Quando o Spam se torna um Incidente de Segurança

Rede Nacional de Ensino e Pesquisa - RNP
Centro de Atendimento a Incidentes de Segurança - CAIS
Novembro de 2003

RNP/PAL/0201

CAIS

Sumário

Quando o Spam se torna um Incidente de Segurança

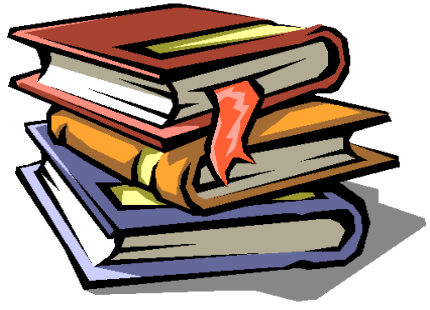
Introdução

- O que é Spam?
- Estatísticas alarmantes
- Spam como veículo para fraudes, golpes e proliferação de vírus e outros malware
- Spam como negócio!
- Impactos do spam:
  - Prejuízos: recursos, produtividade, etc
  - Segurança
  - Viabilidade do uso do e-mail!

CAIS

Spam: um pouco de história

- O primeiro spam segundo o LADO A da História
- No dia 12 de Abril de 1994, dois advogados, Canter e Siegel, postaram uma mensagem em todos os grupos da USENET, fazendo propaganda de uma loteria de “green cards” para imigrantes nos Estados Unidos.
- O primeiro spam segundo o LADO B da História
- No dia 3 de Maio de 1978, um profissional de marketing da DEC, enviou um anúncio de novos modelos do computador DEC-20. Este fato foi caracterizado como spam apenas 15 anos mais tarde.



CAIS

A Evolução do Spam

- O Spam não só cresceu, mas amadureceu!
- Nos primórdios: correntes, boatos e propagandas.
- Evolução: spam como veículo de propagação de fraudes e golpes, disseminação de vírus e outros malware.
- Aumento do volume de e-mails de spam.
  - Brightmail: 50% dos e-mails são spam (Julho/2003)
  - Gartner: 60% dos e-mails serão spam em meados de 2004
  - FTC: 65% do spam que circula pela web traz conteúdo e ofertas falsas.

CAIS

A Evolução do Spam

- 2002: o ano do Spam
- 2003: o ano das Fraudes. O Spam se consolida como ameaça:
  - comprometendo a **segurança** das redes (vírus e malware)
  - causando **prejuízos** financeiros (fraudes, uso indevido e consumo de recursos computacionais, perda de tempo dos funcionários, etc)
  - causando **danos morais** e afetando a **imagem** de empresas e pessoas físicas (golpes);

O Spam como Incidente de Segurança

- O que é um **incidente de segurança**?

  ... de acordo com o CERT/CC e tradução do NBSO:

- "*Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores*"

- "*O ato de violar uma política de segurança, explícita ou implícita*."

- *"Uma atividade nas máquinas ou na rede que possa ameaçar a segurança dos sistemas computacionais."*

O Spam como Incidente de Segurança

- Quando o Spam se torna um incidente de segurança?
  - Fraudes
  - Golpes
  - Propagação de vírus e outros tipos de *malware*
  - Problemas de configuração: *open relays* e *open proxies*
  - Ameaças
  - Pedofilia
  - *Mailbombing*
  - Uso de sistemas comprometidos, invadidos ou contaminados, para o envio de spam.

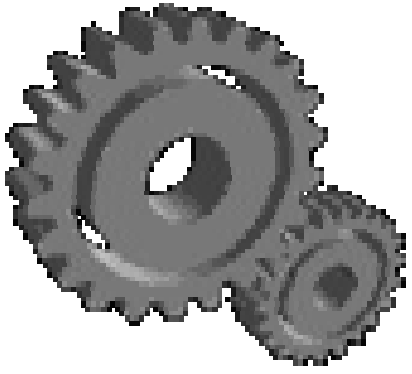
O Spam como Incidente de Segurança

- **Fraudes** (*Frauds*)
  - Páginas falsas e Sites clonados de bancos
  - Instalação de falsos *patches*
- **Golpes** (*Scams*)
  - Big Brother Brasil 4
  - Raspadinha
  - Segredinho
  - Golpes da Nigéria (Nigerian Scams)
  - FTC: "*The Dirty Dozen*" !

CAIS

O Spam como Incidente de Segurança

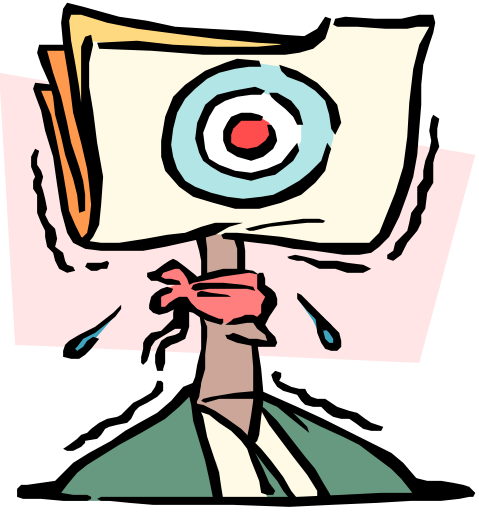
- **Vírus, worms, malware em geral**
  - Utilizam o spam como vetor de propagação
  - Utilizam as máquinas infectadas como base para o envio de spam.
- **Problemas de Configuração**
  - *Open Relays*
  - *Open Proxies*



CAIS

O Spam como Incidente de Segurança

- **Ameaças pessoais**
  - Ex-namorados, ex-esposos, etc
  - Casos de rixas pessoais.
- **Ameaças Institucionais, etc...**
  - Ex-funcionários
  - Funcionários atuais e insatisfeitos!
  - Funcionários atuais, tentando prejudicar colegas, etc.
- **Pedofilia**
  - Spams com conteúdo pornográfico ou pedófilo.



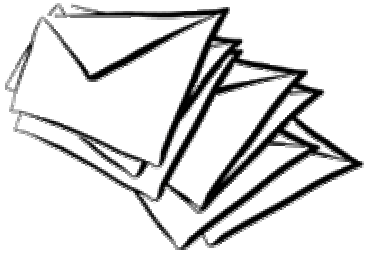
CAIS

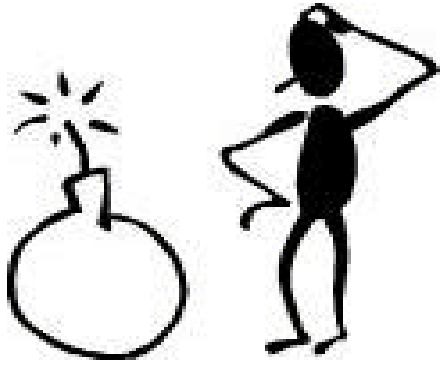
O Spam como Incidente de Segurança

- ***Mailbombing***

  - **Ataques de brute force**, através de programas capazes de enviar um grande volume de e-mails, com campos forjados e usando dicionários de contas padrões (suporte, compras, marketing, etc) e contas com nomes comuns.

  - **Ataques "reflexos"**, quando o spammer envia e-mails forjados com o endereços de determinado domínio. As mensagens de erro e muitas das reclamações são enviadas para o domínio em questão, que se torna vítima de mailbombing, além de já ter sido vítima de impersonificação.

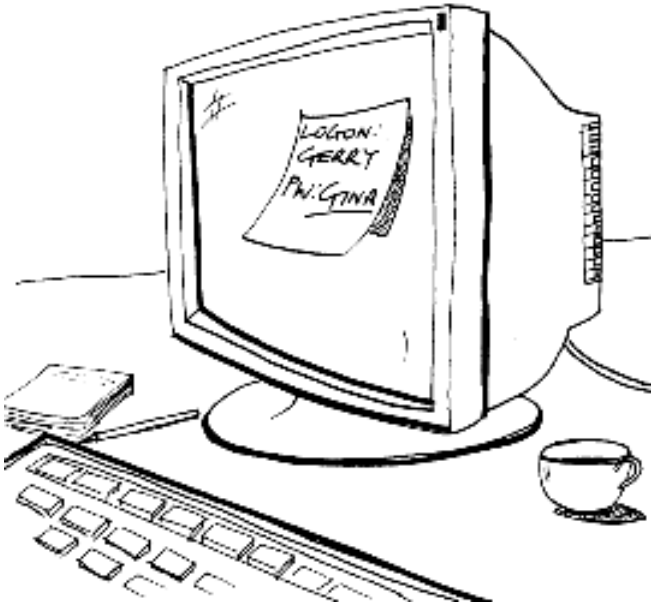




CAIS

O Spam como Incidente de Segurança

- **Uso de sistemas comprometidos para o envio de spam**
- **Sistemas invadidos**
  - Exploração de vulnerabilidades
  - Violações de segurança: senhas, etc.
- **Sistemas contaminados**
  - Vírus de nova geração
  - *Worms*
  - Códigos maliciosos híbridos
  - *Keyloggers*, *screenloggers*, *trojans*



CAIS

Tratamento de Incidentes de Segurança relacionados a Spam

- Reclamar aos contatos técnicos (Whois) e grupos de segurança responsáveis.
- Implementar, acompanhar e responder aos e-mails das contas abuse@ e postmaster@ (RFC 2142).
- Fraudes e golpes: denunciar aos grupos de segurança ou serviços de suporte das Instituições e empresas envolvidas. Envolver a Polícia Federal .
- Vírus e *Malware*: se for possível identificar a máquina infectada com segurança, notificar o referido administrador. Configurar adequadamente os anti-vírus: respostas automáticas, atualizações, etc.

Tratamento de Incidentes de Segurança relacionados a Spam

- Problemas de configuração: solicitar correção imediata.
- Ameaças: boletim de ocorrência, calúnia e difamação, etc.
- Pedofilia: casos de spam envolvendo pedofilia devem ser encaminhados a Polícia Federal.
- *Mailbombing*: difícil contenção. Uma das alternativas é filtrar.
- Máquinas invadidas: solicitar imediata ação dos responsáveis, isolando a máquina da rede até recuperá-la com segurança.

Em tratamento de incidentes de segurança, a resposta é muito importante! Não se esqueça de responder ao reclamante, copiando os grupos de segurança envolvidos!

CAIS

A Atuação dos CSIRTs

- Conscientizar e educar usuários e administradores: melhores práticas, documentos, recomendações, artigos, treinamentos e palestras.

- Disseminar informação para a comunidade sobre as mais recentes ameaças via spam: vírus, worms, fraudes, golpes, etc, através da divulgação de alertas de segurança e notícias.

- Agir como facilitador na interação com os grupos de segurança envolvidos nos incidentes (bancos, empresas, portais, etc), com a Polícia e demais autoridades competentes, com grupos de segurança no exterior.

- Orientar e auxiliar no encaminhamento dos incidentes através do atendimento por e-mail, telefone e outros meios.

A Atuação dos CSIRTs

- Interagir internamente em sua organização, zelando pela segurança de seus usuários ou de sua constituency. Exemplos: filtrar o acesso a páginas de bancos clonadas, divulgar notas internas alertando os usuários sobre novos golpes, etc.
- **Em resumo, os CSIRTs atuam**:
  - **Educando e Conscientizando**...usuários e administradores.
  - **Informando**... a comunidade.
  - **Orientando**... usuários, administradores e a comunidade.
  - **Interagindo**... dentro e fora de sua organização e de seu país de origem.

CAIS

Conclusões

- Será mesmo o fim do E-mail?
  - crise “existencial” do e-mail
  - transição, mudança de paradigma
- Política de Segurança
- Conscientização e educação dos usuários
- Atuação dos ISPs, empresas, etc.
- Regulamentação do Marketing por e-mail
- Legislação: adequada X inadequada

CAIS

Referências

- CAIS/RNP: http://www.rnp.br/cais
- NBSO: http://www.nic.br
- CERT: http://www.cert.org
- SANS: http://www.sans.org
- FIRST: http://www.first.org
- FTC: http://www.ftc.gov
- Brightmail: http://www.brightmail.com
- Por uma Internet sem Spam: http://www.quatrocantos.com/lendas/index.htm
- Terra Informática, Especial Spam: http://informatica.terra.com.br/virusecia/spam/index.html

Quando o Spam se torna um Incidente de Segurança

Perguntas

Contatos

Centro de Atendimento a Incidentes de Segurança – CAIS

cais@cais.rnp.br - http://www.rnp.br/cais

Renata Cicilini Teixeira – renata@cais.rnp.br