

Aspectos Tecnológicos e de Segurança Relacionados com Spam

Klaus Steding-Jessen

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

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

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

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

Roteiro

- Cenário atual
- Fatores técnicos que facilitam o spam
- Recomendações do CT-Spam
- Considerações finais

Cenário atual

- crescente inclusão de redes brasileiras em listas de bloqueio
- abuso dos computadores de usuários finais
 - instalação de bots, usados para envio de spam, e utilização de proxies abertos para anonimato
- consumo de banda, disco, processamento e esforço de implantação de novas tecnologias
- vetor de propagação de vírus/worms e fraudes

Spam como vetor de fraudes

- Atualmente maioria absoluta das fraudes utiliza o envio de cavalos de tróia via spam:
 - Serasa, Receita, TSE, Censo do IBGE, Cartões Virtuais, “Você está sendo traído”, “Recorra das Multas de Trânsito”, irregularidades de CPF, atualizações de antivírus, extrato de operadoras de telefonia, etc.

Exemplo 1: TSE



Detalhes

Resultado do AV Kaspersky:

```
Scanned file:      regulamento.exe
regulamento.exe - packed with PE_Patch.PECompact
regulamento.exe - packed with PecBundle
regulamento.exe - packed with PECompact
regulamento.exe - infected by Trojan-Spy.Win32.Banker.ju
```


Trecho do cabeçalho indicando servidor invadido usado no envio:

```
X-Source: /usr/bin/php
X-Source-Args: php -q enviar1.txt Tribunal de Justica Eleitoral
               informacoes@tse.gov.br Titulo Eleitoral irregular c8.txt tt.htm
X-Source-Dir: /tmp/...
```


Exemplo 2: AACD

AACD - Mozilla

A NOSSA ESTRELA CONTINUA BRILHANDO EM 2005.



Em 2004, ultrapassamos a marca de R\$ 16.616.032,00, que serão destinados para ampliação do atendimento de milhares de crianças deficientes. Seis anos de campanhas realizadas pela AACD, detentora, no Brasil, do projeto Teleton, possibilitou ampliações e melhorias no atendimento a milhares de portadores de deficiência física. A receita do Teleton 2003 permitiu a construção de mais um Centro de Reabilitação AACD, desta vez em Nova Iguaçu, na Baixada Fluminense (RJ), inaugurado no final do mês de setembro último.



Hoje estamos parabenizando você com a reprodução de um cartão virtual feito por um de nossos pacientes.

[Ver Cartão AACD 2005](#)

Copyright © 2005, AACD / Teleton

http://www.construmar.com.br/htmlarea/images/cartao.scr

Resultado do AV Kaspersky

```
Scanned file:   cartao.scr
cartao.scr - packed with PE_Patch.PECompact
cartao.scr - packed with PecBundle
cartao.scr - packed with PECompact
cartao.scr - infected by Trojan-Spy.Win32.Banker.ju
```

Fatores técnicos que facilitam o spam

Fatores que facilitam o spam

- máquinas com serviço de proxy mal configurado podem ser abusadas:
 - para envio de spam e realização de ataques
 - fornecem anonimato
 - geralmente são máquinas domésticas com banda larga
- máquinas vulneráveis comprometidas por bots permitem:
 - controle remoto por parte do invasor/spammer
 - utilização em esquemas de fraude, envio de spam, etc.

Softwares de “bulk email”

- extremamente fáceis de obter e usar
- permitem uso de proxies e relays abertos, ou envio direto
- muitos “vendedores” oferecem serviços como envio diário de listas de proxies abertos
- são alimentados por listas de e-mails obtidas de páginas Web, newsgroups, etc.
- tentam evitar emails que pareçam ser “spam traps”, .mil, .gov, abuse, etc.

Recomendações do CT-Spam

Recomendações do CT-Spam

- combater proxies e relays abertos
- eliminar a conexão direta de clientes domésticos a servidores SMTP, na porta 25
 - uso da porta 587 (*mail submission port*)
 - uso de autenticação para envio de mensagens (SMTP AUTH)
- limitar a vazão de emails nos servidores SMTP
- restringir a criação automática de contas
- técnicas de validação de mensagens (SPF, DKIM)

Recomendações do CT-Spam (cont)

- Acompanhamento de notificações de abuso
 - criar os emails `security@`, `abuse@` e manter os contatos de Whois atualizados
 - tratar todas as notificações recebidas
- Implementação de políticas
 - devem prever como uso abusivo de recursos tanto o envio de spam como a hospedagem de páginas referenciadas em spams

Considerações finais

Além destas recomendações, também é importante:

- estimular o opt-in para o uso de email com fins comerciais
- aumentar a segurança das máquinas de usuários, evitando que sejam comprometidas por malwares e bots
- se for criada uma lei, que não legitime o spam

Informações adicionais

- CGI.br
<http://www.cgi.br/>
- CERT.br
<http://www.cert.br/>
- Tecnologias e Políticas para Combate ao Spam
<http://www.cgi.br/eventos/int-ctspam.htm>