# *Implementando Políticas ANTI-SPAM*

Émerson Virti

emerson@tche.br

## *Resumo*

- Motivação - Problemática do Spam
- Os Remetentes
- Formas de Controle de Spam
- Controlando Spam no POP-RS
- Conclusões

## *Problemática do Spam*

- Crescente número de spans circulando na Internet
  - Até março deste ano, cerca de 86% de todos os e-mails trocados na Internet são SPAMS

(fonte: Eletronic Commerce in Canada)
http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/Intro

- Porcentagem de tráfego desnecessário
  - Bloqueio de spam apenas no destino
    - Consumo de recursos
      - Processamento
      - Disco

## *Os Remetentes*

- Vírus/Worms
- Garantia de anonimato:
  - Open Proxy
  - Open Relay

## *Formas de Controle de Spam*

- Filtragens antes do armazenamento do mail
  - DNS
  - SPF
  - RBL
  - Blacklists Pessoais
  - lists
- Filtragens depois do armazenamento do mail
  - Antivírus
  - Detector de spam

## *Formas de Controle de Spam*

- DNS – Domain Name System
  - Aceitar mails apenas de hosts com reverso?
    - Vantagens:
      - Eliminar os spans enviados de hosts sem reverso: tipicamente, computadores que fazem transporte confiável de mails, têm reverso.
    - Desvantagens:
      - Dependendo da clientela, pode impedir que usuários confiáveis consigam enviar mails.

## *Formas de Controle de Spam*

- SPF – Sender Policy Framework
  - Divulgação através do DNS
  - Evita o envio de mails com o remetente adulterado
    - Mails com o domínio “instituição.tche.br” só podem ser enviados da rede X.X.X.X.

*Formas de Controle de Spam*

- SPF – Sender Policy Framework
  - Problema:
    - Transporte para outros domínios;
    - Diferença entre “MAIL FROM:” do protocolo e “From:” do cabeçalho.

## *Formas de Controle de Spam*

- SPF – exemplo (comandos executados em um host da rede tche)
  - telnet smtp.tche.br 25

    Trying 200.19.246.66...

    Connected to smtp.tche.br.

    Escape character is '^]'.

    220 urano.pop-rs.rnp.br ESMTP Postfix

    **HELO reuniao.rede.tche**

    250 urano.pop-rs.rnp.br

    **MAIL FROM: emerson@terra.com.br**

    250 Ok

    **RCPT TO: emerson@tche.br**

    554 <emerson@tche.br>: Recipient address rejected: Please see http://spf.pobox.com/why.html?sender=emerson%40terra.com.br&ip=200.132.0.68&receiver=urano.pop-rs.rnp.br

## *Formas de Controle de Spam*

- RBL – Real Time Spam Blacklists
  - Listas atualizadas constantemente que contêm os IPs dos hosts acusados de estarem enviando spans
    - Desvantagens
      - É preciso confiar na RBL
      - Um host da sua rede, pode estar listado

## *Formas de Controle de Spam*

- Blacklists Pessoais
  - Forma de evitar que hosts conhecidos como divulgadores de spans possam enviar mails a partir do servidor
    - Desvantagem:
      - Necessita constante atualização

## *Formas de Controle de Spam*

- Forma de filtro de mails onde existe um banco de dados de IPs e envelopes que é conferido a cada nova mensagem.
  - Caso o IP e o envelope já estejam no banco de dados – mensagem aceita
  - Caso o IP e o envelope não estejam no banco de dados – mensagem recusada por erro temporário e cadastro da mensagem é realizado
    - Presunção de que a origem irá retransmitir o mail

## *Formas de Controle de Spam*

- Anti-vírus
  - Controle de Vírus e Worms
  - Necessidade de atualização
  - Não enviar mensagens aos remetentes

## *Formas de Controle de Spam*

- Detector de Spam
  - Parte final da filtragem
  - Exige mais processamento
  - Necessidade de aprendizagem

## *Controlando Spam no POP-RS*

- Postfix – SMTP
  - Controle com DNS
  - Controle com SPF
  - Controle com RBL
- Amavis
  - Clamav – antivírus
- Dspam – detector de spam

## *Controlando Spam no POP-RS*

- Postfix – SMTP
  - Controle com DNS
  - Controle com SPF
  - Controle com RBL
  - Parâmetros de controle de autenticação
    - Autenticar por usuário
    - Autenticar por IP

## *Controlando Spam no POP-RS*

- Amavis
  - Faz a comunicação entre o Postfix (SMTP) e o antivírus – Clamav
  - Possibilita a implementação de outro detector de spam – Spamassassin (perl)

- Clamav – antivírus
  - Escrito em C
  - Boa performance

## *Controlando Spam no POP-RS*

- Dspam – detector de spam
  - Etapa que exige mais processamento
  - Possibilidade de armazenamento de informações por mysql
  - Necessidade de treinamento inicial
  - Treinamento pode ser feito pelos usuários através do envio de mails HAM ou SPAM para um endereço definido pelo administrador
  - Possibilidade de uma base para cada usuário
  - Desvantagem: não pode ser criado whitelists

## *Controlando Spam no POP-RS*

dspam

Go Ahead | Send me Viagra

## *Controlando Spam no POP-RS*

- Estatísticas de 13/07/05
  - Mails que passaram pelos servidores: 48.814
  - Mails rejeitados na postagem: 32.430
  - Mails contendo vírus/worms: 72
  - Mails detectados como spam: 1.475
  - Mails considerados não-spam: 14.837
  - Mails enviados: 16.312

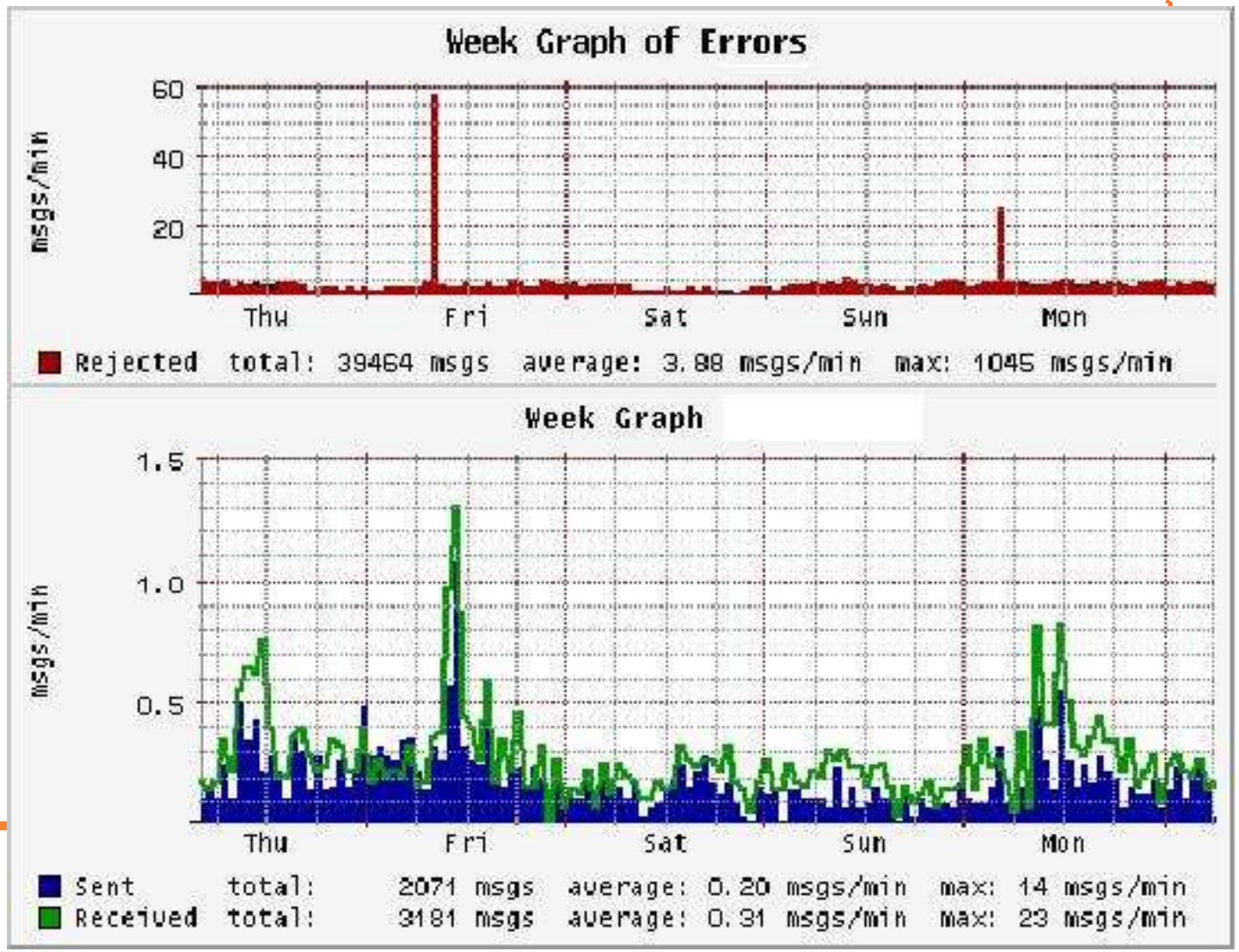
## *Conclusões e Recomendações*

- Utopia: bloquear spams na origem
  - Vírus/worms
  - Usuários mal intencionados
- Política de envio de mensagens que esteja de acordo com as necessidades dos usuários

## *Conclusões e Recomendações*

- Necessidade de poupar processamento detectando spam antes do armazenamento em fila

## *Conclusões e Recomendações*



***Perguntas?***

emerson@tche.br