nic.br cgi.br | cert.br

11º Fórum Brasileiro de CSIRTs

31 de julho de 2023

Utilizando dados do CERT.br para alimentar os seus processos de *Threat Hunting* e Detecção de Incidentes

Cristine Hoepers
Gerente Geral, 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

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 ASN alocados ao Brasil
- domínios sob o ccTLD .br

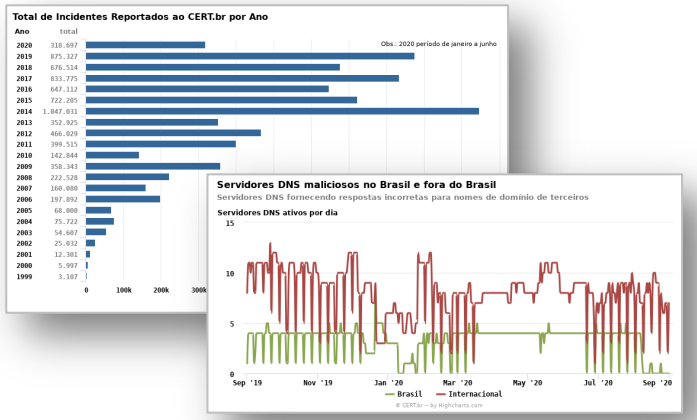
Principais Atividades

- 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

Gestão de Incidentes e Consciência Situacional: **Fontes dos Dados, Métricas e Compartilhamento**

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



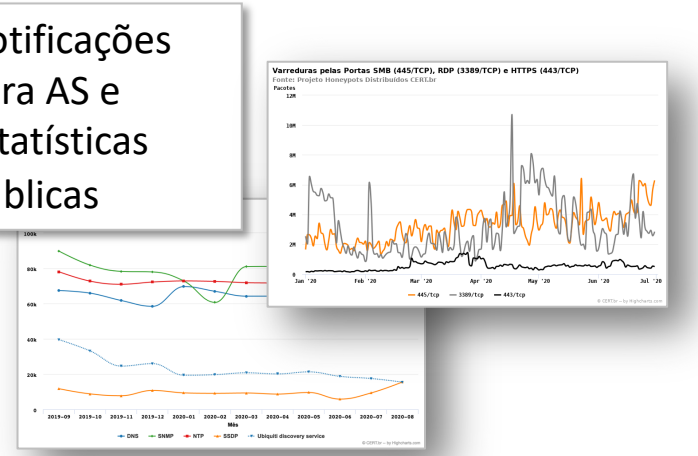
Compartilhamento via MISP

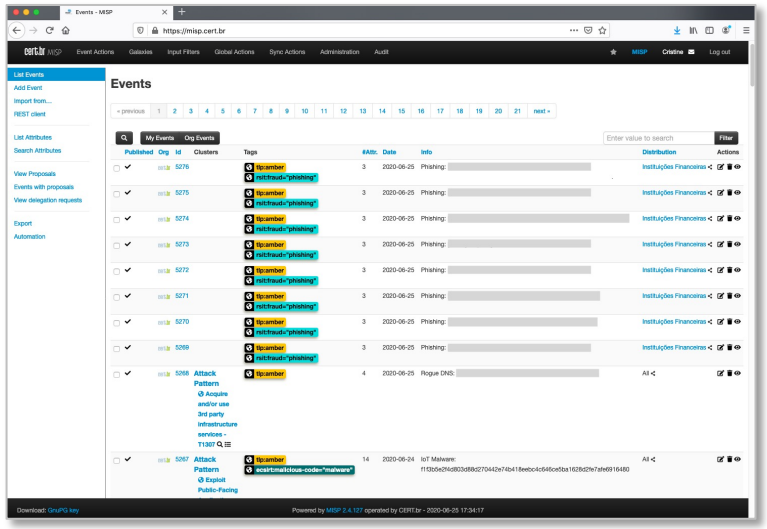
- Indicadores selecionados são compartilhados com parceiros
  - Servidores DNS maliciosos
  - *Phishing*
  - Binários e Comando e Controle de *botnets* IoT
  - Amplificadores usados em ataques DDoS

Threat feeds

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

Notificações para AS e estatísticas públicas





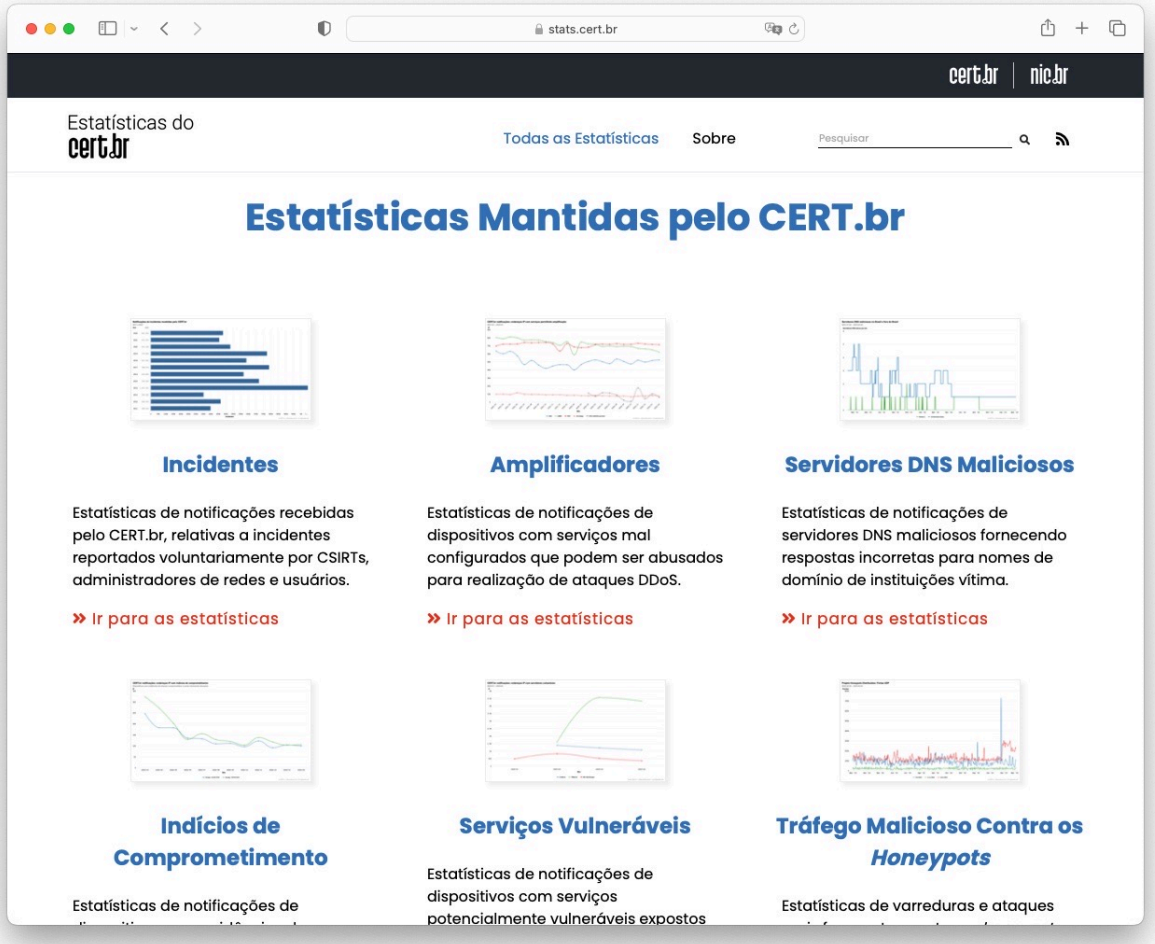
https://stats.cert.br/

https://cert.br/misp/

Portal de Estatísticas do CERT.br
`https://stats.cert.br/`

TLP:CLEAR

- 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*



Demonstração:
Portal de Estatísticas & MISP

cert.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