



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

GTS-13 - 20 de junho de 2009



**1 Ano do Catálogo de  
Fraudes RNP: Números,  
tendências e próximos  
passos**

**Ronaldo Castro de Vasconcellos**



**GTS** Grupo de Trabalho em Segurança



# 1 Ano do Catálogo de Fraudes RNP



## Agenda

- Introdução
- Números
- Tendências
- Próximos Passos

# 1 Ano do Catálogo de Fraudes RNP



## Introdução

- 2005: Criação das contas de contribuição nos Alertas CAIS
    - artefatos@cais.rnp.br
    - phishing@cais.rnp.br
- (Sirvam-se, Spam Bots!)

- Colaborações espontâneas
- Percebemos o desejo das pessoas comuns em colaborar



# 1 Ano do Catálogo de Fraudes RNP



## Introdução (2)

- Março de 2008: Lançamento do site público
- Disponível em **<http://www.rnp.br/cais/fraudes.php>**
- Boa repercussão na mídia
  - assessoria de imprensa RNP (TV, rádio, jornais de grande circulação)
  - segunda página do CAIS mais visitada
  - usuários aflitos que buscam informações pelo Google
    - fraudes: posição #3
  - aumento considerável no número de amostras
- Serviço simples e despretensioso, mas mesmo assim teve uma aceitação que não esperávamos.

# 1 Ano do Catálogo de Fraudes RNP



## Introdução (3)

- A grande divulgação trouxe problemas inesperados
- Ironia - Fraudes fazendo referência às imagens do Catálogo
  - Solução: marca d'água e URL do catálogo em cada imagem
- Freqüente aparecimento de fraudes com várias etapas
  - Mensagem, Website (algumas vezes mais de um), Applet Java
  - Solução: Possibilidade de inclusão de mais de uma imagem
- Tags para organizar



## Introdução (4)

- Campos
  - Tipo – descrição curta
  - Data, From, Subject
  - Tag – categoria da fraude. Cada fraude pode ser classificada em mais de uma tag
  - Texto ASCII, Imagem, nome do arquivo malicioso (quando disponível)
  - Comentário – Comentários específicos, vírus identificado
    - Anti-vírus com melhor reputação no mercado (F-Secure, Trend)
    - Texto para usuário comum, não análise de malware.

# 1 Ano do Catálogo de Fraudes RNP



## Números

- 740 registros (19 de junho)
  - tentamos evitar registros duplicados
  - foco em fraudes do Brasil
    - não Scam 419 Nigéria
    - não bancos do exterior
    - não sites de e-commerce do exterior
- Inicialmente 2 pessoas
  - hoje 5 pessoas em rodízio



# 1 Ano do Catálogo de Fraudes RNP



## Números (2)

- 5 mil mensagens por mês em média
  - Spam espontâneo nas contas devido a divulgação dos mailbox
    - o lado bom e o lado ruim da divulgação
    - Spam Spam e Spam Fraude
  - Triagem é necessária
    - cerca de 300 mensagens por mês após triagem
    - muitas mensagens duplicadas
    - muitas mensagens inutilizáveis
      - encaminhamento inadequado



# 1 Ano do Catálogo de Fraudes RNP



## Números (3)

- Mais de 150 tags
  - escolhidos e criados com base na opinião de quem cadastra
- Principais classes de tags
  - classificação em mais de 1 tag se necessário
  - fotos, videos, bancos, sexo, noticias, compras, tragedias, amor, debitos, atualizacao (de segurança, de certificado digital), celular, cartaovirtual, contas (serviços)
- Principais tags específicos
  - orkut, bradesco, bigbrotherbrasil, caixaeconomicafederal, vivo, microsoft

# 1 Ano do Catálogo de Fraudes RNP



## Números (4)

- Alguns casos especiais
  - alguns pedidos de fornecimento de dados adicionais feito por Ministério da Justiça
  - diversos pedidos de empresas afetadas
  - diversos pedidos de ajuda por vítimas de golpes
    - infelizmente no modelo atual não é possível oferecer atendimento individual

# 1 Ano do Catálogo de Fraudes RNP

## Tendências

- Óbvias
  - Exploração de assuntos do momento
  - Air France, Isabella Nardoni, Santa Catarina e outros casos de destaque
  - Cada vez mais rápido: 24 horas, 7 até o momento
    - desaparecimento do avião em 1 de junho, primeira mensagem recebida em 2 de junho
- Mensagens que demonstram alguma garimpagem de dados prévia
  - O começo do fim de:  
  
Olá fulano@example.com!



# 1 Ano do Catálogo de Fraudes RNP



IMAGEM DO CATÁLOGO DE FRADES CAIS/RNP  
[WWW.RNP.BR/CAIS/](http://WWW.RNP.BR/CAIS/)



**Imagens de objetos e vítimas encontradas no mar já estão disponíveis pela nossa equipe.**

**N**ossa equipe com exclusividade e com parceria com a FAB (Força Aérea Brasileira) já teve contato com o comandante do Hércules, aeronave que transporta a equipe que fez as imagens do Airbus da Air France.

[imagem1.jpg](#)

**Preserve o Meio Ambiente. Apenas imprima este e-mail se houver real necessidade.**

# 1 Ano do Catálogo de Fraudes RNP



IMAGEM DO CATÁLOGO DE FRAUDES CAIS/RNP  
[WWW.RNP.BR/CAIS/](http://WWW.RNP.BR/CAIS/)



## Aeronáutica e Marinha localizam dois sobreviventes do voo AF447

Os comandos da Marinha e da Aeronáutica anunciaram nesta quarta a localização de dois sobreviventes, vítimas do acidente com o voo AF447 da Air France, desaparecido desde o último domingo (31). Com isso, chega a expectativa de mais sobreviventes a serem resgatados pelas equipes de buscas, que trabalham há sete dias.

Veja Video:



[clique na imagem "real player" para ver o video.](#)

# 1 Ano do Catálogo de Fraudes RNP



IMAGEM DO CATÁLOGO DE FRAUDES CAIS/RNP  
[WWW.RNP.BR/CAIS/](http://WWW.RNP.BR/CAIS/)



## IML e PF terminam primeira fase de identificação dos corpos das vítimas.

O Airbus da Air France transportava 228 pessoas de 32 nacionalidades, entre passageiros e tripulantes. O voo, de número 447, deixou o Rio de Janeiro no dia 31 de maio às 19h30 (horário de Brasília) e fez o último contato de voz às 22h33. Às 22h48, o avião saiu da cobertura do radar de Fernando de Noronha.

A Marinha, Aeronáutica com aval do **Instituto de Medicina Legal (IML)** está disponibilizando algumas imagens dos corpos de alguns passageiros.

 [ANEXO FOTOS.ZIP](#) (150kb)



Foto: Infraco do Brasil

2000-2009 [globo.com](http://globo.com) Todos os direitos reservados

# 1 Ano do Catálogo de Fraudes RNP



IMAGEM DO CATÁLOGO DE FRAUDES CAIS/RNP  
[WWW.RNP.BR/CAIS/](http://WWW.RNP.BR/CAIS/)

terra 

Se você ainda não viu as imagens do Desastre.

Airbus 300 da Air France / Vôo AF 447 - Primeiro vídeo, feito pela FAB (Força Aérea Brasileira), do local do acidente... Cenas fortes, tem que ter estomago... (assistam logo antes que tirem do ar.) Cuidado !!! imagens Fortes !!!!!!!

veja rapido podem tirar do ar a qualquer momento  
!!!! Video Inédito



[http://www.fab.mil.br/portal/imagens/voo447\\_videos\\_fotos.php](http://www.fab.mil.br/portal/imagens/voo447_videos_fotos.php)

The screenshot shows a web page from Terra. At the top, there is a blue banner with the text 'IMAGEM DO CATÁLOGO DE FRAUDES CAIS/RNP' and the URL 'WWW.RNP.BR/CAIS/'. Below this is the Terra logo. The main text describes a video of the Air France Airbus 300 (AF 447) crash site, warning that the content is disturbing and should be viewed quickly. A YouTube video player is embedded in the page, but the video itself is not visible, only a play button is shown. At the bottom of the screenshot, a URL is provided: 'http://www.fab.mil.br/portal/imagens/voo447\_videos\_fotos.php'. The background of the screenshot has a faint, repeating watermark of the CAIS logo.

## Tendências (2)

- Está cada vez mais fácil conhecer o comportamento das massas na internet
  - Google Zeitgeist e outras estatísticas que mecanismos de busca publicam
  - Twitter
    - TweetTabs.com: dados em tempo real sobre busca e tendências nos "twits"
  - Notícias mais lidas nos sites mais populares de notícias





# 1 Ano do Catálogo de Fraudes RNP



## Tendências (3)

- Sim, explorar curiosidade ainda funciona muito bem!
  - Em um ano, 7% dos brasileiros fizeram sexo com pessoas encontradas pela web (Folha Online 18 de junho de 2009)
    - Pesquisa divulgada pelo Ministério da Saúde
  - Fotos de traição, fotos de pessoas mortas em acidentes, vídeos eróticos e pornográficos, mensagens de supostas ex-namoradas, casos de destaque sem solução, etc.
- A venda de computadores pessoais aumentou consideravelmente nas grandes lojas populares
  - A cada dia milhares de pessoas tem seu primeiro dia na Internet
    - *Uau, o banco já sabe o meu endereço de e-mail! A Internet é demais mesmo.*

# 1 Ano do Catálogo de Fraudes RNP



## Tendências (4)

- Encurtadores de URL são um grande problema!
  - Twitter e o limite de 140 caracteres apenas fez o problema piorar
  - bit.ly, TinyURL, is.gd, migre.me (Brasil)
    - Adoraríamos um contato no Migre.me
    - Festival de malware
  - um encurtador sobre o outro
  - encurtadores mais obscuros
  - URL Shorteners: Which Shortening Service Should You Use?  
<http://searchengineland.com/analysis-which-url-shortening-service-should-you-use-17204>

# 1 Ano do Catálogo de Fraudes RNP



## Próximos passos

- Mais informações (FAQ)
- Estatísticas
- Melhorias na interface gráfica
- Submissão de amostras pela Web
- Melhorias na busca por amostras
- Feed RSS

# 1 Ano do Catálogo de Fraudes RNP



## Contato

Centro de Atendimento a Incidentes de Segurança – CAIS

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



Ronaldo Castro de Vasconcellos  
ronaldo@cais.rnp.br