



# **Inside one of the biggest data leaks in Brazil**

Take a deeper look into our discovery of a collection of personal records compiled by FIESP, the Federation of Industries of the State of São Paulo

# FACTSHEET

**Database:** Unprotected Elasticsearch instance

**Country:** Brazil

**Type of data exposed:** Personal Identifiable Information (PII): names, DOBs, addresses, IDs, tax IDs, emails

**Number of records:** 180,104,892

**Estimated number of people affected:** 34,817,273


**Found on:** Nov 12, 2018

**Reported on:** Nov 12, 2018

**Secured on:** Nov 17, 2018

**Company/organization responded:** No

Type	elasticsearch
elasticsearch.version	6.3.2
elasticsearch.cluster_nodes	5
elasticsearch.size_in_bytes	86821215238
elasticsearch.docs	179942663
elasticsearch.indices	invalidos, municipios, bigdata, bigdata_sgest_pj, receiptaws, sgc, fiesp, ecool, sce, campaigns, permissions, dashlogs, api, apilogs, pf_index, pj_index, fiesp_backup, pf_index_dist, campaigns, users, aknalist, sr1, celulares, fiesp2, sgc1, messages, campaign, rm, notifications, bigdata_sgis, ceps, externo_cels, cep, bigdata_sgest, fiesp_pj, sr_pj, fiesp_test, fiesp1_pf, rm1, sr, externo, bigdata_sisae, groups, listtosend, filters, campaignfilters, celulares_rj, pf, user, bigdata_sieja

	11/12/18 8:30 PM Tag: database	8000/tcp	elasticsearch	<b>Open/Exposed</b> elasticsearch.version: 6.3.2 elasticsearch.cluster_name: es-docker-fiesp elasticsearch.cluster_nodes: 5 elasticsearch.docs: 179942663 elasticsearch.indices: 50 elasticsearch.name: node3 ostype: Linux
---	-----------------------------------	----------	---------------	--

A quick glimpse at the Brazilian cybersecuritylandscape with the help of **Binaryedge.io** scanning engine shows:

- 265 open/exposed Elasticsearch instances
- 541 unprotected MongoDB databases
- 168 Redis
- 6,738 open SMB shares

## DANGER OF OPEN ELASTICSEARCH INSTANCES

We have previously reported that the lack of authentication allowed the installation of malware or ransomware on the Elasticsearch servers. The public configuration allows the possibility for cybercriminals to manage the whole system with full administrative privileges. Once the malware is in place criminals could remotely access the server's resources and even launch a code execution to steal or completely destroy any saved data that the server contains.

## CONTACT US

To learn on how you can minimize the risks of your cloud infrastructure becoming exposed.