nic.br cgi.br | cert.br

***Workshop* CKN**

07 de dezembro de 2021

Evento *Online*

TLP:WHITE

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 Político

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

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

[1] https://cert.br/sobre/estudo-cgibr-1996.html | [2] https://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 administrados pelo NIC.br

- endereços IP ou ASNs alocados ao Brasil
- domínios sob o ccTLD .br

Governança

Mantido pelo **NIC.br** – Núcleo de Informação e Coordenação do .br

- todas as atividades são sustentadas pelo registro de domínios .br

O NIC.br é o **braço executivo do CGI.br** – Comitê Gestor da Internet no Brasil

- entidade multissetorial, coordenada pelo MCTI
- responsável por coordenar e integrar as iniciativas e serviços da Internet no País

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

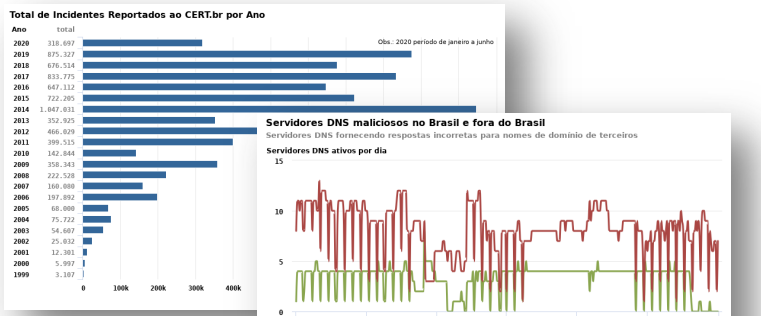
Uso do MISP pelo CERT.br

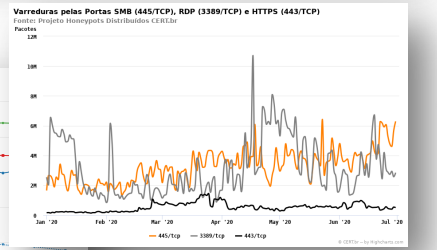
Dr. Klaus Steding-Jessen
Gerente Técnico
jessen@cert.br

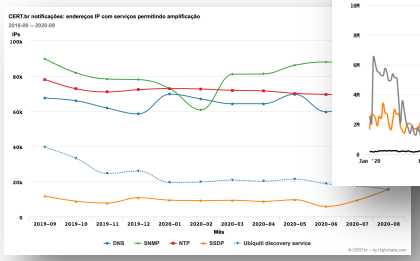
cert.br nic.br cgi.br

TLP:WHITE

Compartilhamento de Indicadores para Consciência Situacional

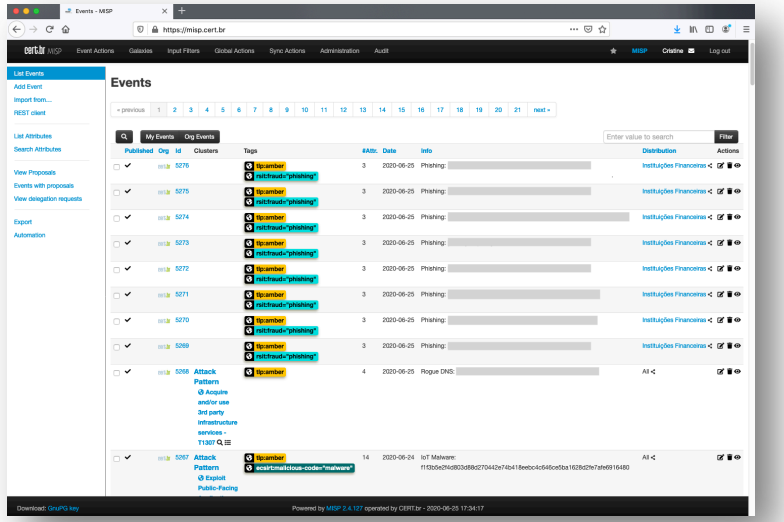






Notificações de Incidentes

Honeypots e *Threat Feeds*



Notificações para os Sistemas Autônomos

Estatísticas Públicas
https://cert.br/stats/

Compartilhamento de indicadores via MISP
https://cert.br/misp/

TLP:WHITE

Como sua Organização pode Usar os IoCs do CERT.br

Todas as Comunidades

- Servidores DNS maliciosos

  Fonte: notificações / *threat feeds* / *honeypots*

  Uso:

  - identificar usuários/clientes consultando esses servidores (via *netflow*)
  - identificar *phishings* e solicitar *takedown*

- Binário, *hash*, IP de *download* e CnC de *botnets* IoT

  Fonte: *threat feeds* / *honeypots*

  Uso:

  - identificar usuários/clientes infectados
    - acessando o IP/URL de *download* (via *netflow* ou *proxy*)
    - acessando o CnC (via *netflow*)
  - procurar pelo *hash* em ferramentas/bases locais
  - analisar o binário, se for de interesse

Setor Financeiro

- *Phishings*

  Fonte: notificações

  Uso:

  - identificar campanhas
  - *takedown*

Operadoras de Telecom

- Amplificadores

  Fonte: *threat feeds*

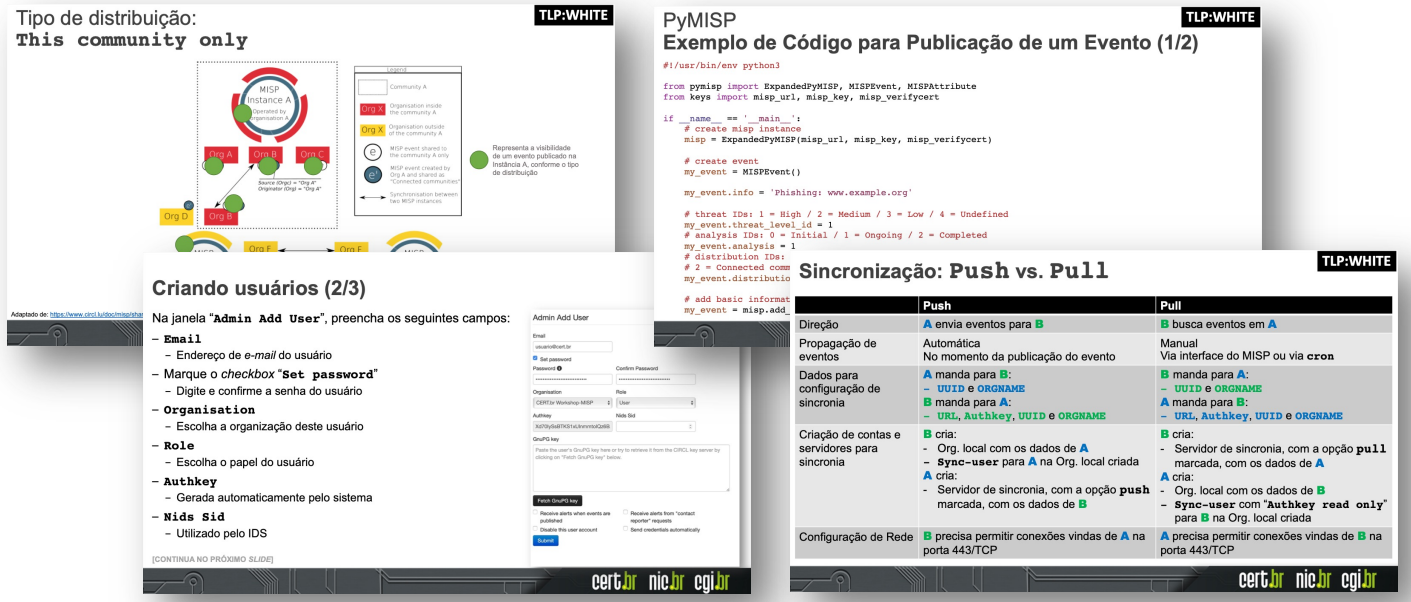
  Uso:

  - identificar clientes afetados
  - corrigir o problema

TLP:WHITE

https://cert.br/misp/
Referências em Português sobre MISP

- Lista de discussão
  https://listas.cert.br/mailman/listinfo/misp-br
- Passo-a-passo de instalação em um sistema Ubuntu
  https://cert.br/misp/tutorial-ubuntu/
  Incluindo:
  - Considerações de Segurança
    - Não Utilizar Imagens Baixadas da Internet para Instâncias em Produção
    - Cuidados com o Certificado Digital
    - Cuidados com *Firewall*, WAF e Anti-DDoS Corporativos
  - Instalação e *Hardening* Básicos do SO
  - Instalação do MariaDB, Apache, PHP e outras Dependências do MISP
  - Instalação do MISP
  - Configuração Inicial do MISP
    - Criar os arquivos de configuração e definir as credenciais de acesso
    - Definir as configurações iniciais do MISP
- Passo-a-passo de configuração e operação
  https://cert.br/misp/certbr-passo-a-passo-misp-2021-08-19.pdf
  Incluindo:
  - Primeiro *login*, criação e administração de usuários, atualização do MISP
  - Geração e uso de `authkeys`
  - Sincronização entre instâncias, *Communities* e Distribuição de Eventos
  - Automatização com `curl` e PyMISP



Obrigado

jessen@cert.br

Notificações para: cert@cert.br

@certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br