

# Pro Tips for Defending Your Organization from Data Breaches



Bob Diachenko



Adam Stetson

# 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](#)

## 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



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

# 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



Home » Security » Ride-hailing app leaks personal data of millions of Iranians

## Ride-hailing app leaks personal data of millions of Iranians

📅 APRIL 25TH, 2019    ✉ RYAN DE SOUZA    📁 LEAKS, SECURITY    💬 0 COMMENTS

Trends

## Youth-run agency AIESEC exposed over 4 million intern applications

By inventiva - January 21, 2019

👍 Нравится 3

# 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

# 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

digital shadows\_

Too Much Information: 2.3 Billion Files Exposed Across Online File Storage Technologies

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

Shodan Developers Book View All... Show API Key Help Center

SHODAN Elastic Indices: country:us Explore Downloads Reports Developer Pricing Enterprise Access My Account

Exploits Maps Share Search Download Results Create Report

**TOTAL RESULTS**  
12,185

**TOP COUNTRIES**



United States 12,185

**TOP CITIES**

Ashburn	4,706
Boardman	2,151
Columbus	1,555
New York	610
Mountain View	395

**TOP SERVICES**

HTTP	6,744
ElasticSearch	5,313
HTTP (8080)	33
8060	4
ntp	4

**TOP ORGANIZATIONS**

Amazon.com	8,119
Google Cloud	805
Digital Ocean	672

**34.193.159.9**  
ec2-34-193-159-9.compute-1.amazonaws.com  
Amazon.com  
Added on 2019-03-04 02:04:24 GMT  
United States, Ashburn

cloud database

1.0 MB	1 Nodes
--------	---------

Cluster Name synapse-es-cluster  
Status yellow  
Number of Indices 6

HTTP/1.1 200 OK  
content-type: application/json; charset=UTF-8  
content-length: 498

**Elastic Indices:**

- synapse
- sentence
- twitter
- synapse\_n\_grams
- synapse\_words
- synapse\_sentence

**54.174.129.171**  
ec2-54-174-129-171.compute-1.amazonaws.com  
Amazon.com  
Added on 2019-03-04 02:05:12 GMT  
United States, Ashburn

cloud database compromised

16.0 kB	1 Nodes
---------	---------

Cluster Name 301109733911.coxauto-es-datapipeline-mb  
Status yellow  
Number of Indices 2

HTTP/1.1 200 OK  
Access-Control-Allow-Origin: \*  
Content-Type: application/json; charset=UTF-8  
Content-Length: 461  
Connection: keep-alive

**Elastic Indices:**

- admin
- readme

**18.191.12.95**  
ec2-18-191-12-95.us-east-2.compute.amazonaws.com

HTTP/1.1 200 OK



# Example: How Easy is To Find Public Data

 52.34.235.252 

ec2-52-34-235-252.us-west-2.compute.amazonaws.com

Amazon.com

Added on 2019-03-04 01:35:57 GMT

 United States, Boardman

cloud database



Cluster Name 056092588914.propertyprofile

Status green

Number 2  
of  
Indices

HTTP/1.1 200 OK  
Access-Control-Allow-Origin: \*  
Content-Type: application/json; charset=UTF-8  
Content-Length: 342  
Connection: keep-alive

Elastic Indices:

.kibana  
propertyprofiles\_1

 52.7.195.176 

ec2-52-7-195-176.compute-1.amazonaws.com

Amazon.com

Added on 2019-03-04 01:25:42 GMT

 United States, Ashburn

cloud database



Cluster Name 509783430292.loganalysisdomain

Status yellow

Number 6  
of  
Indices

HTTP/1.1 200 OK  
Access-Control-Allow-Origin: \*  
Content-Type: application/json; charset=UTF-8  
Content-Length: 344  
Connection: keep-alive

Elastic Indices:

admin  
jbossmq-httpil  
zabbix  
.kibana  
prathilog  
invoker

# Example: Remote Desktop Protocols

The screenshot displays a web interface for SHODAN, a search engine for Internet-connected devices. The search query is "country:DE" and the results are filtered to "Images". A "Logout" button is visible in the top right corner.

The main content area is a grid of seven remote desktop sessions:

- Top Row:**
  - Session 1: Windows Server 2012 R2 desktop with Administrator login screen.
  - Session 2: Windows 7 Ultimate desktop with Administrator login screen.
  - Session 3: Windows Small Business Server 2011 desktop with FAST\admin login screen.
  - Session 4: Webcam feed of a street intersection with a white van, labeled "Webcam In Rastede".
- Bottom Row:**
  - Session 5: Windows Server 2012 R2 desktop with Administrator login screen.
  - Session 6: Desktop with a scenic background and "opc" logo.
  - Session 7: Windows Server 2012 R2 desktop with Administrator login screen.
  - Session 8: Windows Server 2008 R2 desktop with Administrator and Paul Administrator icons.



# 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
```





# Example: MongoDB

**94.177.229.25**

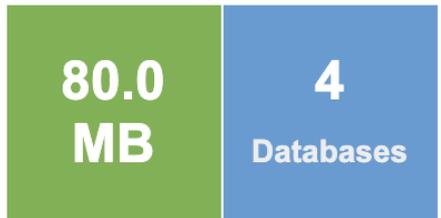
host25-229-177-94.static.arubacloud.de

**Aruba S.p.A.**

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

 Germany, Frankfurt

database



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 screenshot of the Jenkins Credentials page. The browser address bar shows `/job/[redacted]/credentials/`. The Jenkins header shows the breadcrumb `infrastructure > Credentials` and a search bar.

## Credentials

T	P	Store	Domain	ID	Name
		[redacted]	(global)	jenkins-ssh	[redacted]
		[redacted]	(global)	aws-secret	[redacted]
		[redacted]	(global)	access_key_id	[redacted]
		[redacted]	(global)	aws-access-key-id	[redacted]
		[redacted]	(global)	aws-secret-access-key	[redacted]
		[redacted]	(global)	[redacted]	[redacted]

Icon: [S](#) [M](#) [L](#)

### Stores scoped to [redacted]

P	Store	Domains
	[redacted]	(global)

### Stores from parent

P	Store	Domains
	Jenkins	(global)  [redacted]  [redacted]



# Example: SonarQube

The screenshot displays the SonarQube web interface. At the top, there is a navigation bar with links for Projects, Issues, Rules, Quality Profiles, and Quality Gates. Below this, the current project is identified as 'master'. The main navigation includes Overview, Issues, Security Reports, Measures, Code, and Activity. A search bar for files is present, and the current file being viewed is 'config.js'. The code content is as follows:

```
...  
1 ... module.exports = {  
2 ...   DB_HOST: '...',  
3 ...   DB_SCHEMA: '...',  
4 ...   DB_UN: '...',  
5 ...   DB_PW: '...',  
6 ...   AWS_ACCESS_KEY_ID: '...',  
7 ...   AWS_SECRET_ACCESS_KEY: '...',  
8 ...   AWS_S3_BUCKET: '...',  
9 ...   JWT_SECRET: '...',  
10 ...   SMS_FROM: '...',  
11 ...   SMS_ACCOUNT_SID: '...',  
12 ...   SMS_AUTH_TOKEN: '...',  
13 ... };
```

# GootKit case

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

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

IP	Port	Type	Summary
 [REDACTED] 7/4/19 11:15 AM Tag: database	27017/tcp	mongodb	<b>Open/Exposed</b> mongodb.version: 3.4.18 mongodb.totalSize: 114235453440 mongodb.names: 5  admin gootkit4 gootkit4_remote gootkit_3010 local
 [REDACTED] 7/4/19 10:50 AM Tag: database	27017/tcp	mongodb	<b>Open/Exposed</b> mongodb.version: 3.4.17 mongodb.totalSize: 184738762752 mongodb.names: 4  admin gootkit4 gootkit_3010 local



# 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.

- ▶ botlocalvars
- ▶ bots
- ▶ botupdates
- ▶ botuploads
- ▶ cardbins
- ▶ certs
- ▶ cookies
- ▶ distinct
- ▶ domainblacklists
- ▶ domainglobalstats
- ▶ domains
- ▶ forms
- ▶ ftps
- ▶ hookconfigs
- ▶ injectiondebugrecords
- ▶ logmessages
- ▶ logs
- ▶ luhnforms
- ▶ onlinegraphs
- ▶ pagefragments
- ▶ pdbrecords
- ▶ processes
- ▶ screenshots
- ▶ securedeviceevents
- ▶ serverglobals
- ▶ spconfigs
- ▶ useremails
- ▶ useruploads
- ▶ webnotifyconfigs
- ▶ windowlogs
- ▶ windowscredentials
- ▶ xmppconfigs



# 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.

```
],
  "IsVirtualMachine" : false,
  "asnNumber" : ██████████,
  "asnShortName" : "VODAFONE-IT-ASN",
  "asnLongName" : "Vodafone Omnitel N.V.",
  "asnCidrAddress" : ██████████,
  "installDate" : ISODate("2017-06-05T15:11:11.418+0000"),
  "vendor" : ██████████,
  "isMaximumRatingRaised" : false,
  "isBadProcessDetectedOnce" : false,
  "memo" : "\r\nhotmail : ██████████@hotmail.it; ██████████\r\nhotmail : ██████████@hotmail.it; ██████████",
  "privateInject" : "{\\"injects\\":{\\"base\\":{\\"url\\":{\\"https://jquery*.js*\\",\\"https://apis.google.com/js/client.js*\\",\\"ht",
  "privateScript" : "process.cookieGrabber.grabCookiesToServer = true; /*auto-generated by paypal plugin*/\r\n"
}

-----

  "_id" : ObjectId("██████████e1e"),
  "guid" : "██████████e89848ec44",
  "processName" : "C:\\Windows\\system32\\██████████",
  "last_vendor" : [
    ██████████
  ],
  "internalAddress" : ██████████,
  "externalAddress" : ██████████,
  "reverseAddr" : "██████████.net",
  "country" : "FR",
  "os" : "Windows NT 6.1.7601 (ia32)",
  "ie" : ██████████,
  "ver" : "v0.11.15.31.05.17.1441",
  "uptime" : 1138802,
  "upspeed" : 0,
  "downspeed" : 0,
  "lastActivity" : ISODate("2017-08-02T18:56:17.970+0000"),
  "HomePath" : "\\Users\\██████████",
  "ComputerName" : "██████████",
  "SystemDrive" : "C:",
  "SystemRoot" : "C:\\Windows",
  "UserDomain" : "██████████",
  "UserName" : "██████████",
  "UserProfile" : "C:\\Users\\██████████",
  "LogonServer" : "\\",
  "tmpdir" : "C:\\Users\\██████████\\AppData\\Local\\Temp",
  "domain" : "██████████.com",
  "freemem" : 1550098432,
  "totalmem" : 3081797632.0,
  "networkInterfaces" : [
    ██████████
  ]
}
```

# GootKit case

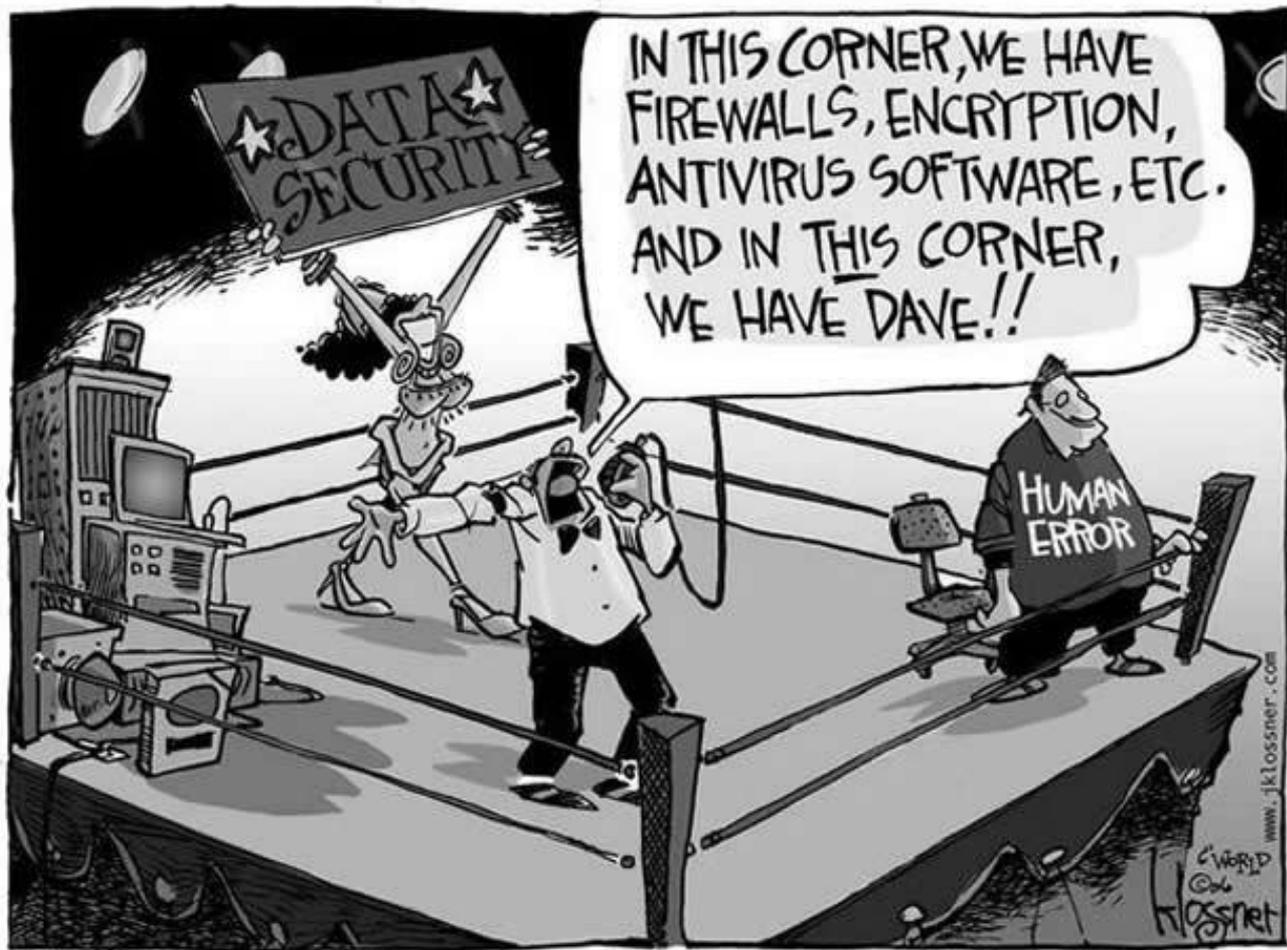
In total, we estimate the following amount of information was compromised:

- **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.



# 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. [HavelBeenPwned 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



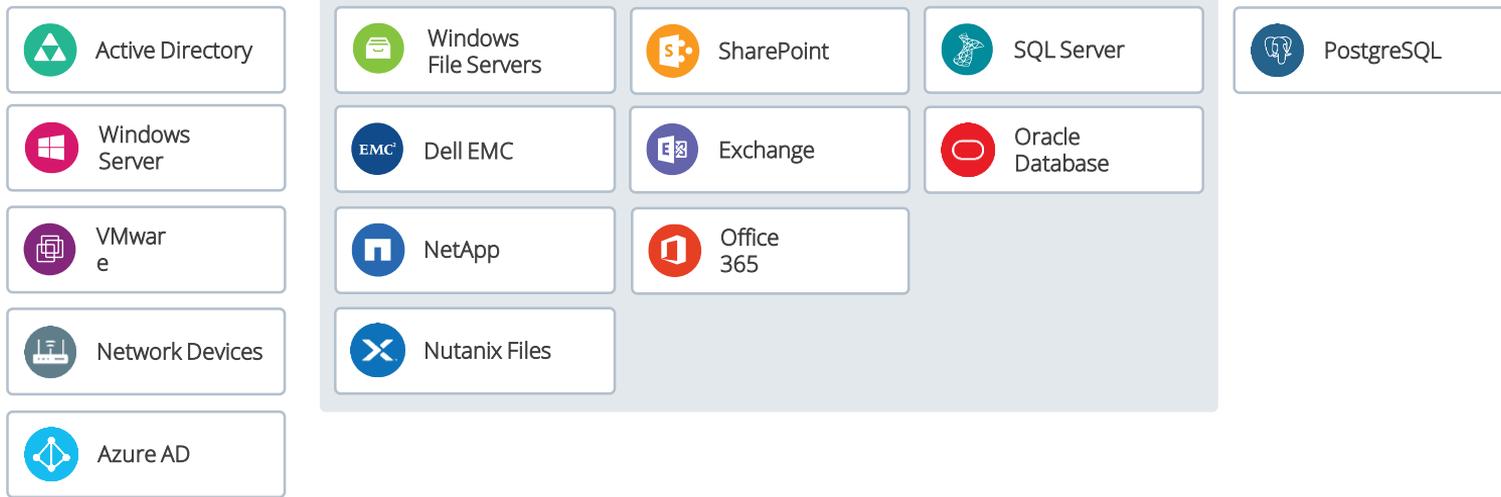
**Realize the full business value** of enterprise content



**Increase the productivity**  
of IT teams and knowledge workers

# Netwrix Data Sources

## Audit





# Demonstration

# Useful Links



Free trial

[netwrix.com/](https://netwrix.com/)

Set up Netwrix in your own test environment



In-browser demo

[netwrix.com/go/browser\\_demo](https://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](https://netwrix.com/one-to-one)

Request a personal demo



# Questions?

Thank You!