# Big Data, Big Security Issues


## Thiago Bordini – NS Prevention

# Introdução

**A implementação de soluções de Big Data tem crescido nos últimos anos devido a necessidade de consolidação de informações em uma plataforma que permita um crescimento rápido com pesquisa ágeis e correlacionadas entre as mais diversas fontes de informação de uma empresa.**

**Mas qual o problema?**

# Big Data em números

JUNHO 1, 2016

## Relatório do IDC prevê crescimento de 50% no mercado de Big Data e Análise até 2019

Em seu último relatório semestral "Big Data and Analytics Spending Guide", a empresa de inteligência de mercado International Data Corporation (IDC) prevê que as receitas no mercado de Big Data e análise devem chegar a US$ 187 bilhões até 2019, crescimento de 50% em relação aos US$ 122 bilhões de faturamento em 2015.

O otimismo se deve à percepção, nas empresas, de que soluções de análise são um diferencial no mercado. Segundo Dan Vesset, vice-presidente de Análise e Gerenciamento da Informação do IDC, *"empresas capazes de aproveitar os recursos da nova geração de soluções de análise de dados conseguem se adaptar melhor a mudanças e se diferenciar frente à competição nos seus mercados"*.

Segundo o relatório, o mercado de serviços deve ser a grande fonte de oportunidades para os fornecedores de soluções de análise: mais da metade do montante de investimento previsto até 2019 deve estar nesse mercado. Logo atrás vem o mercado de software cujo investimento – principalmente em ferramentas de análise e relatórios e de gerenciamento de data warehouse – deve chegar aos US$ 55 bi.

Em termos de indústria, a bancária e a de saúde estão entre as que devem experimentar maior investimento em soluções de big data e análise, mas o relatório aponta que praticamente todas as indústrias devem aumentar seus investimentos nessas soluções em até 50% no período.

Fonte: https://seginfo.com.br/2016/06/01/relatorio-do-idc-preve-crescimento-de-50-no-mercado-de-big-data-e-analise-ate-2019/

# Big Data + Botnets

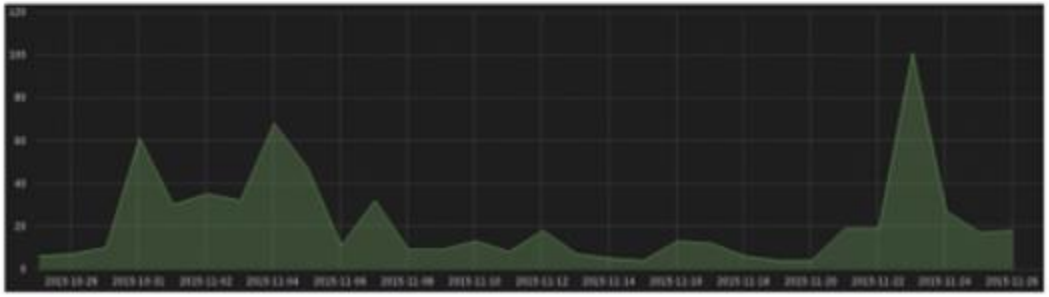
## ElasticZombie Botnet - Exploiting Elasticsearch Vulnerabilities

With the rise of inexpensive Virtual Servers and popular services that install insecurely by default, coupled with some juicy vulnerabilities (read: RCE - Remote Code Execution), like CVE-2015-5377 and CVE-2015-1427, this year will be an interesting one for Elasticsearch. Elasticsearch provides plenty of targets for people to exploit and create server-based botnets but in fairness it is not only Elasticsearch that suffers from critical vulnerabilities there is also ShellShock, mongodb-exploits and very recently a bug that hit WebSphere, JBoss, Jenkins and OpenNMS.

This blog post analyzes what happens if you run a vulnerable service that is connected to the internet resulting in your server becoming a compliant member of a botnet.

With our analysis we concentrate on how the infection happens, what the bots are doing and whom they communicate with, but not the code itself. For a nice read on dissecting Linux-based malware we'd suggest you read the articles from @MalwareMustDie.

Over a period of 3-months we collected more than 30 different bots, giving us enough interesting stuff to play with and analyze.



Exploits against ElasticZombie - Honeypots, 30 days

Fonte: https://www.alienvault.com/blogs/labs-research/elasticzombie-botnet-exploiting-elasticsearch-vulnerabilities

# Big Data em problemas

DEC 28, 2015 @ 08:50 AM 198,726 VIEWS

## 191 Million US Voter Registration Records Leaked In Mystery Database

**Thomas Fox-Brewster**
FORBES STAFF
*I cover crime, privacy and security in digital and physical forms.*
FULL BIO >

A whitehat hacker has uncovered a database sitting on the Web containing various pieces of personal information related to 191 million American citizens registered to vote. On top of the concomitant problems of disclosing such a significant leak to that many people, no one knows who is actually responsible for the misconfiguration that left the data open to anyone.

Researcher Chris Vickery, who this month found myriad databases left open to all and sundry, told FORBES he has his hands on all 300GB of voter data, which includes names, home addresses, phone numbers, dates of birth, party affiliations, and logs of whether or not they had voted in primary or general elections. The data appears to date back to 2000. It does not contain financial data or social security numbers.

## Philippines elections hack 'leaks voter data'

**The Philippines may have suffered its worst-ever government data breach barely a month before its elections.**

Personal information, including fingerprint data and passport information, belonging to around 70 million people is said to have been compromised by hackers.

The **Philippine Commission on the Elections** (Comelec) saw its website defaced at the end of March.

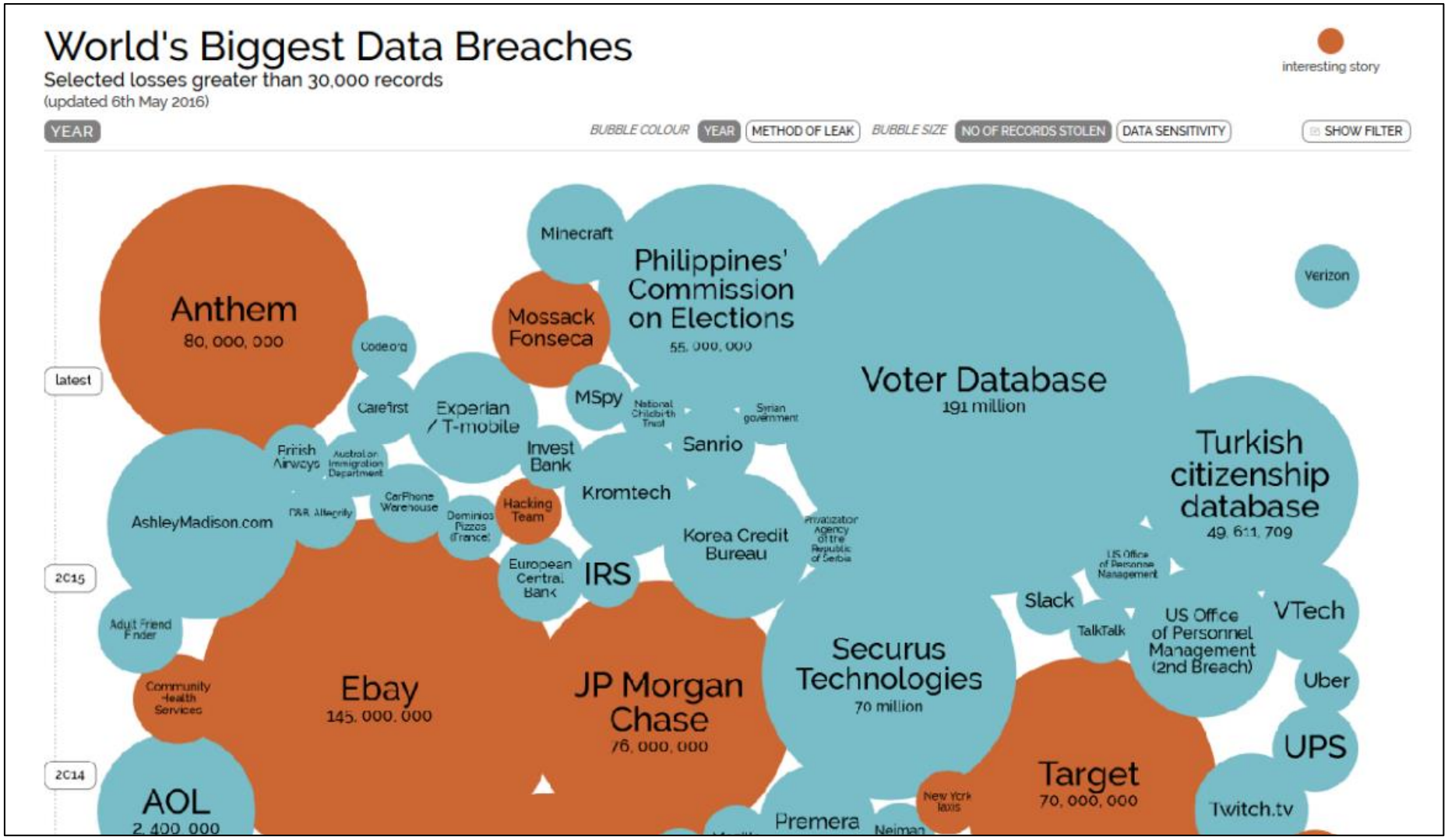
## *Millions of Anthem Customers Targeted in Cyberattack*

Anthem, one of the nation's largest health insurers, said late Wednesday that the personal information of tens of millions of its customers and employees, including its chief executive, was the subject of a "very sophisticated external cyberattack."

The company, which is continuing its investigation into the exact scope of the attack, said hackers were able to breach a database that contained as many as 80 million records of current and former customers, as well as employees. The information accessed included names, Social Security numbers, birthdays, addresses, email and employment information, including income data.

Fonte: http://www.forbes.com/sites/thomasbrewster/2015/12/28/us-voter-database-leak/#5062a3de1bb9 / http://www.bbc.com/news/technology-36013713 / http://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html?_r=0

# Big Data em problemas

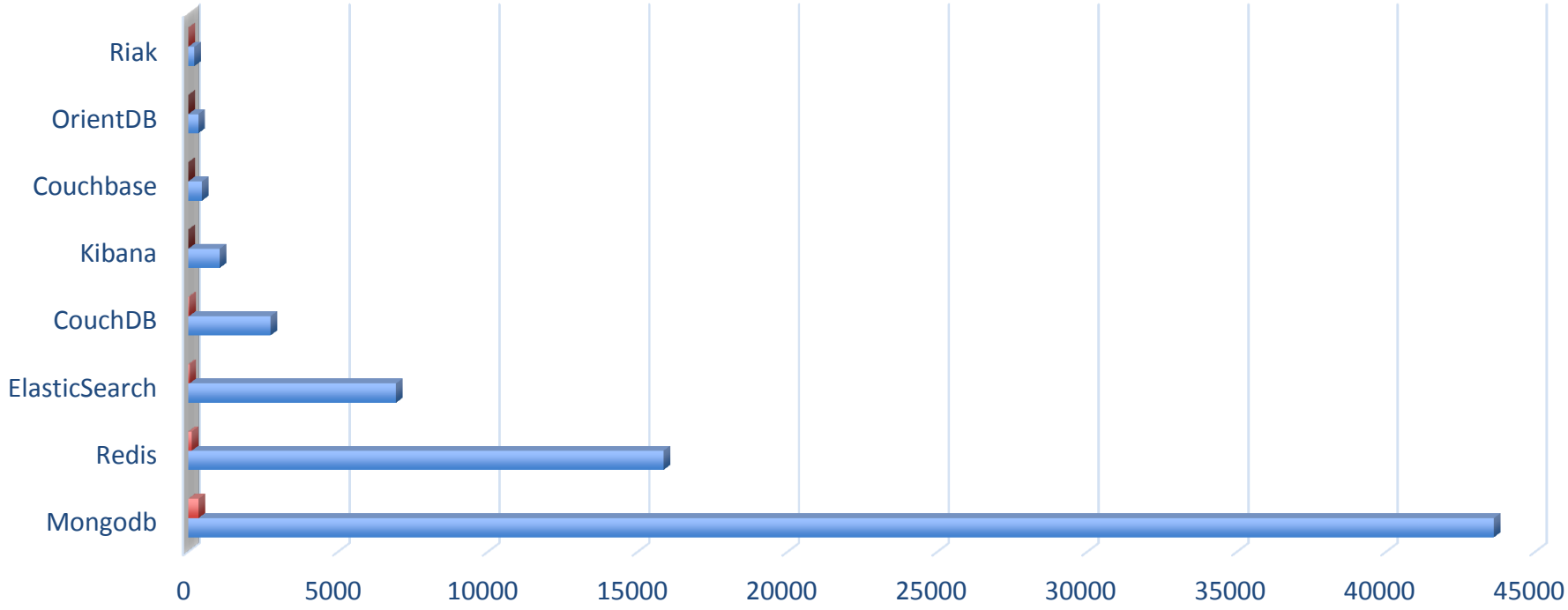



Fonte: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

# Big Data em números

GRUPO NEW SPACE
A Visão do Futuro

## Principais sistemas NoSQL utilizados em soluções de BigData – 05/2016




| | Mongodb | Redis | ElasticSearch | CouchDB | Kibana | Couchbase | OrientDB | Riak |
|---|---|---|---|---|---|---|---|---|
| BR | 345 | 117 | 46 | 32 | 2 | 1 | 2 | 6 |
| Qtd Total | 43616 | 15859 | 6939 | 2752 | 1051 | 462 | 335 | 209 |

Fonte: http://www.shodanhq.com

# Big Data em problemas

GRUPO NEW SPACE
A Visão do Futuro

## Around 36 Million Records From 110 MongoDB Servers Leaked By GhostShell

June 4, 2016 The White Cat 736 Views 0 Comment data breach, GhostShell, Pastebin, Security

24 year old Romanian hacker GhostShell has leaked more than 36 million user's accounts among which 3.6 million records include passwords of several accounts. The hacker announced the data leak on Twitter and posted a link to a PasteBin URL where users can find a statement about this hack. The reason was to raise awareness about the poor security infrastructure implemented on MongoDB databases by their owners.

The download package is a 598 MB ZIP file, which decompresses to 5.6 GB of data, containing 110 folders named based on the hacked server's IP. There are 110 IP addresses that were breached and to every IP there is a dedicated folder with the DB data, proof and general information. The data varies from server to server but reveals a lot of sensitive info such as username, password, full name, phone, address, 627,296 email addresses and more.

Fonte: https://latesthackingnews.com/2016/06/04/around-36-million-records-from-110-mongodb-servers-leaked-by-ghostshell/

# Problemas – Exposição de dados

GRUPO NEW SPACE
A Visão do Futuro

**Problem Scope**

There's a total of **595.2 TB of data** exposed on the Internet via publicly accessible MongoDB instances that don't have any form of authentication. To determine the scale of the problem I downloaded the data using the Shodan command-line tool:

```
shodan download --limit -1 mongodb "product:MongoDB"
```

And then I ran a small Python script to aggregate the total size of all exposed databases. I also looked at which database names were most popular:

1. **local**: 27,108
2. **admin**: 22,286
3. **db**: 9,895
4. **test**: 6,818
5. **config**: 1,119
6. **mydb**: 498

Fonte: https://blog.shodan.io/its-the-data-stupid/

# Problemas – Exposição de dados

GRUPO NEW SPACE
A Visão do Futuro

179.[redacted]
[redacted].com.br
[redacted]Informatica S.A.
Added on 2016-05-14 00:20:07 GMT
Brazil
Details

| 103.3 GB | 21 Databases |
|---|---|

| Database Name | Size |
|---|---|
| EventsHook | 81.9 GB |
| Tracking | 17.9 GB |
| DSGaming | 2.0 GB |
| DSPublicidade | 208.0 MB |
| DSGamingDev | 80.0 MB |

```
MongoDB Server Information
{
    "metrics": {
        "getLastError": {
            "wtime": {
                "num": 0,
                "totalMillis": 0
            },
            "wtimeouts": 0
        },
        "storage": {
            "freelist": {
                "search": {
                ...
```

200.[redacted]
Added on 2016-05-14 03:40:57 GMT
Brazil
Details

| 118.1 GB | 4 Databases |
|---|---|

| Database Name | Size |
|---|---|
| [redacted]i_xml | 117.9 GB |
| test | 208.0 MB |
| admin | 1 byte |
| local | 1 byte |

```
MongoDB Server Information
{
    "backgroundFlushing": {
        "last_finished": "2016-05-14T03:54:19.603000",
        "last_ms": 0,
        "flushes": 237167,
        "average_ms": 0.27949082292224464,
        "total_ms": 66286
    },
    "connections": {
        "current": 3,
        "av...
```

Fonte: http://www.shodanhq.com

# Problemas – Exposição de dados

GRUPO NEW SPACE
A Visão do Futuro

54.[redacted]

Added on 2016-05-14 08:56:43 GMT

Brazil

Details

| 287.8 GB | 6 Databases |
|---|---|

| Database Name | Size |
|---|---|
| [redacted]bs | 269.8 GB |
| [redacted]bs_response | 17.9 GB |
| [redacted]tz | 80.0 MB |
| config | 16.0 MB |
| admin | 16.0 MB |

```
MongoDB Server Information
{
    "connections": {
        "current": 445,
        "available": 50755,
        "totalCreated": 49609
    },
    "uptime": 6157404.0,
    "metrics": {
        "getLastError": {
            "wtime": {
                "num": 0,
                "totalMillis": 0
...
```

104.[redacted]

Added on 2016-04-24 17:45:56 GMT

Brazil

Details

| 341.9 GB | 2 Databases |
|---|---|

| Database Name | Size |
|---|---|
| [redacted]ria | 341.8 GB |
| local | 80.0 MB |

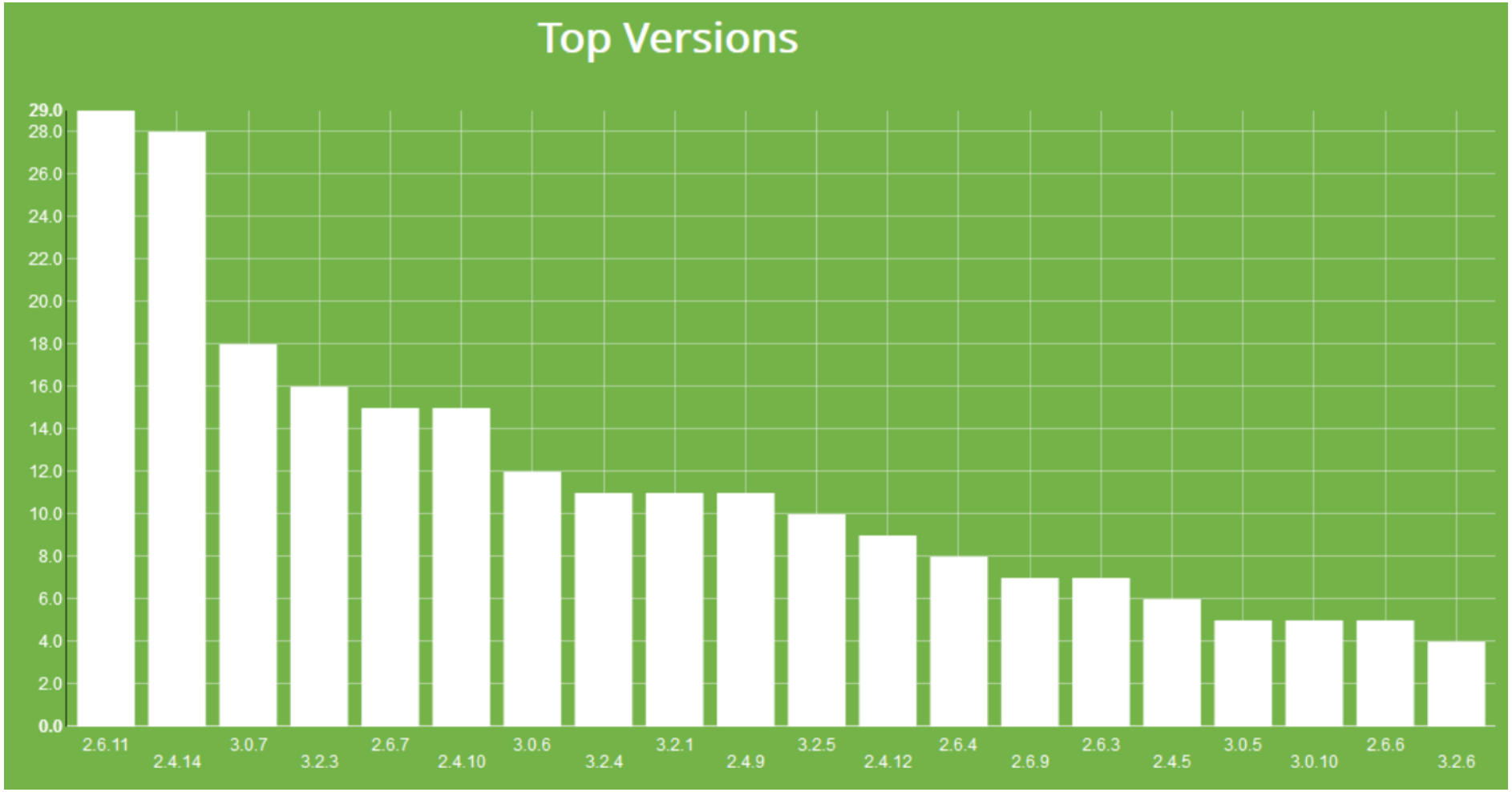
```
MongoDB Server Information
{
    "metrics": {
        "commands": {
            "updateUser": {
                "failed": 0,
                "total": 0
            },
            "dropRole": {
                "failed": 0,
                "total": 0
            },
            "renameCollection...
```

Fonte: http://www.shodanhq.com

# Problemas – Vulnerabilidades

GRUPO NEW SPACE
A Visão do Futuro

## 294 Servidores MongoDBs – Somente Brasil




Fonte: http://www.shodanhq.com

# Problemas – Vulnerabilidades

GRUPO NEW SPACE
A Visão do Futuro

## 294 Servidores MongoDBs – Somente Brasil

| # | CVE ID | CWE ID | # of Exploits | Vulnerability Type(s) | Publish Date | Update Date | Score | Gained Access Level | Access | Complexity | Authentication | Conf. | Integ. | Avail. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | CVE-2015-1609 | 20 | | DoS | 2015-03-30 | 2015-10-22 | 5.0 | None | Remote | Low | Not required | None | None | Partial |
| MongoDB before 2.4.13 and 2.6.x before 2.6.8 allows remote attackers to cause a denial of service via a crafted UTF-8 string in a BSON request. | | | | | | | | | | | | | | |
| 2 | CVE-2014-3971 | 20 | | DoS | 2014-12-25 | 2014-12-29 | 5.0 | None | Remote | Low | Not required | None | None | Partial |
| The CmdAuthenticate::_authenticateX509 function in db/commands/authentication_commands.cpp in mongod in MongoDB 2.6.x before 2.6.2 allows remote attackers to cause a denial of service (daemon crash) by attempting authentication with an invalid X.509 client certificate. | | | | | | | | | | | | | | |
| 3 | CVE-2013-4650 | 264 | | | 2013-07-04 | 2013-07-05 | 6.5 | User | Remote | Low | Single system | Partial | Partial | Partial |
| MongoDB 2.4.x before 2.4.5 and 2.5.x before 2.5.1 allows remote authenticated users to obtain internal system privileges by leveraging a username of __system in an arbitrary database. | | | | | | | | | | | | | | |
| 4 | CVE-2013-3969 | 399 | | DoS Exec Code | 2013-10-01 | 2013-10-02 | 6.5 | None | Remote | Low | Single system | Partial | Partial | Partial |
| The find prototype in scripting/engine_v8.h in MongoDB 2.4.0 through 2.4.4 allows remote authenticated users to cause a denial of service (uninitialized pointer dereference and server crash) or possibly execute arbitrary code via an invalid RefDB object. | | | | | | | | | | | | | | |
| 5 | CVE-2013-2132 | | | DoS | 2013-08-15 | 2013-10-07 | 4.3 | None | Remote | Medium | Not required | None | None | Partial |
| bson/_cbsonmodule.c in the mongo-python-driver (aka. pymongo) before 2.5.2, as used in MongoDB, allows context-dependent attackers to cause a denial of service (NULL pointer dereference and crash) via vectors related to decoding of an "invalid DBRef." | | | | | | | | | | | | | | |
| 6 | CVE-2013-1892 | 20 | 2 | DoS Exec Code | 2013-10-01 | 2013-11-30 | 6.0 | None | Remote | Medium | Single system | Partial | Partial | Partial |
| MongoDB before 2.0.9 and 2.2.x before 2.2.4 does not properly validate requests to the nativeHelper function in SpiderMonkey, which allows remote authenticated users to cause a denial of service (invalid memory access and server crash) or execute arbitrary code via a crafted memory address in the first argument. | | | | | | | | | | | | | | |
| 7 | CVE-2012-6619 | 20 | | DoS | 2014-03-06 | 2014-05-06 | 6.4 | None | Remote | Low | Not required | Partial | None | Partial |
| The default configuration for MongoDB before 2.3.2 does not validate objects, which allows remote authenticated users to cause a denial of service (crash) or read system memory via a crafted BSON object in the column name in an insert command, which triggers a buffer over-read. | | | | | | | | | | | | | | |

Fonte: http://www.cvedetails.com

# Problemas – Vulnerabilidades

## 6.448 Servidores Elasticseach Global – 05/2016

| Top Countries | |
|---|---|
| 1. United States | 2,287 |
| 2. China | 714 |
| 3. France | 568 |
| 4. Netherlands | 368 |
| 5. Singapore | 338 |
| 6. Germany | 308 |
| 7. Ireland | 288 |
| 8. United Kingdom | 210 |
| 9. Japan | 175 |
| 10. Canada | 126 |

Fonte: http://www.shodanhq.com

# Problemas – Vulnerabilidades

GRUPO NEW SPACE A Visão do Futuro

## Elasticseach RCE – CVE-2015-1427

**Vulnerability Details : CVE-2015-1427 (1 Metasploit modules)**

The Groovy scripting engine in Elasticsearch before 1.3.8 and 1.4.x before 1.4.3 allows remote attackers to bypass the sandbox protection mechanism and execute arbitrary shell commands via a crafted script.

Publish Date : 2015-02-17 Last Update Date : 2015-06-25

Collapse All Expand All Select Select&Copy ▾ Scroll To ▾ Comments ▾ External Links

Search Twitter Search YouTube Search Google

**– CVSS Scores & Vulnerability Types**

| | |
|---|---|
| CVSS Score | 7.5 |
| Confidentiality Impact | Partial (There is considerable informational disclosure.) |
| Integrity Impact | Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.) |
| Availability Impact | Partial (There is reduced performance or interruptions in resource availability.) |
| Access Complexity | Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit. ) |
| Authentication | Not required (Authentication is not required to exploit the vulnerability.) |
| Gained Access | None |
| Vulnerability Type(s) | Execute Code Bypass a restriction or similar |
| CWE ID | 284 |

Fonte: http://www.cvedetails.com

# Problemas – Vulnerabilidades

## 57 Servidores Elasticseach Vulneráveis Global – CVE-2015-1427

TOP COUNTRIES

| | |
|---|---|
| United States | 28 |
| France | 4 |
| China | 4 |
| Netherlands | 3 |
| India | 3 |

TOP ORGANIZATIONS

| | |
|---|---|
| Amazon.com | 16 |
| Google Cloud | 3 |
| XS4ALL Internet BV | 2 |
| SoftLayer Technologies | 2 |
| Optimum Online | 2 |

TOP OPERATING SYSTEMS

| | |
|---|---|
| Linux 3.x | 2 |

Total results: 57

52.[redacted]

1.compute.amazonaws.com

**Amazon.com Tech Telecom**

Added on 2016-05-29 14:28:15 GMT

Singapore, Singapore

Details

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-
Content-Length: 345

{
  "status" : 200,
  "name" : "[redacted]",
  "cluster_name" : "elasticsearch",
  "version" : {
    "number" : "1.4.3",
    "build_hash" : "36a29a7144cfde87a960ba03
    "build_timestam...
```

2600:3c[redacted]

Added on 2016-05-29 12:38:28 GMT

United States

Details

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-
Content-Length: 336

{
  "status" : 200,
  "name" : [redacted],
```

Fonte: http://www.shodanhq.com

# Problemas – Vulnerabilidades

## Exploit público – CVE-2015-1427

### ElasticSearch Unauthenticated Remote Code Execution

| | | |
|---|---|---|
| **EDB-ID:** 36337 | **CVE:** 2015-1427 | **OSVDB-ID:** 118239 |
| **EDB Verified:** ✓ | **Author:** Xiphos Research Ltd | **Published:** 2015-03-11 |
| **Download Exploit:** Source Raw | **Download Vulnerable App:** N/A | |

« Previous Exploit  Next

```
#!/bin/python2
# coding: utf-8
# Author: Darren Martyn, Xiphos Research Ltd.
# Version: 20150309.1
# Licence: WTFPL - wtfpl.net
import json
import requests
import sys
import readline
readline.parse_and_bind('tab: complete')
readline.parse_and_bind('set editing-mode vi')
__version__ = "20150309.1"

def banner():
    print """\x1b[1;32m
```


```
  Exploit for ElasticSearch , CVE-2015-1427   Version: %s\x1b[0m""" %(__version__)
```

Fonte: https://www.exploit-db.com/

# Problemas – Vulnerabilidades

## Servidores Elasticseach Vulneráveis Global – CVE-2015-5531

### Vulnerability Details : CVE-2015-5531 (1 Metasploit modules)

Directory traversal vulnerability in Elasticsearch before 1.6.1 allows remote attackers to read arbitrary files via unspecified vectors related to snapshot API calls.

Publish Date : 2015-08-17 Last Update Date : 2015-08-19

Collapse All Expand All Select Select&Copy Scroll To Comments External Links

Search Twitter Search YouTube Search Google

#### – CVSS Scores & Vulnerability Types

| | |
|---|---|
| CVSS Score | 5.0 |
| Confidentiality Impact | Partial (There is considerable informational disclosure.) |
| Integrity Impact | None (There is no impact to the integrity of the system) |
| Availability Impact | None (There is no impact to the availability of the system.) |
| Access Complexity | Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit. ) |
| Authentication | Not required (Authentication is not required to exploit the vulnerability.) |
| Gained Access | None |
| Vulnerability Type(s) | Directory traversal |
| CWE ID | 22 |

Fonte: http://www.cvedetails.com

# Problemas – Vulnerabilidades

## 434 Servidores Elasticseach Vulneráveis Global - CVE-2015-5531

TOP COUNTRIES

| | |
|---|---|
| United States | 147 |
| China | 83 |
| Netherlands | 38 |
| Ireland | 22 |
| France | 21 |

TOP ORGANIZATIONS

| | |
|---|---|
| Amazon.com | 69 |
| Digital Ocean | 25 |
| Hangzhou Alibaba Advertising Co.,Ltd. | 16 |
| Aliyun Computing Co., LTD | 15 |
| Microsoft Azure | 14 |

TOP OPERATING SYSTEMS

| | |
|---|---|
| Linux 3.x | 4 |

Total results: 434

191 [redacted]

Microsoft Azure

Added on 2016-05-30 18:53:07 GMT

United States, Washington

Details

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=
Content-Length: 344

{
  "status" : 200,
  "name" : "Raza",
  "cluster_name" : "elasticsearch",
  "version" : {
    "number" : "1.6.0",
    "build_hash" : "cdd3ac4dde4f69524ec0
    "build_timestamp" : "...
```

31. [redacted]

Added on 2016-05-30 14:50:56 GMT

Russian Federation

Details

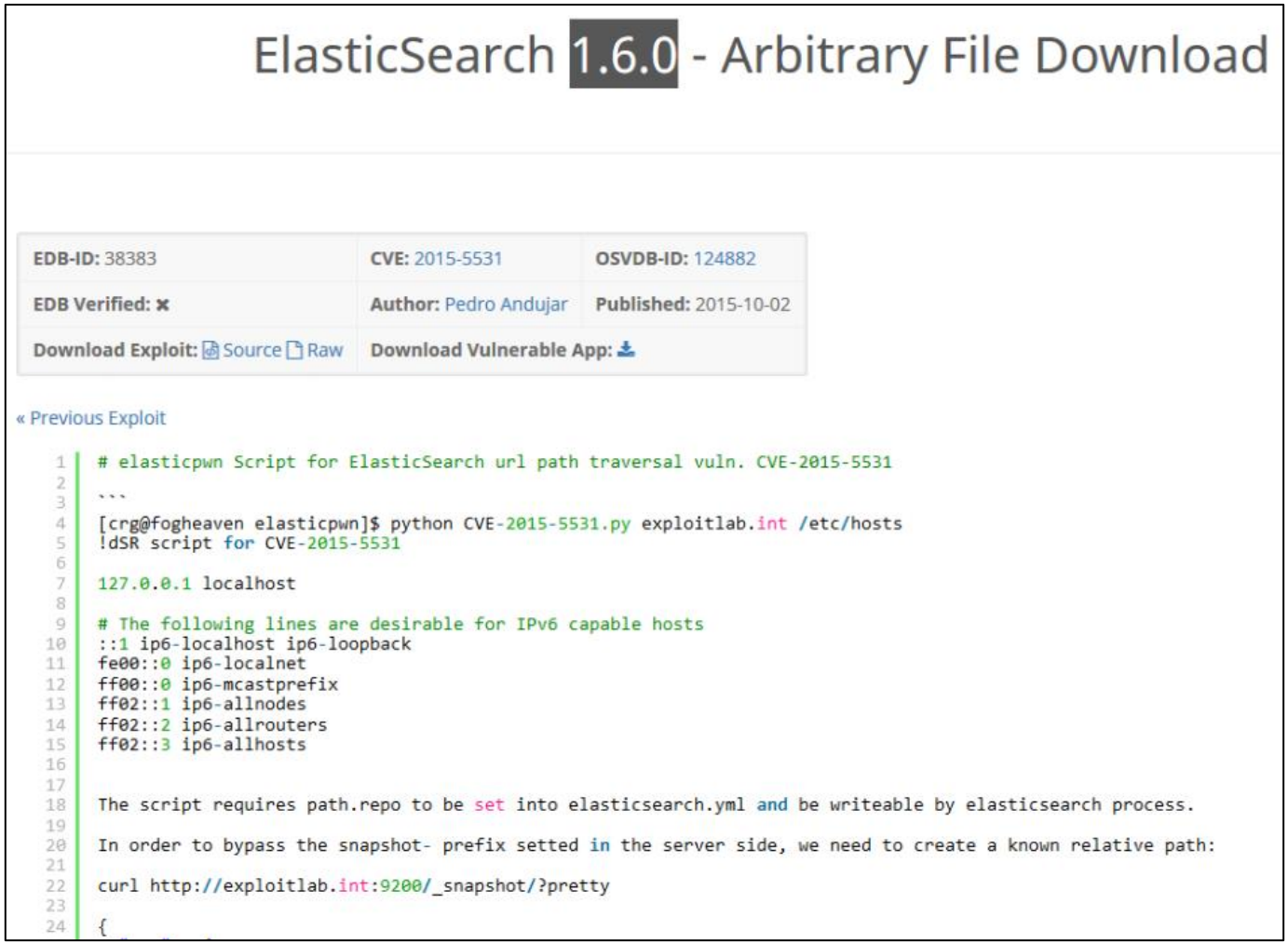
```
HTTP/1.1 200 OK
Content-Type: application/json; charset=
Content-Length: 339

{
  "status" : 200,
  "name" : "[redacted]",
```

Fonte: http://www.shodanhq.com

# Problemas – Vulnerabilidades

## Exploit público – CVE-2015-5531



ElasticSearch 1.6.0 - Arbitrary File Download

| | | |
|---|---|---|
| **EDB-ID:** 38383 | **CVE:** 2015-5531 | **OSVDB-ID:** 124882 |
| **EDB Verified:** ✖ | **Author:** Pedro Andujar | **Published:** 2015-10-02 |
| **Download Exploit:** Source Raw | **Download Vulnerable App:** | |

« Previous Exploit

```
# elasticpwn Script for ElasticSearch url path traversal vuln. CVE-2015-5531

```
[crg@fogheaven elasticpwn]$ python CVE-2015-5531.py exploitlab.int /etc/hosts
!dSR script for CVE-2015-5531

127.0.0.1 localhost

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts


The script requires path.repo to be set into elasticsearch.yml and be writeable by elasticsearch process.

In order to bypass the snapshot- prefix setted in the server side, we need to create a known relative path:

curl http://exploitlab.int:9200/_snapshot/?pretty

{
```

Fonte: https://www.exploit-db.com/
```

# E os grandes players?

## Oracle – 36.463 Servidores expostos

TOP COUNTRIES

| | |
|---|---|
| United States | 11,839 |
| Brazil | 2,990 |
| Germany | 2,118 |
| China | 1,759 |
| France | 1,709 |

TOP SERVICES

| | |
|---|---|
| HTTP (8080) | 10,815 |
| HTTP | 8,181 |
| GlassFish Server | 6,235 |
| HTTPS | 6,043 |
| 4848 | 2,829 |

TOP ORGANIZATIONS

| | |
|---|---|
| Amazon.com | 3,746 |
| Oracle Corporation | 1,432 |
| OVH SAS | 884 |
| Digital Ocean | 548 |
| AMAZON | 304 |

Total results: 36,463

**GlassFish Server 3.1.2 - Server Running**

[redacted]

Added on 2016-06-06 12:54:23 GMT

Romania

Details

Diffie-Hellman Parameters

Fingerprint: Java 7/Hardcoded

768-bit prime

```
HTTP/1.0 200 OK
X-Powered-By: Servlet/3.0 JSP/2.2 (G
Server: GlassFish Server Open Source
Accept-Ranges: bytes
ETag: W/"4759-1342009546000"
Last-Modified: Wed, 11 Jul 2012 12:2
Content-Type: text...
```

[redacted]41

Added on 2016-06-06 12:54:18 GMT

United States, Fort Lauderdale

Details

```
HTTP/1.1 200 OK
Date: Mon, 06 Jun 2016 12:54:16 GMT
Server: GlassFish Server Open Source Edition  4.1
X-Powered-By: Servlet/3.1 JSP/2.3 (GlassFish Server Open Source Editi
Content-Type: text/html
Content-Length: 15
```

[redacted]me

Added on 2016-06-06 12:53:33 GMT

United States, Redwood City

Details

```
HTTP/1.1 200 OK
X-Powered-By: Servlet/3.0 JSP/2.2 (Oracle GlassFish Server 3.1.2.2 Ja
Server: Oracle GlassFish Server 3.1.2.2
Accept-Ranges: bytes
ETag: W/"4356-1442943734000"
Last-Modified: Tue, 22 Sep 2015 17:42:14 GMT
```

Fonte: https://www.exploit-db.com/

# E os grandes players?

## Microsoft SQL Server – 28.288 Servidores expostos

TOP COUNTRIES

| | |
|---|---|
| United States | 5,332 |
| India | 1,484 |
| Turkey | 1,471 |
| Brazil | 1,240 |
| China | 1,080 |

TOP ORGANIZATIONS

| | |
|---|---|
| TE Data | 786 |
| HiNet | 579 |
| Telmex | 578 |
| Turk Telekom | 481 |
| Comcast Cable | 202 |

TOP VERSIONS

| | |
|---|---|
| 8.00.194 | 7,943 |
| 10.50.1600.1 | 3,410 |
| 9.00.5000.00 | 2,340 |
| 10.50.4000.0 | 2,325 |
| 10.50.2500.0 | 1,695 |

Total results: 28,288

[redacted]

Added on 2016-06-06 13:05:59 GMT

Jordan

Details

-ServerName;[redacted]6ID;InstanceName;BKUPEXEC;IsClustered;No;Version;9.00.5000.00;tcp;49370;np;\\WIN-[redacted]
;11.0.3000.0;tcp;49570;np;\[redacted]5ID\pipe\MSSQL$VEEAMSQL2012\sql\...

[redacted]

Added on 2016-06-06 13:05:39 GMT

Colombia

Details

ServerName;SERVIDOR;InstanceName;[redacted]IsClustered;No;Version;9.00.4035.00;tcp;49395;np;\\SERVIDOR\pipe
tcp;50853;np;\\SERVIDOR\pipe\MSSQL[redacted]sql\query;;

[redacted]

Added on 2016-06-06 13:05:19 GMT

India, Delhi

Details

bServerName[redacted];InstanceName;SQLEXPRESS;IsClustered;No;Version;10.50.1600.1;;ServerName[redacted]InstanceName;SQL20
1600.1;;ServerName;[redacted]InstanceName;MSQL2008;IsClustered;No;Version;10.5...

Fonte: https://www.exploit-db.com/

# E os grandes players?

## Splunk – 182 Servidores expostos

TOP COUNTRIES

| | |
|---|---|
| France | 117 |
| United States | 37 |
| Ireland | 5 |
| China | 5 |
| Germany | 4 |

TOP SERVICES

| | |
|---|---|
| HTTP | 127 |
| HTTPS | 22 |
| 9443 | 8 |
| SMB | 6 |
| 8649 | 3 |

TOP ORGANIZATIONS

| | |
|---|---|
| Iliad Hosting | 115 |
| Amazon.com | 21 |
| AMAZON | 3 |
| TrueServer BV | 2 |
| Server Block | 2 |

Total results: 182

[redacted]

Added on 2016-06-06 11:41:42 GMT

Australia, Sydney

Details

SSL Certificate

Issued By:

|- Common Name: DigiCert SHA2 Secure Server CA

|- Organization: DigiCert Inc

Issued To:

|- Common Name: [redacted]

|- Organization:

Supported SSL Versions

TLSv1, TLSv1.1, TLSv1.2

Diffie-Hellman Parameters

Fingerprint: mod_ssl 2.2.x/Hardcoded 1024-bit prime

```
HTTP/1.1 401 Authorization Required
Date: Mon, 06 Jun 2016 11:41:29 GMT
Server: Apache/2.2.15 (CentOS)
WWW-Authenticate: Basic realm="[redacted]ctiveDirectory - Please use your SPlunk Credential>"
Content-Length: 495
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

[redacted]

Added on 2016-06-06 09:44:53 GMT

France

Details

```
HTTP/1.1 401 Unauthorized
Server: nginx/0.7.67
Date: Mon, 06 Jun 2016 09:44:50 GMT
Content-Type: text/html
Content-Length: 597
Connection: keep-alive
WWW-Authenticate: Basic realm="Splunk Authentication Required"
```

Fonte: https://www.exploit-db.com/

# Principais problemas

GRUPO NEW SPACE
A Visão do Futuro

1. Fragilidade nos mecanismos de autenticação/autorização
2. Fragilidade nos controle de acessos administrativos
3. Implementações default
4. Implementações com múltiplas interfaces em modo listen
5. Ausência de criptografia
6. Falsa inferência que sistemas NoSQL são mais seguros que banco de dados relacionais que são suscetíveis a ataques SQL Injection
7. Ausência de aplicação de técnicas de "Hardening"
8. Ausência de atualizações constantes
9. Não implementação de sensores de monitoramento como SIEM, IDS, IPS
10. Ausência de segmentação de tráfego

# Principais desafios

1. Secure computations in distributed programming frameworks
2. Security best practices for non-relational data stores
3. Secure data storage and transactions logs
4. End-point input validation/filtering
5. Real-time security/compliance monitoring
6. Scalable and composable privacy-preserving data mining and analytics
7. Cryptographically enforced access control and secure communication
8. Granular access control
9. Granular audits
10. Data provenance

Fonte: https://www.isaca.org/Groups/Professional-English/big-data/GroupDocuments/Big_Data_Top_Ten_v1.pdf

**Obrigado**

**Thiago Bordini**

**thiago.bordini@nsprevention.com.br**