nic.br cgi.br | cert.br

Comitê Gestor da Internet no Brasil
23 de outubro de 2020

Responsabilidades e Atividades do CERT.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Dra. Cristine Hoepers
Gerente Geral
cristine@cert.br

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

cert.br nic.br 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**
  - grupo 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 (Grupos de Tratamento de Incidentes) 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 grupo com responsabilidade nacional[2]

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

cert.br

Tratamento de Incidentes	Treinamento e Conscientização	Análise de Tendências
▶ Articulação	▶ Cursos	▶ *Honeypots* Distribuídos
▶ Análise Técnica	▶ Palestras	▶ SpamPots
▶ Apoio à recuperação	▶ Boas Práticas	▶ Processamento de *threat feeds*
	▶ Reuniões	

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

https://cert.br/sobre/
https://www.first.org/members/teams/cert-br
https://www.trusted-introducer.org/directory/teams/certbr.html
https://apwg.org/sponsor-solutions/research-partners/

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 alocados pelo NIC.br (endereços IP ou ASNs alocados ao Brasil e domínios sob o ccTLD .br).

Foco das Atividades

- **Ponto de contato** nacional
- **Trabalho colaborativo** com outras entidades
- Auxiliar 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 23 anos:
Aumentar a Capacidade Nacional de Tratamento de Incidentes

Nenhum grupo 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 Grupos** 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

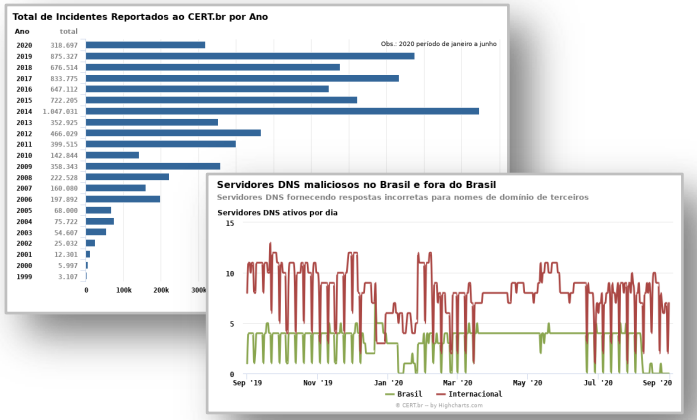
Tratamento de Incidentes
e
Análise de Tendências

cert.br nic.br cgi.br

Tratamento de Incidentes e Análise de Tendências: **Fontes dos Dados, Métricas e Compartilhamento**

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

- Volume em 2019: 4.086.406 de *e-mails* tratados, relativos a 875.327 incidentes notificados ao CERT.br



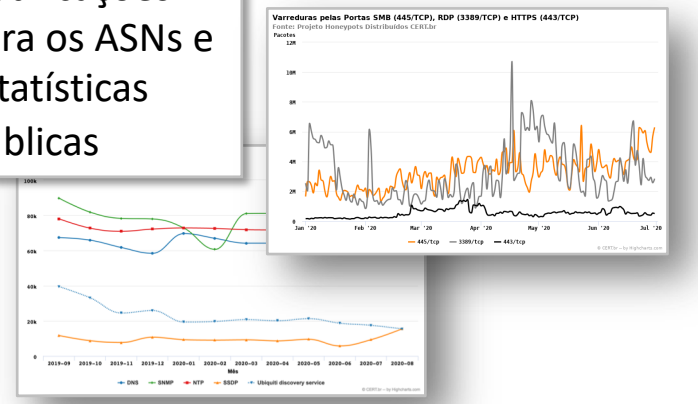
Compartilhamento via MISP

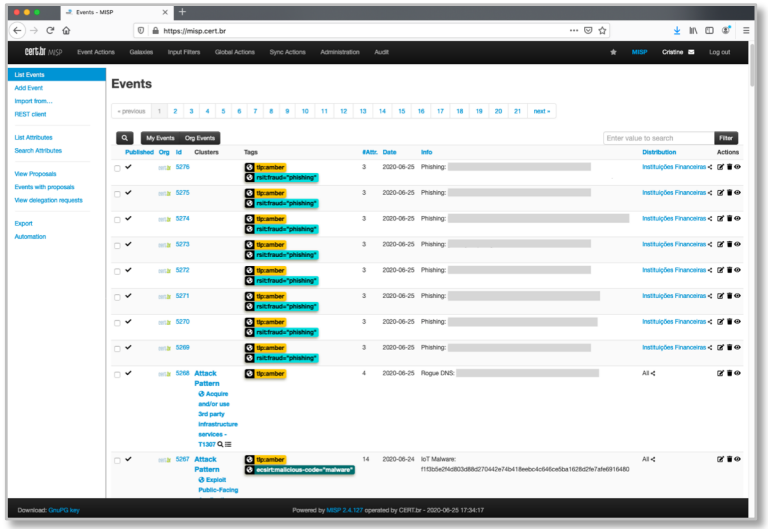
- Indicadores selecionados são compartilhados com parceiros
  - Servidores DNS maliciosos
  - *Phishing*
  - Binários e Comando e Controle de *botnets* IoT
  - Amplificadores usados em ataques DDoS

Threat feeds

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

Notificações para os ASNs e estatísticas públicas





https://cert.br/stats/

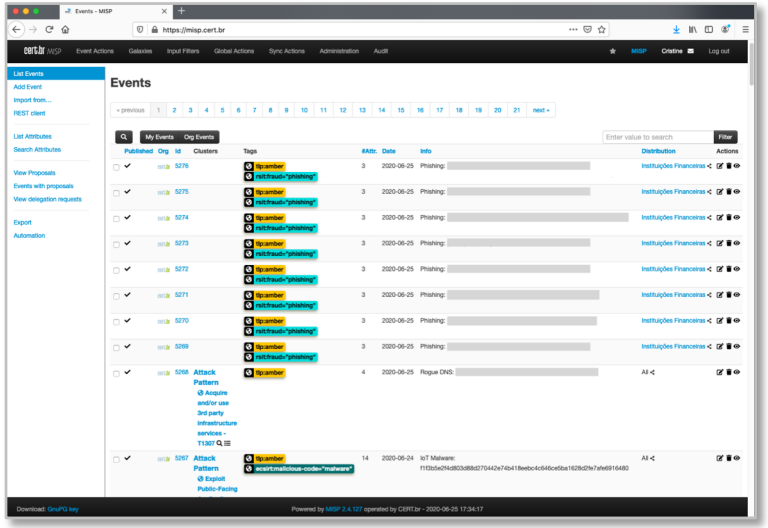
https://cert.br/misp/

Tratamento de Incidentes e Análise de Tendências: **Compartilhamento de Dados via MISP**

O que é o MISP

– uma plataforma de software livre para compartilhamento de dados de inteligência de ameaças, e

– um conjunto de padrões abertos para compartilhamento destas informações.



Atividades promovidas pelo CERT.br

– Impulsionando o uso por diversos setores
  – financeiro
  – energia
  – acadêmico
  – governo
  – operadores de redes

– Promovendo treinamentos
  – *Workshop* MISP, junto ao Fórum Brasileiro de CSIRTs
  – *Workshop* para o setor financeiro
  – Tutorial *online* disponibilizado na página do CERT.br

    https://cert.br/misp/

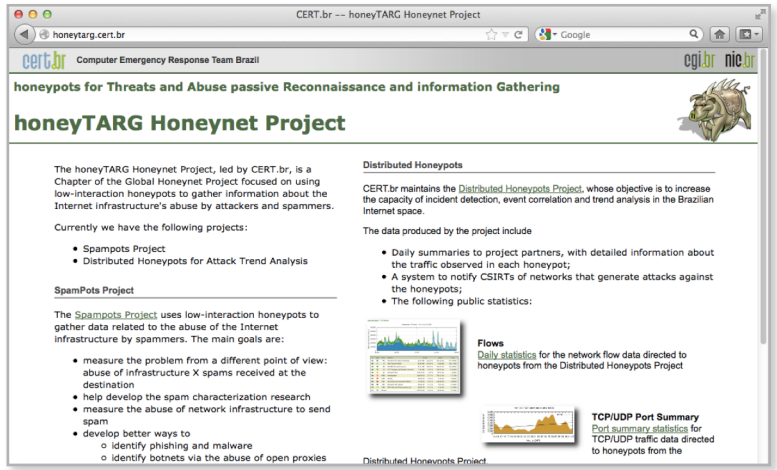
Análise de Tendências:
Projetos Envolvendo Sensores Próprios

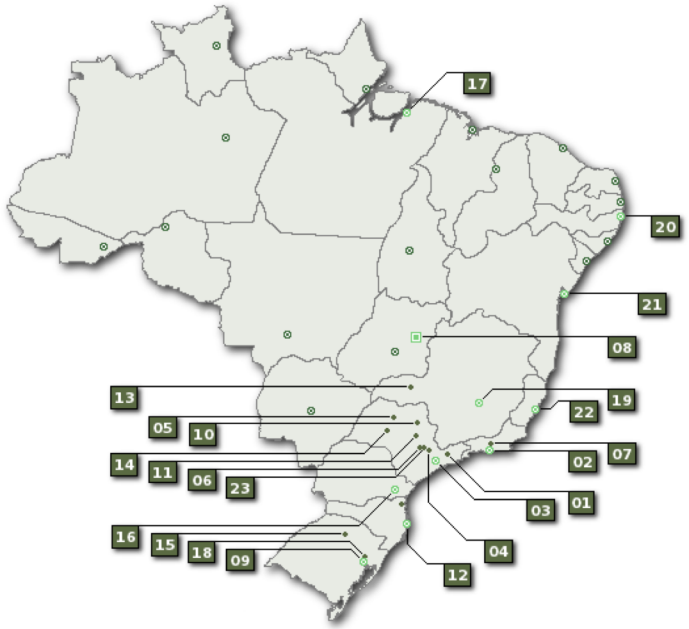
Objetivos

- Ter um “termômetro” das atividades maliciosas na Internet e manter estatísticas públicas sobre as tendências observadas
- Entender o abuso da infraestrutura da Internet por atacantes, *spammers* e fraudadores
- Propor técnicas para proteger os usuários e coibir o abuso
- Notificar *sites* brasileiros com problemas
- Compartilhar dados com parceiros internacionais

Projetos

- *Honeypots* Distribuídos
- *SpamPots*





The Honeynet Project honeyTARG Chapter

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

Cooperação Internacional:
Construção de Confiança

FIRST

Fórum existe desde 1992

- membro desde 2002

É uma Rede Global de CSIRTs

- fomenta a cooperação
- acesso a times e especialistas do mundo todo

Destaques da Participação:

- *Co-chair* do *Membership Committee* e do *Security Lounge SIG*
- *Chair* da Conferência 2020
- Coordenação de conteúdo do padrão *FIRST CSIRT Services Framework*
- Viabilização da parceria entre o FIRST e o LACNIC
  - CERT.br é *co-host* dos TCs e Simpósios na região

Rede de CSIRTs Nacionais

Existe desde 2006

Fórum para discussão de assuntos específicos para grupos de responsabilidade nacional

- CERT.br e CTIR Gov são membros

Maiores parceiros do CERT.br:

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

LAC-CSIRTs

Reunião de Grupos de Resposta a Incidentes de Segurança (CSIRTs) da região da América Latina e o Caribe – ocorre durante o LACNIC

LAC-AAWG – *Latin American and Caribbean Anti-Abuse Working Group – co-chair*

Iniciativa conjunta do:

- M³AAWG - *Messaging, Malware and Mobile Anti-Abuse Working Group*
- LACNOG - *Latin American and Caribbean Network Operators Group*

Principal resultado até o momento:

- BCOP *Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition*

Disponível em:

- Português, Inglês, Japonês e Coreano

www.m3aawg.org/CPESecurityBP-Portuguese
www.lacnog.net/docs/lac-bcop-1
www.m3aawg.org/CPESecurityBP

Treinamento e Conscientização

cert.br nic.br cgi.br

Público Técnico:
Capacitação em Tratamento de Incidentes

SEI Partner
Carnegie Mellon

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

Cursos de Gestão de Incidentes

Ministra os cursos do *CERT® Division, do SEI/Carnegie Mellon,* desde 2004:

- https://cert.br/cursos/
  - *Overview of Creating and Managing CSIRTs*
  - *Fundamentals of Incident Handling*
  - *Advanced Incident Handling for Technical Staff*
- 800+ profissionais treinados em tratamento de incidentes

Público Técnico:
Boas Práticas com Base nos Incidentes mais Prevalentes

Objetivo de fomentar a adoção de boas práticas de segurança por profissionais da área técnica:

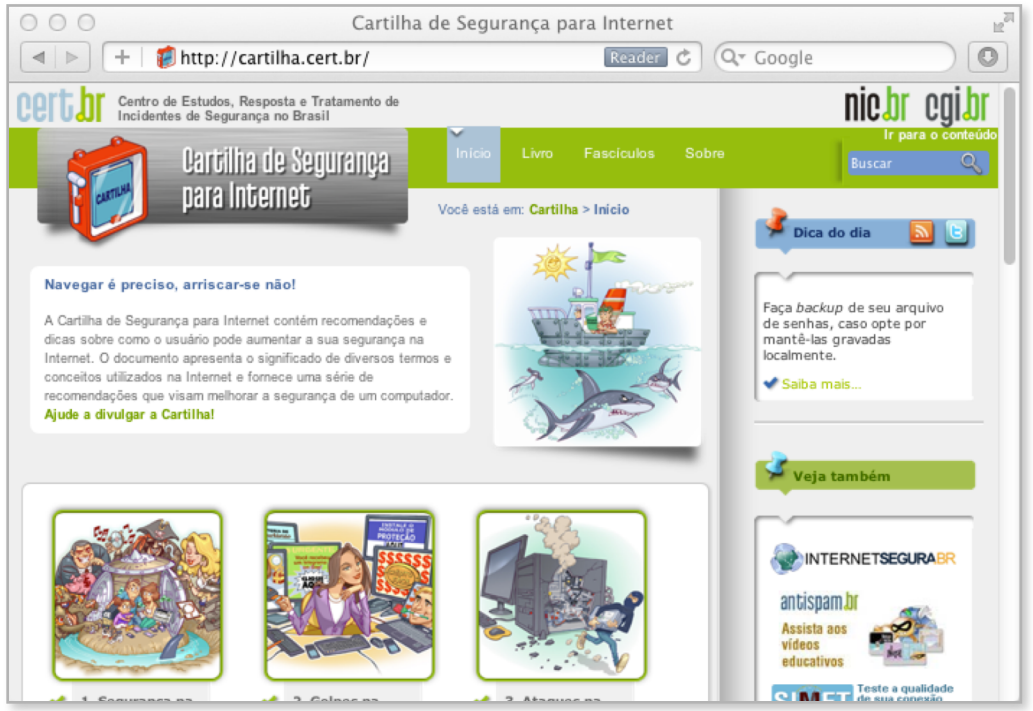
- Recomendações para Melhorar o Cenário de Ataques DDoS
  https://cert.br/docs/whitepapers/ddos/
- Recomendações para Notificações de Incidentes de Segurança
  https://cert.br/docs/whitepapers/notificacoes/
- Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos
  https://cert.br/docs/whitepapers/dns-recursivo-aberto/
- Práticas de Segurança para Administradores de Redes Internet
  https://cert.br/docs/seg-adm-redes/
- *Honeypots* e *Honeynets*: Definições e Aplicações
  https://cert.br/docs/whitepapers/honeypots-honeynets/
- Boas Práticas para Reduzir *Spam*
  https://antispam.br/admin/

Público em Geral:
Cartilha de Segurança para Internet

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

- Livro (PDF e ePub) e conteúdo no *site* (HTML5)
- Dica do dia no *site*, via *Twitter* e RSS
- Impressões em pequena escala enviadas a escolas e centros de inclusão digital
- Uso por instituições para treinar funcionários
- Nova versão está sendo finalizada

https://cartilha.cert.br/



Cartilha de Segurança para Internet: **Fascículos e *Slides***

Organizados de forma a facilitar a difusão de conteúdos específicos:

- Redes Sociais
- Senhas
- Comércio Eletrônico
- Privacidade
- Dispositivos Móveis
- *Internet Banking*
- Computadores
- Códigos Maliciosos
- Verificação em Duas Etapas
- Redes
- *Backup*
- Boatos

Acompanhados de *slides* de uso livre para:

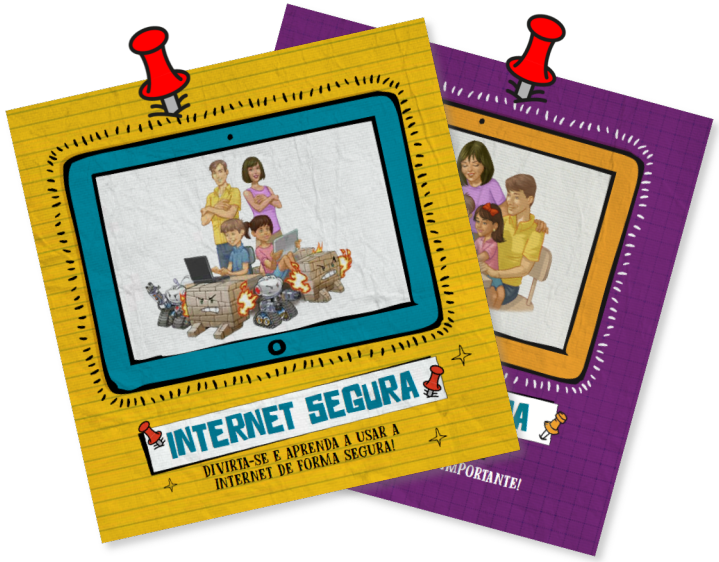
- ministrar palestras e treinamentos
- complementar conteúdos de aulas

Materiais para Crianças:
Guia com Dicas e Desafios + Personagens de Montar

Guias Internet Segura

- Disponível Gratuitamente
- Parcerias com Escolas e outras Instituições
- Material de apoio para pais

https://internetsegura.br/



Personagens para montar

Monte os bonecos de papel tridimensionais da turma do bem e da turma do mal e crie suas próprias histórias! É só baixar os arquivos, imprimir e começar a brincar!

Antivírus: ajuda a turma do bem a detectar, anular e eliminar vírus e outros tipos de códigos maliciosos do computador.

Autenticação: o segurança da turma. Confirma se quem está ali é mesmo o dono do dispositivo. Pede senhas e outros códigos de verificação, checa tudo antes de liberar a entrada.

Backup: salva todas as informações do seu computador em outro dispositivo e não perde nada.

Firewall: é o dispositivo de segurança usado para dividir e controlar o acesso entre redes de computadores.

Spyware: espião da turma. Observa o que você faz no

Trojan: também chamado de Cavalo de Tróia. Além de

Vírus: espalha-se pela rede inserindo cópias dele

Zumbi: esse é o nome do computador que foi

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