nic.br cgi.br | cert.br

# Workshop MISP - Dia 1
## CERT.br, ABBC e Anbima

03 de agosto de 2021– Evento *Online*

# MISP: Instalação e *Hardening*

**Marcus Vinícius Lahr Giraldi**
**Analista de Projetos de Segurança**
**marcus@cert.br**

cert.br nic.br cgi.br

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
- 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/

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

TLP:WHITE

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

- 2020: 2.017.263 de *e-mails* tratados, relativos a 665.079 incidentes notificados ao CERT.br

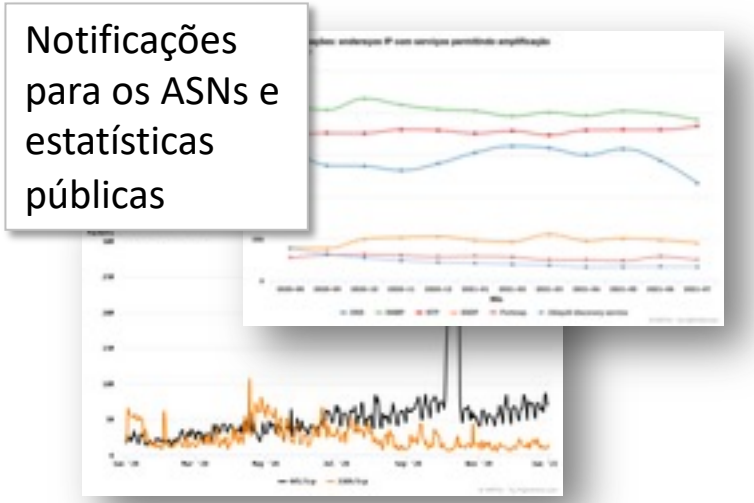
Compartilhamento via MISP

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

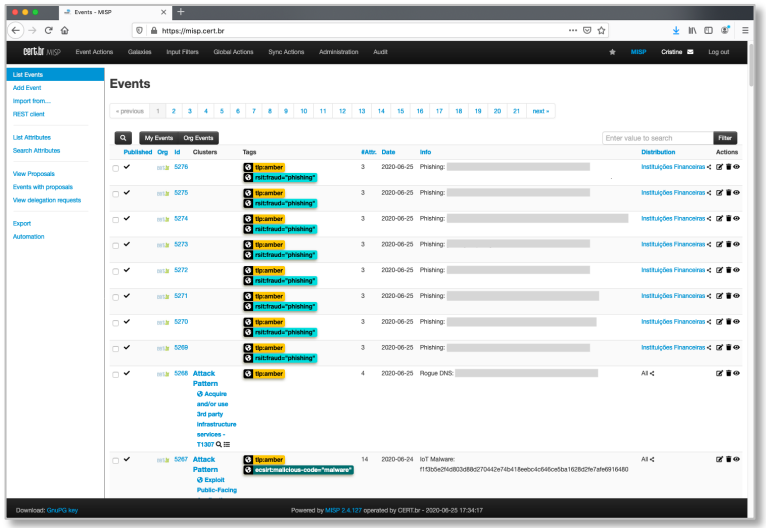
*Threat feeds*

- *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/

# Considerações de Segurança

cert.br nic.br cgi.br

# Considerações de Segurança

Este tutorial é focado na instalação de um servidor MISP com um *hardening* básico e configurações de segurança, incluindo:

– ***Firewall*** de *host* permitindo entrada da **rede de gerência** e de instâncias de parceiros, e permitindo saída para a Internet;

– Acesso via **SSH somente com chave criptográfica**, para minimizar o sucesso de ataques de força bruta de senhas;

– **Atualização do sistema** e configuração para recebimento de **alertas relativos a atualizações disponíveis**;

– Criação de **senhas fortes** para o MISP e o Banco de Dados.

# Não Utilizar Imagens Baixadas da Internet para Instâncias em Produção

TLP:WHITE

Existem diversas imagens virtuais disponíveis na Internet com instâncias MISP prontas para utilizar. Porém, estas imagens devem ser utilizadas somente para testes e para aprender a tecnologia.

Ao colocar uma instância em produção há diversos problemas na utilização destas imagens prontas da Internet:

– Não é possível **garantir que a imagem não possua** nenhum tipo de **Cavalo de Troia**;

– As imagens podem ter **vulnerabilidades** que não sejam fáceis de identificar;

– Pode **não ser possível recuperar as senhas** criadas no Banco de Dados e na instância MISP;

– Podem haver personalizações ou configurações feitas nas imagens, que podem **atrapalhar processos futuros de atualização** do sistema e do MISP.

# Cuidados com o Certificado Digital

O objetivo do MISP é ser utilizado para conectar em instâncias de parceiros para compartilhar informações relacionadas com segurança.

É imprescindível que a instância MISP implemente boas práticas no uso do certificado digital:

- **Usar sempre um certificado válido**, neste tutorial usaremos certificados Let's Encrypt;
- **Não utilizar certificados auto assinados**;
- **Nunca desligar a checagem de certificados** para aceitar certificados auto-assinados de outras instâncias MISP;
- Se a sua Autoridade Certificadora (AC) tiver suporte, configurar o sistema para **atualizar o certificado automaticamente**
  - ***Firewalls*** de *host* e corporativo **devem permitir entrada de conexões vindas da AC** na porta 80/TCP.

# Cuidados com *Firewall,* WAF e Anti-DDoS Corporativos

A instância MISP precisa ser mantida atualizada e potencialmente terá em seus eventos *payloads* maliciosos (*malware*, URLs de *phishing* e IoCs variados).

É imprescindível que:

– A **instância MISP possa acessar a Internet**, principalmente os servidores de **atualização do sistema** e as **atualizações do MISP** (GitHub);

– O **WAF** corporativo ou *proxy* reverso (se houver) **não interfira** no tráfego do MISP;

– Ferramentas **Anti-DDoS não devem classificar acessos de instâncias parceiras** como ataques (por exemplo, classificar muitos SYNs como DDoS).

# Agenda

cert.br nic.br cgi.br

# Agenda

- **Instalação e *Hardening* Básicos**
  - *Firewall*, acesso via chaves, sincronia de tempo e atualizações
- **Instalação do MariaDB, Apache e outras dependências do MISP, incluindo**
  - Criação e configuração do certificado digital
- **Instalação do MISP, incluindo**
  - CakePHP
  - Banco de dados do MISP
  - Configurações do site e rotação de *logs*
- **Configuração do MISP, incluindo**
  - Criação dos arquivos de configuração e definição das credenciais de acesso
  - Definição das configurações iniciais

# *Hands On*

**https://cert.br/misp/**
**https://cert.br/misp/tutorial-ubuntu/**

**Lista de Discussão:**
**https://listas.cert.br/mailman/listinfo/misp-br**

cert.br nic.br cgi.br

# Obrigado

marcus@cert.br

Notificações para: cert@cert.br

@certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br