Tecnologias e Políticas para Combate ao Spam

Cristine Hoepers

Klaus Steding-Jessen

Rubens Kühl Jr.

CT-Spam – Comissão de Trabalho sobre Spam do
Comitê Gestor da Internet no Brasil

http://www.cgi.br/

Roteiro

- Motivações
- Recomendações do documento “Tecnologias e Políticas para Combate ao Spam”

Motivações

- número grande de spams circulando na Internet
- crescente inclusão de redes brasileiras em listas de bloqueio
- bloqueio de spam apenas no destino não é ideal
  - consumo de banda, disco, processamento
  - contínuo esforço de configuração e de implantação de novas tecnologias

Motivações (cont)

- abuso dos computadores de usuários finais
  - instalação de bots, utilizados para DDoS e envio de spam
  - utilização de proxies abertos para anonimato
- vetor de progagação de vírus/worms
- spam como meio para a prática de fraudes
  - envio com entrega direta
  - usando proxies abertos

Recomendações para Operadoras de Telecomunicações

Fechar proxies abertos

problema: abuso da conexão de maneira anônima

recomendações:

- filtragem de portas típicas de proxy;
- varreduras proativas;
- monitoração proativa de fluxos;
- monitoração das notificações de abusos;
- ação efetiva junto ao usuário nos casos de detecção de proxy aberto ou máquina comprometida

Impedir envio direto de mensagens

problema: entrega direta é normalmente utilizada por spammers/vírus/worms e fraudes

recomendações:

- eliminar a conexão direta de clientes domésticos a servidores SMTP, na porta 25
- uso da porta 587 (*mail submission port*), com autenticação

Recomendações para Provedores de Email

Implementar SMTP autenticado

problema: spammers/vírus/worms podem enviar emails sem autenticação, usando máquinas comprometidas

recomendações:

- uso de autenticação para envio de mensagens (SMTP AUTH)
- usuários instruídos a usar port 587 (*mail submission port*)

Limitar a vazão de envio de emails

problema: softwares de bulk mailing, usados por spammers, enviam um número altíssimo de emails

recomendações:

- limitar a vazão de envio de emails nos servidores SMTP
- manter uma contagem do número total de destinatários, de um mesmo remetente, por unidade de tempo

Corrigir relays abertos

problema: máquinas com relays mal configurados podem ser utilizadas por terceiros para o envio de spam

recomendações:

- servidores SMTP dever ser configurados corretamente e testados de modo a assegurar que não estejam atuando como relays abertos

Restringir a criação automática de contas

problema: spammers utilizam-se de mecanismos automatizados para criação de contas de emails

recomendações:

- implementar métodos para impedir a criação automática, como testes para assegurar que o criador da conta é uma pessoa
- provedores pagos podem exigir algum tipo de comprovação de pagamento

Combate à falsificação de emails

problema: spammers/vírus/worms enviam mensagens com remetentes falsos

recomendações:

- adoção de técnicas que permitam a validação, por outros servidores de correio, das mensagens enviadas
  - SPF
  - DomainKeys

Recomendações Gerais

Acompanhamento de notificações de abuso

problema: nem sempre as notificações de abuso são recebidas/lidas

recomendações:

- 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

Implementar políticas

problema: muitas redes possuem clientes que oferecem serviços de envio em massa de spams ou hospedagem de páginas referenciadas em spams

recomendações:

- todas as redes devem possuir políticas de uso aceitável que prevejam como uso abusivo de recursos tanto o envio de spam como a hospedagem de páginas referenciadas em spams