Pro Tips for Defending Your Organization from Data Breaches


Bob Diachenko


Adam Stetson

netwrix

Agenda

- Recent data breaches and data leaks
- Shodan search engine
- Gootkit case
- Cyber hygiene rules
- Behavior anomaly discovery

Who am I?

Bob Diachenko is a Cyber Threat Intelligence Director and journalist at **SecurityDiscovery.com**

Bob is on the mission to make the cyber world safer by **educating businesses and communities worldwide**. Many of Bob's discoveries have been covered in major news and technology media, earning himself a reputation as one of the reputable data security analytics.

Some highlights (for the last 2-3 months)

1. Trump Campaign Email Server Was Left Open To Attack
2. CenturyLink customer records exposed on misconfigured cloud database
3. Tax and PII records of 20 million Russians stored without encryption
4. GE Aviation server exposed in DNS misconfiguration
5. Spanish brothel chain leaves internal database exposed online
6. Choice Hotels Data Breach Affects 700,000 Records
7. Unsecured server exposes data for 85% of all Panama citizens

Mail Online

Home | News | U.S. | Sport | TV&Showbiz | Australia | Femail | Health | Science | Money

Latest Headlines | Science | Discounts

Email addresses of almost a BILLION people are leaked in one of the biggest data breaches ever - and hackers could now have access to your name, date of birth and even where you LIVE

- 'Email validation' firm was taken offline when the enormous breach was reported
- Personal information like names, address and employer were also exposed
- Verifications.io is a company offering 'enterprise email validation' as a service
- Validators ensure that the email addresses in a list are valid and won't bounce

By VICTORIA BELL FOR MAILONLINE
PUBLISHED: 10:38 BST, 29 March 2019 | **UPDATED:** 15:49 BST, 29 March 2019

ElasticSearch server exposed the personal data of over 57 million US citizens

Leaky database taken offline, but not after leaking user details for nearly two weeks.

By Catalin Cimpanu for Zero Day | November 28, 2018 -- 15:00 GMT (07:00 PST) | Topic: Security

TC

Login

Startups
Apps
Gadgets
Videos
Audio
Extra Crunch NEW

We found a massive spam operation — and sunk its server

Five million emails in ten days

Trends

Youth-run agency AIESEC exposed over 4 million intern applications

By **inventiva** - January 21, 2019

Нравится 3

netwrix

How do I find these and yours data?

To discover data breaches, leakages, and vulnerabilities on the Internet, we use Shodan search engine (and similar) together with internally-developed Public Exposed Data Analyzer.

Shodan: a search engine for Internet-connected devices. The basic unit of data that Shodan gathers is the **banner**. E.g., here is the typical HTML-banner:

```
HTTP/1.1 200 OK
Server: nginx/1.1.19
Date: Sat, 03 Oct 2015 06:09:24 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 6466
Connection: keep-alive
```

What do we know about data?

Shodan Search Engine API helps us find specific information about hosts connected to the Internet, including:

- Uptime
- Count of containing elements in data store
- Date of scan
- IP address
- Port
- Hostname
- Size of particular data service

netwrix

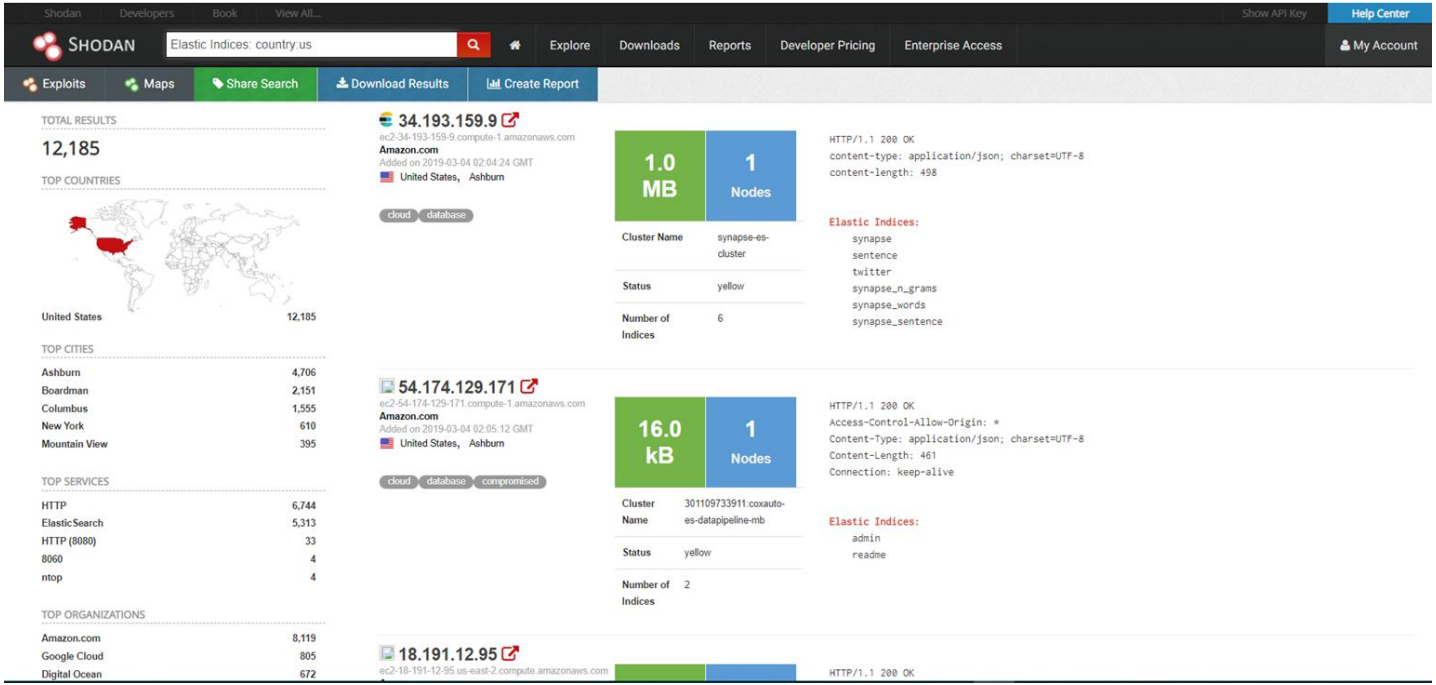
Type of data we analyze

- NoSQL Databases
  - CouchDB (port:5984)
  - MongoDB (port:27017)
  - Elasticsearch (port:9200) / Kibana interface
  - CrateDB
  - RethinkDB
  - Solr (port:8983)
- Amazon AWS S3 buckets / Google buckets
  - Now everybody's trying to guess a bucket name :)
- Service instances
  - Jenkins, Sonarqube
  - Kubernetes
  - Apache services (Kafka, Zookeeper etc)
- Network-Attached Storages (Buffalo Terastation etc.) / SMB

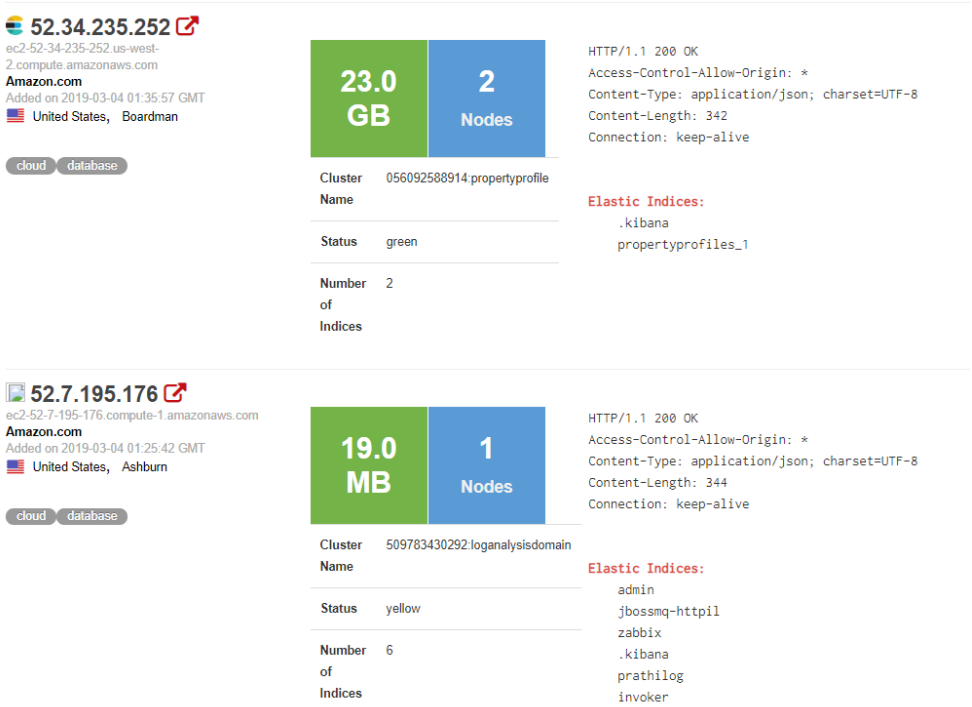
Too Much Information

1. SMB-enabled file shares,
2. misconfigured network-attached storage (NAS) devices,
3. File Transfer Protocol (FTP)
4. rsync servers, and
5. Amazon S3 buckets

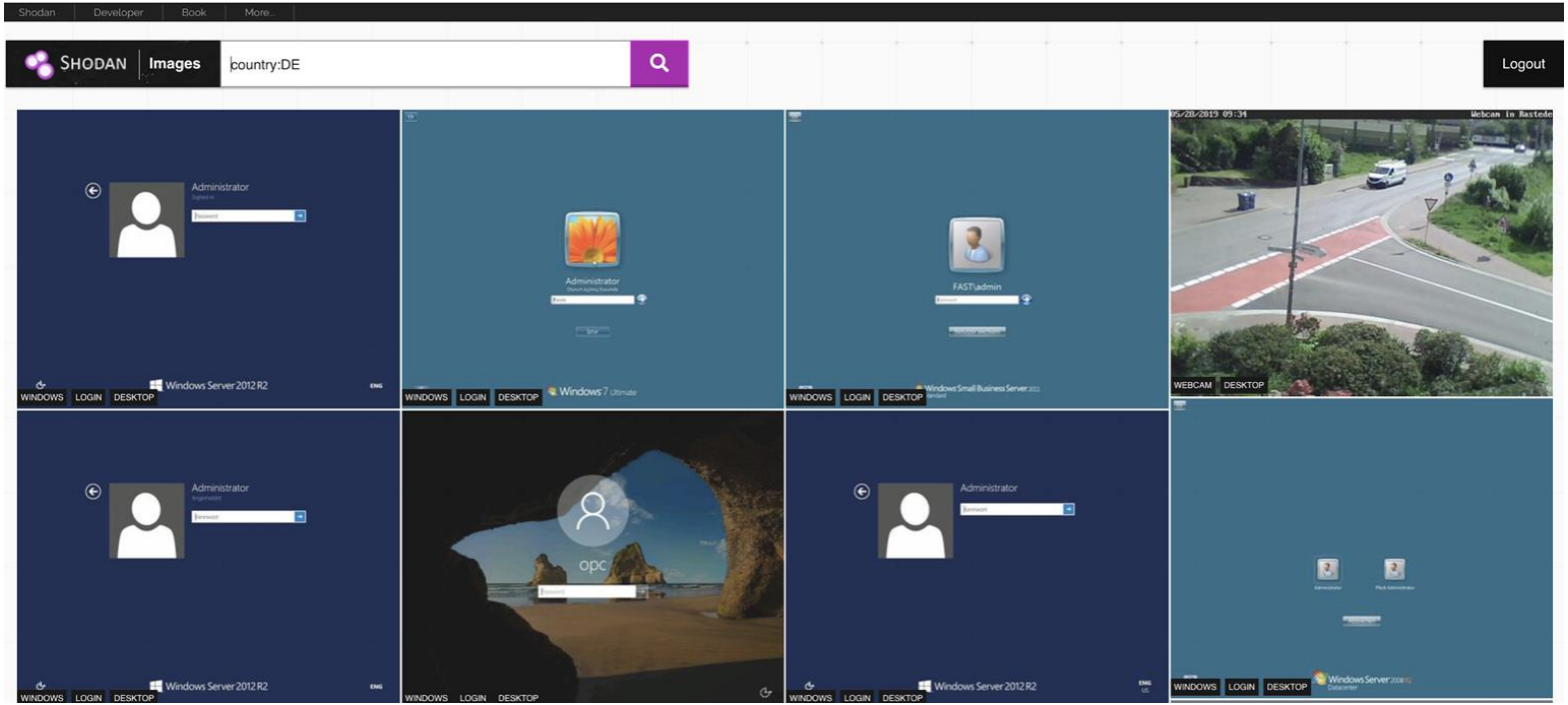
Example: How Easy is To Find Public Data



Example: How Easy is To Find Public Data



Example: Remote Desktop Protocols



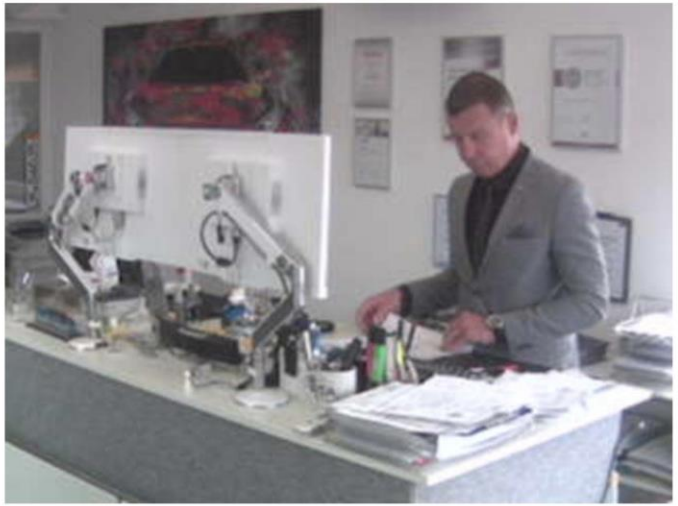
netwrix

Example: Webcams misconfigs

3000
tcp
http-simple-new

D-Link/Airlink IP webcam http config Version: 1.0

```
HTTP/1.0 200 OK
Server: Camera Web Server/1.0
Auther: Steven Wu
MIME-version: 1.0
Cache-Control: no-cache
Content-Type: text/html
Content-Length: 1681
```



netwrix

Example: MongoDB

94.177.229.25

host25-229-177-94.static.arubacloud.de

Aruba S.p.A.

Added on 2019-05-28 07:22:10 GMT

Germany, Frankfurt

database

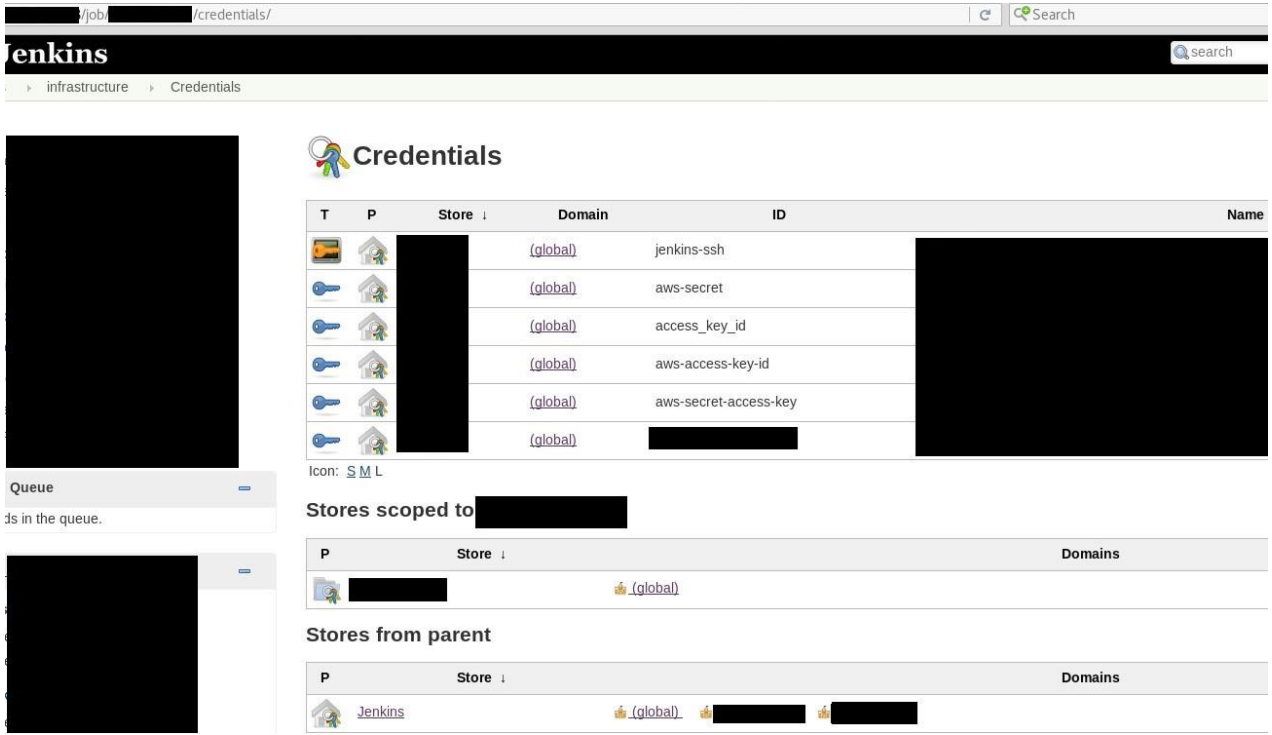
80.0 MB	4 Databases

Database Name	Size
hacked_by_unistellar	80.0 MB
admin	1 byte
playground	1 byte
transport	1 byte

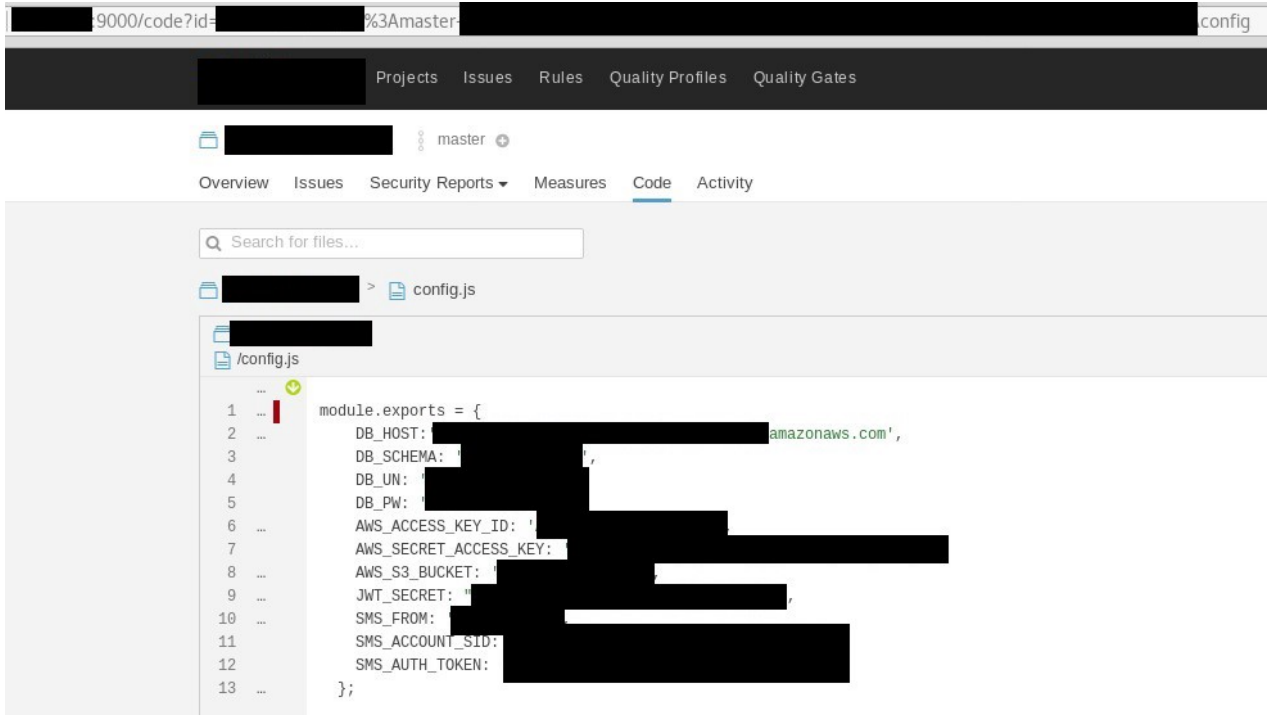
MongoDB Server Information


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

Example: Jenkins



Example: SonarQube

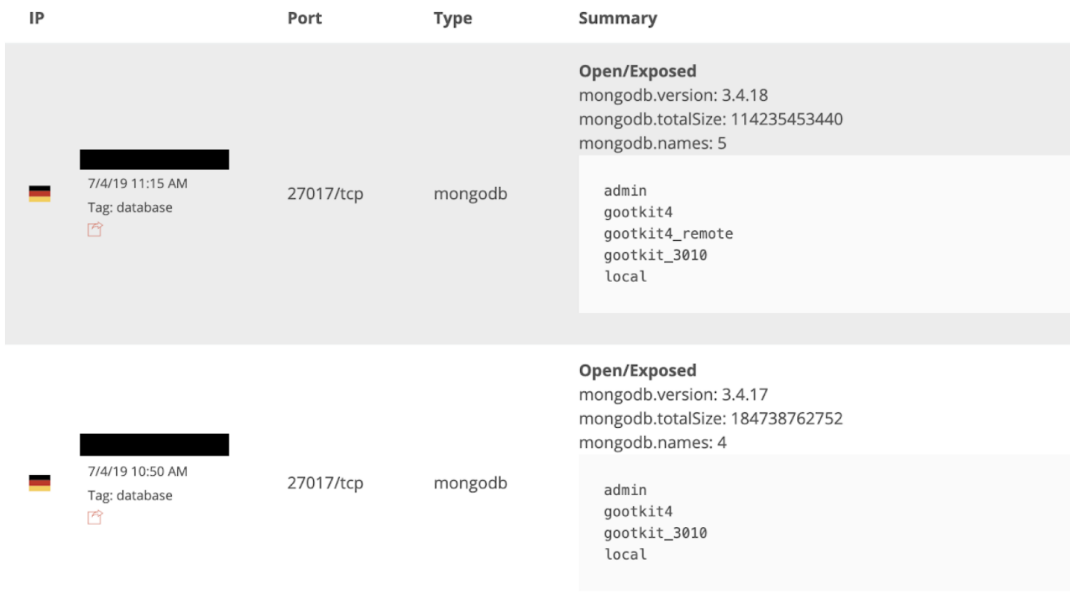


netwrix

GootKit case

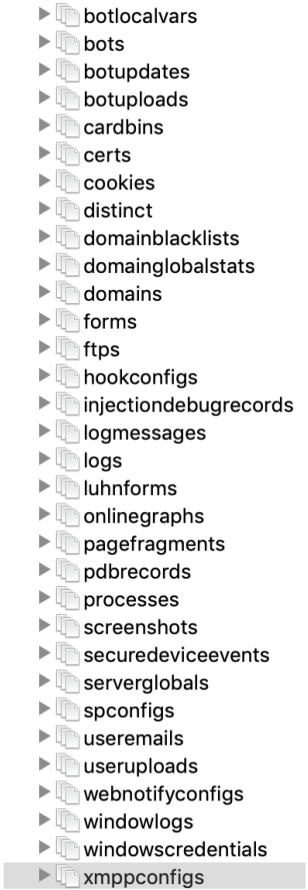
The two Gootkit MongoDBs were public for a week in July.

They went down after that, and never came back online.



GootKit case

The two servers were both running MongoDB, and based on their content, they appeared to be aggregating data from three Gootkit sub-botnets, and a total of 38,653 infected hosts.



netwrix

GootKit case

The two Gootkit MongoDBs also contained configuration files that were being sent to infected hosts. These files contained links to other Gootkit modules. Infected hosts were supposed to download and run these modules to improve the malware's features.

GootKit case

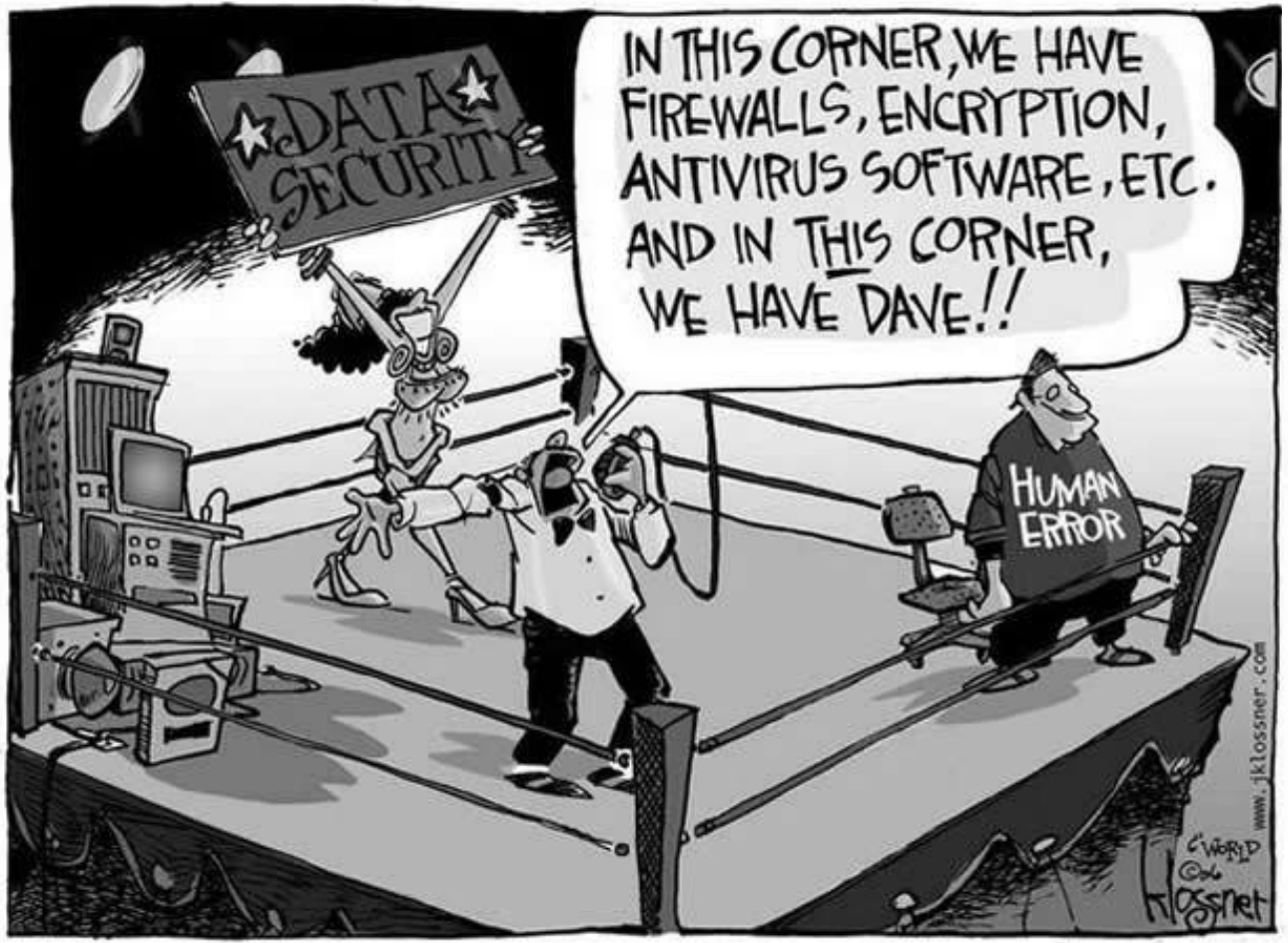
In total, we estimate the following amount of information was compromised:

- **1,444,375** email accounts
- **2,196,840** passwords and configuration pairs: online shops, emails, banking applications, streaming and other online services, internal network passwords, and many more.
- **752,645** usernames

Why Data Breaches Like This Happen?

Misconfiguration caused by firewall settings change, human error or device reset can happen to every company (we don’t talk about targeted hacker attacks).

In cases with misconfigurations and responsible disclosure, companies fail to properly react and communicate because they are scared, stressed, and no one want to take responsibility.


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©2006 JKLOSSNER

2+2 Cyber Hygiene Rules

Follow these three simple cyber hygiene rules:

1. Constantly check your IPs for the critical servers and services from public Internet by using these awesome tools:
    a. Shodan
    b. Zoomeye
    c. BinaryEdge
    d. Censys
    e. RiskIQ analysis

2. Do not reuse passwords. Check emails and passwords for being compromised in data breaches by using:
    a. HaveIBeenPwned tool by Troy Hunt

2+2 Cyber Hygiene Rules

Follow these three simple cyber hygiene rules:

1. Read documentation for your specific database or IoT device: most have best practices on how to secure them (note Elasticsearch news)
2. Add FireWall rules / Access Control Lists so that external / non-authorized devices can't access your data from the Internet

PS: When possible, aggregate what you need and purge the rest. Logs are liability

PPS: Stop hashing in MD5, it is obsolete.

How Netwrix Can Help

Netwrix enables information security and governance professionals to reclaim control over sensitive, regulated and business-critical data, regardless of where it resides.

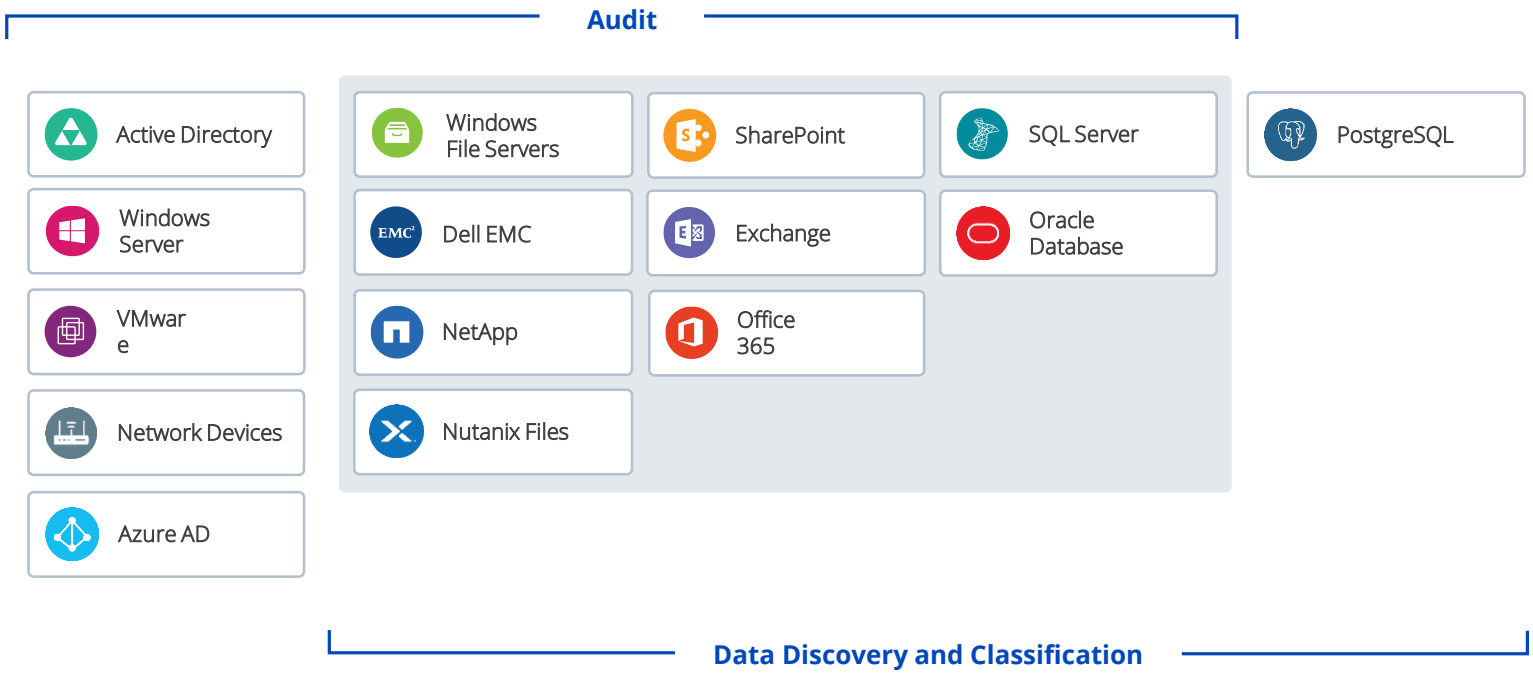
Secure sensitive data

Pass compliance audits with less effort and expense

Realize the full business value of enterprise content

Increase the productivity of IT teams and knowledge workers

Netwrix Data Sources



Demonstration

Useful Links

Free trial

netwrix.com/

Set up Netwrix in your own test environment

In-browser demo

netwrix.com/go/browser_demo

Run a demo right in your browser with no need to install anything

One-to-One demo

netwrix.com/one-to-one

Request a personal demo

Questions?

Thank You!