CERT.br
Responsabilidades e Atividades

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

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

Foco do CERT.br nestes 27 anos:
Aumentar a Capacidade Nacional de Tratamento de Incidentes

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

Fomentar e Fortalecer a 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

Inserir-se na 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

Cooperação Internacional:
Pessoas e Relações de Confiança Fazem a Diferença

CSIRTs operam em um esquema de governança em rede

- **não** há hierarquia
- há a construção de redes de **confiança** globais e locais
- resolução de incidentes envolve **cooperação** entre múltiplas organizações, redes e países

Maturidade evoluiu para um código de ética e modelos de acreditação e certificação

- EthicsfIRST
- SIM3 - *Security Incident Management Maturity Model*
- *TF-CSIRT Trusted Introducer Accreditation and Certification*

Diversas Comunidades Formais

Participação do CERT.br:

FIRST – Fórum Global de CSIRTs

- membro desde 2002

TF-CSIRT – Fórum mantido pela OpenCSIRT Foundation

- Membro *Accredited* desde 2020

NatCSIRT – Reunião anual de CSIRTs de responsabilidade nacional, organizada pelo CERT/CC

- participamos desde a criação, em 2006
- atualmente participam CERT.br e CTIR Gov

LAC-CSIRTs – Reunião de CSIRTs da região

- Organizada em conjunto com o LACNIC desde 2011

Outras organizações com foco em comunidades específicas:

- APCERT, AfricaCERT, OIC-CERT, EU e-CSIRT Network

Cooperação Internacional:
Destaques da Participação Ativa do CERT.br

FIRST

Atual:

- Membro do *Membership Committee*
- Organização do CTF da Conferência desde 2012
- Participação ativa nos seguintes SIGs (Grupos de Interesse Especial):
  - *CSIRT Framework Development*
  - *DNS Abuse*
  - *Ethics*
  - *Security Lounge* (do qual é *co-chair*)
  - Padrão TLP (*Traffic Light Protocol*)

Anterior:

- Membro do Conselho Diretor em 2012/2013
- Coordenação de conteúdo do padrão *FIRST CSIRT Services Framework*
- *Chair* da Conferência 2020
- Viabilização da parceria entre o FIRST e o LACNIC
  - CERT.br é *co-host* dos Simpósios do LAC-CSIRTs

Cooperação com CERTs Nacionais

Maiores parceiros diretos do CERT.br:

CERT/CC	CISA	CERT.at
JPCERT/CC	NISC JP	CERT.LV
CERT.PL	NCSC-NL	NCSC-FI
HKCERT	TWCERT/CC	

OpenCSIRT Foundation

- Dois auditores SIM3 certificados
- Gerente do CERT.br foi eleita em 2023 para o *Board of Comissioners* da organização

IGF – 2014/2015

- Coordenação do Fórum de Boas Práticas para CSIRTs
- Coordenação do Fórum de Combate a Spam

Criação de Uma Comunidade Atuante no Brasil:
Fomento à Cooperação e Criação de CSIRTs

Objetivo

- Criar/aproximar CSIRTs (Grupos de Tratamento de Incidentes de Segurança) no Brasil
- Possuir profissionais preparados para resolver os problemas de segurança no país

Fórum Brasileiro de CSIRTs

- Evento anual para profissionais da área de Tratamento de Incidentes
- *Workshops* sobre assuntos específicos
- https://forum.cert.br/

Fomento à adoção da Plataforma MISP para compartilhamento de ameaças

- https://cert.br/misp/

Exercício Guardião Cibernético

- integrante como órgão parceiro
- cooperação na produção de material didático personalizado

Grupos de Trabalho Setoriais

- Febraban
  Fórum de Incidentes Cibernéticos e Resposta a Incidentes (FICRI)
- ABBC
  Comissão de Segurança Cibernética e Acordo de Cooperação na área Conscientização
- Anatel GTCiber
  GT fraudes SMS
  GT Compartilhamento de Informações
  GT Equipamentos

Criação de Uma Comunidade Atuante no Brasil: **Cursos de Gestão de Incidentes**

SEI Partner Network

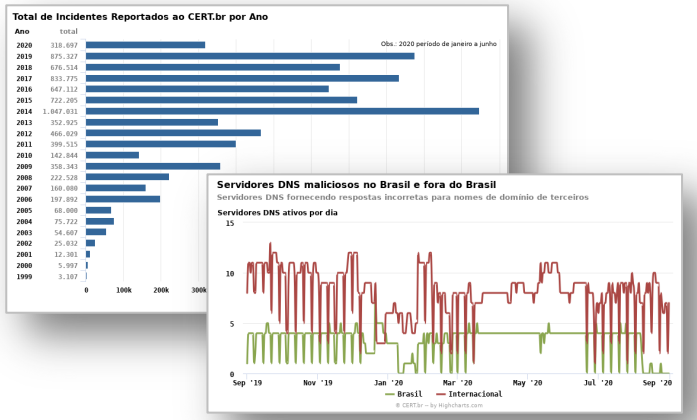
Licencia os cursos do *CERT® Division, do SEI/Carnegie Mellon,* desde 2003:

- https://cursos.cert.br/
- **107 turmas**, atingindo **2712 profissionais** de diversos setores
  - incluindo por exemplo: ABIN, Anatel, BB, BNDES, Bradesco, BTG Pactual, C6 Bank, CAIXA, Câmara dos Deputados, CISC Gov BR, CDCiber, CNJ, CPTM, CTIR Gov, DASA, DATAPREV, Eletrobrás, Eletronuclear, Exército, FINEP, Força Aérea, Furnas, Getnet, Global Hitss, Globo, Intelbras, IPV7, INSS, ITAIPU Binacional, Itaú, MJ, Marinha, Natura, Neon Pagamentos, Nubank, OEC, Oncoclínicas, Opice Blum | Bruno Advogados, Petrobras, Porto de Santos, Presidência, RNP, RTM, Sabesp, SERPRO, STF, STJ, TRE-TO, TRE-MG, TRT-1, TRT-3, TRT-5, TRT-7, TRT-8, TST, UNB, Unicamp, USP, TCU, Vale e VIVO.
- Turmas especiais e gratuitas para os grandes eventos - 176 profissionais treinados
- Turma especial em 2023 para órgãos do SISP em parceria com a SGD/MGI, com 30 participantes

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

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

- 2023:
  1.588.077 *e-mails* tratados
  621.537 incidentes
- 2024 (janeiro a abril):
  450.327 *e-mails* tratados
  146.386 incidentes



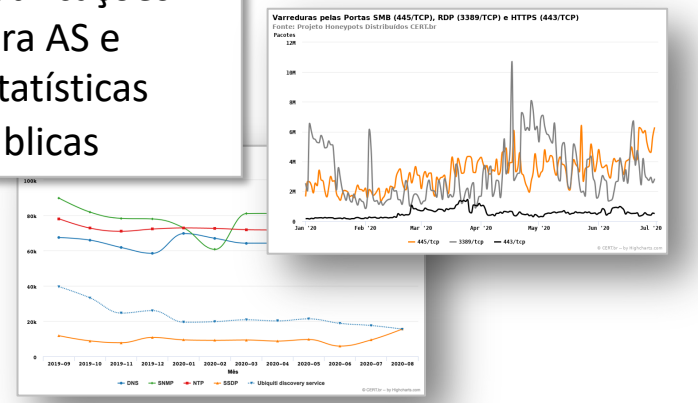
Compartilhamento via MISP

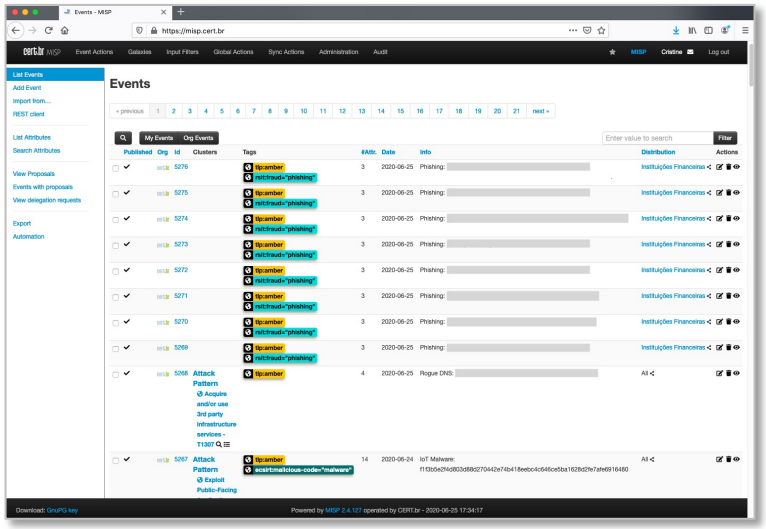
- Indicadores selecionados são compartilhados com parceiros
  - Servidores DNS maliciosos
  - *Phishing*
  - Binários e Comando e Controle de *botnets* IoT
  - Amplificadores usados em ataques DDoS

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

- 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
  - Servidores DNS maliciosos
  - Dispositivos permitindo amplificação
  - Dispositivos com indícios de comprometimento
  - Dispositivos com serviços potencialmente vulneráveis
- Tráfego malicioso observado em *honeypots*

http://stats.cert.br/

Programa por uma Internet mais Segura:
Atividades Desenvolvidas pelo CERT.br

Obtenção de dados:

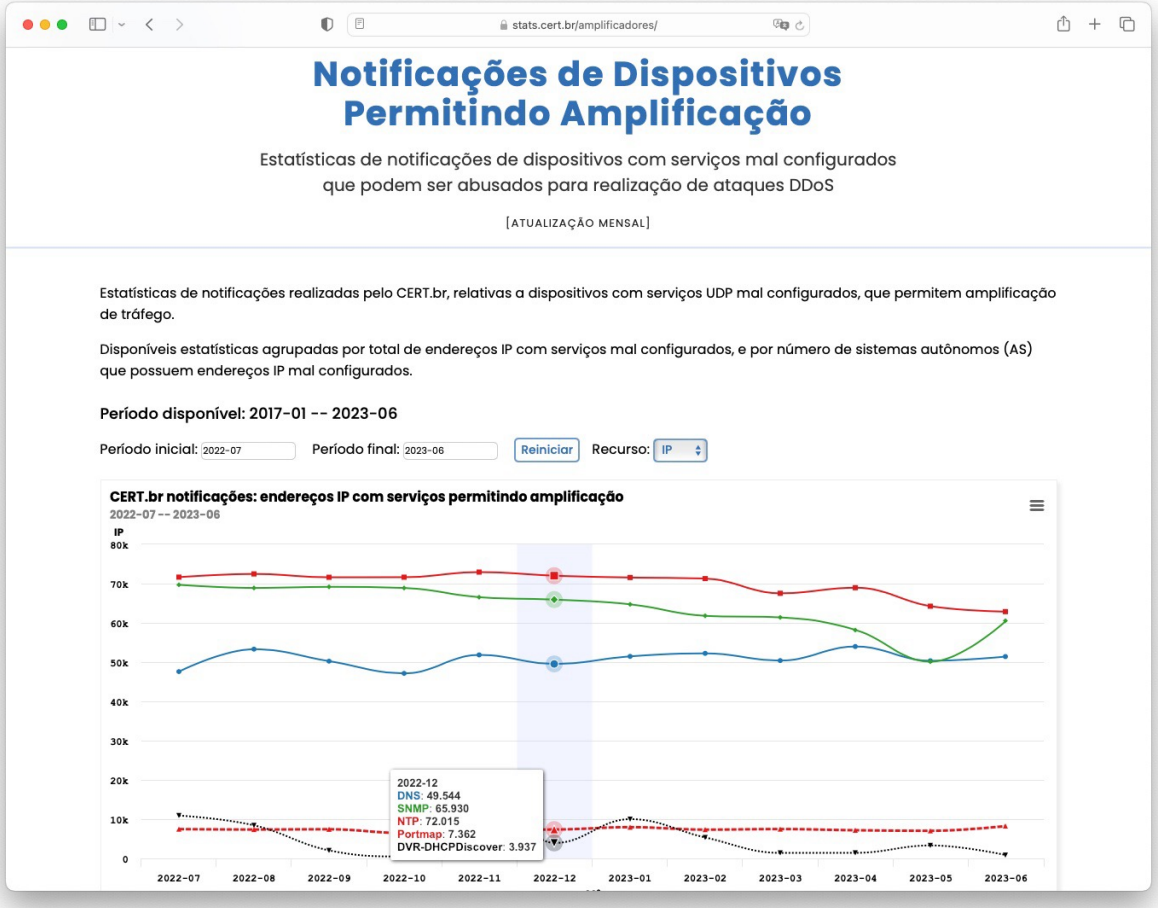
- Ataques observados pelos próprios *honeypots*
- Dados de parceiros internacionais (*threat feeds*)

Refinamento dos dados:

- Consolidar as fontes e validar os dados recebidos de terceiros

Métricas e notificações:

- Notificação individualizada para os Sistemas Autônomos
- Geração das métricas do Programa https://stats.cert.br/amplificadores/



Conscientização – Público Geral:
Fascículos da Cartilha de Segurança para Internet

Conteúdo disponível *online* gratuitamente sob Licença *Creative Commons*

– **Fascículos** que cobrem assuntos específicos relacionados com segurança na Internet

  – Dica do dia no *site*, via *Twitter* e RSS

  – Impressões em pequena escala enviadas a escolas e centros de inclusão digital

  – Possível gerar versões personalizadas com logo da instituição

  Exemplos de parceiros de divulgação:

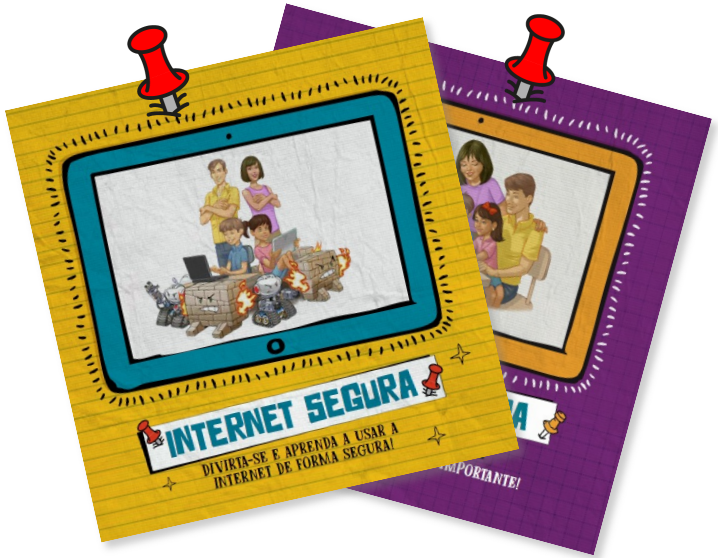
  Agência 3C's Criações, Avantsec, Banco Next, SESIC/GSI/PR, Gov.br, Guardião Cibernético, Eletronuclear, ELO, Itaipu, Leroy Merlin, Lumen Compliance, Marbon, Metrô SP, Microsoft, Ministério Público do Mato Grosso, Polícia Civil Santa Catarina, Procergs, SESI/SENAI SP, Secretaria de Educação - Gov/RJ, Sicoob, Sincoplastic, TRT-7 Ceará, TecKids, Telebras e Unimed Maceió.

https://cartilha.cert.br/

Conscientização – Público Infantil:
Guia com Dicas e Passatempos + Personagens de Montar

Guias Internet Segura

- Disponíveis Gratuitamente
- Parcerias de impressão com escolas privadas
- Traduzido pelo NCSC da Finlândia
  - distribuído em todas as escolas
- Parceria similar em andamento com o NCSC da Estônia



https://internetsegura.br/criancas/

Conscientização – Público Infantil:
Jogo de Tabuleiro Internet Segura

Discussão divertida sobre comportamento *online*, em família ou na escola

- Seguir as dicas de segurança dá bônus e pode levar à chegada rapidinho
- Comportamentos arriscados implicam em voltar atrás ou ficar sem jogar

https://internetsegura.br/tabuleiro/

Obrigado

@ Notificações para: cert@cert.br 𝕏 @certbr

https://cert.br/

17 de maio de 2024

nic.br cgi.br

www.nic.br | www.cgi.br

Histórico:
Criação do CERT.br

1995: o pleno do CGI.br solicitou a especialistas uma análise sobre a situação nacional de segurança, e uma proposta para uma estrutura de coordenação

Agosto/1996: o relatório "Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil" é publicado pelo CGI.br[1]

- Levantamento da situação no País
- Definição de prioridades
- Levantamento do **melhor modelo para agir como facilitador para o tratamento de incidentes de segurança**
  - time autônomo e neutro, para atuar como ponto de contato nacional
  - orientar tecnicamente sobre prevenção e resposta a incidentes
  - fomentar treinamento, atualização e cooperação
  - fomentar a criação de novos CSIRTs (Times de Tratamento de Incidentes de Segurança em Computadores) no País

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

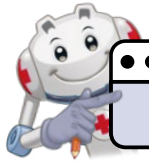
[1] https://cert.br/sobre/estudo-cgibr-1996.html
[2] https://nic.br/pagina/gts/157

Nova Organização do Conteúdo dos Fascículos da Cartilha
Adaptado para Espaços Reduzidos como Mídias Sociais

SAIBA OS CANAIS OFICIAIS DA INSTITUIÇÃO FINANCEIRA

Golpistas criam páginas e perfis falsos, e os promovem via anúncios em *sites* de busca, redes sociais e aplicativos de mensagens. Você pode acabar vítima de golpes se seguir os *links* desses anúncios.

- » Acesse o *site* oficial digitando o endereço (URL) diretamente no navegador
  - use sempre conexão segura (https)
- » Salve a página nos "Favoritos" para facilitar futuros acessos
- » Cheque no *site* da instituição quais são os outros canais oficiais



Veja mais dicas no fascículo "*Phishing* e Outros Golpes".

O QUÊ
- A dica de segurança em si
- Texto simples, ao ponto
- Usuários mais experientes não precisam ler além desse texto

PORQUÊ
- Por que me importar com isso?
- O que eu ganho se seguir?

COMO
- Passos para implementar
- Ferramentas e comportamento

VEJA MAIS (opcional)
- Aponta que há dicas relacionadas em outro fascículo

QUADRO (opcional)
- Esclarecer termos
- Cuidados/alertas

PLANEJE-SE PARA RECUPERAR SUAS CONTAS E DADOS DEPOIS

Para recuperar suas contas e dados em outro aparelho, algumas ações e configurações devem ser feitas antes que o furto ocorra.

- » Defina um número de celular alternativo para recuperação de contas, como a do Apple ID
- » Gere e tenha em fácil acesso códigos de *backup* para contas que usem verificação em duas etapas
- » Faça *backups*

Códigos de *backup* são gerados pela função de verificação em duas etapas para serem usados quando outros métodos de autenticação não estiverem disponíveis.