GT-EWS: Building a Cybersecurity Early Warning System based on Social Networks

Speaker:

Michael Stanton
Rede Nacional de Ensino e Pequisa – RNP
(Brazil's NREN)

Objective of GT-EWS

GT-EWS is a research and development workgroup supported by the Brazilian National Research and Educational Network (RNP), that aims to build an Early Warning System (EWS) to anticipate security events and incidents against network and computer systems located on the RNP infrastructure.

Team

USP (University of São Paulo)
Daniel Macêdo Batista

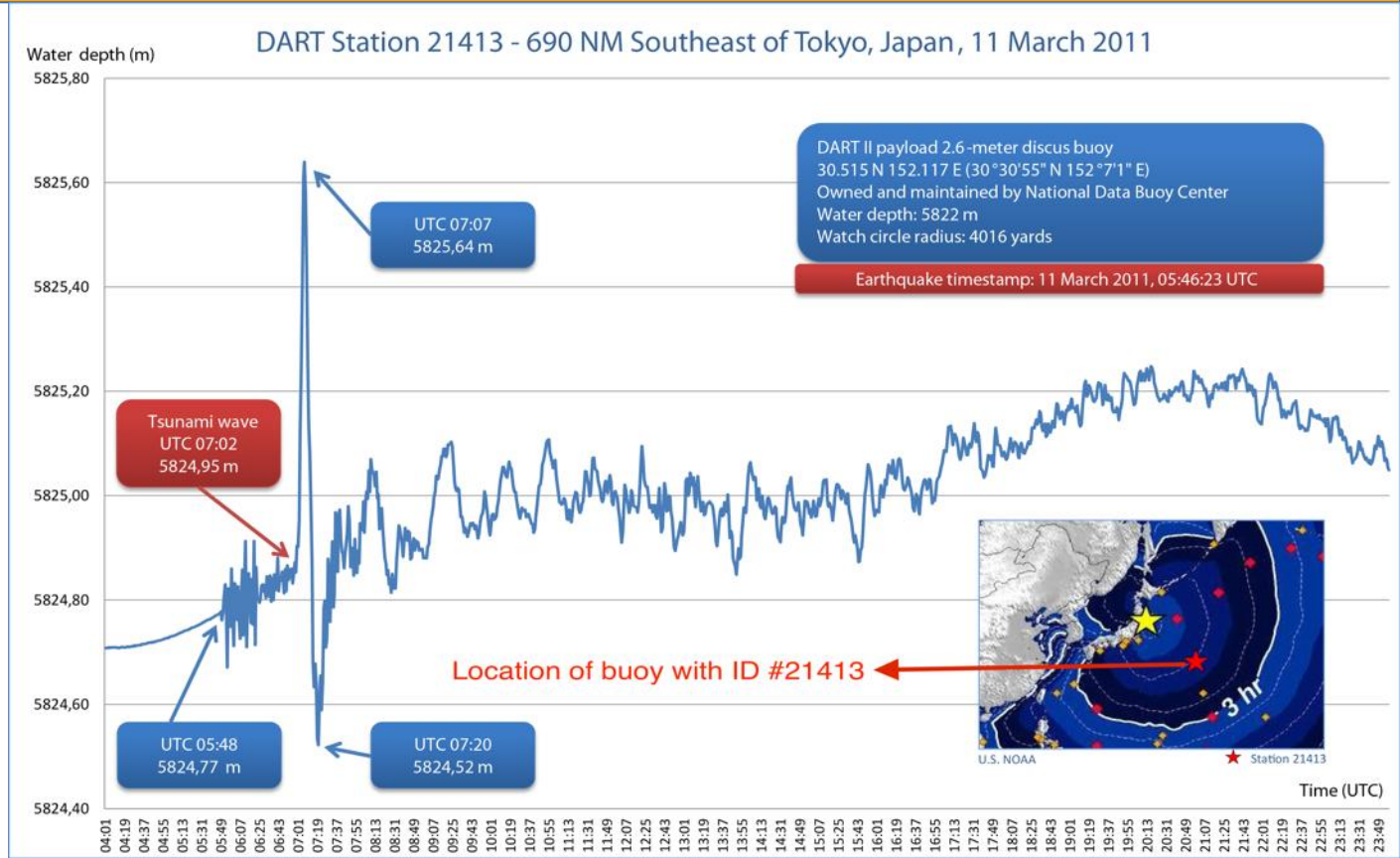
UTFPR (Federal University of Technology - Paraná)
Rodrigo Campiolo, Luiz Arthur Feitosa dos Santos, Wagner A. Monteverde, Marlon Fernandes Antonio, Éder Ferreira, Thiago Lima Vieira.

RNP (Brazilian National Research and Educational Network) Fausto Vetter

Introduction
and
Motivation

Traditional EWS

Example of the Tohoku tsunami, Japan, 2011



Security and early warning

Cybersecurity *Early Warning Systems*

- Early warning about new threats, vulnerabilities, DDoS orchestrations, attack rumours, etc.
- Fast dissemination of alerts
- Proactive protection or fast reaction

GT-EWS focuses on monitoring social networks (which is its main contribution)

Social networks

Social networks (Statistic Brain, 2015)

- Facebook: 1.3 billions of users
- Twitter: 58 millions of messages per day
- Google+: 300 millions of active users per month

As demonstrated in previous work, there are messages related to computer and network security in social networks

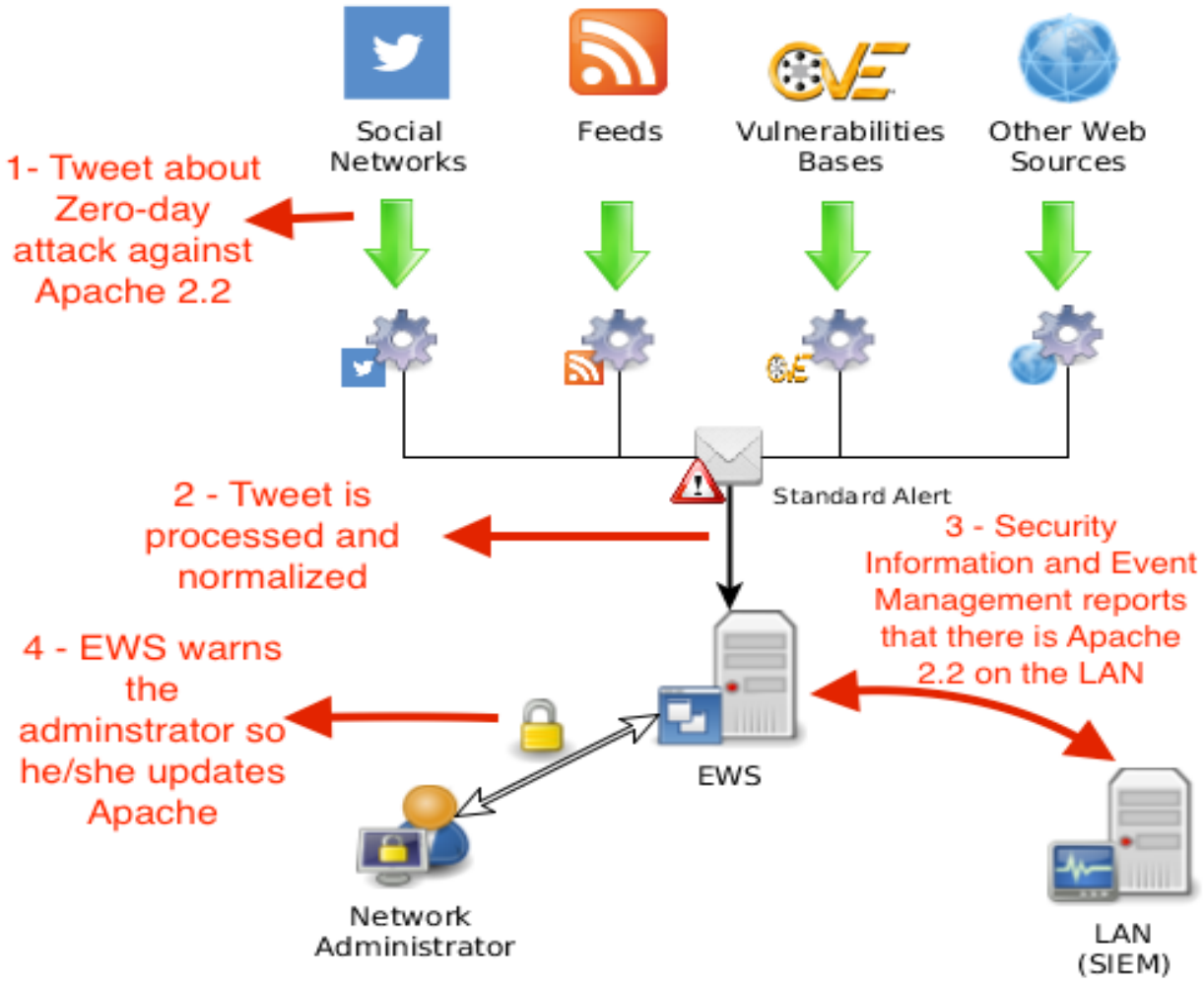
- CAMPIOLO, R.; SANTOS, L.A.F.; BATISTA, D. M.; GEROSA, M.A.. Evaluating the utilization of Twitter messages as a source of security alerts. In: Proceedings of the 28th Annual ACM SAC '13.p. 942-2.

EWS and social networks (1)

On 18th March 2014 user *AnonymousBR* tweeted:
"Operation Hacking World Cup DoS (Denial of Service)
DDos attack against government servers
Secrets revealed"
After that, several government web servers suffered DoS attacks

On 19th April 2016, several users retweeted:
"@Anatel_Informa Bring people pressure on them? Petition? DDoS #Target"
The following day, Anatel (Brazilian Telecommunications Agency) web servers suffered a massive DDoS attack and **4 days later**, sensitive data was publicly leaked

EWS and social networks (2)



EWS and social networks (3)

Challenges

- Big data processing: Textual data
- Unstructured data sources
  - Facebook, Twitter, etc

Problem

- How to search and prioritize security alerts/threats from unstructured data?

EWS and social networks (4)

Examples of false positives

EUobserver @euobs · 8h

#Thalys gun attack raises questions on security - euobserver.com/justice/129964

IRC #anonops - Would anyone know the port to do a ddos attack on the sky to shut down the rain service?

It is important to understand the context, not just the words

Our proposal: GT-EWS

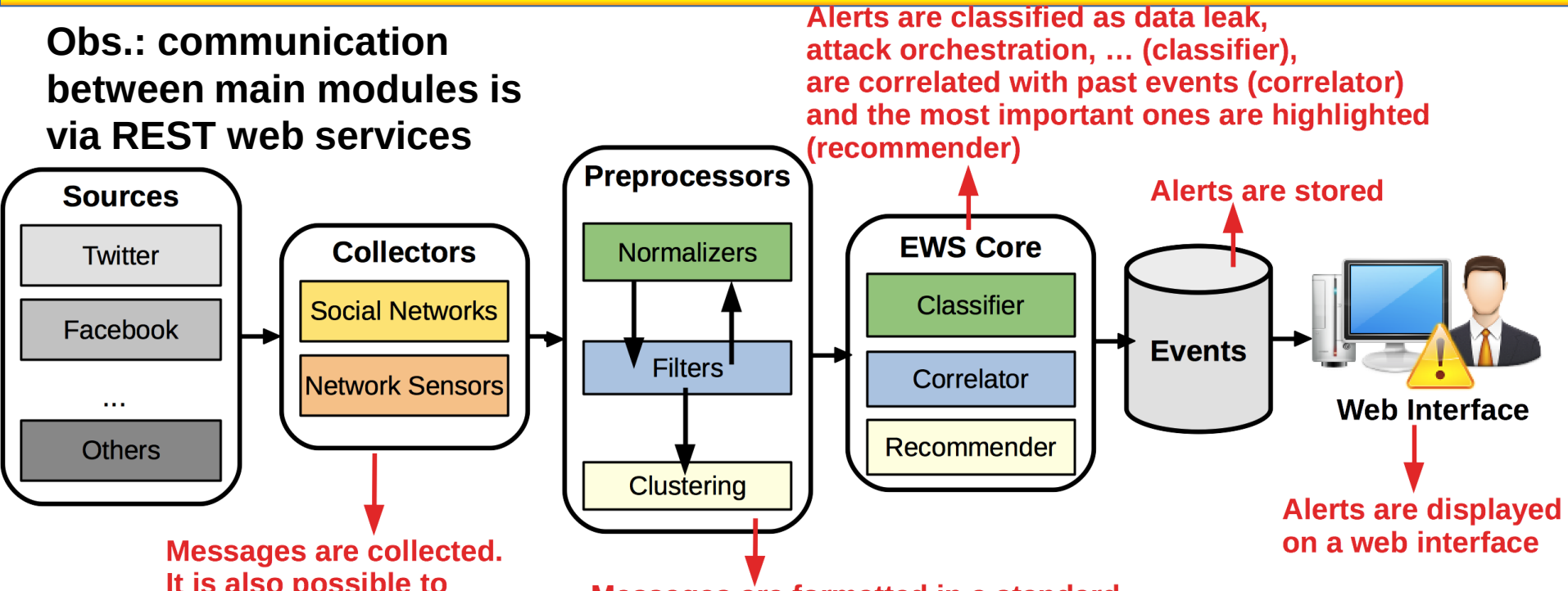
Main techniques

Techniques which we use to process alerts in textual data:

- Information Retrieval (IR)
- Clustering and classification
- Natural Language Processing (NLP)
- Heuristics
- Recommender Systems

Processing flow

Obs.: communication between main modules is via REST web services



Alerts are classified as data leak, attack orchestration, … (classifier), are correlated with past events (correlator) and the most important ones are highlighted (recommender)

Alerts are stored

Messages are collected. It is also possible to collect logs from traditional network sensors

Messages are formatted in a standard format (normalizers), considering the rules defined by the administrator (filters) and similar messages are joined as 1 alert (clustering)

Alerts are displayed on a web interface

Web Interface (1)

attack http://www.stf.jus.br/portal/p twitterOlympic 13 days ago

target: https://t.co/RMOSGKmT8r #exploitED / https://t.co/sD9RYyIHG8 #ThewikiboatBrazil @TheWikiBoatBR

Detected terms target, exploit,

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

Url: http://www.stf.jus.br/portal/p

Entities

Url: http://pastebin.com/75EnBaZQ | User: TheWikiBoatBR | IP Address: 201.49.144.135 | Url: http://www.stf.jus.br/portal/p | IP Address: 104.20.64.56

Additional data

Web Interface (2)

Edit | Send | Notify | Associated at | 2

attack http://www.stf.jus.br/portal/p twitterOlympic 13 days ago

The system detected 2 similar posts

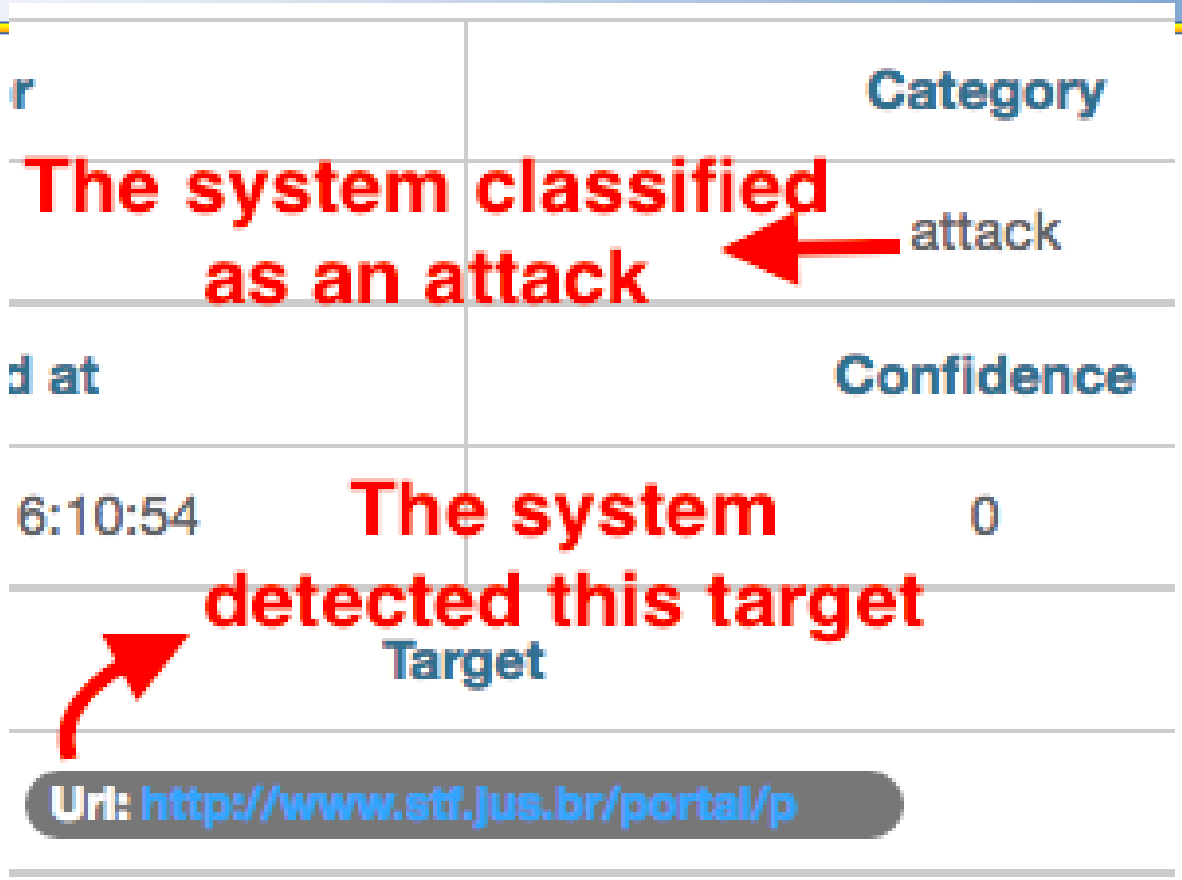
target: https://t.co/RMOSGKmT8r #exploitED / https://
#ThewikiboatBrazil @TheWikiBoatBR

The system highlighted the main terms

Detected terms target, exploit,

The system allows collaboration

Web Interface (3)



Web Interface (4)

Entities

Url: http://pastebin.com/75EnBsZQ | User: TheWikiBoatBR | IP Address: 201.49.144.135

The system extracted several entities

The system saved screenshots from the URLs

Additional data

Other features

- Remote management of collectors (easy to add new rules)
- Standard alert format
- Sensor template (easy to add new collectors)
- Visualisation of geographic data and timeline

Collectors deployed

FacebookSearch: monitoring hackers pages, hackers groups and suspected profiles

TwitterSearch: monitoring tweets about infrastructure of RNP and suspected profiles

TwitterOlympic: monitoring tweets related to the Olympics security and cyber security

Future: IRC, blogs and forums

Some results

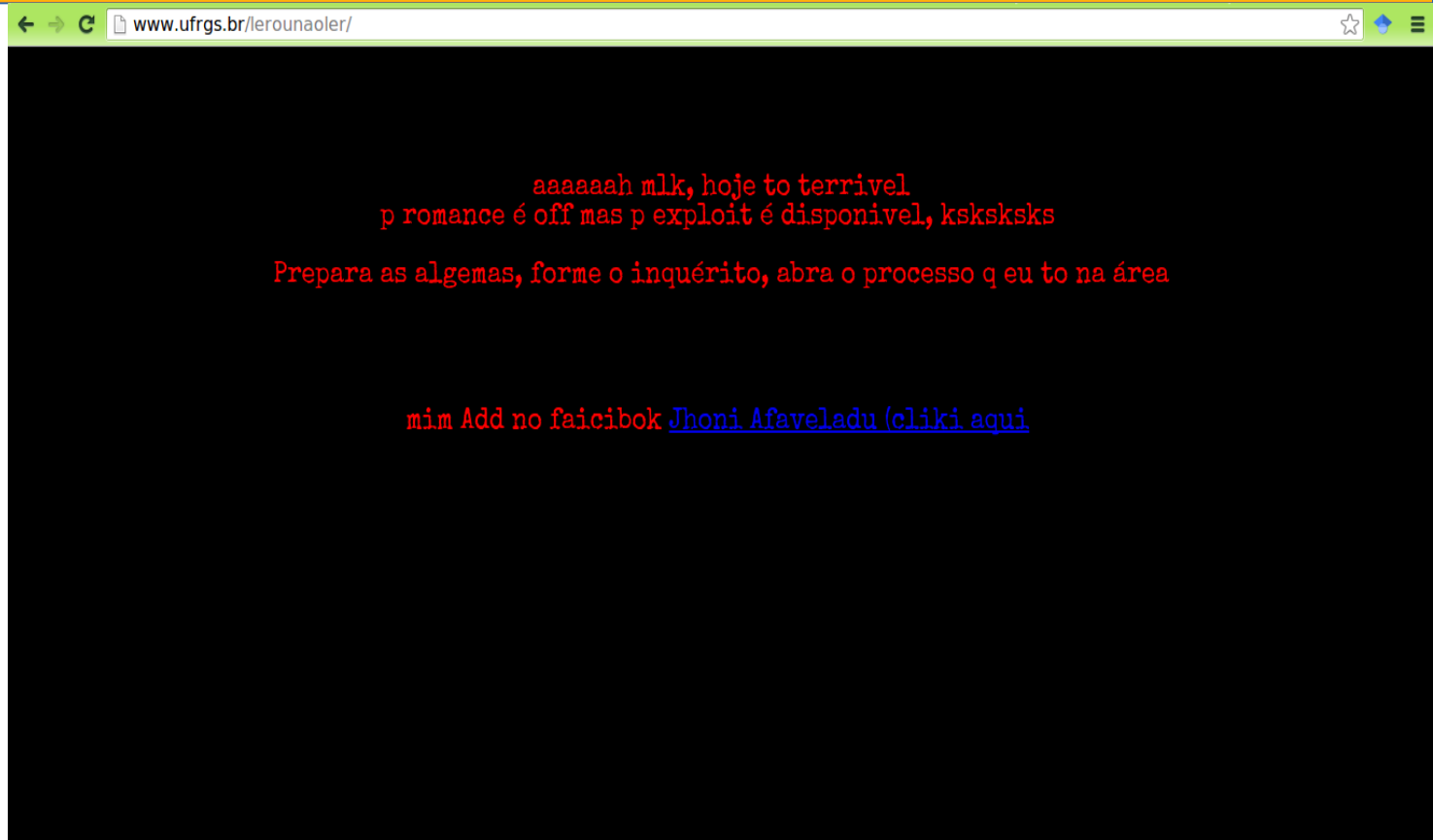
Defacement alert (1)

Defacement Alert

An alert was generated based on posts in the Facebook page of a hacker group. The target was the URL of a Brazilian federal university

Defacement alert (2)

The page after the attack:



Data leak alerts

- An alert was generated based on posts in the Facebook page of a hacker group (the group was promising to leak data from the Brazilian Electricity Regulatory Agency). Some time ago, the data was publicly leaked

- A similar event happened with data from Military Police of Rio de Janeiro

Other generated alerts

- Attack orchestrations
- Exploits
- DDoS attacks

Partners (already using or interested in use)

University of São Paulo

Federal University of Technology – Paraná

RNP's Service Center for Security Incidents

Partners (already using or interested in use)

Brazilian National Research and Education Network

Amazonas state ICT company

Brazilian Federal Police

https://gtews.ime.usp.br/

Contact:

gt-ews@listas.rnp.br

Speaker:

Michael Stanton