Spam e Fraudes por E-mail:

Iniciativas de Combate no Brasil e no Mundo

Cristine Hoepers
Klaus Steding-Jessen
CERT.br / NIC.br / CGI.br

Danton Nunes
InterNexo

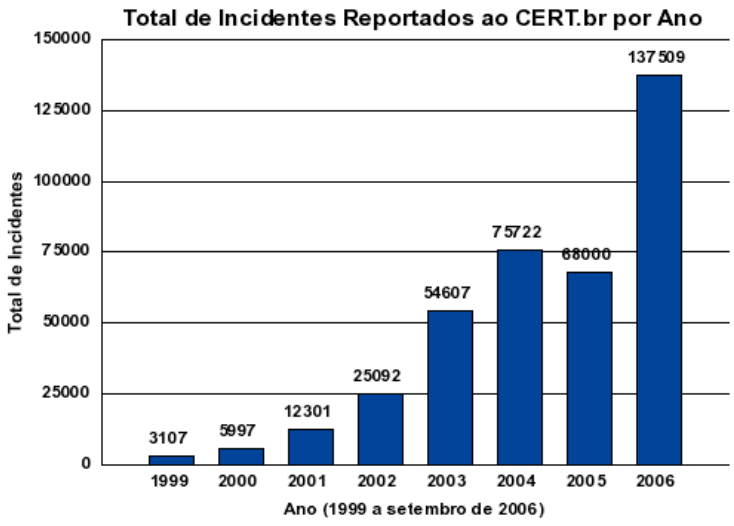
Minitrilha 3: Spam e Fraudes por E-mail

Agenda

- Parte 1 (1 hora)
  CERT.br
  - Indicadores do problema no Brasil
  - Iniciativas de combate no Brasil e no mundo
- Parte 2 (3 horas)
  Danton Nunes - colaborador do CGI.br
  - Tutorial sobre novas tecnologias e técnicas de mitigação
- Material desta trilha estará disponível em:
  http://www.cert.br/docs/palestras/

O Problema no Brasil

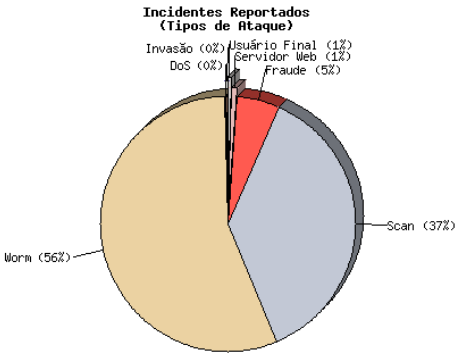
Estatísticas de Notificações de Incidentes ao CERT.br



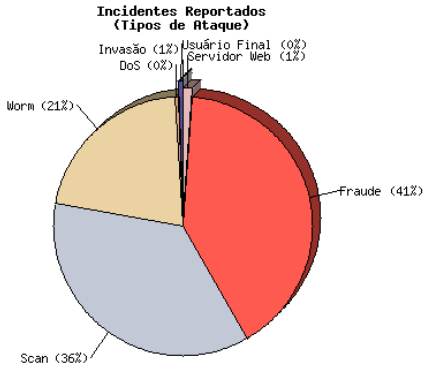
SSI 2006 - Minitrilha 3: Spam e Fraudes por E-mail - 09 de novembro de 2006

Evolução dos Tipos de Ataques

2004



2005



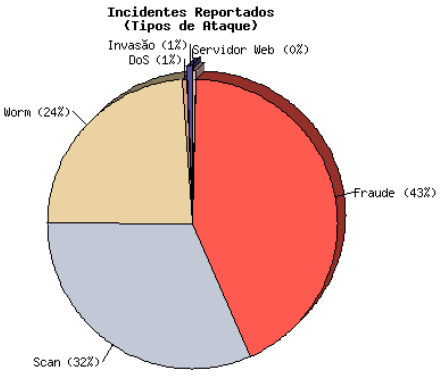
Fraudes: 4.015

Fraudes: 27.292

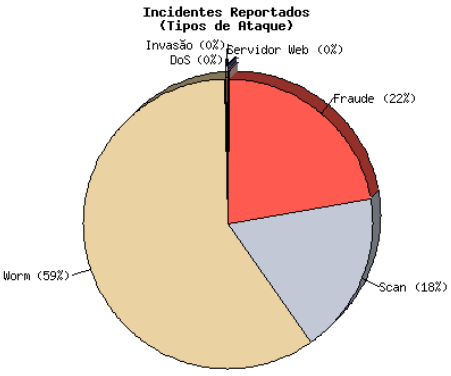
Evolução dos Tipos de Ataques (cont)

2006

1º Trimestre:



2º Trimestre:



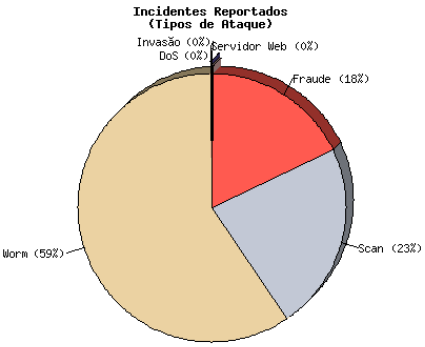
Fraudes: 12.099

Fraudes: 10.939

Evolução dos Tipos de Ataques (cont)

2006

3º Trimestre:



Fraudes: 10.526

Totais da categoria Fraude:

2004: 4.015
2005: 27.292
2006: 33.564 (até setembro)

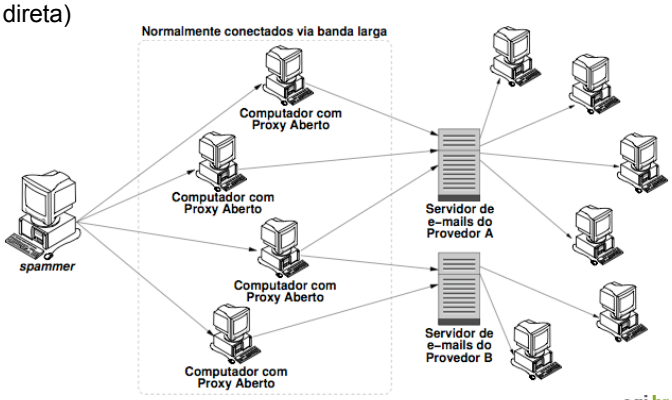
Características:

Spams

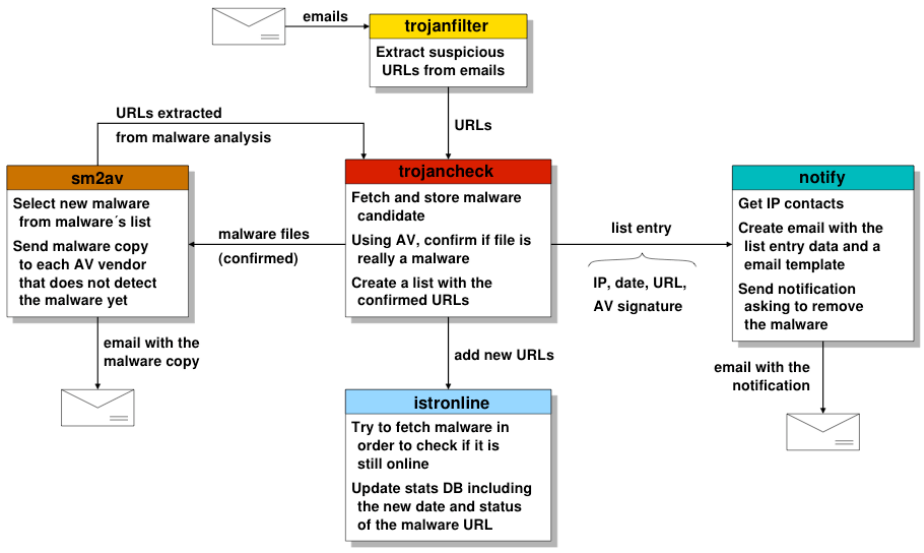
- Em nome das mais variadas instituições e com tópicos diversos
- Com links para códigos maliciosos (cavalos de tróia)
  - Monitoram acessos a sites
  - Coletam: contas, senhas, números de cartões de crédito, credenciais de sites de comércio eletrônico e de sites de relacionamentos, entre outros

Evolução dos Tipos de Ataques (cont)

- Spams são enviados usando *proxies* abertos para prover anonimato
  - Normalmente em máquinas de usuários finais em redes de banda larga
  - Máquinas infectadas por *bots*
- Uso do proxy é bem sucedido
  - É possível o envio direto de mensagens via porta 25 na maior parte das redes (entrega direta)



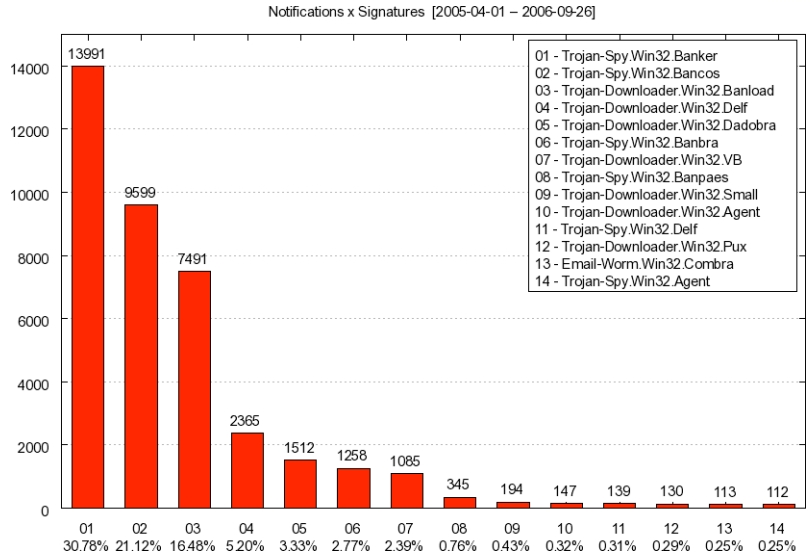
Tratamento de Incidentes Envolvendo Fraudes



Estatísticas de 01/04/2005 a 26/09/2006

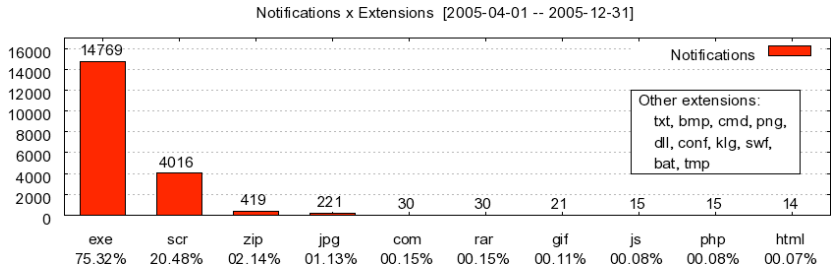
Categoria	Número
Domínios que estavam hospedando *trojans*	6.284
Contatos únicos para os domínios	2.552
Extensões usadas pelos arquivos de *trojans*	68
Nomes de arquivos utilizados pelos *trojans*	14.237
Nomes de máquinas (*hosts*) envolvidas	10.818
Endereços IP únicos	4.686
Países para os quais estavam alocados os IPs	75
E-mails de notificação enviados pelo CERT.br	23.709
URLs únicas encontradas no período	33.946
Assinaturas de antivírus (agrupadas)	161
Assinaturas de antivírus (com variantes)	2.418

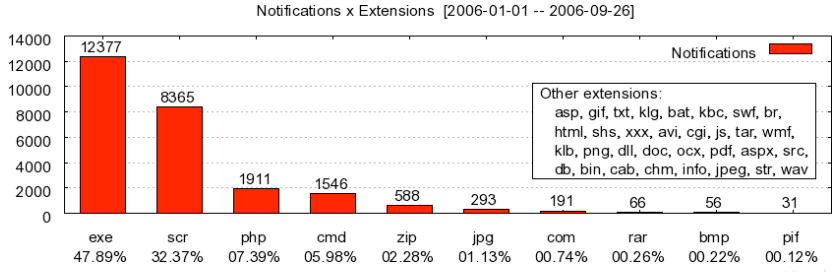
Assinaturas Mais Comuns



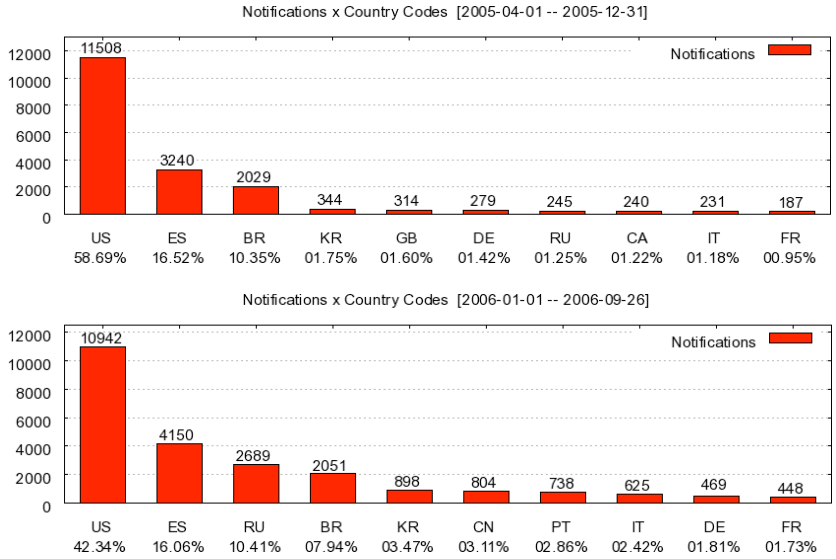
Fonte das assinaturas: Kaspersky Lab.

Extensões Mais Comuns





Países de Alocação dos IPs



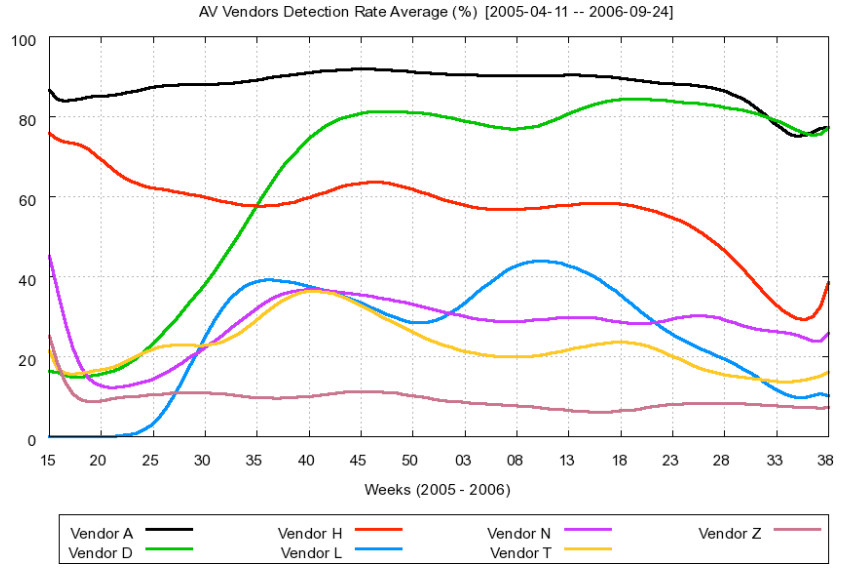
Eficiência dos Antivírus: 06/04/2005 a 26/09/2006

Empresa de Antivírus	Exemplares testados	Exemplares não detectados	Exemplares detectados	Taxa de detecção (%)
Vendor A	26.492	3.164	23.328	88,06
Vendor B	5.651	1.019	4.632	81,97
Vendor C	790	240	550	69,62
Vendor D	26.526	8.300	18.226	68,71
Vendor E	26.342	8.787	17.555	66,64
Vendor F	26.513	8.856	17.657	66,60
Vendor G	26.219	10.512	15.707	59,91
Vendor H	26.527	11.576	14.951	56,36
Vendor I	15.337	7.559	7.778	50,71
Vendor K	17.888	10.846	7.042	39,37
Vendor L	22.462	15.142	7.320	32,59
Vendor N	26.215	18.592	7.623	29,08
Vendor O	26.160	18.653	7.507	28,70
Vendor P	21.988	15.836	6.152	27,98
Vendor Q	26.524	19.168	7.356	27,73
Vendor T	26.509	20.595	5.914	22,31
Vendor Z	26.281	23.906	2.375	9,04

Apenas **2** fabricantes com taxa de detecção acima de **80%**

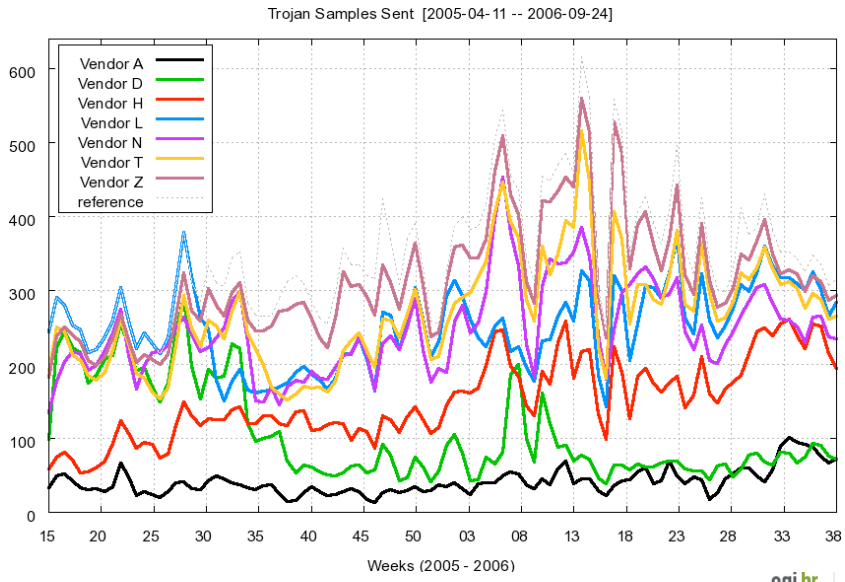
~70% dos fabricantes com menos de **40%** de taxa de detecção

Taxa de Detecção: 11/04/2005 a 24/09/2006



SSI 2006 - Minitrilha 3: Spam e Fraudes por E-mail - 09 de novembro de 2006

Exemplares enviados: 11/04/2005 a 24/09/2006



SSI 2006 - Minitrilha 3: Spam e Fraudes por E-mail - 09 de novembro de 2006

Indicadores do CGI.br

- Parceria com o IBGE e IBOPE/NetRatings
- Pesquisas TIC Domicílios e TIC Empresas 2005, realizadas para o CGI.br, pelo Instituto Ipsos Opinion http://www.nic.br/indicadores/

Objetivos:

- Produzir e divulgar com periodicidade indicadores oficiais sobre penetração e uso da Internet;
- Fornecer subsídios para a elaboração de políticas públicas que garantam o acesso às TICs no Brasil;
- Acompanhar, monitorar e avaliar o impacto sócio econômico das TICs;
- Permitir a comparabilidade da realidade brasileira com outros países.

Proporção de Indivíduos que Acessaram a Internet, de qualquer Local
Percentual sobre o total da população brasileira (8540 domicílios entrevistados)

	< 3 meses	Entre 3 e 6 meses	Entre 6 e 12 meses	+ 12 meses	Nunca usou
Percentual	24,41	2,65	2,26	2,93	67,76

TIC Domícilios

F1 - Problemas de Segurança Encontrados Usando a Internet
Percentual sobre o total de usuários Internet

	Nenhum	Vírus (com acesso não autorizado)	Virus (com danos em SW ou HW)	Abuso de Informação pessoal	Fraude	Outro	Não lembra
Total	40,99	19,64	7,13	1,67	0,94	1,10	0,24

F2 - Medidas de Segurança Tomadas com Relação ao Computador
Percentual sobre o total de usuários Internet que possuem computador

	Antivírus	Firewall Pessoal	Software Anti-spyware
Total	69,76	19,33	22,09

F3 - Freqüência de Atualização do Antivírus
Percentual sobre o total de usuários Internet que possuem computador

	Diária	Semanal	Mensal	Trimestral	Não atualizou
Total	21,11	27,01	17,37	3,47	31,03

TIC Empresas

E1 - Problemas de Segurança Encontrados

Percentual sobre o total de empresas com acesso à Internet

	Vírus	Worms ou Bots	Trojans	Acesso externo não autorizado	Acesso interno não autorizado	DoS	Desfiguração de Servidor Web
Total	50,34	17,44	31,13	10,89	7,61	6,25	11,20

E2 - Medidas de Segurança Adotadas

Percentual sobre o total de empresas com acesso à Internet

	Antivírus	Software Anti-spyware	Firewall	SSL, HTTPs	Autenticação para usuários internos	Autenticação para usuários externos	IDS	Backup	Backup offsite	Programa de Treinamento para Funcionários
Total	95,72	59,46	54,11	49,48	42,33	21,12	29,21	69,62	38,33	19,69

E3 - Freqüência de Atualização do Antivírus

Percentual sobre o total de empresas com acesso à Internet

	Diária	Semanal	Mensal	Trimestral	Semestral/Anual	Não atualizou
Total	41,68	30,02	12,34	5,11	2,11	8,74

Iniciativas de Combate no Brasil

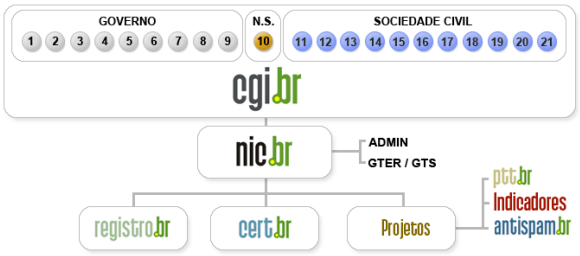
SSI 2006 - Minitrilha 3: Spam e Fraudes por E-mail - 09 de novembro de 2006

Atribuições do CGI.br

Entre as diversas atribuições e responsabilidades definidas no Decreto Presidencial nº 4.829, destacam-se:

- a proposição de normas e procedimentos relativos à regulamentação das atividades na Internet;
- **a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil;**
- o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil;
- **a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país;**
- a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>;
- **a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.**

Comitê Gestor da Internet no Brasil



1 – Ministério da Ciência e Tecnologia (Coordenação)
2 – Ministério das Comunicações
3 – Casa Civil da Presidência da República
4 – Ministério da Defesa
5 – Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 – Ministério do Planejamento, Orçamento e Gestão
7 – Agência Nacional de Telecomunicações (Anatel)
8 – Conselho Nacional de Desenvolvimento Científico e Tecnológico
9 – Fórum Nacional de Secretários Estaduais para Assuntos de C&T
10 – Representante de Notório Saber em assuntos de Internet

11 – provedores de acesso e conteúdo
12 – provedores de infra-estrutura de telecomunicações
13 – indústria de bens de informática, telecomunicações e software
14 – segmento das empresas usuárias de Internet
15-18 – representantes do terceiro setor
19-21 – representantes da comunidade científica e tecnológica

http://www.cgi.br/sobre-cg/

Comissão de Trabalho Anti-Spam - CT-Spam

Criada em 14/01/2005

Para propor uma estratégia nacional visando combater o problema e articular um conjunto de ações que possa mobilizar os diversos atores relevantes envolvidos no tratamento desse problema.

Representantes das seguintes instituições:

CGI.br, NIC.br, CERT.br, Anatel, Ministério da Ciência e Tecnologia, USP e UFRJ

Objetivos:

- Recomendar procedimentos tecnológicos para combate ao Spam
- Disponibilizar informações sobre Spam para os diferentes atores
- Recomendar códigos de conduta para empresas, usuários e administradores de rede
- Recomendar projetos de lei para o poder legislativo
- Promover articulação internacional sobre o tema

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

Ações do CT-Spam

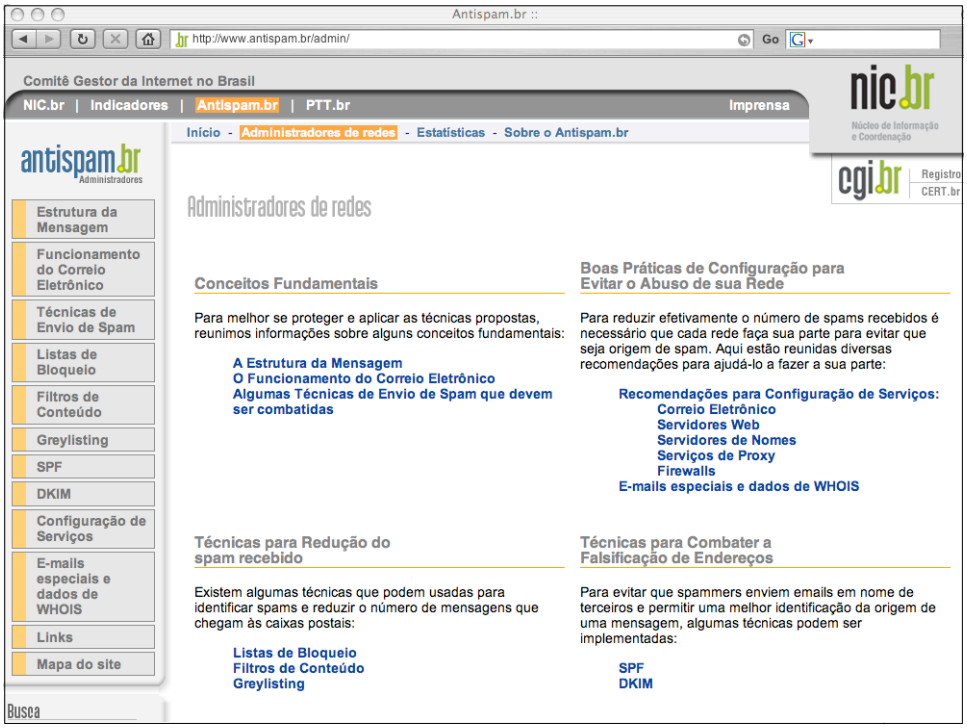
- Produção do documento
  "Tecnologias e políticas para o combate ao Spam"
  http://www.cgi.br/eventos/ctspam/ct-spam-tecnologias-politicas.pdf
  - seminário com representantes de teles e provedores para discutir o documento
  - discussão no grupo CBC-1 da Anatel
- Produção do Relatório
  "Análise Técnica sobre Legislações Anti-Spam"
  http://www.cgi.br/eventos/ctspam/ct-spam-analise-legislacao.pdf
  - Apresentado no seminário Rio Info e encaminhado à Comissão de Ciência e Tecnologia da Câmara dos Deputados
- Participação nos fóruns internacionais para discussão do tema
  - OECD, ITU, APWG e MAAWG

Ações do CT-Spam (cont)

Site http://www.antispam.br/

- Área geral
  - Dicas de filtragem e proteção voltadas para usuários de Internet
  - Conceitos, origens, tipos de spam, glossário, etc
- Área para administradores de redes
  - Dicas de filtragem e proteção voltadas para administradores de redes
  - Descrição de novas tecnologias como SPF, DKIM, Greylisting, etc


Antispam.br ::
http://www.antispam.br/dicas/
Go
Comitê Gestor da Internet no Brasil
Sobre o NIC.br | Indicadores | Antispam.br | PTT.br
nic.br
Núcleo de Informação e Coordenação
cgi.br
Registro CERT.br
antispam.br
Início - Administradores de redes - Estatísticas - Sobre o 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
Mapa do site
Busca
ok
NIC.br
Antispam.br
CERT.br
Registro.br
Dicas
Principais dicas para ajudar o usuário a receber menos spam, preservar sua privacidade e evitar que códigos maliciosos sejam instalados em seu computador:
Preserve sua privacidade
Seja criterioso ao informar seus endereços de e-mail em cadastros, sites de relacionamentos etc.
Tenha e-mails diferentes para uso pessoal, trabalho, compras on-line e cadastros em sites em geral
Evite utilizar e-mails simples, como aqueles formados apenas pelo primeiro nome.
Leia com atenção os formulários e cadastros on-line, evitando preencher ou concordar, inadvertidamente, com as opções para recebimento de e-mails de divulgação do site e de seus parceiros.
Não forneça dados pessoais, documentos e senhas por e-mail ou via formulários on-line.
Verifique a política de privacidade dos sites, onde pretende registrar seus dados.
Mantenha-se informado
Conhecer os tipos de spam ajuda a reconhecer e-mails suspeitos e, eventualmente, não detectados pelos softwares anti-spam.
Acompanhar as notícias e alertas sobre os golpes e fraudes, reduz o risco de ser enganado e/ou prejudicado financeiramente por e-mails desse gênero.
Procurar informações sobre fatos recebidos por e-mail, antes de repassá-los, contribui para a redução do volume de mensagens de correntes, boatos e lendas urbanas, enviadas repetidas vezes na rede.
Procurar informações no site das empresas, ao receber e-mails sobre prêmios e promoções, reduz o risco de ser enganado em golpes propagados por e-mail.
Proteja-se
Utilize softwares de proteção (antivírus, anti-spam, anti-spyware e firewall pessoal) nos computadores de uso doméstico e corporativo, mantendo-os com as versões, assinaturas e configurações atualizadas.
Não seja um "clicador compulsivo". Não execute arquivos anexados em e-mails sem examiná-los previamente com antivírus, bem como,


Antispam.br ::
http://www.antispam.br/admin/
Go
Comitê Gestor da Internet no Brasil
NIC.br | Indicadores | Antispam.br | PTT.br
Imprensa
nic.br
Núcleo de Informação e Coordenação
cgi.br
Registro CERT.br
antispam.br
Administradores
Início - Administradores de redes - Estatísticas - Sobre o Antispam.br
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
Mapa do site
Busca
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

Iniciativas de Combate Internacionais

MAAWG - Messaging Anti-Abuse Working Group

(...) "to bring the messaging industry together to work collaboratively and successfully address forms of messaging abuse such as messaging spam, virus attacks, denial-of-service attacks, and other forms of abuse."

Fonte: http://www.maawg.org/about/

Documentos do MAAWG

- MAAWG Recommendation - Managing Port25
  http://www.maawg.org/port25/
- Important Considerations for Implementers of SPF and/or Sender ID
  http://www.maawg.org/about/whitepapers/spf_sendID/
- Outros documentos:
  http://www.maawg.org/about/publishedDocuments/
  - BIAC-MAAWG Best Practices Expansion Document
    - em conjunto com o *Business and Industry Advisory Comittee* da OECD (*Organisation for Economic Co-operation and Development*)
  - Anti-Phishing Best Practices for ISPs and Mailbox Providers
    - em conjunto com o *Anti-Phishing Working Group* (APWG)
  - Email Metrics Report - June 2006
  - Email Metrics Report - March 2006
  - Code of Conduct

OECD Task Force on Spam

"To support the development of an inclusive and coherent answer to the spam issue, the OECD, has launched an Anti-Spam 'Toolkit'."

— Element I - Anti-Spam Regulation
— Element II - Enforcement
— Element III - Industry-Driven initiatives
— Element IV - Anti-Spam Technologies
— Element V - Education and Awareness
— Element VI - Co-operative Partnerships against spam
— Element VII - Spam Measurement
— Element VIII - Global Co-operation & Concluding remarks

Fonte: http://www.oecd-antispam.org/

StopSpamAlliance

"*The StopSpamAlliance is a joint initiative to gather information and resources on combating spam.*"

Iniciativa conjunta:

- APEC - Asia-Pacific Economic Cooperation
- EU CNSA - European Union Contact Network of Spam Authorities
- ITU - International Telecommunication Union
- London Action Plan - international spam enforcement network
- OECD - Organisation for Economic Co-operation and Development
- Seoul-Melbourne Anti-Spam group

Fonte: http://www.stopspamalliance.org/

Referências Adicionais

- Material desta trilha
  http://www.cert.br/docs/palestras/
- Antispam.br
  http://www.antispam.br/
- Indicadores do CGI.br
  http://www.nic.br/indicadores/

- Livro da Cartilha de Segurança para Internet
  http://cartilha.cert.br/livro/