Pulsedive

Community + Pro

CASE STUDY

Elevating Brazil's Community Cyber Threat Intelligence

OpenCTI.BR leverages Pulsedive, enhanced with Pro to research, analyze, and combat regional cyber threats

A Safer Digital World for Brazil

Kicking off as a volunteer initiative in 2020, OpenCTI.BR is dedicated to developing intelligence-driven security efforts for the entire Brazilian market and ecosystem. OpenCTI.BR unifies local security experts in a shared commitment to mitigate Brazil's role in global crime.

The group recognized an increasing number of major incidents in Brazil, with a large portion attributable to simple or moderately sophisticated attacks using common TTPs for ransomware, banking schemes, and trojans. So OpenCTI.BR launched programs from the ground up to research, create, and share related threat intelligence to progress towards their vision of making the digital world safer for all Brazilians.

Identifying Solution Requirements

The team determined the need for a solution that integrated within their security environment and:

- Provides **enrichment** and **confidence** in IOCs collected and analyzed for finished insights
- Supports **pivoting** between IOCs and contextual data that is hard to find from other samples and sources
- Builds a more **comprehensive view** of suspected IOCs on deep-dive technical investigations
- Is **easy to use** for both analysts and integrations

(continued on next page)

KEY INFORMATION

OpenCTI

OpenCTI.BR is a non-profit project, maintained by IT security enthusiasts and professionals.

The group's aim: contribute and encourage the sharing of information about cyber threats in the Brazilian community.

The team uses Pulsedive to support several initiatives:

- Threat Database
- Threat Feeds Repository
- Sandbox Malware Analysis
- Threat Map
- Threat Analytics Platform
- Threat Reports

Pulsedive features used:

- Critical-Risk Feed
- Screenshots
- Increased API limits
- IOC scanning/enrichment
- Browser Add-on

Pulsedive

> “We are very happy to be this close to the Pulsedive team. Your purpose is genuine, and **one of the sparks that inspired us to create OpenCTI.BR**”
>
> - The OpenCTI.BR Team

CASE STUDY

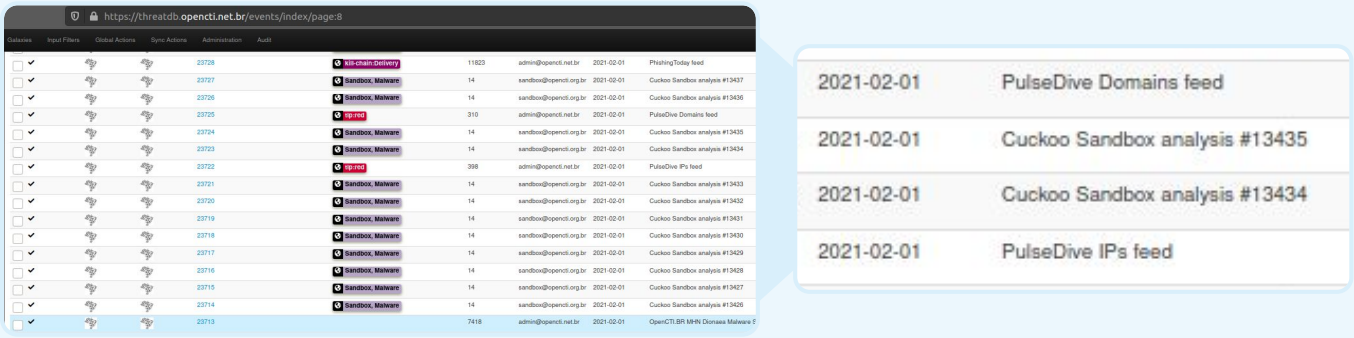
Elevating Brazil’s Community Cyber Threat Intelligence

Already familiar with Pulsedive’s community resources for SecOps and CTI professionals, the leaders of OpenCTI.BR sought to expand their use of Pulsedive to achieve their ambitious project plans.

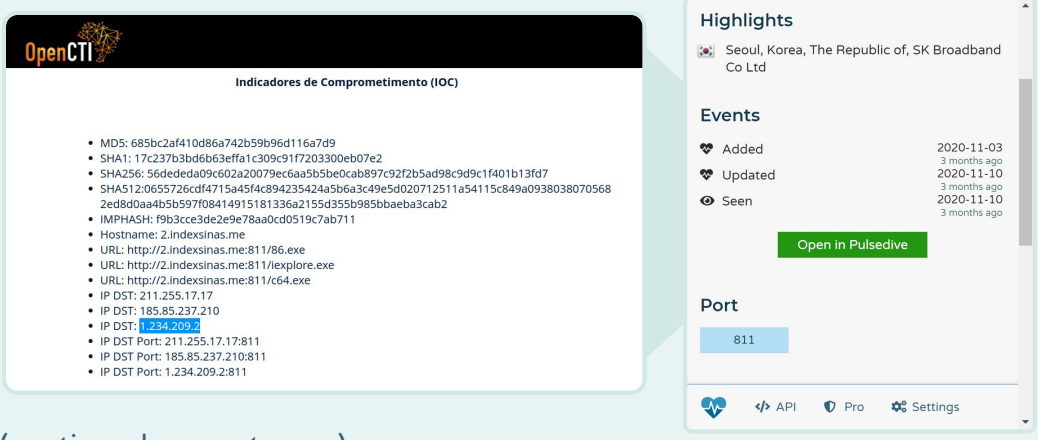
Harnessing Pro for Automation *and* Manual Investigation

OpenCTI.BR brought Pulsedive Pro into **2 primary workstreams** to enrich and investigate IOCs, correlate data, pivot to expand research, and integrate with other tooling.

Pulsedive Threat Feeds are ingested into the OpenCTI.BR MISP instance to process threat data in correlations and analysis, as well as honeypot monitoring.



OpenCTI.BR’s researchers also use **Pulsedive’s web UI and add-on** for seamless, quick pivoting during malware analysis and reporting.



(continued on next page)

Pulsedive

Community + Pro

CASE STUDY

Elevating Brazil's Community Cyber Threat Intelligence

Technical and Strategic Success

OpenCTI.BR realized several goals by using Pulsedive Pro for:

Team Productivity

Pulsedive analyst-optimized interface and responsiveness during research for millions of domains, urls, and IPs

Compounding value with many ways to access the data, including the critical-risk feed and browser add-on

Intelligence Reporting

Validating accuracy as a second opinion for other intelligence collection data points and sources

Retrieving on-demand enrichment and context, like metadata, whois, geo

Publishing key projects, such as:

- January Situational Report
- Ghost Rat Report
- CVE-2018-13379 Report
- Github Feed Repositories
- Live Threat Map

Organizational Growth

OpenCTI.BR has significantly expanded its capabilities and deliverables within its first year, expanding from a founding team of two to over a dozen volunteer contributors and a community of over 700

What's next: OpenCTI.BR's team of security leaders will continue to evolve their threat intelligence programs leveraging Pulsedive's Community platform and Pro feature set - including projects for malware analysis, data analytics, and honeypot platform enhancements.