

Regional Updates: Brazil

Anti-Spam Task Force Developments

Cristine Hoepers
General Manager
cristine@cert.br

CERT.br – Computer Emergency Response Team Brazil
NIC.br - Network Information Center Brazil
CGI.br - Brazilian Internet Steering Committee

Anti-Spam Task Force

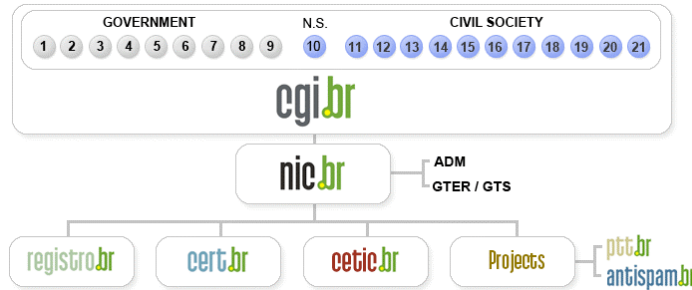
Mission:

- recommend technical procedures to fight spam
- provide information about spam to different players
- recommend proposals for new laws
- be a point of contact for international articulation

Developments and material (in Portuguese):

- <http://www.cgi.br/acoef/antispam.htm>
- <http://www.antispam.br/>

Brazilian Internet Steering Committee (CGI.br) Structure



- | | |
|---|--|
| <ul style="list-style-type: none"> 1 – Ministry of Science and Technology (Coordination) 2 – Ministry of Communications 3 – Presidential Cabinet 4 – Ministry of Defense 5 – Ministry of Development, Industry and Foreign Trade 6 – Ministry of Planning, Budget and Management 7 – National Telecommunications Agency 8 – National Council of Scientific and Technological Development 9 – National Forum of Estate Science and Technology Secretaries 10 – Internet Expert | <ul style="list-style-type: none"> 11 – Internet Service Providers 12 – Telecommunication Infrastructure Providers 13 – Hardware and Software Industries 14 – General Business Sector Users 15 – Non-governmental Entity 16 – Non-governmental Entity 17 – Non-governmental Entity 18 – Non-governmental Entity 19 – Academia 20 – Academia 21 – Academia |
|---|--|

3rd Joint LAP-CNSA Workshop - Washington, DC - October, 2007

Legislative Initiatives

Current Status

- Several projects at Congress and Senate
 - Mainly opt-out
 - Several meetings and hearings, and a lot of controversy
- Anti-Spam Task force contribution
 - Legislation Study in partnership with FGV Law School
 - Evaluated all projects
 - Proposed a substitutive
 - Soft opt-in

Information for Network Operators

Adoption of Best Practices

- Published a recommendation of best practices
 - Port 25 management, e-mail reputation, DKIM, etc
- Helping to produce a business case
 - Costs involved
 - Effectiveness (to justify return on investment)
- SpamPots project is part of the problem awareness

Antispam.br Website - Admin Area

Comitê Gestor da Internet no Brasil

NIC.br | Indicadores | Antispam.br | PTT.br | Imprensa

Início - Administradores de redes - Estatísticas - Sobre o Antispam.br

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

Busca

User Awareness

Antispam.br Website - General Area

cert.br

Comitê Gestor da Internet no Brasil

Sobre o NIC.br | Indicadores | Antispam.br | PTT.br

Inicio - Administradores de redes - Estatísticas - Sobre o Antispam.br

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

NIC.br Antispam.br
 CERT.br Registro.br

nic.br
 Núcleo de Informação e Coordenação

cgi.br Registro CERT.br

Tipos de spam

Códigos maliciosos

São programas que executam ações maliciosas em um computador. Diversos tipos de códigos maliciosos são inseridos em e-mails, contendo textos que se valem de métodos de engenharia social para convencer o usuário a executar o código malicioso em anexo. Em geral, estes códigos também são utilizados em spams enviados por fraudadores.

Dentre os códigos mais comuns enviados via spam, pode-se citar as seguintes categorias:

- **Backdoor:** Programa que permite a um invasor retornar a um computador comprometido. Normalmente este programa é colocado de forma a não ser notado.
- **Spyware:** Termo utilizado para se referir a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma disfarçada, não autorizada e maliciosa.
- **Keylogger:** Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Normalmente, a ativação do keylogger é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um site de comércio eletrônico ou Internet Banking, para a captura de senhas bancárias ou números de cartões de crédito.
- **Screenlogger:** Forma avançada de keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou armazenar a região que circunda a posição onde o mouse é clicado.
- **Cavalo de tróia:** Programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc.) que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

3rd Joint LAP-CNSA Workshop - Washington, DC - October, 2007

cgi.br | nic.br

Antispam.br Website - General Area

The screenshot shows the Antispam.br website interface. At the top right is the cert.br logo. Below it, the browser address bar shows 'http://www.antispam.br/ptiposfraudes/'. The website header includes 'Comitê Gestor da Internet no Brasil' and navigation links for 'Sobre o NIC.br', 'Indicadores', 'Antispam.br', and 'PTT.br'. The main content area is titled 'Tipos de spam' and features an illustration of a computer monitor, keyboard, and mouse with a person's hands raised in a gesture of surprise or frustration. The text discusses 'Fraudes' (Frauds) and 'Golpes (Scams)' (Scams), explaining how fraudsters use e-mails and social engineering to exploit users. A sidebar on the left contains a menu with items like 'O que é spam?', 'Problemas causados pelo spam', and 'Prevenção'. A search bar is located at the bottom left of the sidebar.

3rd Joint LAP-CNSA Workshop - Washington, DC - October, 2007

Cartoons

- 4 videos - 4 minutes each
 - The Internet
 - The Intruders
 - Spam (*)
 - The Defense (*)
- Freely available on the Internet
- In several formats and resolutions
- Possible future development: booklet or comic book
 - To distribute with the DVD version
 - Schools, presentations, libraries, internet cafes, etc
 - Still in discussion (funding and sponsors issues)

(*) To be released November, 2007

3rd Joint LAP-CNSA Workshop - Washington, DC - October, 2007

cert.br

Video 1: The Internet

3rd Joint LAP-CNSA Workshop - Washington, DC - October, 2007

cgi.br | nic.br

cert.br

Video 2: The Intruders

3rd Joint LAP-CNSA Workshop - Washington, DC - October, 2007

cgi.br | nic.br



Stickers



3rd Joint LAP-CNSA Workshop - Washington, DC - October, 2007

Additional References

- This presentation – by the end of the month
<http://www.cert.br/docs/presentations/>
- Awareness videos
<http://www.antispam.br/videos/>
- CERT.br
 Computer Emergency Response Team Brazil
<http://www.cert.br/>

3rd Joint LAP-CNSA Workshop - Washington, DC - October, 2007