17º WRNP

Workshop RNP

30 | 31 MAIO

SALVADOR | BA

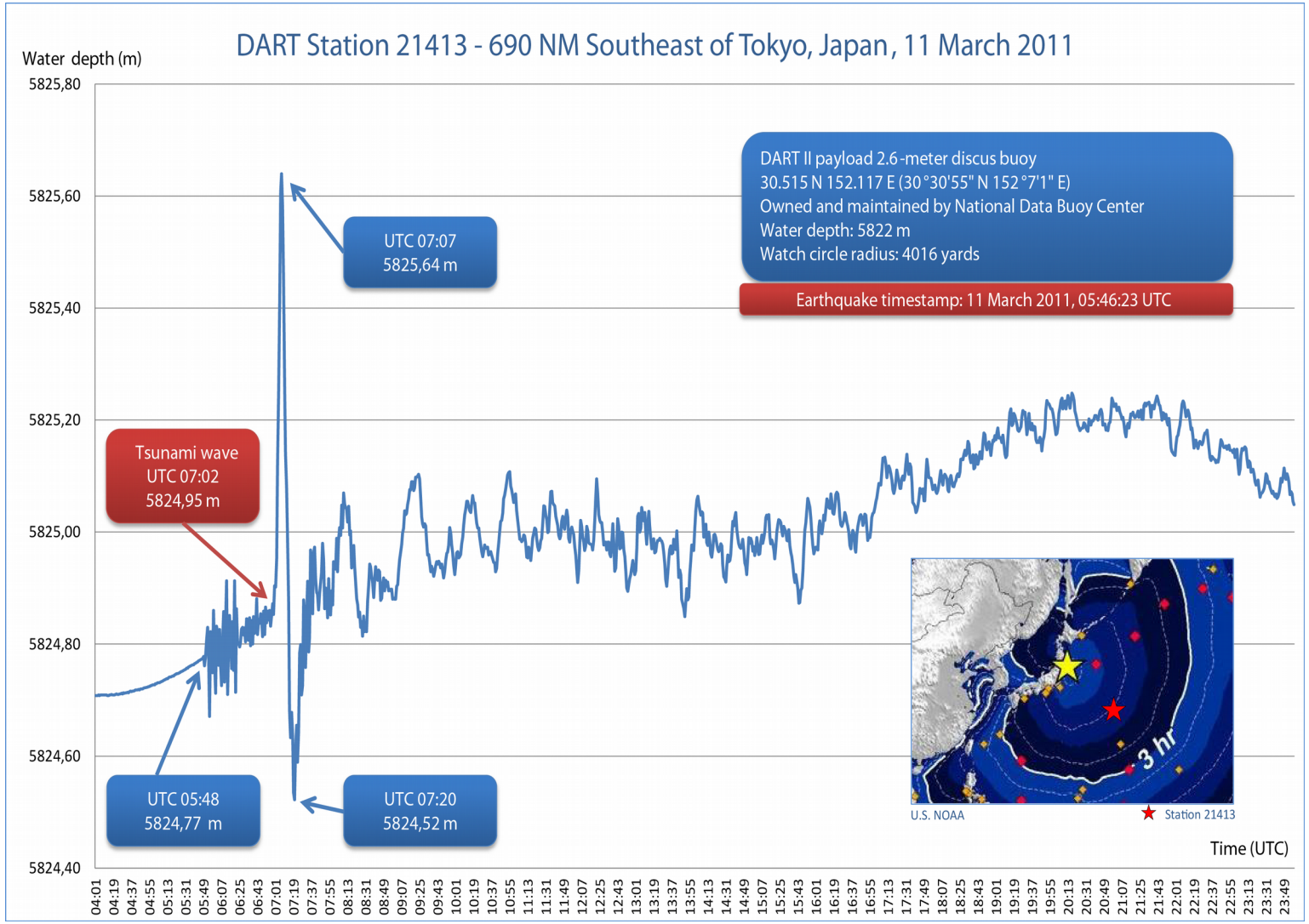
GT – EWS: Mecanismos para um Sistema de Alerta Antecipado

Daniel Macêdo Batista

USP

RNP

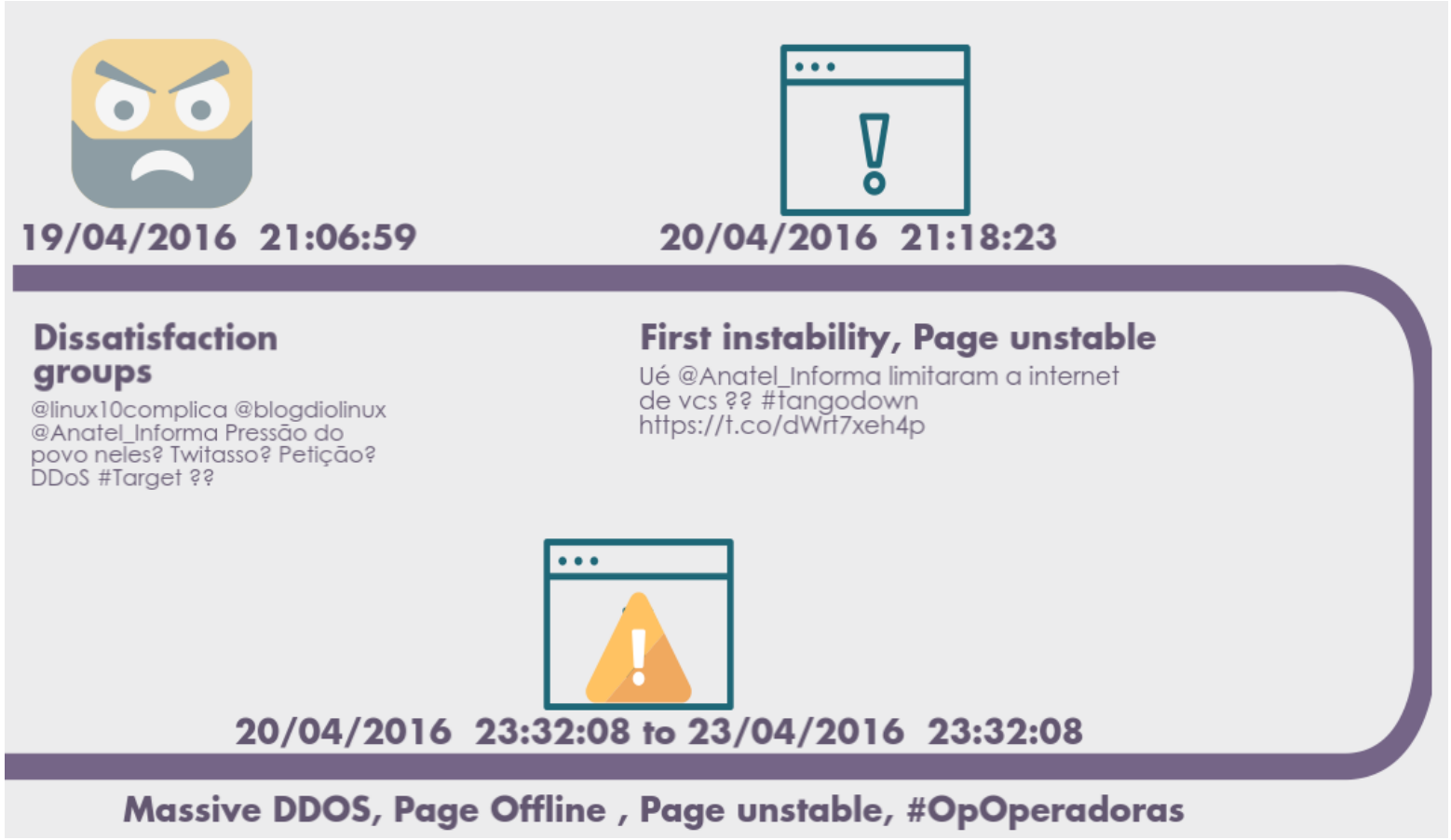
Motivação



Objetivo principal

- **Rápida disseminação de alertas** com o intuito de **proteção proativa** e/ou **rápida reação**
  - Orquestração de ataques (DDoS)
  - Desfiguração de sites
  - Códigos de exploração (*exploits*)
  - Vazamento de dados
  - Foco em redes sociais

- **[Fase 2]**: Piloto de um EWS a ser utilizado pelo CAIS da RNP auxiliando nas atividades de detecção e respostas a incidentes



Parceiros e equipe de desenvolvimento

- Daniel Macêdo Batista (USP) – Coordenador
- Rodrigo Campiolo (UTFPR) – Coordenador adjunto
- Luiz dos Santos (UTFPR) – Coordenador adjunto
- Wagner Monteverde (UTFPR) – Assistente 1 (Gerente de projeto)
- Thiago Vieira (UFSCar) – Assistente 2 (Desenvolvedor)
- Marlon Antonio (UTFPR) – Assistente 2 (Desenvolvedor)
- Éder Ferreira (UTFPR) – Assistente 3 (Desenvolvedor)

- **Parceiros para testes do piloto**

CAIS
Centro de Atendimento a Incidentes de Segurança

POLÍCIA FEDERAL

USP
Universidade de São Paulo

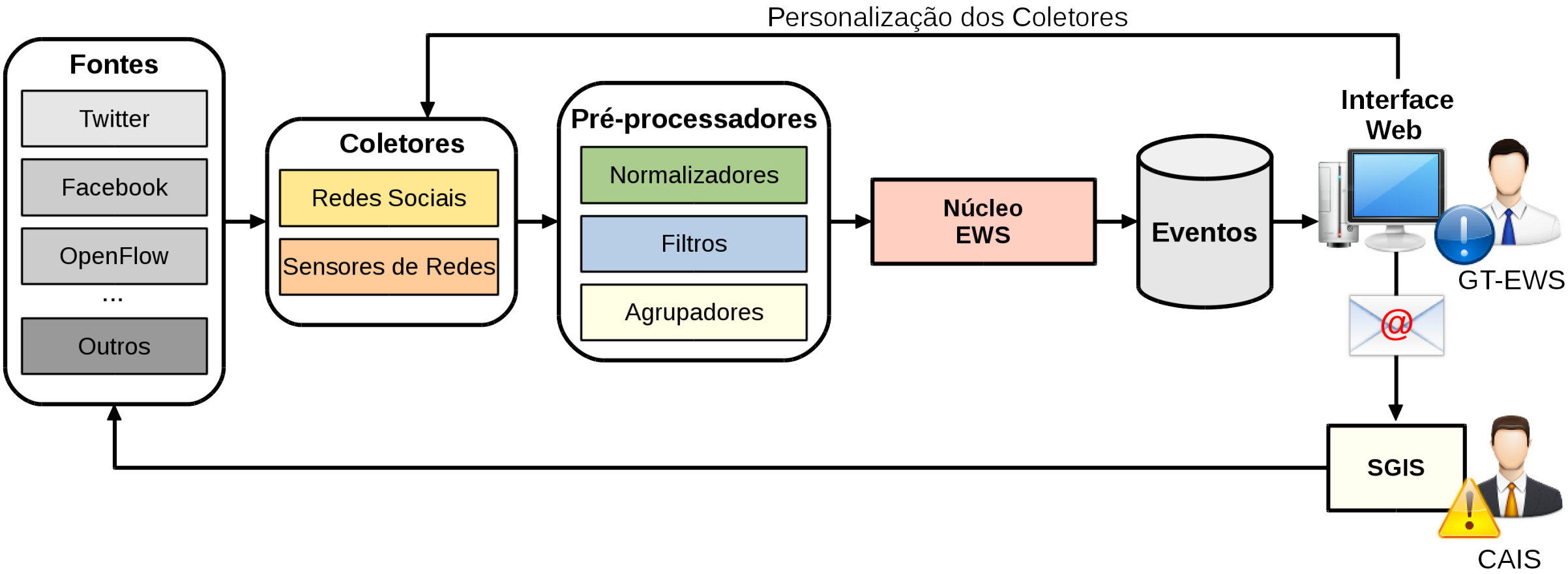
VIRTUTE SPIRITUS
1808

PRODAM

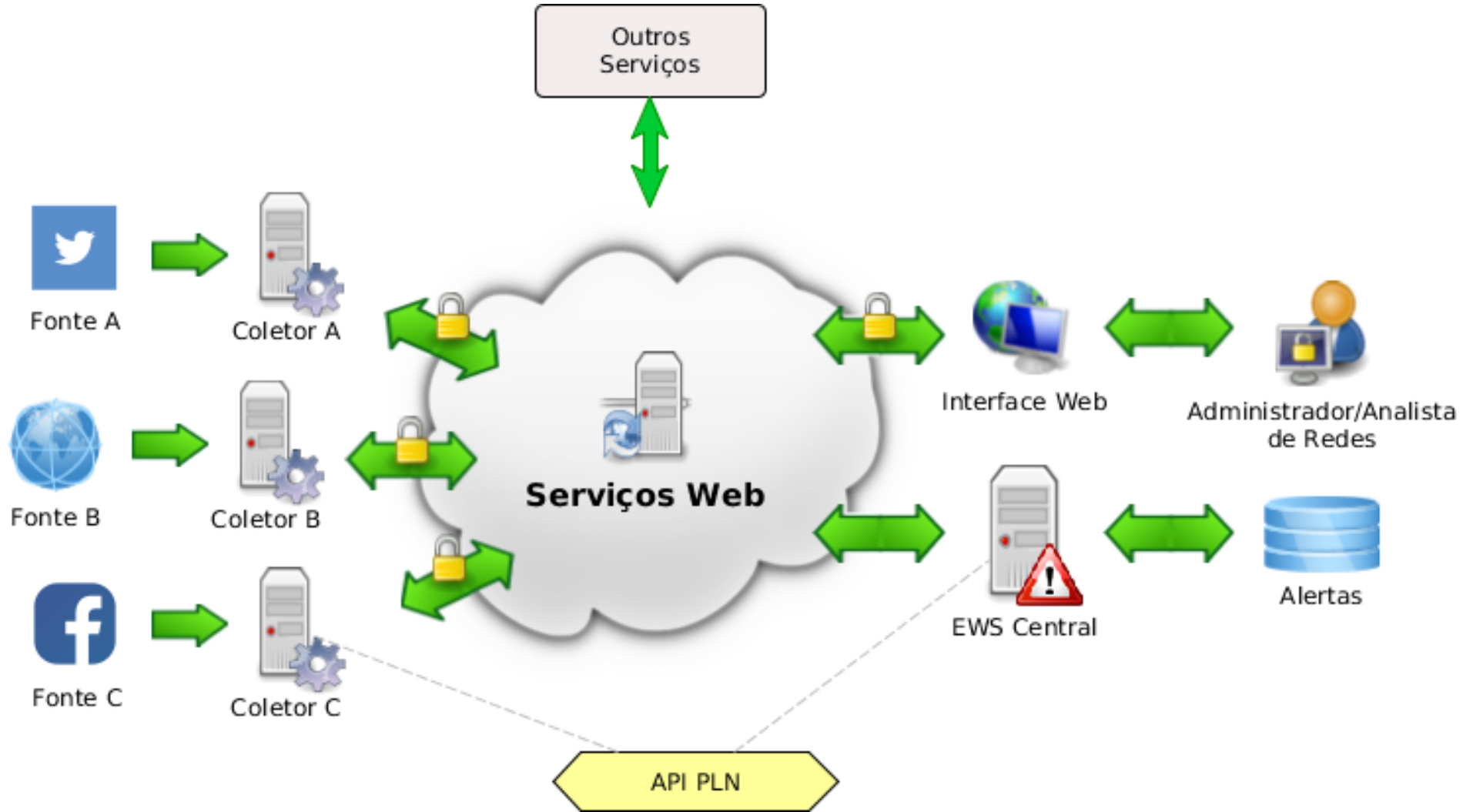
Público-alvo

- Administradores de rede
- Grupos de resposta a incidentes de segurança
- Professores e estudantes de pós-graduação que fazem pesquisa em segurança da informação, processamento de linguagem natural e redes sociais

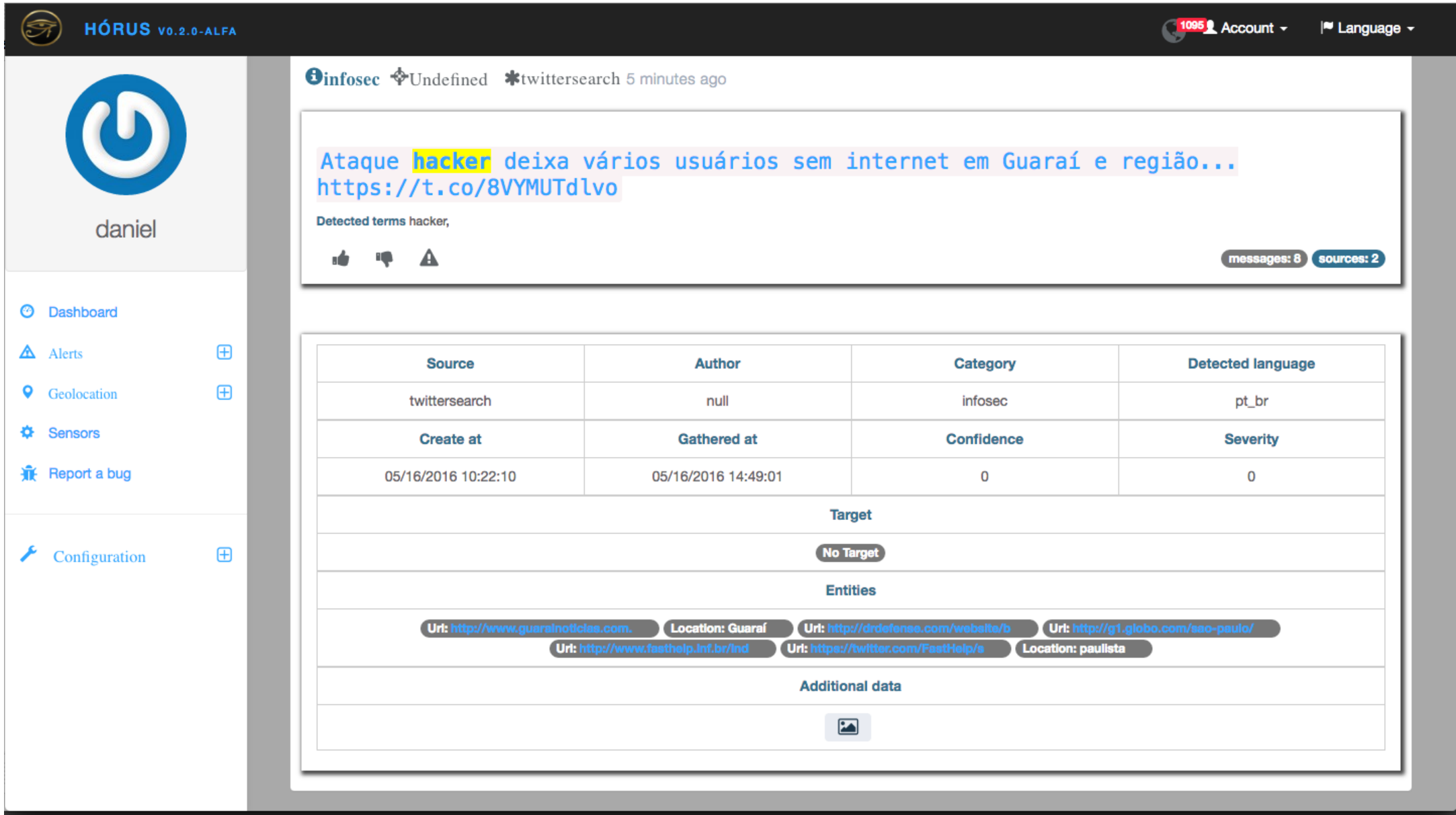
Fluxo de processamento



Arquitetura



Visão atual do sistema

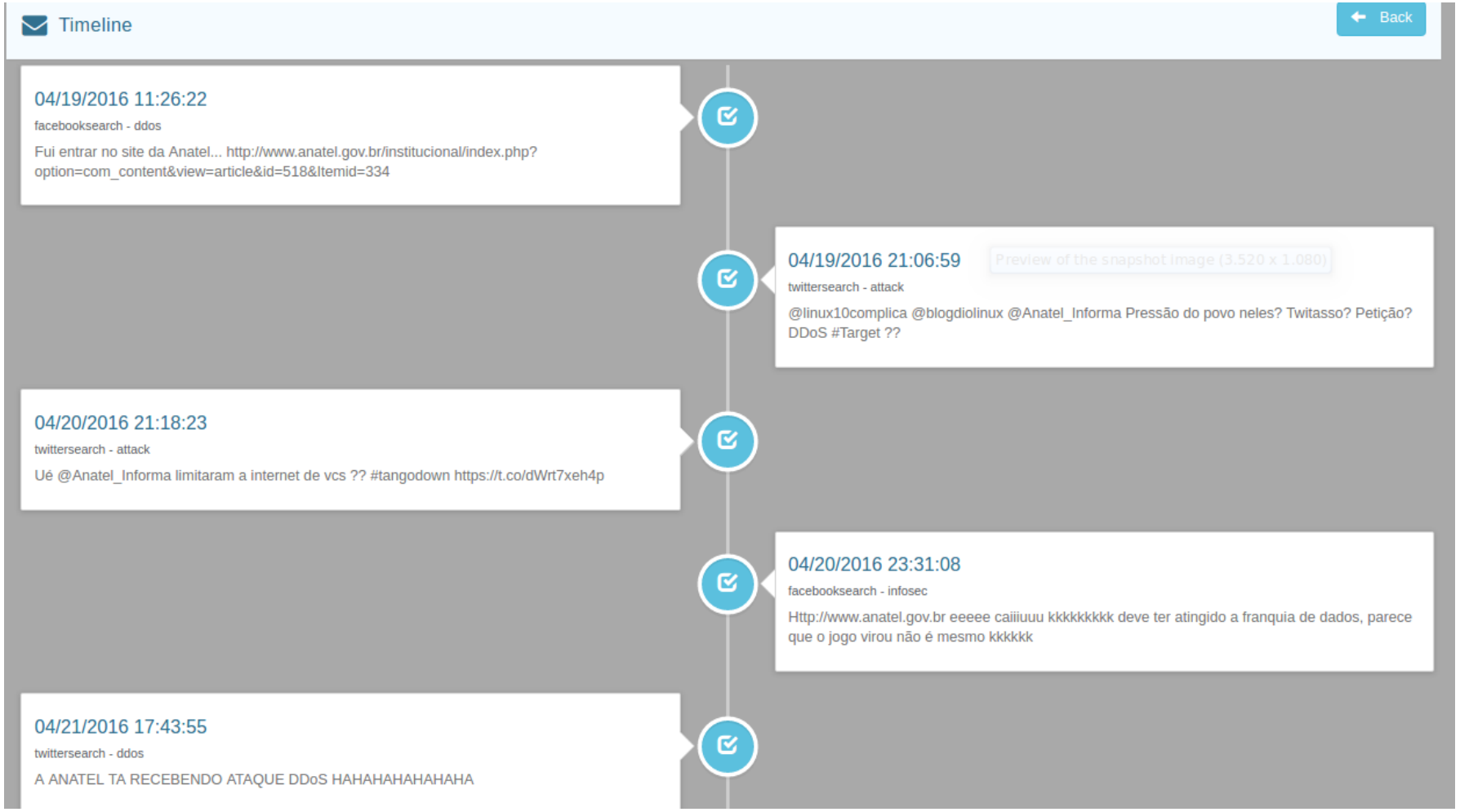


Principais resultados alcançados até o momento (1)

Nova interface gráfica e Padronização dos alertas por e-mail **Hórus**

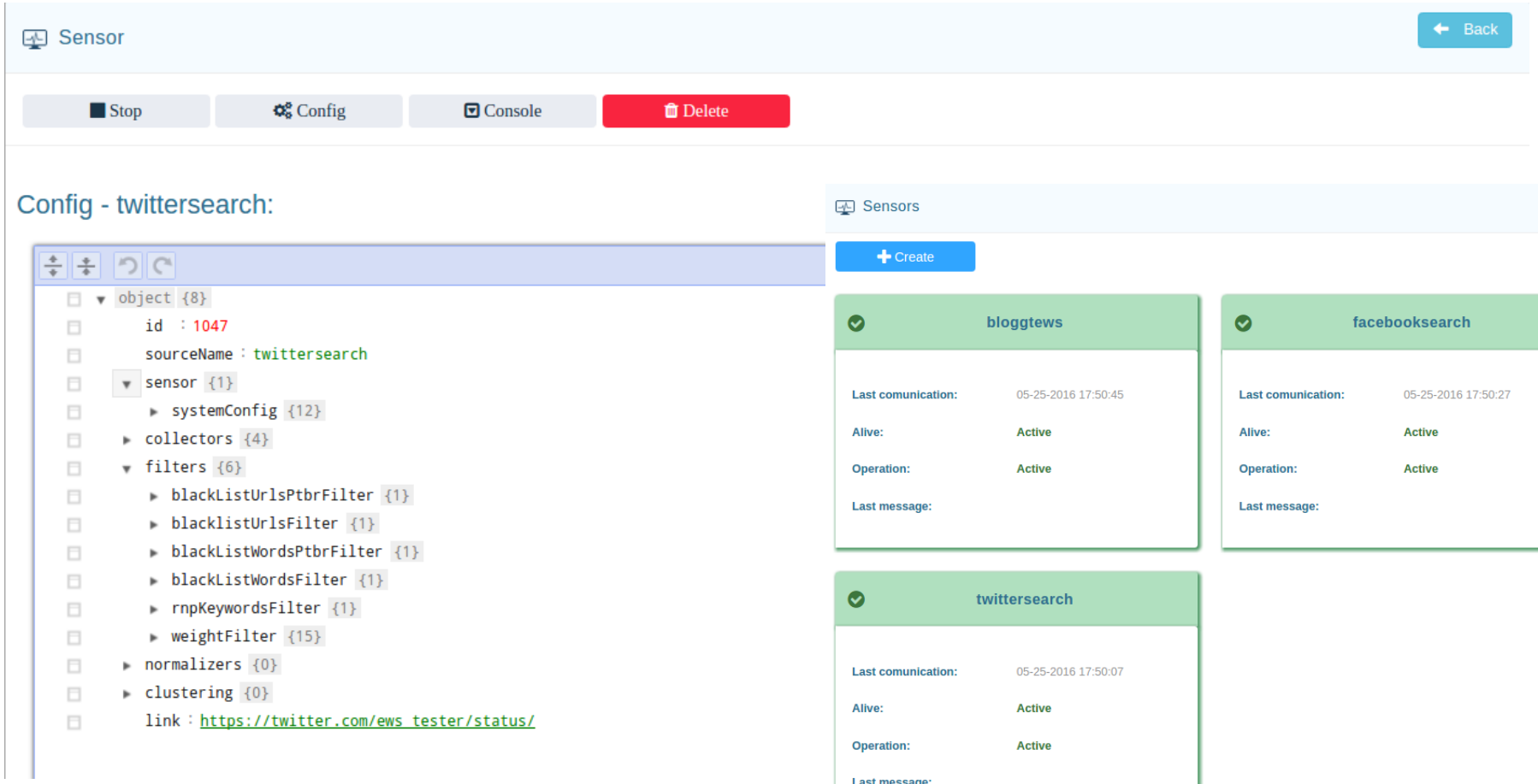
Principais resultados alcançados até o momento (2)

Linha do tempo



Principais resultados alcançados até o momento (3)

Gerenciamento remoto e framework de sensores



Principais resultados alcançados até o momento (4)

Alertas de DDoS

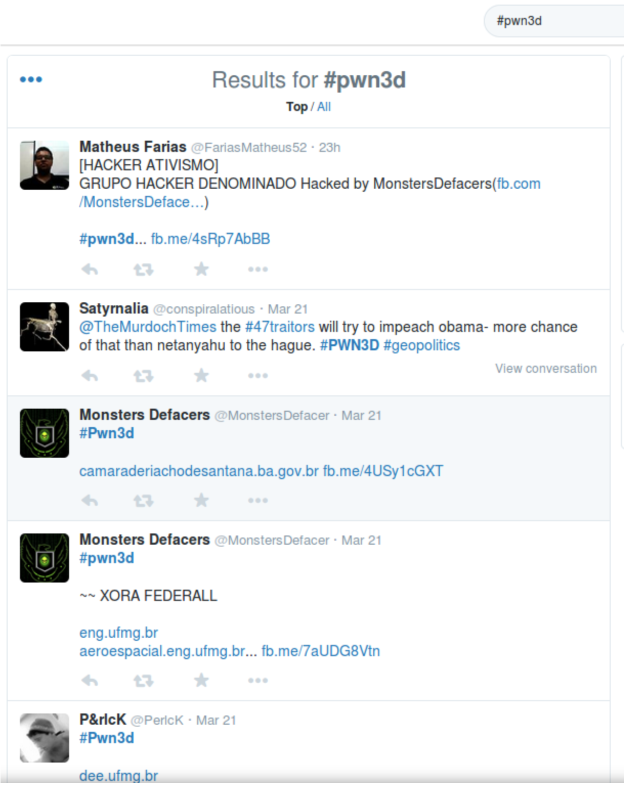
Ataque concluido com sucesso 10 horas offline https://t.co/rbpEiGCBn1 em breve no ar novamente , @LaFirmaSec @AnonBRNews @AsorTeam

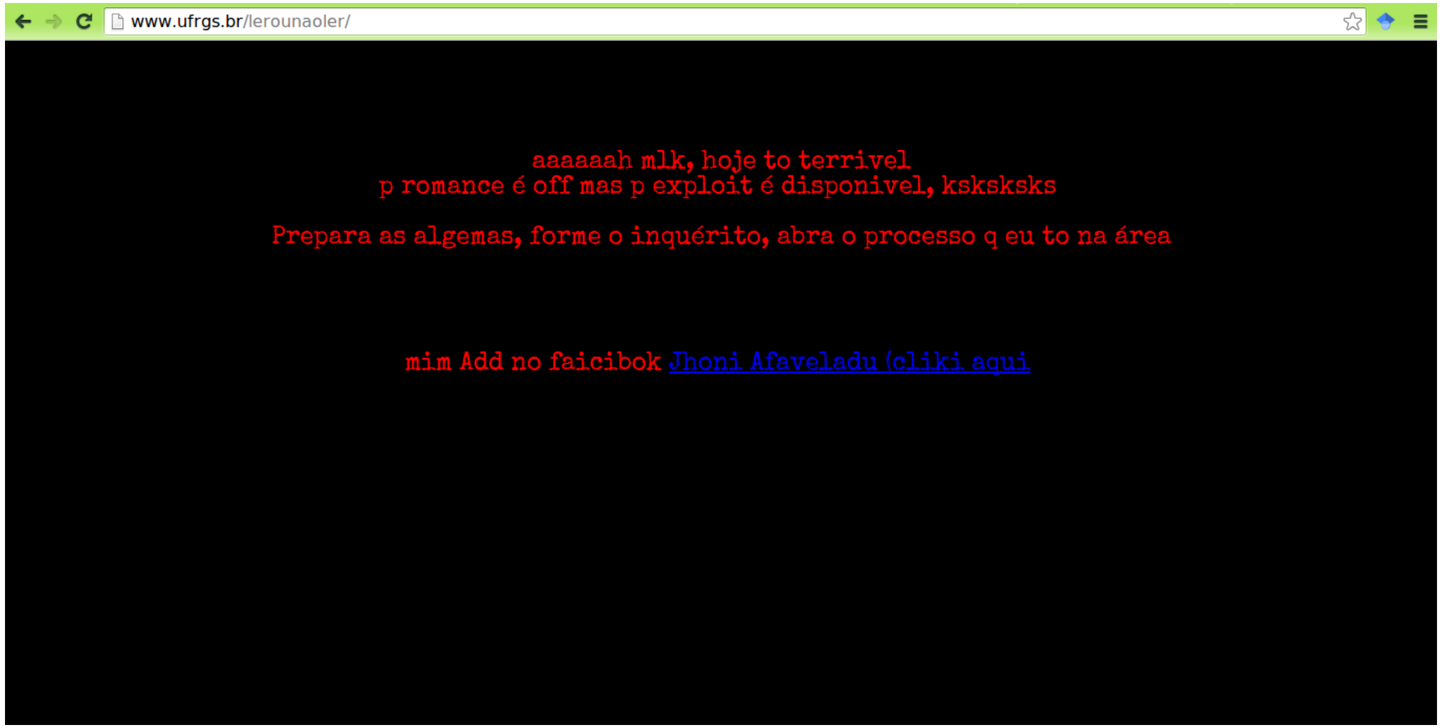
Source: Twitter Oct 24, 2015 11:27:04 PM - Oct 24, 2015 11:27:04 PM (0 Day) Tweets 1 Users 1

RT @HackersSkyForce: #TANGODOWN #ANONYMOUSBRASIL #Enem2015 #HACKERSSKYFORCE NÃO ACABEM COM A NOSSA EDUCAÇÃO! -------- SITE OFF https://t.co…

Principais resultados alcançados até o momento (5)

Alertas de desfiguração de páginas



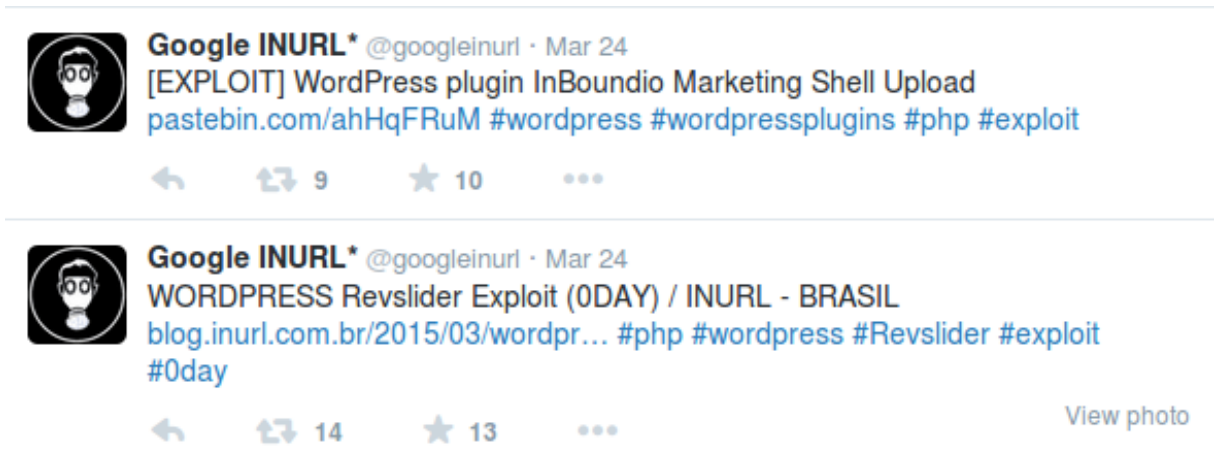


Principais resultados alcançados até o momento (6)

Alertas de *exploits*

medium May 17, 2015 12:11:36 AM - May 17, 2015 10:58:07 AM (0 Day) Tweets 4 Users 1

```
[ + ] Exploit 0day CMS HB 1.5?http://t.co/vIf76QV99Q #0day #exploit #php #web
#pentest #sec #vulner http://t.co/hkugXsD33K
```



Principais resultados alcançados até o momento (7)

Alertas de vazamento de dados

Source: Facebook Oct 6, 2015 12:11:00 AM - Oct 6, 2015 12:11:00 AM (0 Day) Posts 1 Users 1

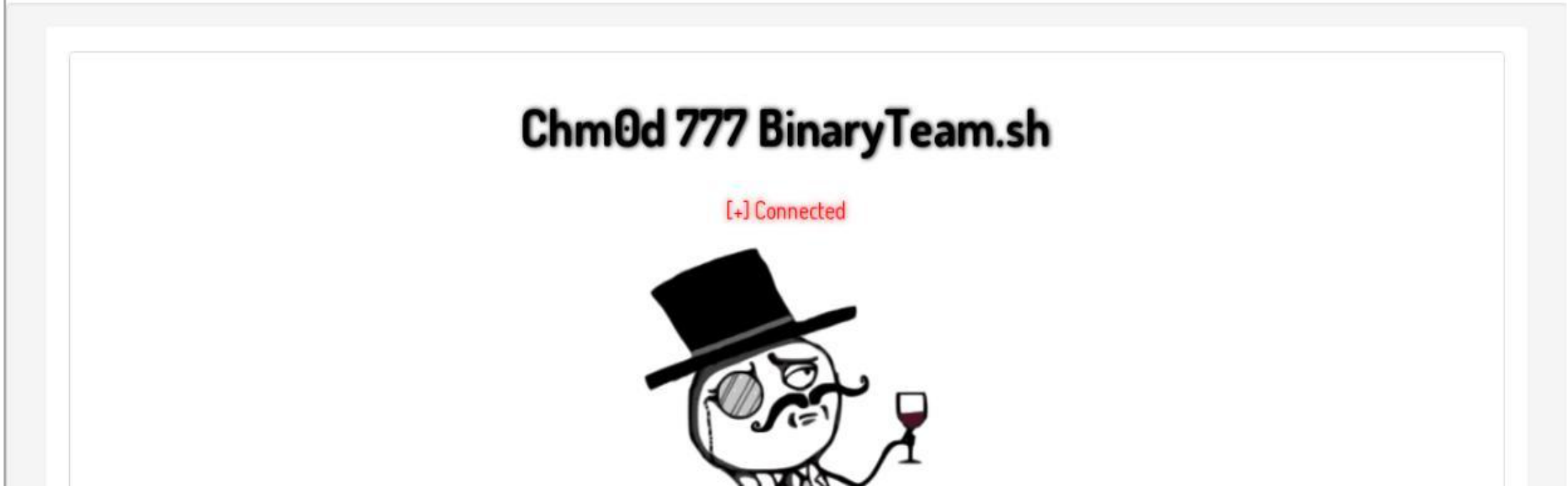
Como prometido no post anterior!??Relatórios de 2003 à 2015 da Aneel (Agência Nacional de Energia Elétrica)??Download aqui: https://mega.nz/#!RwxhQLqA!bfiSQSYFtf70badqk5r_W82emwtvel1BRKQM7EKLhYY??#Anonymous #AntiSec ?ASOR Hack Team

Source: Facebook Aug 29, 2015 12:48:27 AM - Aug 29, 2015 12:48:27 AM (0 Day) Posts 1 Users 1

Como prometido no post anterior!??Database de 4 instituições governamentais do Brasil.??Procon São Paulo, PMERJ (Policia Militar do Estado do Rio de Janeiro), UFPR_(Universidade Federal do Paraná), SaúdeAM (Secretaria de Estado de Saúde do Amazonas).??Link para download: https://mega.nz/#!wg5SRSQB!o9oVFoWx3uzKvSHxNSHArV-C53qJjcHwUm-etP-HjnI??ASOR Hack Team?#Anonymous

Principais resultados alcançados até o momento (8)

Registro forense das atividades maliciosas



Principais resultados alcançados até o momento (9)

Outras funcionalidades:

- Visualização de dados georeferenciados
- Autenticação Oauth
- Gerenciamento de usuários

Componentes

- **"Do zero"**
  - Interface web
  - Ferramentas para monitoramento de redes sociais incluindo um framework para conexão de novas fontes de dados
  - Ferramentas para filtros de análise dependentes do domínio das palavras-chave
  - Núcleo do EWS
  - Módulo para processamento de linguagem natural
- **Adaptados**
  - API e serviço REST para registro de screenshot
- **Reutilizados *AS-IS***
  - Sistema operacional, servidor web, SGBD, interpretadores e compiladores diversos
  - APIs das redes sociais

Melhorias tecnológicas a serem ainda desenvolvidas

- Melhoria contínua da detecção para reduzir falsos positivos
- Melhoria contínua do módulo de processamento de linguagem natural
- Melhoria contínua da interface gráfica (retorno dos parceiros)
- Implementação de um mecanismo de quarentena
- Inclusão do IRC como mais uma fonte de dados
- Integração com a CAFeExpresso

17º WRNP

Workshop RNP

- Contato: gtews@listas.rnp.br
- Sítio Web: https://gtews.ime.usp.br/