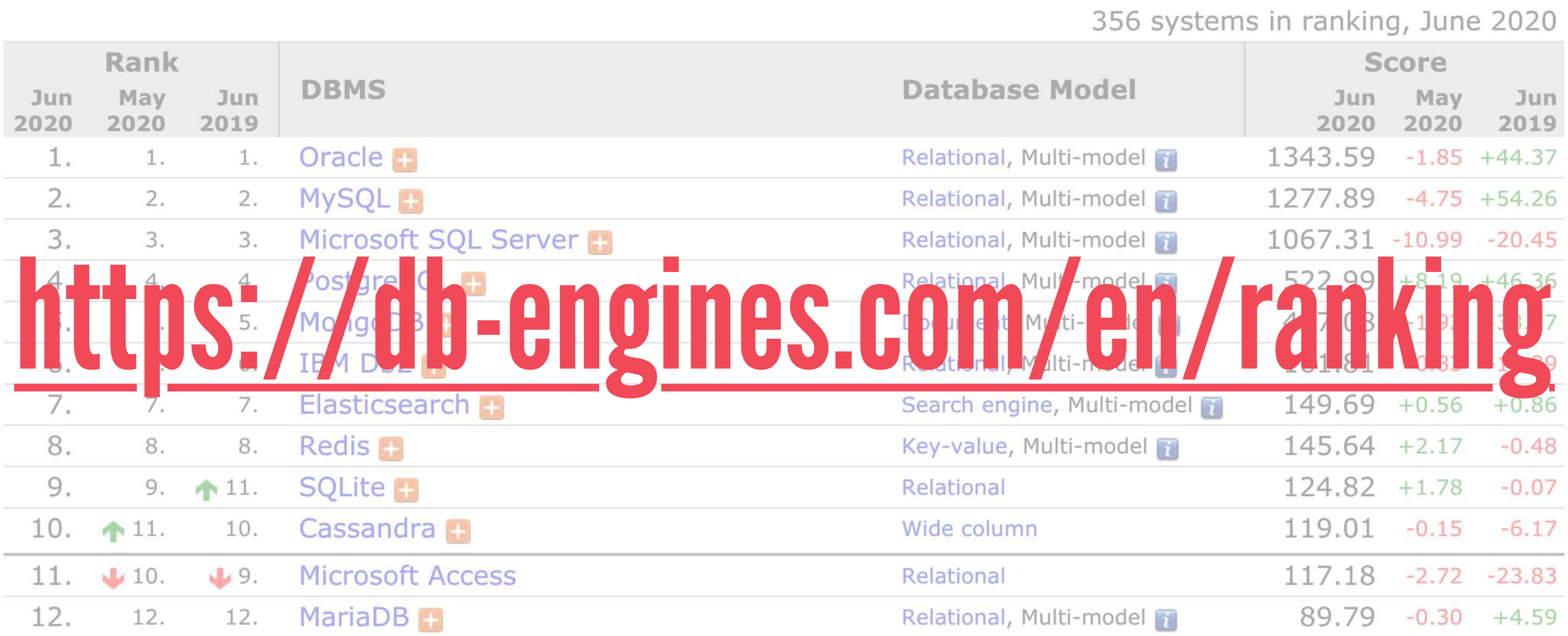
NoSQL MEANS No SECURITY?

Philipp Krenn @xeraa

elastic

elastic

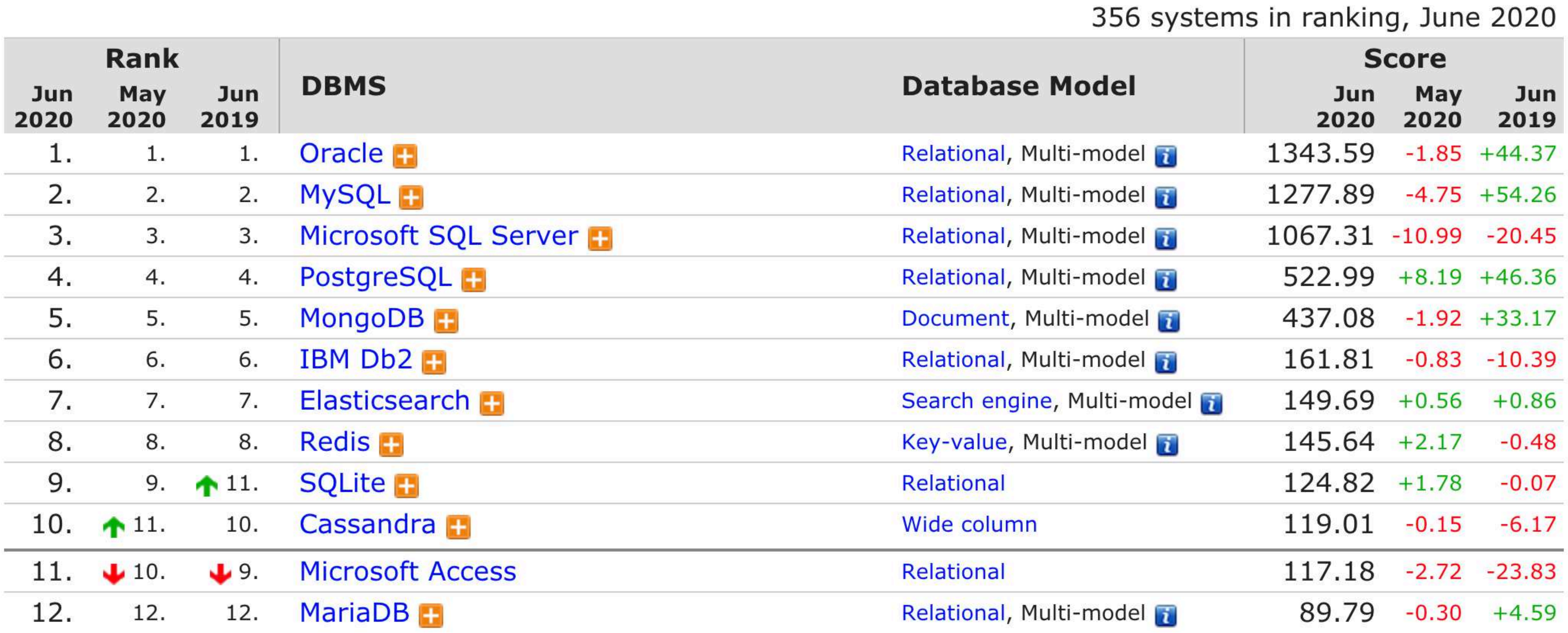
DEVELOPER 🥑



356 systems in ranking, June 2020

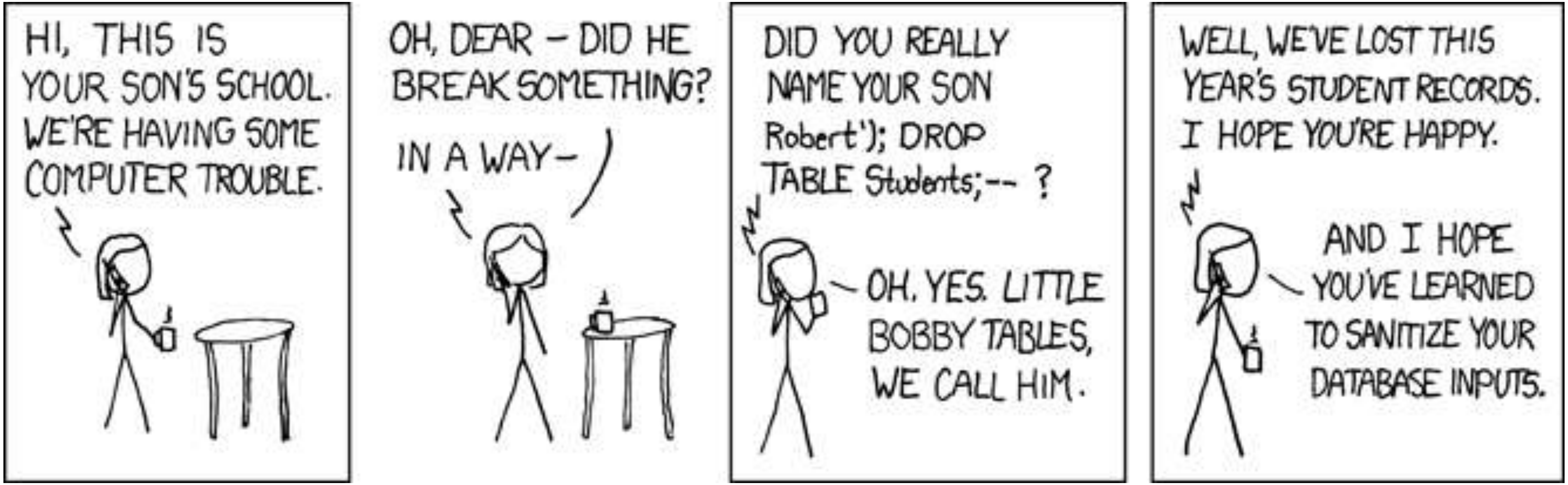
Rank			DBMS	Database Model	Score		
Jun 2020	May 2020	Jun 2019			Jun 2020	May 2020	Jun 2019
1.	1.	1.	Oracle ➕	Relational, Multi-model ℹ	1343.59	-1.85	+44.37
2.	2.	2.	MySQL ➕	Relational, Multi-model ℹ	1277.89	-4.75	+54.26
3.	3.	3.	Microsoft SQL Server ➕	Relational, Multi-model ℹ	1067.31	-10.99	-20.45
4.	4.	4.	PostgreSQL ➕	Relational, Multi-model ℹ	522.99	+8.19	+46.36
5.	[illegible]	5.	MongoDB ➕	Document, Multi-model ℹ	[illegible]	[illegible]	[illegible]
6.	[illegible]	6.	IBM Db2 ➕	Relational, Multi-model ℹ	[illegible]	[illegible]	[illegible]
7.	7.	7.	Elasticsearch ➕	Search engine, Multi-model ℹ	149.69	+0.56	+0.86
8.	8.	8.	Redis ➕	Key-value, Multi-model ℹ	145.64	+2.17	-0.48
9.	9.	↑ 11.	SQLite ➕	Relational	124.82	+1.78	-0.07
10.	↑ 11.	10.	Cassandra ➕	Wide column	119.01	-0.15	-6.17
11.	↓ 10.	↓ 9.	Microsoft Access	Relational	117.18	-2.72	-23.83
12.	12.	12.	MariaDB ➕	Relational, Multi-model ℹ	89.79	-0.30	+4.59

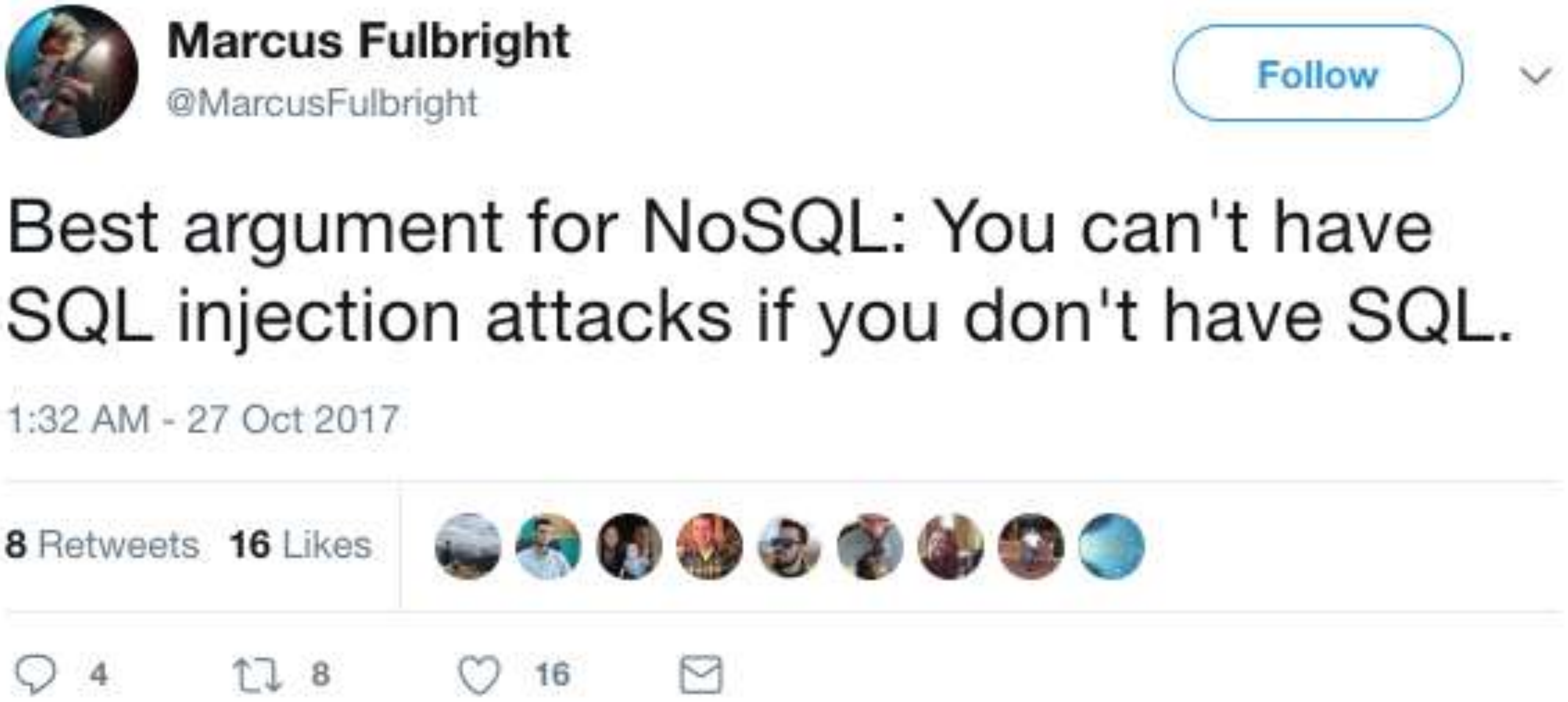
https://db-engines.com/en/ranking



356 systems in ranking, June 2020

Rank			DBMS	Database Model	Score		
Jun 2020	May 2020	Jun 2019			Jun 2020	May 2020	Jun 2019
1.	1.	1.	Oracle	Relational, Multi-model	1343.59	-1.85	+44.37
2.	2.	2.	MySQL	Relational, Multi-model	1277.89	-4.75	+54.26
3.	3.	3.	Microsoft SQL Server	Relational, Multi-model	1067.31	-10.99	-20.45
4.	4.	4.	PostgreSQL	Relational, Multi-model	522.99	+8.19	+46.36
5.	5.	5.	MongoDB	Document, Multi-model	437.08	-1.92	+33.17
6.	6.	6.	IBM Db2	Relational, Multi-model	161.81	-0.83	-10.39
7.	7.	7.	Elasticsearch	Search engine, Multi-model	149.69	+0.56	+0.86
8.	8.	8.	Redis	Key-value, Multi-model	145.64	+2.17	-0.48
9.	9.	↑ 11.	SQLite	Relational	124.82	+1.78	-0.07
10.	↑ 11.	10.	Cassandra	Wide column	119.01	-0.15	-6.17
11.	↓ 10.	↓ 9.	Microsoft Access	Relational	117.18	-2.72	-23.83
12.	12.	12.	MariaDB	Relational, Multi-model	89.79	-0.30	+4.59


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.



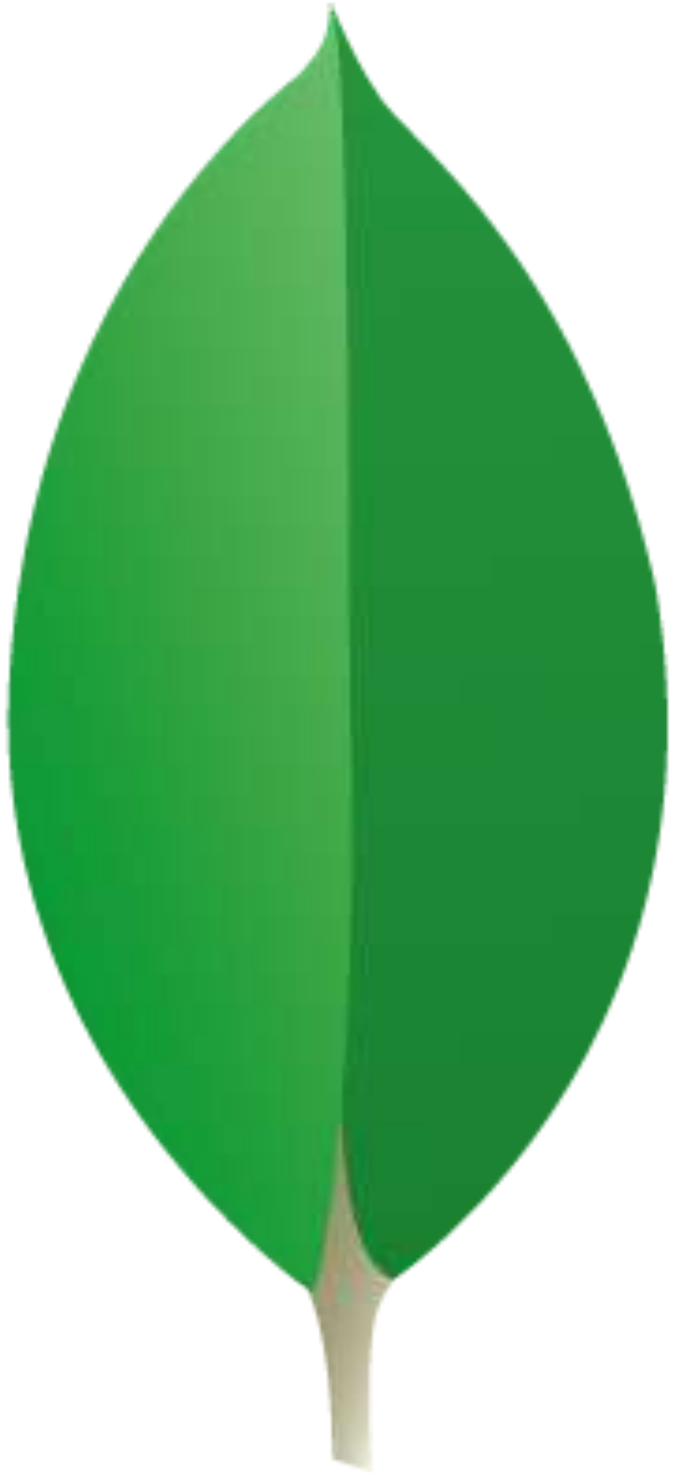
Marcus Fulbright
@MarcusFulbright

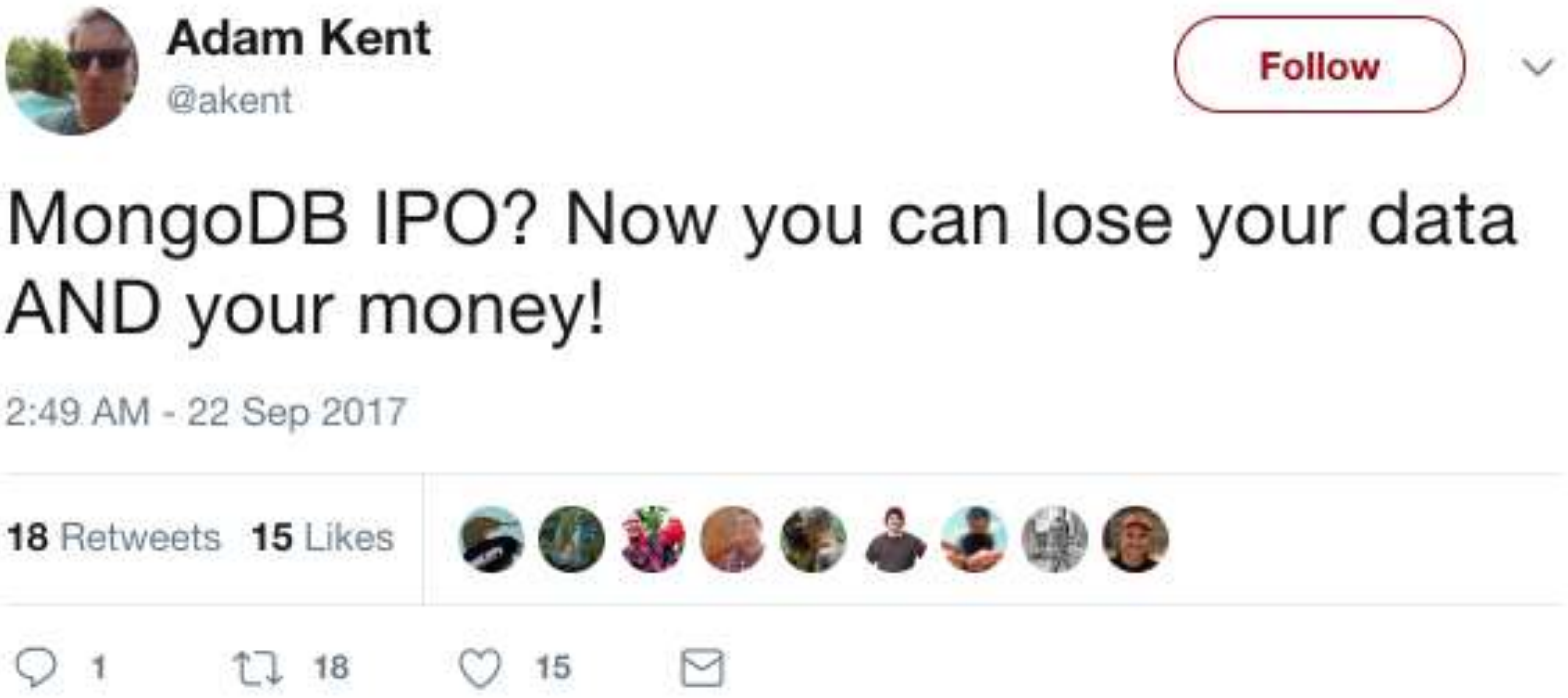
Best argument for NoSQL: You can't have SQL injection attacks if you don't have SQL.

1:32 AM - 27 Oct 2017

8 Retweets 16 Likes

4 8 16





Adam Kent
@akent

MongoDB IPO? Now you can lose your data AND your money!

2:49 AM - 22 Sep 2017

18 Retweets **15** Likes

Injections

JavaScript Injection

HTTP://WWW.KALZUMEUS.COM/2010/09/22/SECURITY-LESSONS-LEARNED-FROM-THE-DIASPORA-LAUNCH/

```
def self.search(query)
  Person.all('$where' => "function() {
    return this.diaspora_handle.match(/^#{query}/i) ||
           this.profile.first_name.match(/^#{query}/i) ||
           this.profile.last_name.match(/^#{query}/i);
  }")
end
```

Problem JS Evaluation

```
$where

db.eval()

db.runCommand( { mapReduce:

db.collection.group()
```

Solution JS Evaluation

`--NOSCRIPTING` **OR** `SECURITY.JAVASCRIPTENABLED: FALSE`

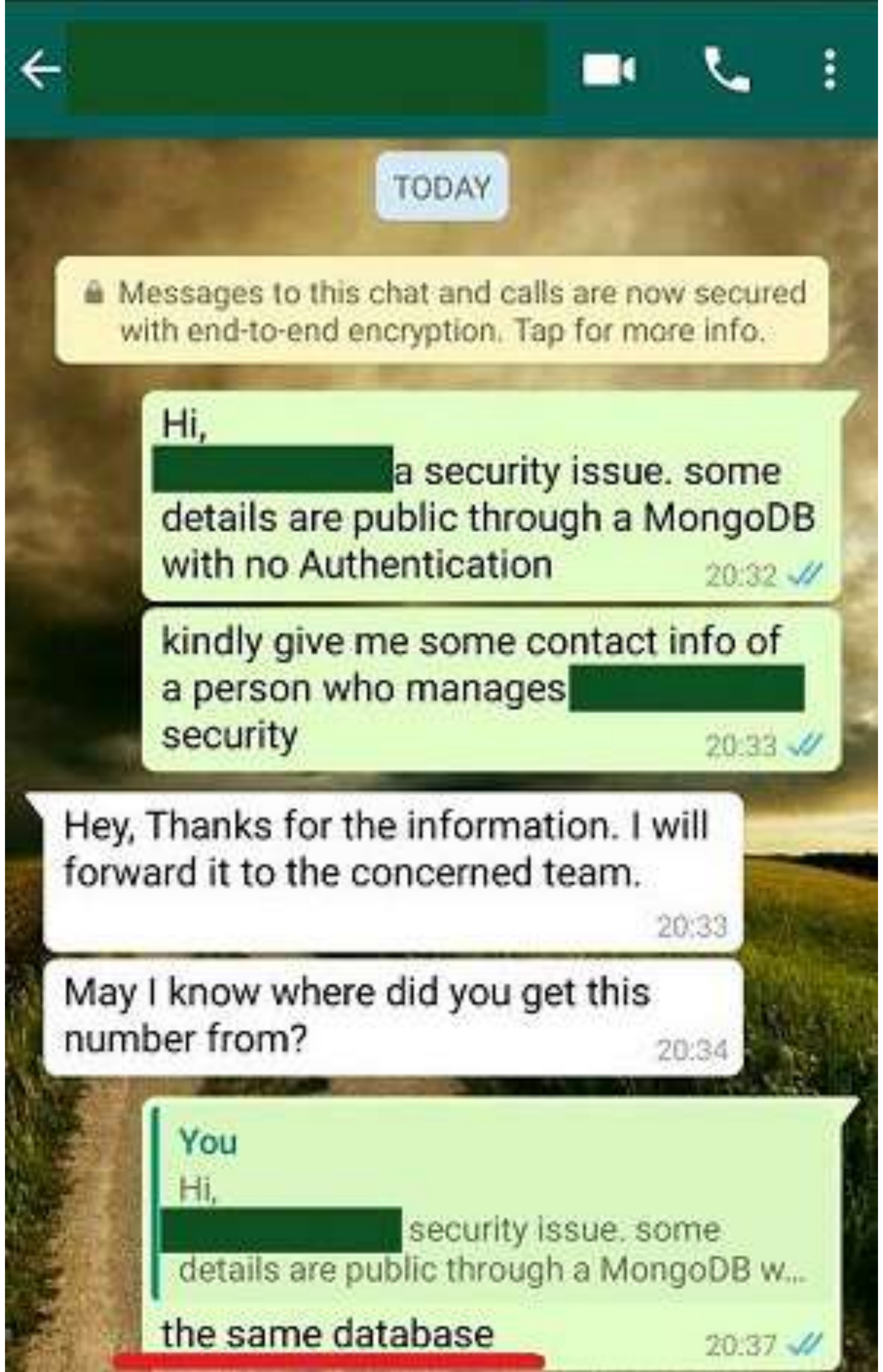
Authentication

Saarbrücker Cybersicherheits-Studenten entdecken bis zu 40.000 ungesicherte Datenbanken im Internet

– http://www.uni-saarland.de/nc/aktuelles/artikel/nr/12173.html, Feb 2015

Massive ransomware attack takes out 27,000 MongoDB servers

– http://www.techrepublic.com/article/massive-ransomware-attack-takes-out-27000-mongodb-servers/, Jan 2017 https://twitter.com/ashu_barot/status/1129081068819058688



[redacted]

TODAY

Messages to this chat and calls are now secured with end-to-end encryption. Tap for more info.

Hi,
[redacted] a security issue. some details are public through a MongoDB with no Authentication 20:32

kindly give me some contact info of a person who manages [redacted] security 20:33

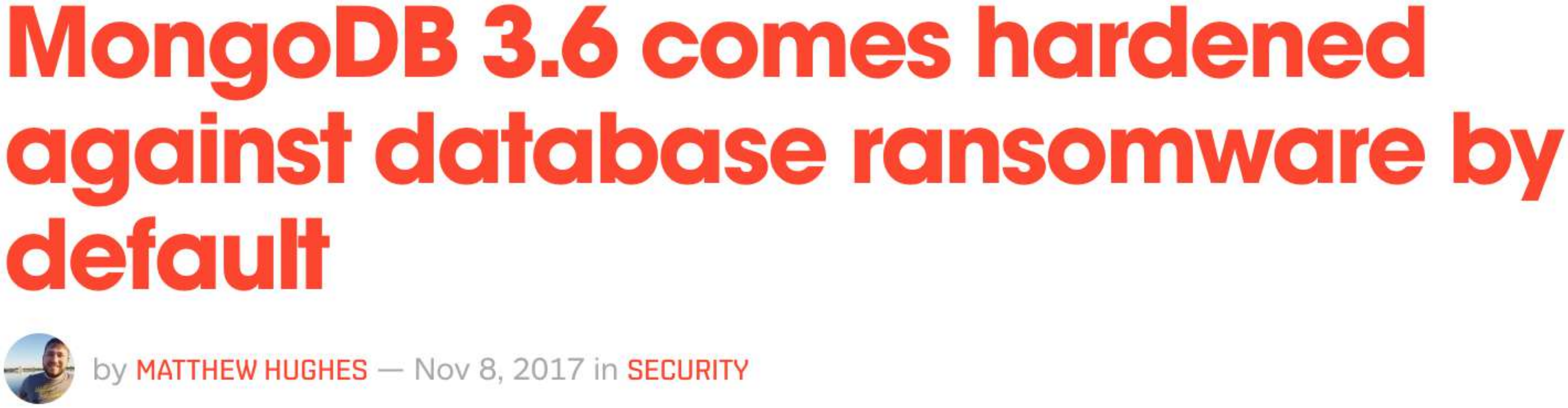
Hey, Thanks for the information. I will forward it to the concerned team. 20:33

May I know where did you get this number from? 20:34

You
Hi,
[redacted] security issue. some details are public through a MongoDB w...

the same database 20:37

Bound to all interfaces by default?



MongoDB 3.6 comes hardened against database ransomware by default

by MATTHEW HUGHES — Nov 8, 2017 in SECURITY

Authentication enabled by default?

Enable

AUTH=TRUE **OR** --AUTH

>=3.0

TLS INCLUDED

(ALMOST) EVERYWHERE

redis

Injections

> While it would be a very strange use case, the application should avoid composing the body of the Lua script using strings obtained from untrusted sources.

– http://redis.io/topics/security

> Redis EVAL command allows execution of Lua scripts, and such feature should be allowed by default since is a fundamental Redis feature.
>
> — http://antirez.com/news/118, Jun 2018

> Redis Lua scripting: several security vulnerabilities fixed

— http://antirez.com/news/119, Jun 2018

Authentication

Research shows 75% of 'open' Redis servers infected

— https://www.incapsula.com/blog/report-75-of-open-redis-servers-are-infected.html, May 2018

> Let's crack Redis for fun and no profit at all given I'm the developer of this thing
>
> – http://antirez.com/news/96, Nov 2015

Bound to all interfaces by default?

Protected Mode

>=3.2.0

ANSWER LOCAL QUERIES
RESPOND WITH AN ERROR FOR REMOTE

<6.0

tiny layer of authentication that is optionally turned on

– http://redis.io/topics/security

`AUTH <PASSWORD>` COMMAND

PLAIN-TEXT PASSWORD IN REDIS.CONF

NO (BUILT-IN) TLS OR RATE LIMITS

>=6.0

ACL: `AUTH <USER> <PASSWORD>`

PLAIN-TEXT XOR SHA-256 IN ACL.CONF

```
MAKE BUILD_TLS=YES
```

Hiding Commands

SET IN REDIS.CONF

RESET AFTER RESTART

```
RENAME-COMMAND CONFIG
MYSECRETCONFIGNAME
```

```
RENAME-COMMAND CONFIG ""
```

elasticsearch

elastic

Bound to all interfaces by default?

FREE SECURITY SINCE 6.8 / 7.1

https://www.elastic.co/blog/security-for-elasticsearch-is-now-free

Authentication enabled by default?

Scripting

ELASTICSEARCH

https://www.elastic.co/community/security

```
CVE-2014-3120 (6.8): Dynamic scripting
CVE-2015-1427 (6.8): Groovy sandbox escape
CVE-2015-5377 (5.1): RCE related to Groovy
```

Painless

HIRED DEVELOPER

1 YEAR DEVELOPMENT

> Why build a brand new language when there are already so many to choose from?
>
> – https://www.elastic.co/blog/painless-a-new-scripting-language

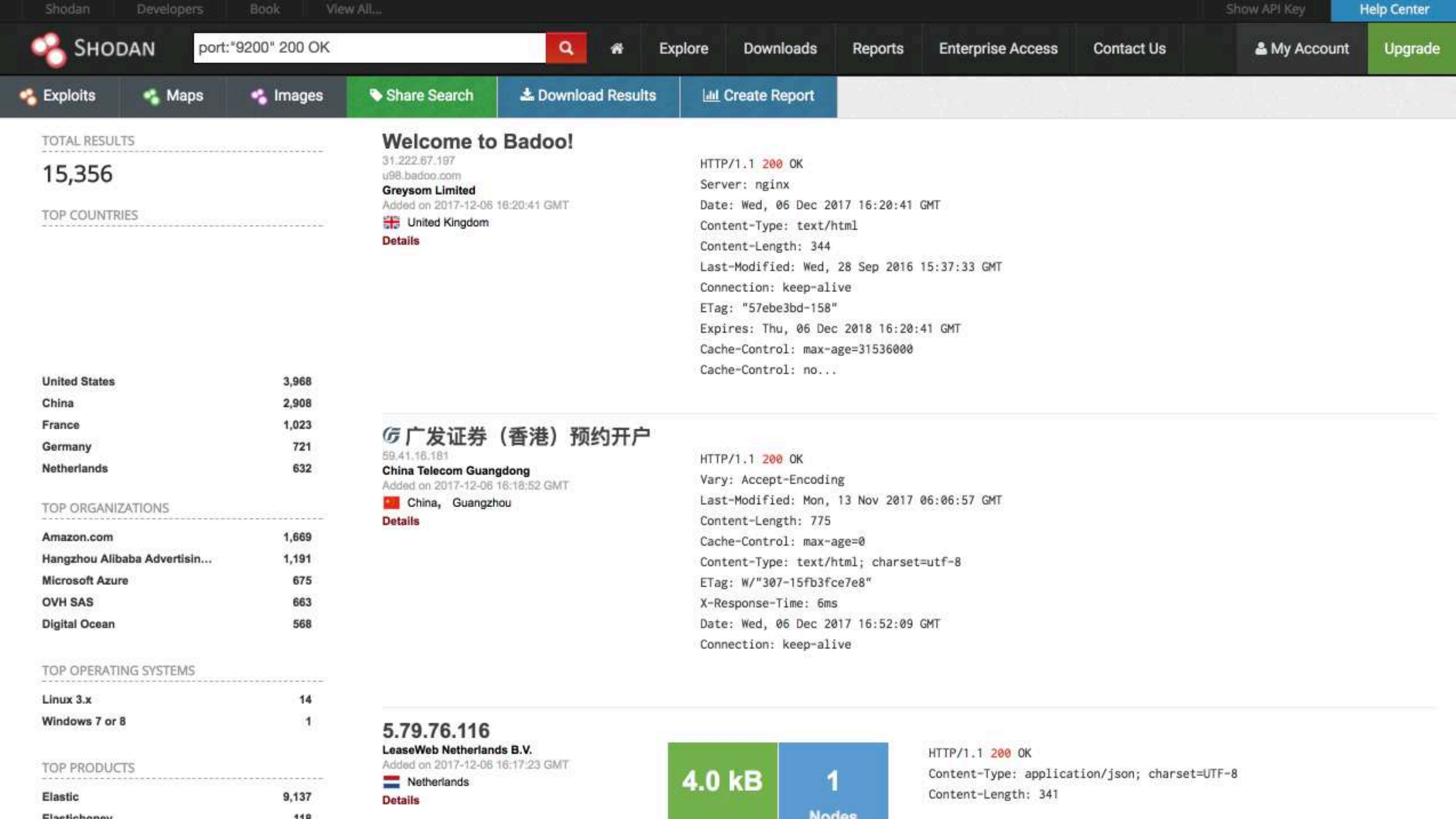
Goal

SECURE & PERFORMANT

Removed

GROOVY, PYTHON, JAVASCRIPT IN 6.0

Ransoming



TOTAL RESULTS

15,356

TOP COUNTRIES

United States	3,968
China	2,908
France	1,023
Germany	721
Netherlands	632

TOP ORGANIZATIONS

Amazon.com	1,669
Hangzhou Alibaba Advertisin...	1,191
Microsoft Azure	675
OVH SAS	663
Digital Ocean	568

TOP OPERATING SYSTEMS

Linux 3.x	14
Windows 7 or 8	1

TOP PRODUCTS

Elastic	9,137
Elastichoney	118

Welcome to Badoo!

31.222.67.197
u98.badoo.com
Greysom Limited
Added on 2017-12-06 16:20:41 GMT
United Kingdom
Details

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 06 Dec 2017 16:20:41 GMT
Content-Type: text/html
Content-Length: 344
Last-Modified: Wed, 28 Sep 2016 15:37:33 GMT
Connection: keep-alive
ETag: "57ebe3bd-158"
Expires: Thu, 06 Dec 2018 16:20:41 GMT
Cache-Control: max-age=31536000
Cache-Control: no...
```

广发证券（香港）预约开户

59.41.16.181
China Telecom Guangdong
Added on 2017-12-06 16:18:52 GMT
China, Guangzhou
Details

```
HTTP/1.1 200 OK
Vary: Accept-Encoding
Last-Modified: Mon, 13 Nov 2017 06:06:57 GMT
Content-Length: 775
Cache-Control: max-age=0
Content-Type: text/html; charset=utf-8
ETag: W/"307-15fb3fce7e8"
X-Response-Time: 6ms
Date: Wed, 06 Dec 2017 16:52:09 GMT
Connection: keep-alive
```

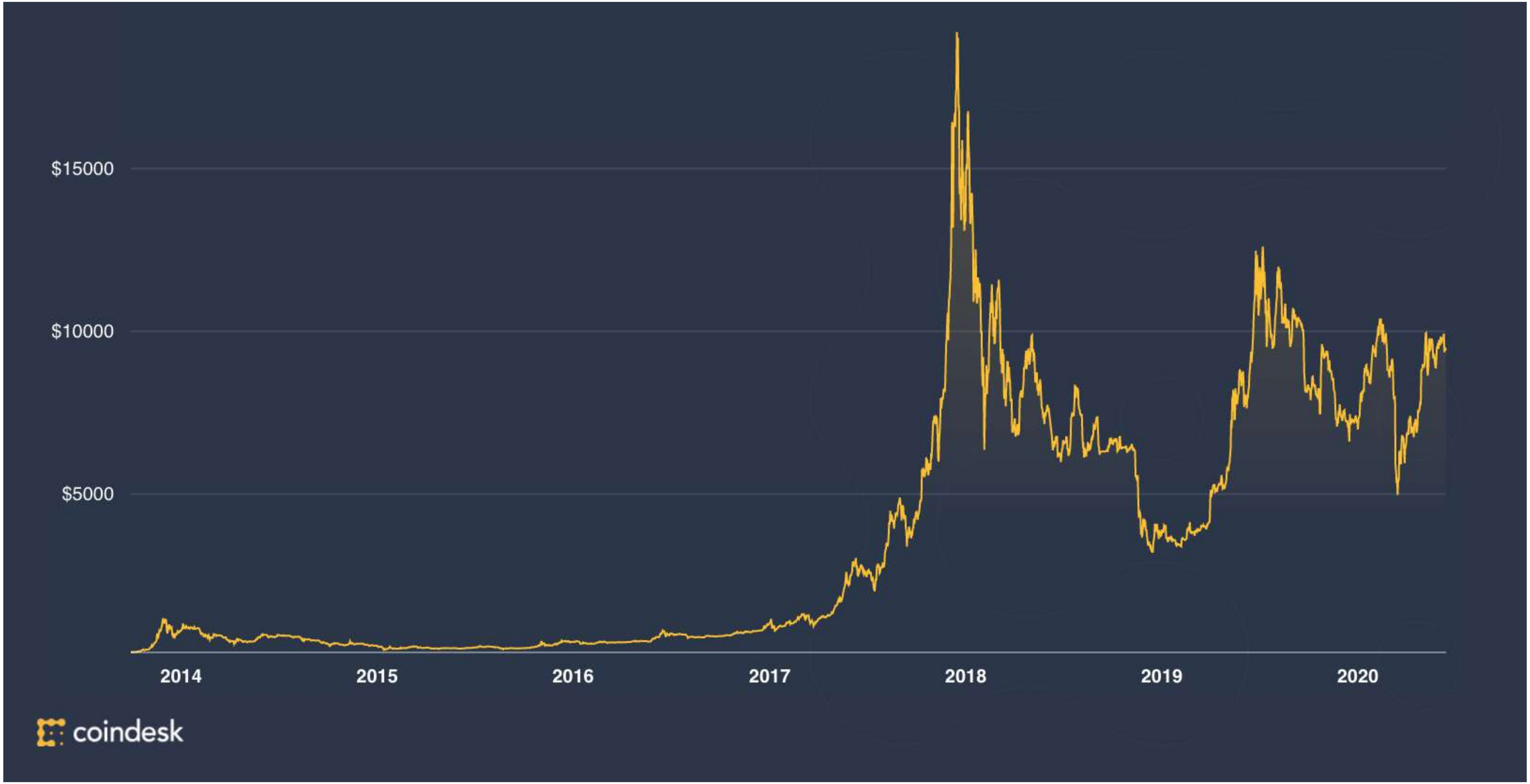
5.79.76.116

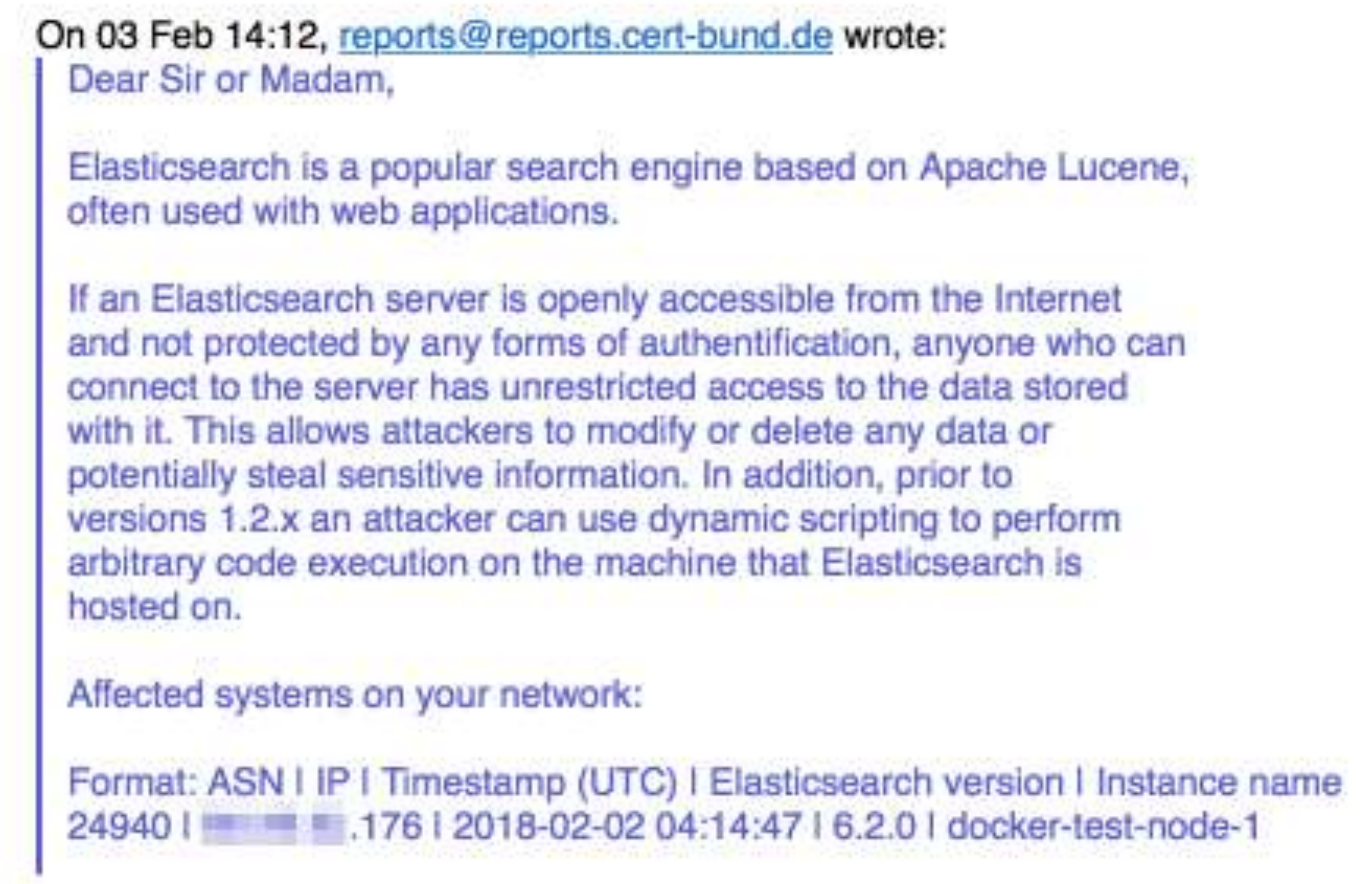
LeaseWeb Netherlands B.V.
Added on 2017-12-06 16:17:23 GMT
Netherlands
Details

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Content-Length: 341
```

```
$ curl -XGET 'http://67.205.153.88:9200/_cat/indices'
yellow open goal12      5 1 9397 0   27mb   27mb
yellow open please_read 5 1    1 0  4.9kb  4.9kb
yellow open un-webhose  5 1 2294 1 25.4mb 25.4mb
yellow open goal11      5 1 4828 0 13.3mb 13.3mb
```

```
$ curl -XGET 'http://67.205.153.88:9200/please_read/_search?pretty'
{
  "took" : 1,
  "timed_out" : false,
  "_shards" : {
    "total" : 5,
    "successful" : 5,
    "failed" : 0
  },
  "hits" : {
    "total" : 1,
    "max_score" : 1.0,
    "hits" : [ {
      "_index" : "please_read",
      "_type" : "info",
      "_id" : "AVm3qmXeus_FduwRD54v",
      "_score" : 1.0,
      "_source" : {
        "Info" : "Your DB is Backed up at our servers, to restore send 0.5 BTC
                  to the Bitcoin Address then send an email with your server ip",
        "Bitcoin Address" : "12JNfaS2Gzic2vqzGMvDEo38MQSX1kDQrx",
        "Email" : "elasticsearch@mail2tor.com"
      }
    } ]
  }
}
```


$15000
$10000
$5000
2014
2015
2016
2017
2018
2019
2020
coindesk



On 03 Feb 14:12, reports@reports.cert-bund.de wrote:

> Dear Sir or Madam,
>
> Elasticsearch is a popular search engine based on Apache Lucene, often used with web applications.
>
> If an Elasticsearch server is openly accessible from the Internet and not protected by any forms of authentification, anyone who can connect to the server has unrestricted access to the data stored with it. This allows attackers to modify or delete any data or potentially steal sensitive information. In addition, prior to versions 1.2.x an attacker can use dynamic scripting to perform arbitrary code execution on the machine that Elasticsearch is hosted on.
>
> Affected systems on your network:
>
> Format: ASN | IP | Timestamp (UTC) | Elasticsearch version | Instance name
> 24940 | [redacted].176 | 2018-02-02 04:14:47 | 6.2.0 | docker-test-node-1

redis elasticsearch

Conclusion

Injections Are Still a Thing

Enable Security

Be Creative — Or Not

Custom Scripting Can Make Sense

Security Takes Time

Thanks!

QUESTIONS?

Philipp Krenn @xeraa

elastic