Brazilian Academic and Research Network CSIRT
CAIS/RNP

FIRST TC October 2009 Santiago - 22 October 2009

One year of RNP Fraud Catalog - Numbers, trends and next steps

Ronaldo Castro de Vasconcellos

Agenda

- Intro
- Numbers
- Trends
- Next steps

Intro

- 2005: accounts for contribution were created and announced in CAIS Advisories (CAIS Alerta)
    - artefatos@cais.rnp.br
    - phishing@cais.rnp.br

  (Be our guests, Spam Bots!)

- Spontaneous collaboration
- A lot of people willing to help

Intro (2)

- March 2008: Public website launched
- Available at **http://www.rnp.br/cais/fraudes.php**
- The media liked that
  - RNP press releases (TV, radio, major newspapers)
  - 2nd CAIS webpage in page views
  - users facing problems look for help in Google (Brazil, portuguese)
    - fraudes: position #4
  - significant raise in number of samples
- Simple service, unexpected reaction.

Intro (3)

- The visibility of the service brought us problems
- Irony – frauds using the catalog image files!
    - Solution: watermark and URL in each image
- Frauds with more than one step involved
    - E-mail, Website (sometimes more than 1), Java Applet
    - Solution: More than 1 image feature
- Tags

Intro (4)

- Fields
  - Kind – short description
  - Date, From, Subject
  - Tag – category. Each fraud can be classified with more than 1 tag
  - ASCII text, image (screenshot), malware filename (when available)
  - Comments – Specific comments, malware name
    - Antivirus engines with better reputation (F-Secure, Trend)
    - Text targeted to end users, not malware analysis.

One year of RNP Fraud Catalog

Numbers

- 932 entries (22 october)
  - we try to avoid duplicates
  - focus on Brazil
    - no Scam 419 Nigeria
    - no foreign banks
    - no foreign e-commerce sites
- At first 2 analysts
  - today 5 analysts (in shifts)

One year of RNP Fraud Catalog

Numbers (2)

- Average 5k messages/month
  - Spontaneous Spam
    - good and bad
    - Spam Spam e Fraud Spam
  - Triage is necessary
    - 300 messages/month after triage
    - many duplicates
    - many useless samples
      - inappropriate forwarding, mainly by end users

Numbers (3)

- More than 160 tags
  - chosen based on analyst opinion
- Main tag categories
  - more than 1 tag if necessary
  - fotos, videos, bancos, sexo, noticias, compras, tragedias, amor, debitos, atualizacao, celular, cartaovirtual, contas
- Top tags
  - fotos, bancos, videos, cartaovirtual, noticias, bradesco, sexo, orkut, tragedias, compras, contas, bigbrotherbrasil, caixaeconomicafederal, amor, terra, atualizacao, debitos, globo.com, vivo, bancodobrasil

One year of RNP Fraud Catalog

Numbers (4)

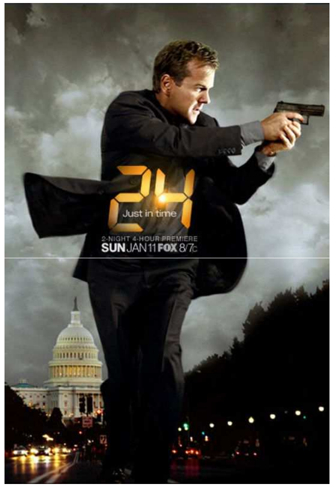
- Some special cases
  - some requests from Brazilian Federal Police (samples, more info)
  - affected companies
  - some victims desperate for help
    - unfortunately the current model can’t offer individual handling

One year of RNP Fraud Catalog

Trends

- Obvious
  - News
  - Air France, Isabella Nardoni, Santa Catarina and other cases
  - Cada vez mais rápido: 24 horas
    - Air France plane disappearedon 1st June, first message received on 2nd June
- Messages demonstrate some previous data harvesting
  - No more:

    Hello john_doe@example.com!



One year of RNP Fraud Catalog

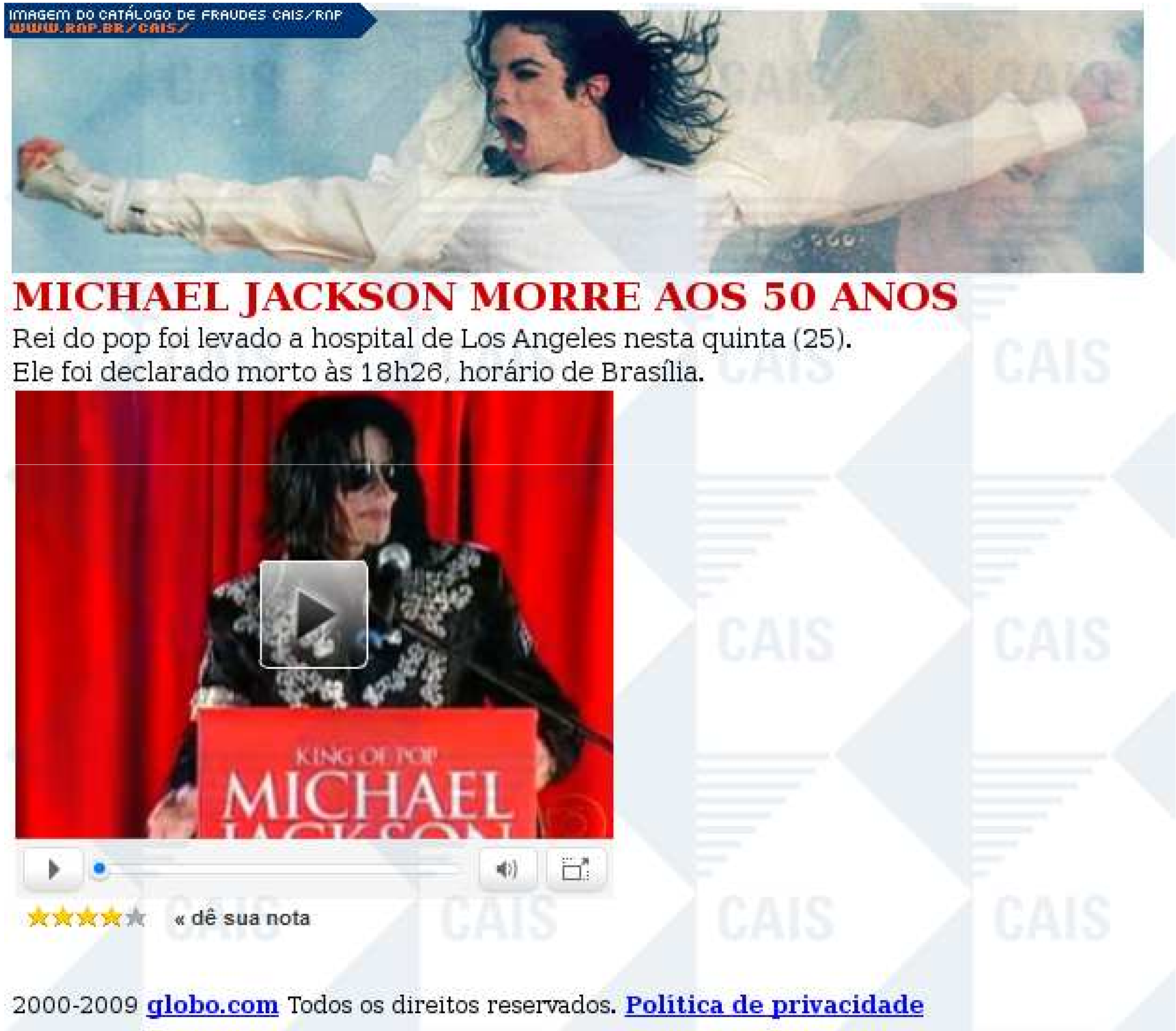


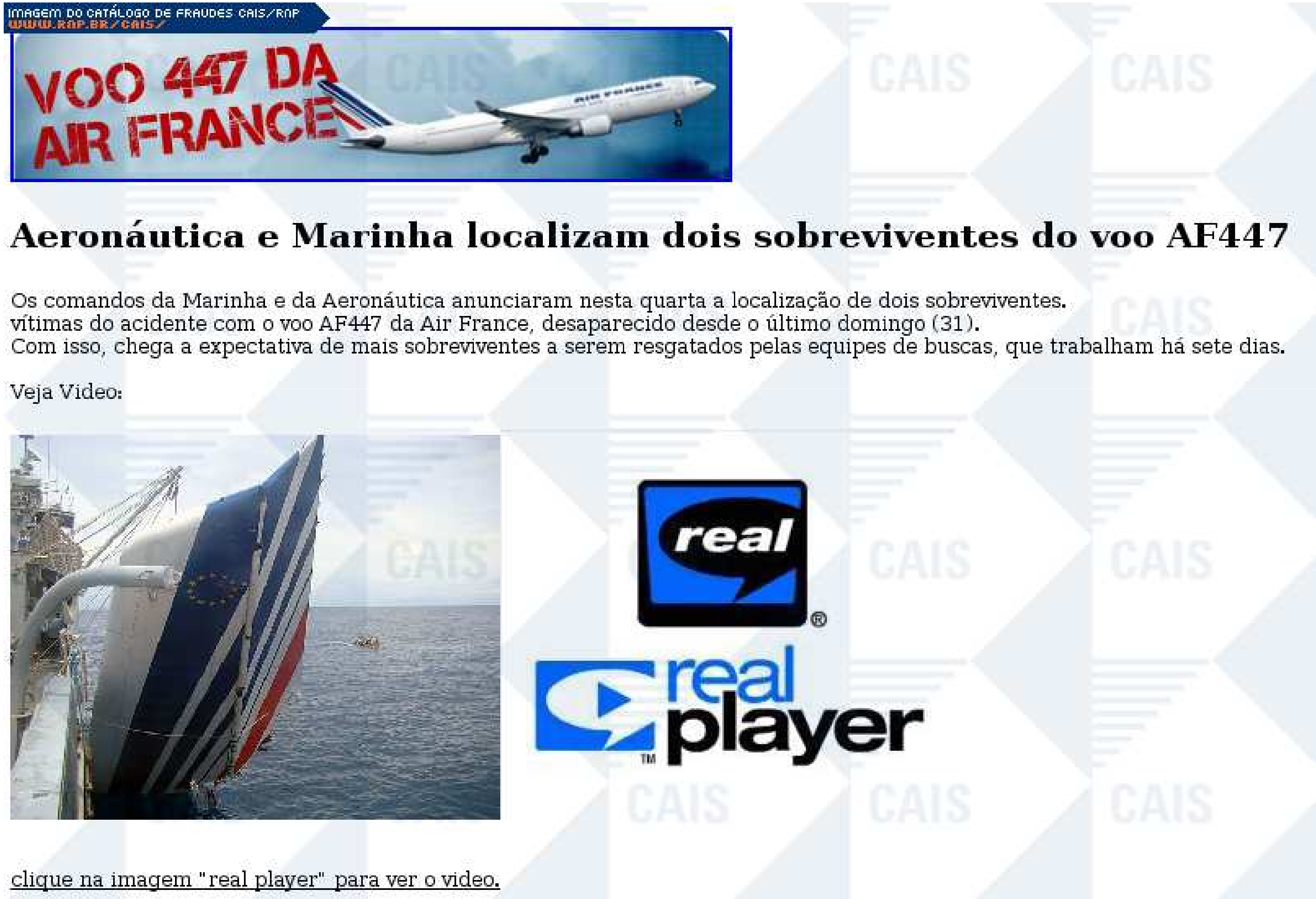
IMAGEM DO CATÁLOGO DE FRAUDES CAIS/RNP
WWW.RNP.BR/CAIS/

MICHAEL JACKSON MORRE AOS 50 ANOS

Rei do pop foi levado a hospital de Los Angeles nesta quinta (25).
Ele foi declarado morto às 18h26, horário de Brasília.

2000-2009 globo.com Todos os direitos reservados. Política de privacidade

One year of RNP Fraud Catalog



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.

One year of RNP Fraud Catalog

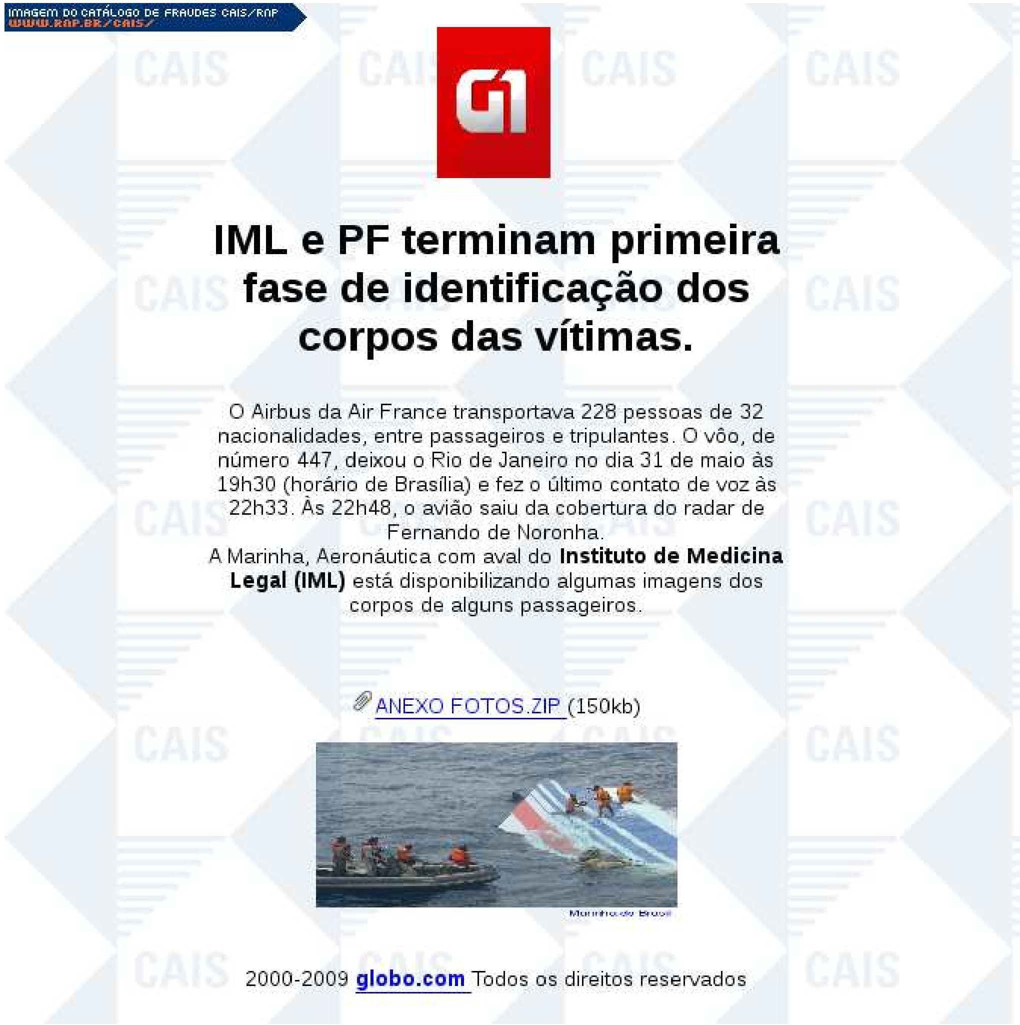


IMAGEM DO CATÁLOGO DE FRAUDES CAIS/RNP
WWW.RNP.BR/CAIS/

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 vôo, 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)

Marinha do Brasil

2000-2009 **globo.com** Todos os direitos reservados

One year of RNP Fraud Catalog

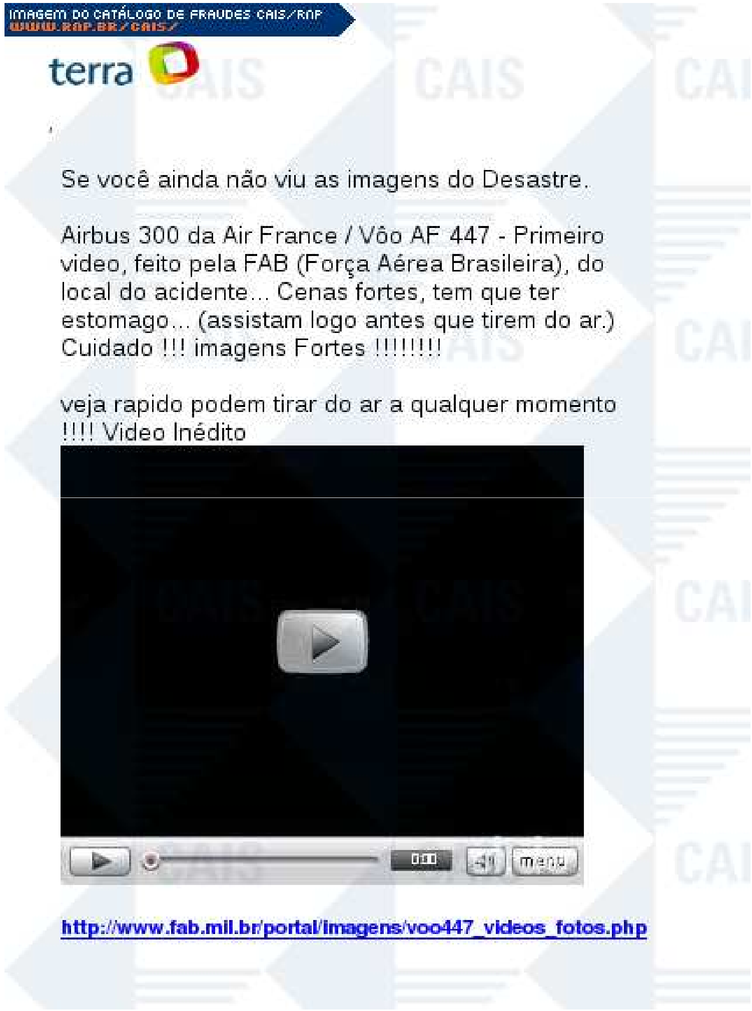


IMAGEM DO CATÁLOGO DE FRAUDES CAIS/RNP
WWW.RNP.BR/CAIS/

Se você ainda não viu as imagens do Desastre.

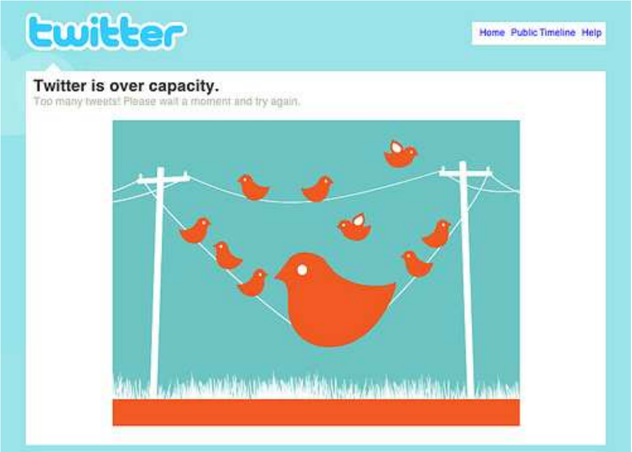
Airbus 300 da Air France / Vôo AF 447 - Primeiro video, feito pela FAB (Força Aérea Brasileira), do local do acidente... Cenas fortes, tem que ter estomago... (assistam logo antes que tirem do ar.) Cuidado !!! imagens Fortes !!!!!!!!

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

http://www.fab.mil.br/portal/imagens/voo447_videos_fotos.php

Trends (2)

- Easier to recognize the behavior of the masses
  - The so called **Real Time Web**
    - Buzz word alert!
  - Google Zeitgeist and other stats published by search engines
  - Twitter
    - TweetTabs.com: real time data about trends in twits
  - Most read news, evey news site provide this info



Twitter is over capacity.

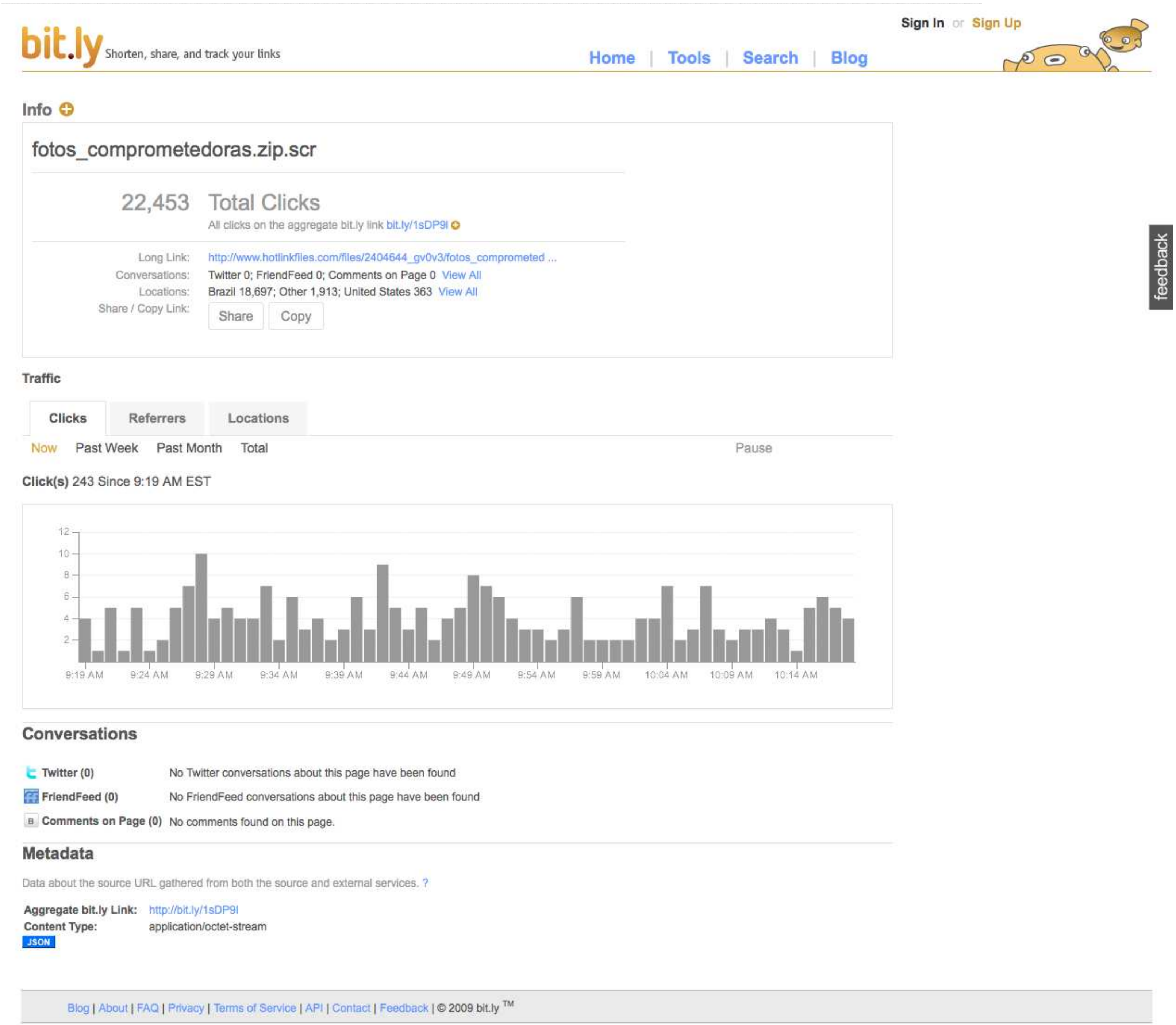
Too many tweets! Please wait a moment and try again.

Trends (3)

- Exploiting curiosity still works!
  - In 1 year, 7% of brazilians had sex with people met on web (Folha Online 18 june 2009)
    - Survey by Brazilian Ministry of Health
  - Betrayal photos, corpses from accidents, erotic / porn videos, supposed ex-girlfriends, famous cases with no solution, famous people who "died", etc.
- More personal computers sold in Brazil in the last few years
  - Every day thousands of people have their first contact with the Internet
    - **GREAT!** ***My bank already knows my e-mail address! Internet is really cool!***

Trends (4)

- URL shorteners are a HUGE problem!
    - Twitter and the 140 characters made things worse
    - bit.ly, TinyURL, is.gd, migre.me (Brazil)
        - A great number of providers of this kind of service
        - Malware festival
        - bit.ly, tinyurl are responsible
            - no cross-reference between shorteners
            - abuse handling, etc.
    - obscure shorteners
    - URL Shorteners: Which Shortening Service Should You Use?
      http://searchengineland.com/analysis-which-url-shortening-service-should-you-use-17204



bit.ly Shorten, share, and track your links
Sign In or Sign Up
Home | Tools | Search | Blog
feedback

Info

fotos_comprometedoras.zip.scr

22,453 Total Clicks

All clicks on the aggregate bit.ly link bit.ly/1sDP9l

Long Link:	http://www.hotlinkfiles.com/files/2404644_gv0v3/fotos_comprometed ...
Conversations:	Twitter 0; FriendFeed 0; Comments on Page 0 View All
Locations:	Brazil 18,697; Other 1,913; United States 363 View All
Share / Copy Link:	Share Copy

Traffic

Click(s) 243 Since 9:19 AM EST

Conversations

Twitter (0)	No Twitter conversations about this page have been found
FriendFeed (0)	No FriendFeed conversations about this page have been found
Comments on Page (0)	No comments found on this page.

Metadata

Data about the source URL gathered from both the source and external services. ?

Aggregate bit.ly Link:	http://bit.ly/1sDP9l
Content Type:	application/octet-stream

JSON

Blog | About | FAQ | Privacy | Terms of Service | API | Contact | Feedback | © 2009 bit.ly ™

One year of RNP Fraud Catalog

CAIS

Next steps

- More info (FAQ)
- Estats
- Better graphic interface
- Web submissions
- Better search for samples
- RSS Feed

Contato

Brazilian Academic and Research Network CSIRT

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

Ronaldo Castro de Vasconcellos
ronaldo@cais.rnp.br