

Boas Práticas para Mitigação de Spams e de Fraudes via E-mail

Klaus Steding-Jessen
jessen@cert.br

Centro de Estudos, Resposta e Tratamento
de Incidentes de Segurança no Brasil – CERT.br

<http://www.cert.br/>
cert@cert.br

Comitê Gestor da Internet no Brasil – CGI.br

<http://www.cgi.br/>

Roteiro

- Motivação
- Formas de mitigação
- Educação dos usuários
 - site antispam.br
- Referências

Motivação

- número grande de spams circulando na Internet
- abuso dos computadores de usuários finais
 - instalação de bots, utilizados para DDoS e envio de spam
 - utilização de proxies abertos para anonimato
- e-mail como vetor de propagação de vírus/worms
- spam como meio para a prática de fraudes
- bloqueio de spam apenas no destino não é ideal
 - consumo de banda, disco, processamento
 - contínuo esforço de configuração e de implantação de novas tecnologias

Dificultando o Abuso de Sua Rede

Spammers, bots, worms e vírus usam o envio direto de e-mails de um cliente para um MTA destino para se propagar.

- fechar *proxies* e *relays* abertos
- impedir o envio direto de e-mail a partir de estações clientes
 - bloquear a porta 25/TCP para conexões de saída
 - utilizar a porta 587/TCP (*mail submission port*)
- implementar SMTP autenticado

Combatendo a Falsificação de E-mails

Fraudadores e códigos maliciosos costumam forjar os remetentes das mensagens.

- DKIM (*Domain Keys Identified Mail*)
 - técnica que permite checar o **cabeçalho** de uma mensagem (campo `From:`)
 - consiste em assinar as mensagens para garantir a autenticidade do remetente
- SPF (*Sender Policy Framework*)
 - técnica que permite checar o campo `MAIL FROM` do **envelope** de uma mensagem

SPF

- permite anunciar quais servidores podem enviar e-mail em nome de um domínio
 - anúncio feito via registro TXT do DNS

```
example.com.      IN      TXT      "v=spf1 a mx ip4:192.0.2.32/27 -all"
```

- permite checar se um e-mail foi enviado a partir de um servidor autorizado
- o anúncio e a checagem são operações independentes
- diversas redes já estão utilizando SPF

SPF (cont)

```
planalto.gov.br.          3600      IN        TXT       "v=spf1 ip4:200.181.15.0/24
ip4:200.198.192.192/27 ~all"

stj.gov.br.              10800     IN        TXT       "v=spf1 mx -all"

ctir.gov.br.            86400     IN        TXT       "v=spf1 mx -all"

caixa.gov.br.           3600      IN        TXT       "v=spf1 mx a:200.201.164.40
a:200.201.164.41 a:200.201.164.42 a:200.201.164.43 mx:200.201.166.143
mx:200.201.166.204 ~all"

cert.br.                 86400     IN        TXT       "v=spf1 mx a:listas.cert.br
-all"

uol.com.br.             2108      IN        TXT       "v=spf1 ip4:200.221.11.0/24
ip4:200.221.29.0/24 ip4:200.221.4.0/24 -all"

terra.com.br.           6159      IN        TXT       "v=spf1 ip4:200.154.55.0/24
ip4:200.176.2.0/23 ip4:200.176.10.0/23 include:tmp-spf.terra.com.br
include:ti-spf.terra.com.br include:te-spf.terra.com.br -all"
```

Acompanhamento de notificações de abuso

- criar emails da RFC 2142 (security@, abuse@)
- manter os contatos de Whois atualizados
- o contato técnico do domínio deve ser um profissional que tenha contato com as equipes de abuso
- redes com grupos de resposta a incidentes de segurança devem anunciar o endereço do grupo junto à comunidade
- os endereços de contato não podem ter as mesmas regras anti-spam que o resto da organização

Educação dos Usuários

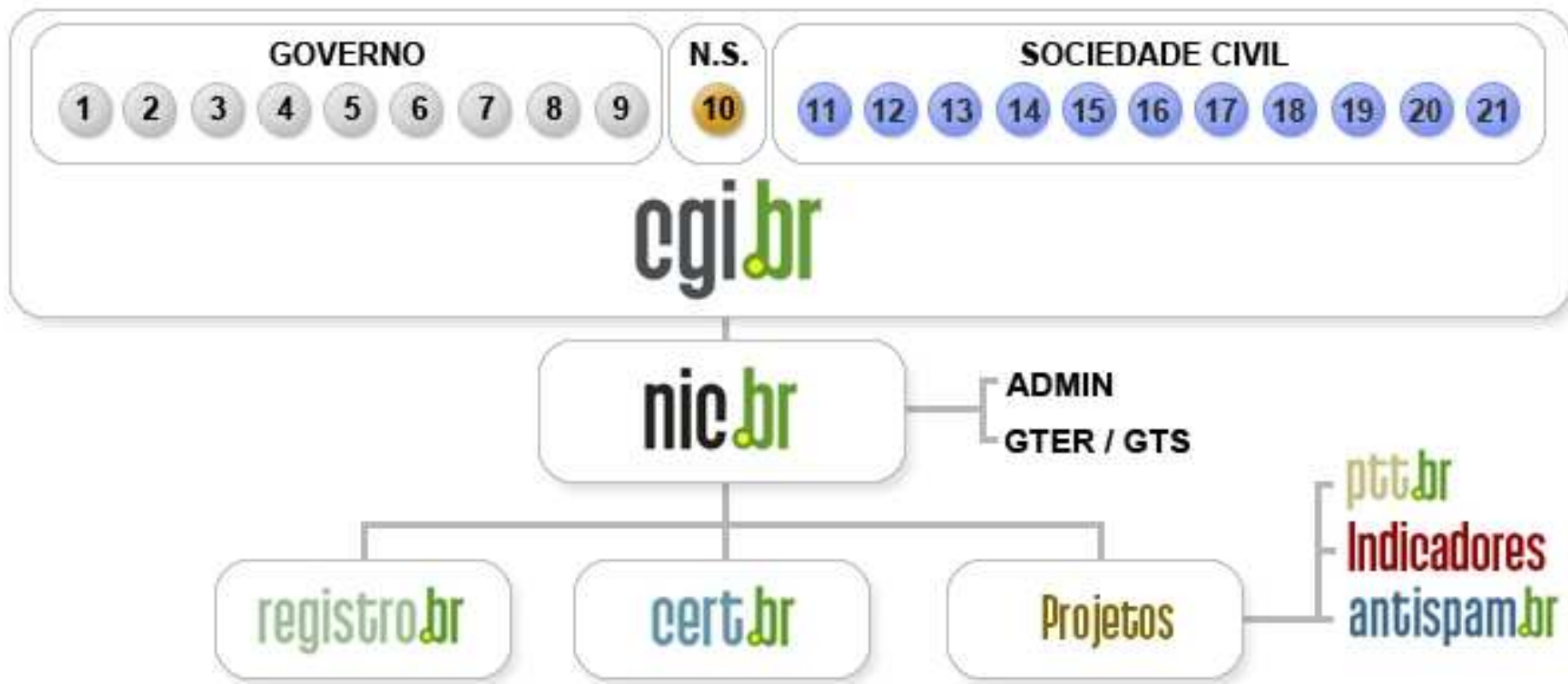
Antispam.br

- iniciativa da Comissão de Trabalho Anti-Spam do CGI.br

<http://www.cgi.br/sobre-cg/antispam.htm>

- objetiva informar o usuário e o administrador de redes sobre o combate ao spam, suas implicações e formas de proteção

CGI.br e o Antispam.br



http://www.antispam.br/

Antispam.br :: - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.antispam.br/

Comitê Gestor da Internet no Brasil

Sobre o NIC.br | Indicadores | **Antispam.br** | PTT.br

Inicio - Administradores de redes - Estatísticas - Sobre o Antispam.br - Mapa do site

antispam.br

- O que é spam?
- Problemas causados pelo spam
- Origem e curiosidades
- Tipos de spam
- Como identificar
- Prevenção
- Boas práticas
- Dicas
- Como reclamar
- FAQ
- Links
- Glossário
- Créditos

O que é spam?

Veja os conceitos de spam e de spam *zombies* - que podem fazer com que você envie spam mesmo sem saber. Conheça também as motivações que levam tantas pessoas a enviar e-mails não solicitados.

Participe da campanha

Divulgue esta iniciativa para estimular o uso cada vez mais saudável, correto e seguro das redes ligadas à internet.

Como identificar

O que você precisa saber para detectar spams. Saiba quais são as técnicas que estão sendo usadas para fazer o spam chegar em sua caixa de correio.

Dicas de prevenção

Como se prevenir dos spams, que lotam as caixas de e-mails, demandam precioso tempo e atrapalham a evolução dos negócios.

Não deixe seu computador se tornar um spam zombie

Se você não é cuidadoso ao usar a internet e, entre outros procedimentos, não usa antivírus e não possui um firewall pessoal, você está correndo sério risco. Saiba o porquê.

Participe da campanha

cert.br
Cartilha de Segurança para Internet

nic.br
Indicadores

registro.br

cgi.br
Comitê Gestor da Internet no Brasil

nic.br
Núcleo de Informação e Coordenação

registro.br
Registro de Domínios para a Internet no Brasil

cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes

Valido XHTML - CSS

Antispam.br (cont)

Material de apoio para a educação dos usuários:

- tipos de spam e como identificá-los
- fraudes e sua prevenção
- boas práticas e dicas para proteção
- origem e curiosidades
- links para ferramentas e outros documentos

http://www.antispam.br/admin/

Antispam.br :: - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.antispam.br/admin/

Comitê Gestor da Internet no Brasil

Sobre o NIC.br | Indicadores | **Antispam.br** | PTT.br

nic.br
Núcleo de Informação e Coordenação

cgj.br | Registro CERT.br

Início - **Administradores de redes** - Estatísticas - Sobre o Antispam.br - Mapa do site

antispam.br
Administradores

Estrutura da Mensagem

Funcionamento do Correio Eletrônico

Técnicas de Envio de Spam

Listas de Bloqueio

Filtros de Conteúdo

Greylisting

SPF

DKIM

Configuração de Serviços

E-mails especiais e dados de WHOIS

Links

Busca

ok

NIC.br Antispam.br

CERT.br Registro.br

Administradores de redes

Conceitos Fundamentais

Para melhor se proteger e aplicar as técnicas propostas, reunimos informações sobre alguns conceitos fundamentais:

A Estrutura da Mensagem
O Funcionamento do Correio Eletrônico
Algumas Técnicas de Envio de Spam que devem ser combatidas

Boas Práticas de Configuração para Evitar o Abuso de sua Rede

Para reduzir efetivamente o número de spams recebidos é necessário que cada rede faça sua parte para evitar que seja origem de spam. Aqui estão reunidas diversas recomendações para ajudá-lo a fazer a sua parte:

Recomendações para Configuração de Serviços:
Correio Eletrônico
Servidores Web
Servidores de Nomes
Serviços de Proxy
Firewalls
E-mails especiais e dados de WHOIS

Técnicas para Redução do SPAM recebido

Existem algumas técnicas que podem usadas para identificar spams e reduzir o número de mensagens que chegam às caixas postais:

Listas de Bloqueio
Filtros de Conteúdo
Greylisting

Técnicas para Combater a Falsificação de Endereços

Para evitar que spammers enviem emails em nome de terceiros e permitir uma melhor identificação da origem de uma mensagem, algumas técnicas podem ser implementadas:

SPF
DKIM

CC
ALGUNS DIREITOS RESERVADOS
Válida XHTML - CSS

Referências

- Esta Palestra
<http://www.cert.br/docs/palestras/>
- Antispam.br
<http://www.antispam.br/>
- Comitê Gestor da Internet no Brasil
<http://www.cgi.br/>
- CERT.br
<http://www.cert.br/>
- Cartilha de Segurança para Internet
<http://cartilha.cert.br/>