

GT – EWS: Mecanismos para um Sistema de Alerta Antecipado

Daniel Macêdo Batista

USP

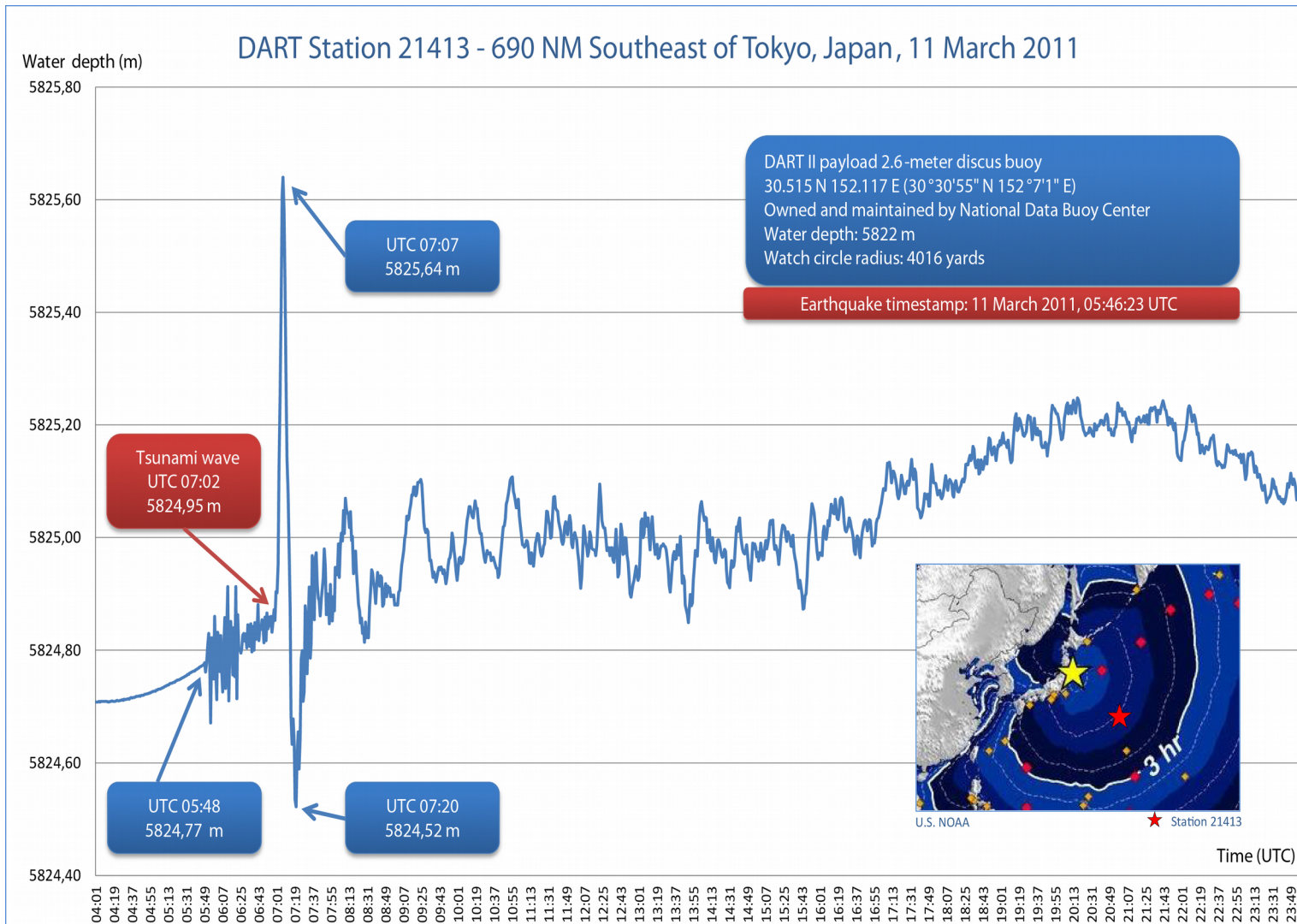
17º WIRNP

Workshop RNP

30 | 31 MAIO
SALVADOR | BA



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



19/04/2016 21:06:59

Dissatisfaction groups

@linux10complica @blogdiolinux
@Anatel_Informa Pressão do povo neles? Twitasso? Petição? DDoS #Target ??



20/04/2016 21:18:23

First instability, Page unstable

Ué @Anatel_Informa limitaram a internet de vcs ?? #tangodown
<https://t.co/dWrt7xeh4p>



20/04/2016 23:32:08 to 23/04/2016 23:32:08

Massive DDOS, Page Offline , Page unstable, #OpOperadoras

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**



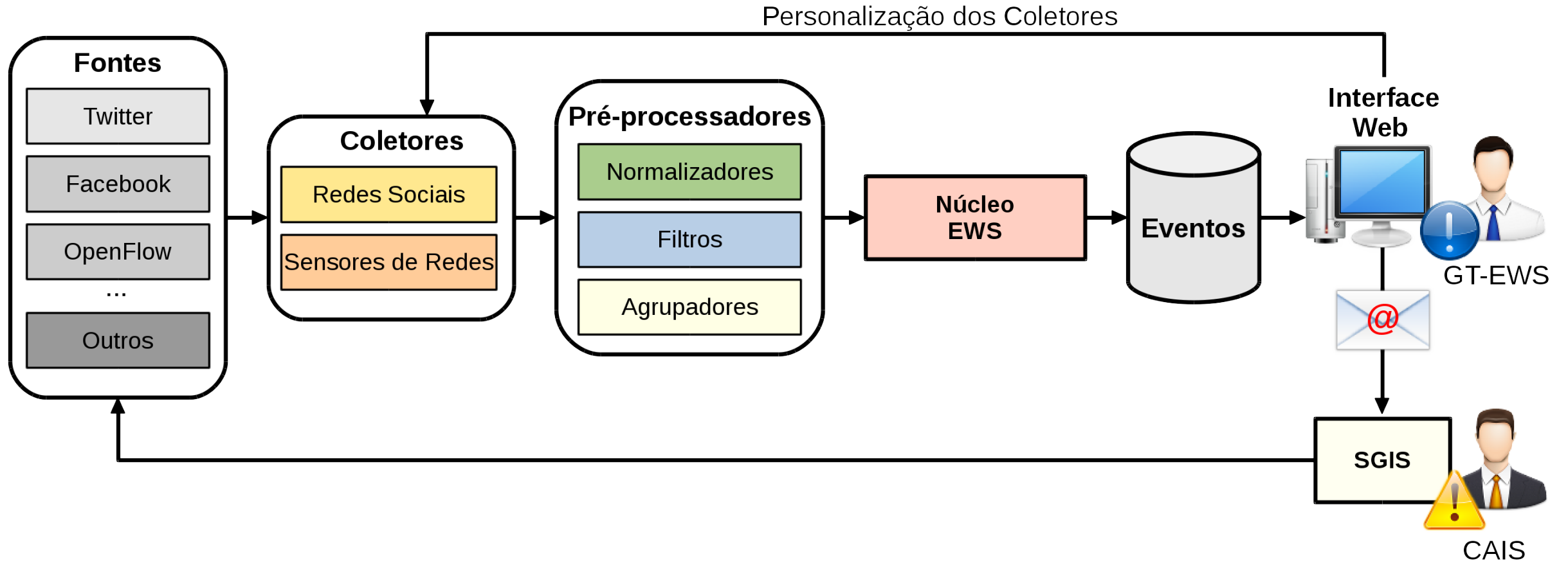
Centro de Atendimento a Incidentes de Segurança



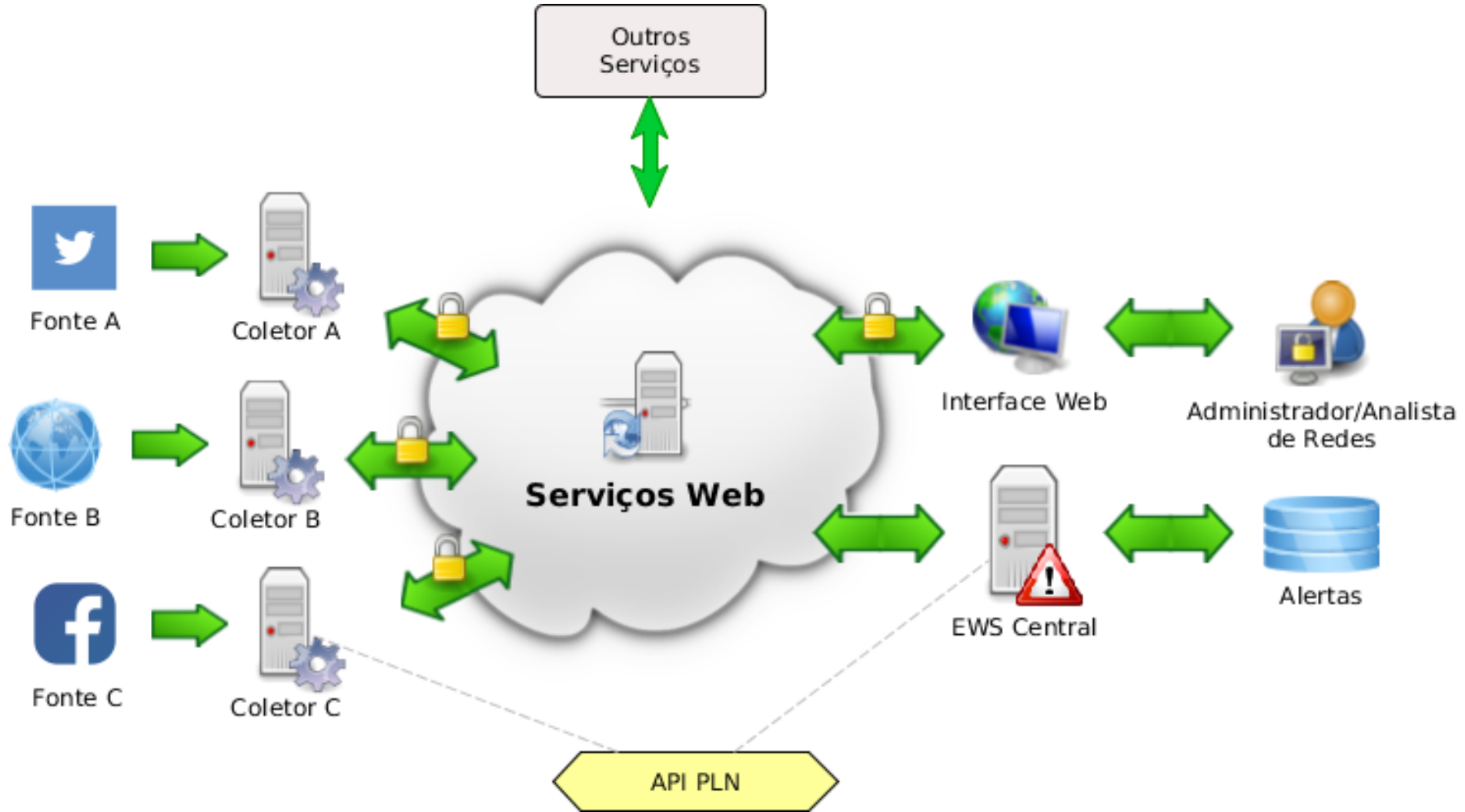
Público-alvo

- 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


HÓRUS V0.2.0-ALFA

1095 Account
Language



daniel

- [Dashboard](#)
- [Alerts](#)
- [Geolocation](#)
- [Sensors](#)
- [Report a bug](#)
- [Configuration](#)

infosec
Undefined
twittersearch 5 minutes ago

Ataque **hacker** deixa vários usuários sem internet em Guaraí e região...
<https://t.co/8VYMUTdlvo>

Detected terms hacker,

messages: 8 sources: 2

Source	Author	Category	Detected language
twittersearch	null	infosec	pt_br
Create at	Gathered at	Confidence	Severity
05/16/2016 10:22:10	05/16/2016 14:49:01	0	0

Target


No Target

Entities

Uri: <http://www.guarainoticias.com>
Location: Guaraí
Uri: <http://drdefensa.com/webalite/b>
Uri: <http://g1.globo.com/sao-paulo/>

Uri: <http://www.fasthelp.inf.br/ind>
Uri: <https://twitter.com/FastHelp/s>
Location: paulista

Additional data



Principais resultados alcançados até o momento (1)
 Nova interface gráfica e Padronização dos alertas por e-mail
Hórus

Alert Detail ← Back

Edit Send Notify Associated at | 2 Remove

attack http://www.stf.jus.br/portal/p twitterOlympic 32 minutes ago
 Agrupamento de alertas

Target: <https://t.co/RMOSGKmT8r> #EXPLOITED / <https://t.co/sD9RYyIHG8> #ThewikiboatBrazil @TheWikiBoatBR

Detected terms target, exploit,

👍 👎 ⚠️
Colaboração de usuários
messages: 2 source: 1

Source	Author	Category	Detected language
twitterOlympic	null	attack	pt_br
Create at	Gathered at	Confidence	Severity
05/25/2016 16:05:13	05/25/2016 16:10:54	0	0

Target Detecção de alvos

Uri: <http://www.stf.jus.br/portal/p>

Entities

Uri: <http://pastebin.com/75EnBsZQ>
User: TheWikiBoatBR
IP Address: 201.49.144.135
Uri: <http://www.stf.jus.br/portal/p>
IP Address: 104.20.64.56

Additional data

Extração de entidades

Principais resultados alcançados até o momento (2)

Linha do tempo

Timeline

← Back

04/19/2016 11:26:22
facebooksearch - ddos
Fui entrar no site da Anatel... http://www.anatel.gov.br/institucional/index.php?option=com_content&view=article&id=518&Itemid=334

04/19/2016 21:06:59 Preview of the snapshot image (3.520 x 1.080)
twittersearch - attack
@linux10complica @blogdiolinux @Anatel_Informa Pressão do povo neles? Twitasso? Petição? DDoS #Target ??

04/20/2016 21:18:23
twittersearch - attack
Uê @Anatel_Informa limitaram a internet de vcs ?? #tangodown <https://t.co/dWrt7xeh4p>

04/20/2016 23:31:08
facebooksearch - infosec
<Http://www.anatel.gov.br> eeeee caiiuuu kkkkkkkk deve ter atingido a franquia de dados, parece que o jogo virou não é mesmo kkkkkk

04/21/2016 17:43:55
twittersearch - ddos
A ANATEL TA RECEBENDO ATAQUE DDoS HAHHAHAHAHAHA

Principais resultados alcançados até o momento (3)

Gerenciamento remoto e framework de sensores

Sensor ← Back

Stop Config Console Delete

Config - twittersearch:

```

object {8}
├── id : 1047
├── sourceName : twittersearch
├── sensor {1}
│   ├── systemConfig {12}
│   ├── collectors {4}
│   └── filters {6}
│       ├── blacklistUrlsPtbrFilter {1}
│       ├── blacklistUrlsFilter {1}
│       ├── blacklistWordsPtbrFilter {1}
│       ├── blacklistWordsFilter {1}
│       ├── rnpKeywordsFilter {1}
│       └── weightFilter {15}
├── normalizers {0}
├── clustering {0}
└── link : https://twitter.com/ews_tester/status/
                    
```

Sensors ← Back

+ Create
Order by Name ▾

✔ blogtews

Last communication: 05-25-2016 17:50:45

Alive: Active

Operation: Active

Last message:

✔ facebooksearch

Last communication: 05-25-2016 17:50:27

Alive: Active

Operation: Active

Last message:

✔ twitterOlympic

Last communication: 05-25-2016 17:50:05

Alive: Active

Operation: Active

Last message:

✔ twittersearch

Last communication: 05-25-2016 17:50:07

Alive: Active

Operation: Active

Last message:

Principais resultados alcançados até o momento (4)

Alertas de DDoS

Ataque concluído 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 #HACKERSKYFORCE NÃO ACABEM COM A NOSSA EDUCAÇÃO! ----- SITE OFF <https://t.co...>

Principais resultados alcançados até o momento (5)

Alertas de desfiguração de páginas

#pwn3d

Results for #pwn3d
Top / All

Matheus Farias @FariasMatheus52 · 23h
[HACKER ATIVISMO]
GRUPO HACKER DENOMINADO Hacked by MonstersDefacers(fb.com /MonstersDeface...)
#pwn3d... fb.me/4sRp7AbBB

Satymalia @conspiratious · Mar 21
@TheMurdochTimes the #47traitors will try to impeach obama- more chance of that than netanyahu to the Hague. #PWN3D #geopolitics

Monsters Defacers @MonstersDefacer · Mar 21
#Pwn3d
camaraderiachodesantana.ba.gov.br fb.me/4USy1cGXT

Monsters Defacers @MonstersDefacer · Mar 21
#pwn3d
~~ XORA FEDERALL
eng.ufmg.br
aeroespacial.eng.ufmg.br... fb.me/7aUDG8Vtn

P&ricK @PericK · Mar 21
#Pwn3d
dee.ufmg.br

Monsters Defacers @MonstersDefacer · Mar 21
#Pwn3d
camaraderiachodesantana.ba.gov.br fb.me/4USy1cGXT

www.ufrgs.br/lerounaoler/

aaaaaah mlk, hoje to terrivel
p romance é off mas p exploit é disponivel, ksksksks

Prepara as algemas, forme o inquerito, abra o processo q eu to na área

mim Add no faicibok [Jhoni Afaveladu \(cliki aqui\)](#)

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



Google INURL* @googleinurl · Mar 24

[EXPLOIT] WordPress plugin InBoundio Marketing Shell Upload
pastebin.com/ahHqFRuM #wordpress #wordpressplugins #php #exploit

← ↻ 9 ★ 10 ...



Google INURL* @googleinurl · Mar 24

WORDPRESS Revslider Exploit (0DAY) / INURL - BRASIL
blog.inurl.com.br/2015/03/wordpr... #php #wordpress #Revslider #exploit #0day

← ↻ 14 ★ 13 ...

View photo

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/#!RwxhOLqA!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

Entities
Uri: http://www.tbqps.org.br/
Additional data


Chm0d 777 BinaryTeam.sh

[+] Connected



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 WIRNP

Workshop RNP

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



Ministério da
Defesa

Ministério da
Cultura

Ministério da
Saúde

Ministério da
Educação

Ministério da **Ciência,**
Tecnologia, Inovações e
Comunicações

GOVERNO FEDERAL