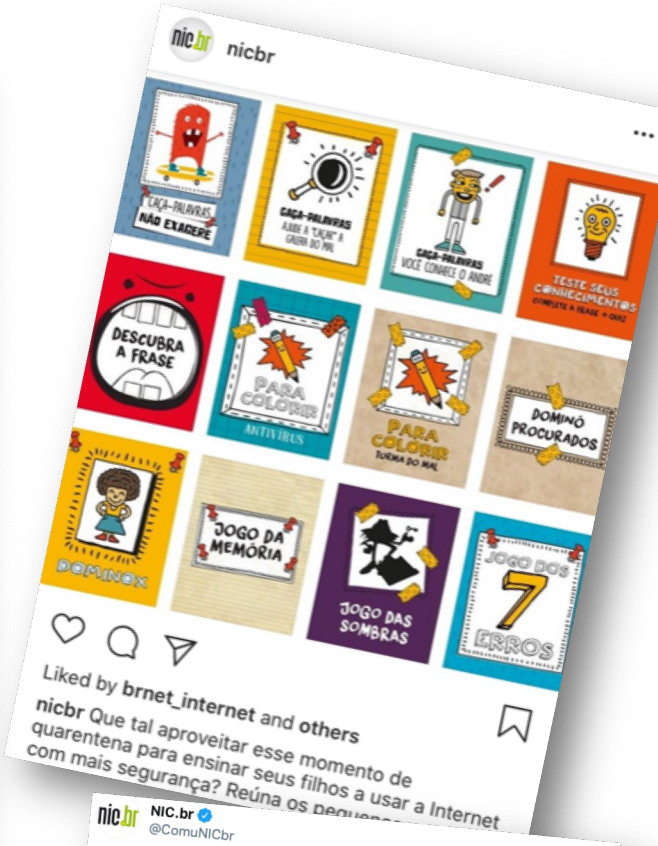
TLP:WHITE

Awareness Materials:
InternetSegura.br Portal


NIC.br
@ComuNICbr
Algumas senhas podem ser facilmente descobertas, e é importante tomar alguns cuidados no momento de elaborá-las. Além disso, uma 2ª camada de segurança deve ser adicionada p/ reforçar a segurança de seus acessos e dispositivos. Veja mais dicas importantes:
internetsegura.br/coronavirus/
Fascículo Verificação em duas etapas
#InternetSeguraCoronavírus
creative commons


nicbr
Fascículo
Códigos maliciosos
#InternetSeguraCoronavírus
creative commons
Liked by pessoapp and others
nicbr Pessoas mal intencionadas podem aproveitar a pandemia dao #Covid19 para aplicar golpes pela Internet e apps de mensagem. Saiba como se... more


internetsegura.br
nic.br
INTERNET SEGURA BR
Sobre
Outras iniciativas
Como Pedir Ajuda
Edição Especial COVID-19
#InternetSeguraCoronavírus
Infelizmente, em momentos de incerteza e de busca por informações como os que estamos vivendo com a pandemia do Coronavírus, algumas pessoas se aproveitam para aplicar golpes e espalhar notícias falsas.
Por isso é importante que você adote na Internet a mesma postura preventiva que vem adotando para se proteger do Coronavírus. Para ajudá-lo nisso preparamos algumas dicas:
• Boatos ajudam a espalhar desinformação pela Internet e podem conter códigos maliciosos e tentativas de golpes. Ao receber notícias sobre o tema Coronavírus seja cuidadoso ao compartilhar, verifique a fonte da informação e em caso de dúvidas, não compartilhe e ajude a tornar a Internet um ambiente mais saudável, seguro e confiável.
• Caso tenha dúvidas sobre a veracidade de uma informação, como por exemplo um remédio milagroso, procure consultar outras fontes antes de repassá-la.
• Cuidado com mensagens solicitando doações para as vítimas da doença. Apesar de existirem várias ações reais a respeito, muitos golpistas exploram a propensão à caridade que as pessoas demonstram em momentos difíceis como estes para criar campanhas falsas. Antes de doar procure obter mais informações consultando os sites oficiais de Campanhas.
• Caso perceba pessoas em seus grupos compartilhando mensagens com suspeitas de golpes, alerte-os sobre o conteúdo malicioso.
• Cuidado com mensagens que tentem induzi-lo a fornecer informações pessoais e dados bancários, como páginas que prometem fazer testes on-line para verificar se você está infectado, mas que solicitam os números do seu cartão de crédito.
• Tenha cuidado ao instalar aplicativos que prometam informações sobre a pandemia, procure baixá-los de desenvolvedores e lojas oficiais, como as do sistema operacional do seu aparelho. Ao instalar aplicativos, evite fornecer dados e permissões quando não forem realmente necessários.


nicbr
CAÇA-PALAVRAS NÃO EXAGERE
CAÇA-PALAVRAS
CAÇA-PALAVRAS
TESTE SEUS CONHECIMENTOS
DESCUBRA A FRASE
PARA COLORIR
PARA COLORIR
DOMINÓ PROCURADOS
DOMINOX
JOGO DA MEMÓRIA
JOGO DAS SOMBRAS
JOGO DOS 7 ERROS
Liked by brnet_internet and others
nicbr Que tal aproveitar esse momento de quarentena para ensinar seus filhos a usar a Internet com mais segurança? Reúna os pequ


NIC.br
@ComuNICbr
Além de ficar em casa e se proteger, lembre-se de proteger também seus equipamentos, mantendo-os atualizados e instalando mecanismos de segurança. Confira mais dicas para usar a Internet de forma segura:
internetsegura.br/coronavirus/ #FiqueEmCasaSeguro
Fascículo Dispositivos móveis
#InternetSeguraCoronavírus
creative commons

Portfolio under Creative Commons License
Including Training Teachers to Use it in Class

TLP:WHITE

Some materials in Spanish, in partnership with ISOC: https://cartilla.cert.br/

Thank You

cristine@cert.br

Incident reports to: cert@cert.br

@certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br