CERT.br / NIC.br
Papel na Resiliência da Internet no Brasil

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

Klaus Steding-Jessen
Gerente Técnico, CERT.br/NIC.br
jessen@cert.br

cert.br nic.br cgi.br

TLP:CLEAR

Quem mantém o CERT.br:
Núcleo de Informação e Coordenação do Ponto BR – NIC.br

Pessoa jurídica de direito privado, **sem fins lucrativos**, criada para **implementar as decisões e os projetos do Comitê Gestor da Internet no Brasil - CGI.br**.

Dentre suas **atribuições** estão:

- promover estudos e recomendar normas e padrões para a segurança das redes e serviços Internet
- Registro.br
  - registro de domínios sob o <.br>
  - alocação de Sistema Autônomos (ASN) e endereços IPv4 e IPv6
- **CERT.br**
  - **apoio ao tratamento de incidentes**
  - **em articulação e cooperação com as entidades e os órgãos responsáveis**
- IX.br
  - interconexão direta entre redes
- Ceptro.br
  - distribuição da Hora Legal brasileira (NTP.br)
  - treinamentos sobre boas práticas

https://nic.br/sobre/ | https://nic.br/estatuto-nic-br/

TLP:CLEAR

Objetivos do NIC.br:
Fomentar uma Internet Estável e Resiliente no Brasil

Robustez e qualidade da Infraestrutura

- Segurança e resiliência dos serviços de DNS
  - DNSSEC desde 2007
  - espelhos dos servidores-raiz
- Aumento da eficiência e redução de custos
  - pontos de interconexão do IX.br em 36 cidades
  - compartilhamento de infraestrutura no OpenCDN

Perenidade e estabilidade dos serviços

- Equipes altamente qualificadas
- Pouca rotatividade

Parcerias internacionais com instituições correlatas

- Mais de 40 parceiros

Segurança e tratamento de incidentes

- CERT.br como contato nacional de último recurso
- Fomento para iniciativas de segurança e tratamento de incidentes

Métricas relevantes e confiáveis para orientar políticas públicas

- Projeto SIMET
  - medição da qualidade da banda larga e de outros serviços
- Cetic.br, centro regional da UNESCO
  - Indicadores sobre o uso das TICs e da Internet

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: Membro pleno desde 2002 **TF-CSIRT Trusted Introducer:** *Accredited* desde 2020

APWG: *Research partner* desde 2004 **SEI/CMU:** Cursos autorizados desde 2003

***Honeynet Project*:** Mantém o capítulo do Brasil desde 2003

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

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

Principais Atividades

- Facilitar a coordenação do tratamento de incidentes entre as partes
  - Ponto de contato nacional de último recurso
  - Trabalho colaborativo com outras entidades
  - Auxílio 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

TLP:CLEAR

Foco do CERT.br nestes 26 anos:
Aumentar a Capacidade Nacional de Tratamento de Incidentes

Nenhum time ou estrutura única conseguirá fazer sozinho a segurança ou a resposta a incidentes

Comunidade Nacional

- Ações junto a setores chave, para **criação e treinamento de Times** de Tratamento de Incidentes de Segurança (CSIRTs)
- **Auxiliar na análise** técnica e **facilitar** o tratamento de incidentes por outros CSIRTs
- Gerar massa crítica para possibilitar a **cooperação** e melhora na segurança das redes
- Ter uma visão sobre as principais **tendências** de ataques no Brasil

Comunidade Internacional

- Estabelecer **relações de confiança**
  - facilitar a comunicação em casos de incidentes
  - dar acesso a informações que ajudem a comunidade local
- **Influenciar** os padrões e certificações sendo construídos para CSIRTs
- Levar a **visão nacional** aos fóruns pertinentes

TLP:CLEAR

Representação Internacional do Brasil:
Principais Fóruns com Participação do CERT.br

FIRST

Fórum Global de CSIRTs, que existe desde 1992

- membro desde 2002

Destaques da Participação:

- Desenvolvimento do *FIRST CSIRT Services Framework*
- Organização do CTF da Conferência Anual
- *Membership Committee*
- Conselho Diretor em 2012/2013
- Viabilização da parceria entre o FIRST e o LACNIC
  - CERT.br é *co-host* dos Simpósios na região
  - **Simpósio 2023 no Brasil**
    Fortaleza 06 de outubro

NatCSIRTs - organizado pelo CERT/CC

CERT.br está presente desde 2006

Reunião anual de CSIRTs de responsabilidade nacional

- participam CERT.br e CTIR Gov

OpenCSIRT Foundation

- Representação no Conselho de Administração
- Trazendo o Modelo de Maturidade SIM3 para o Brasil

LAC-CSIRTs

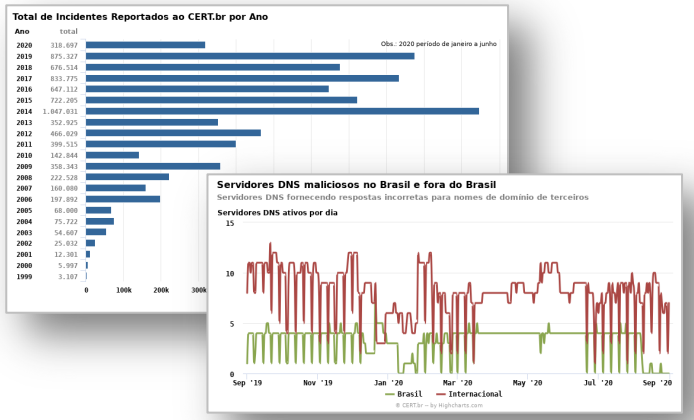
(CSIRTs) da região da América Latina e o Caribe
– reuniões durante o LACNIC

TLP:CLEAR

Tratamento de Incidentes e Consciência Situacional:
Alertar sobre problemas, gerar métricas e apontar soluções

Notificações voluntárias de incidentes enviadas para: cert@cert.br

- Volume em 2022: 1.287.133 *e-mails* tratados, relativos a incidentes voluntariamente notificados ao CERT.br



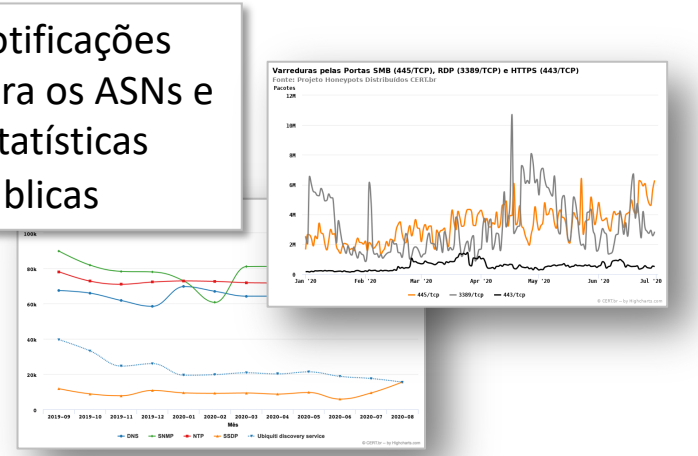
Compartilhamento via MISP

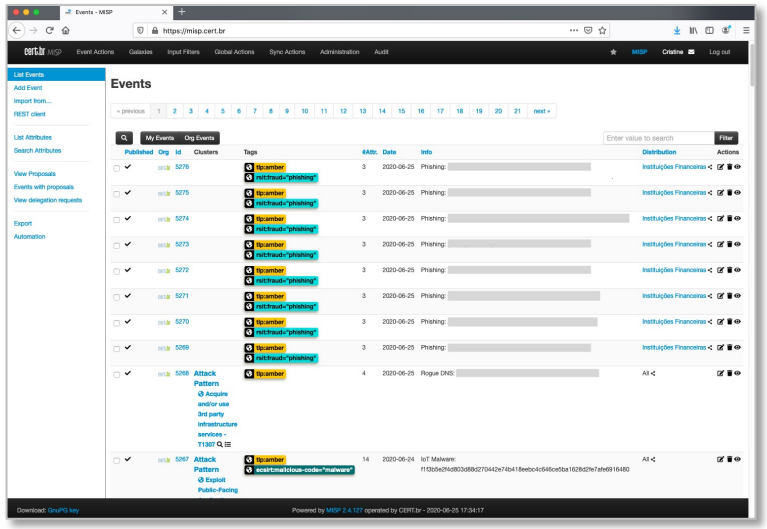
- Indicadores compartilhados com diversos setores
  - financeiro
  - energia
  - acadêmico
  - governo
  - operadores de redes

Threat feeds

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

Notificações para os ASNs e estatísticas públicas





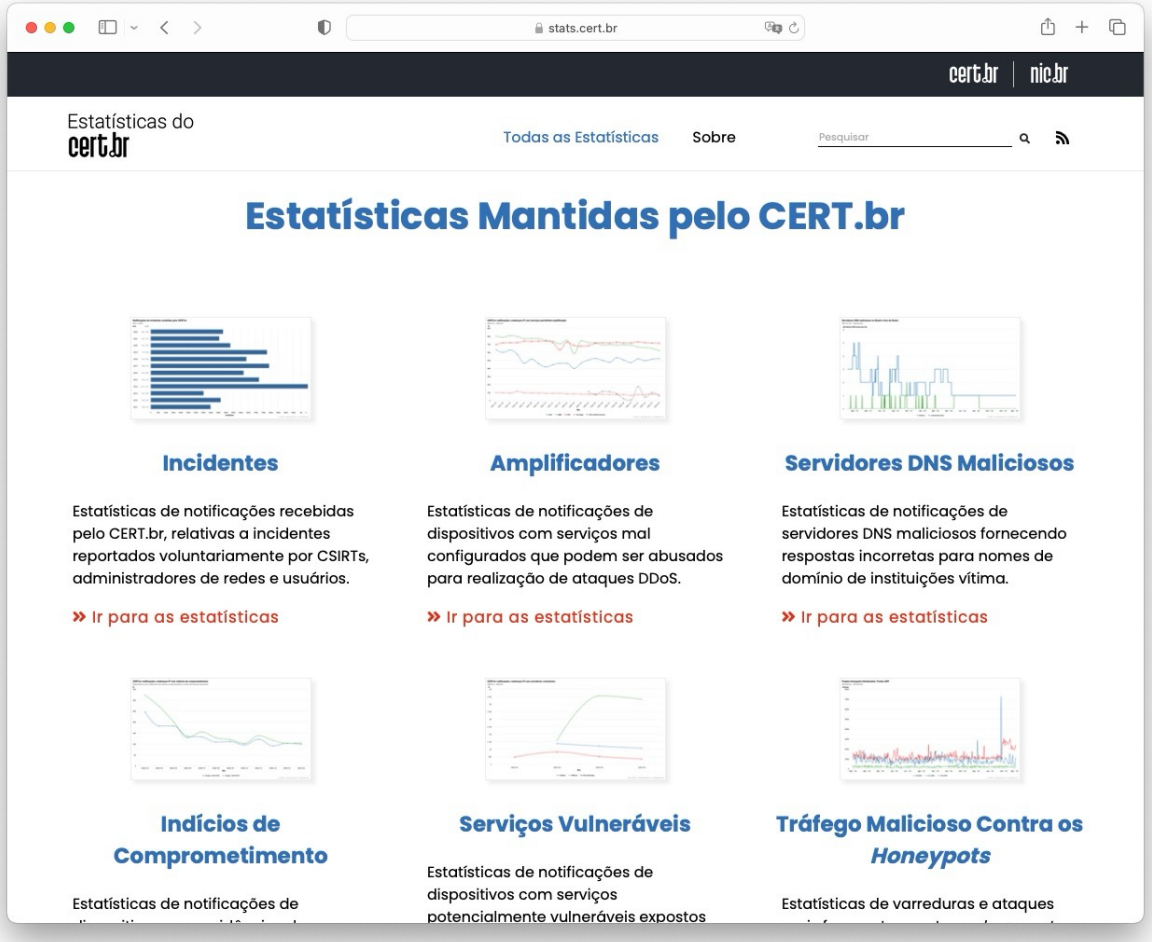
https://stats.cert.br/

https://cert.br/misp/

TLP:CLEAR

Acompanhamento de tendências no Brasil: **Portal de Estatísticas do CERT.br**

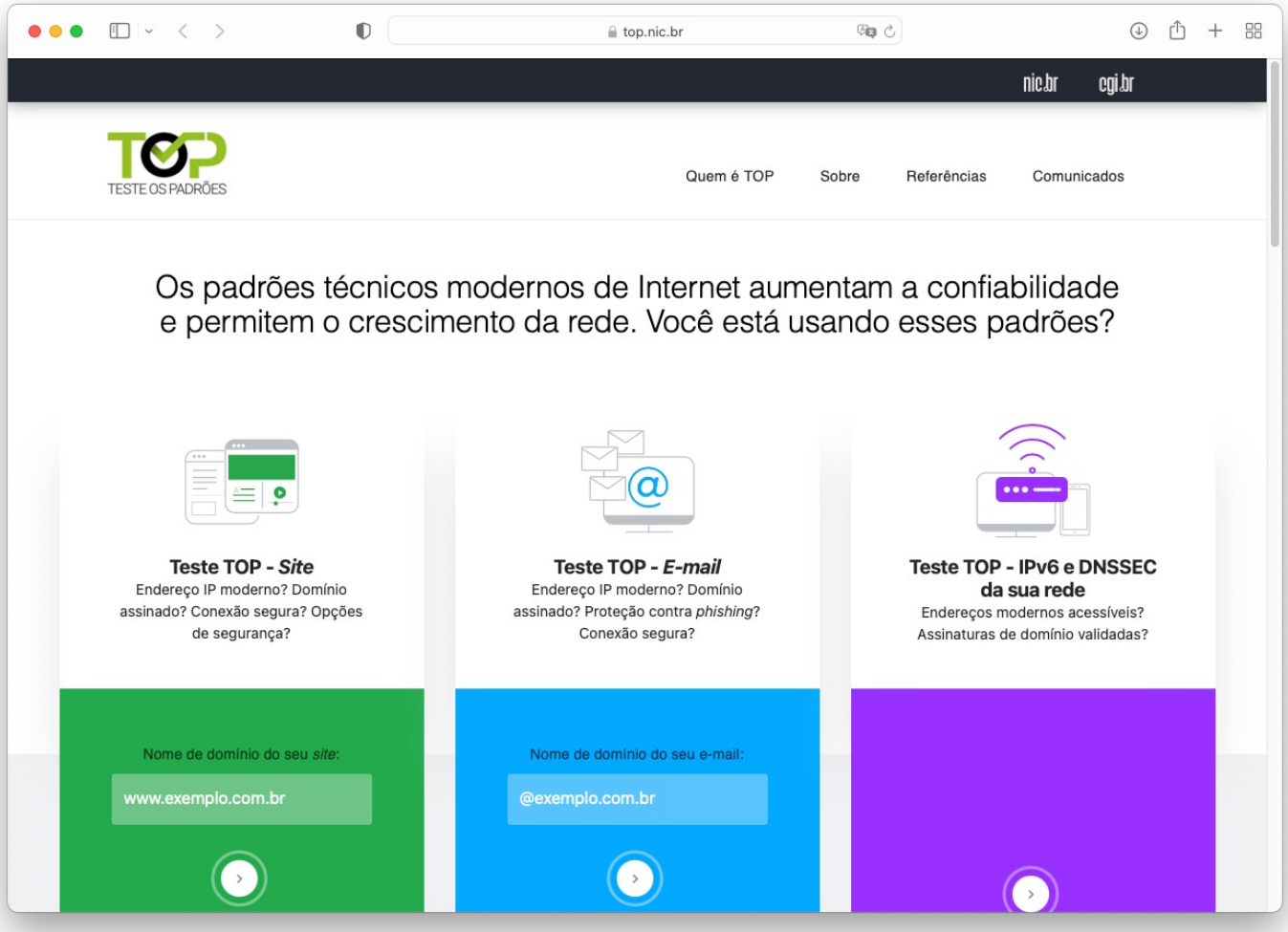
- Notificações voluntárias para o CERT.br
  - Incidentes notificados ao CERT.br
  - Páginas falsas utilizadas em tentativas de *phishing*
  - Reclamações de *spam*
- Notificações enviadas pelo CERT.br para responsáveis por recursos Internet
  - Dispositivos permitindo amplificação
  - Servidores DNS maliciosos
  - Dispositivos com indícios de comprometimento
  - Dispositivos com serviços potencialmente vulneráveis
- Tráfego malicioso observado em *honeypots*



https://stats.cert.br/

TLP:CLEAR

Estímulo à implementação de boas práticas:
Protocolos modernos e seguros para *sites*, *e-mail* e conectividade



https://top.nic.br/

Testa a correta implementação de

- IPv6
- DNSSEC
- TLS e cifras
- SPF / DKIM / DMARC
- STARTTLS / DANE

Apoiadores

conexis brasil.digital
REDETELESUL
abranet Associação Brasileira de Internet
abrint
AbraHosting
TelComp Competição para o Futuro Digital
abramulti
APRONET Associação Catarinense dos Provedores de Internet
InternetSul

TLP:CLEAR

Contato com o CERT.br

– Notificações de incidentes somente via *e-mail*: **<cert@cert.br>**

– Para comunicação segura, utilizar a chave PGP:
  - Chave PGP 2023
    PGP Key ID: **0xBE634C8F**
    Fingerprint: **48D0 D3F3 D6C7 2AE7 65A5 45C7 CB75 CE22 BE63 4C8F**

– Mais informações em:

https://cert.br/contato/

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

https://cert.br/sobre/

Obrigado

@ notificações para: cert@cert.br

https://cert.br/

02 de outubro de 2023

nic.br cgi.br

www.nic.br | www.cgi.br