
mongoDB
Graph
• InfiniteGraph
• DEX
• Neo4j
• OrientDB
•NuvolaBase
Document
•RavenDB
• MongoDB
• CouchDB
• Cloudant
•DynamoDB
• Redis-to-go
• Riak
Membrain
{ "_id" : ObjectId("506c734adbd73afa9
"bd" : "-2208932970",
"cd" : 1349183839,
"em" : "unesco@gmail.com",
"hhid" : ObjectId("506ae95f053b045f0f00001a"),
"ia" : 1,
"id" : "2",
"ll" : 1349183839,
"nm" : "UNESCO",
"pl" : "",
"pt" : "50b8a347f1c7
"pw" : "nGGnRYx0p03
"ty" : 3,
"ud" : 1349183839
LOL
MUNDO HACKER
By s4ur0n

MONGOLOL

Whoami

Deloitte.
CyberSOC Academy

```
class PedroC:
    def __init__(self):
        self.name = 'Pedro Candel'
        self.email1 = 'pcandel@cybersoc.deloitte.es'
        self.email2 = 's4ur0n@s4ur0n.com'
        self.website = 'http://www.s4ur0n.com'
        self.nickname = '@NN2ed_s4ur0n'
        self.role = 'Security Researcher'
        self.interest = [ 'Reversing', 'Malware', 'Offensive Security' ]
        self.member_of = [ 'mlw.re', 'OWASP', 'FAQin', ... ]
```

MONGOL_OL

General Concepts

Introducción

- **MongoDB** es un sistema gestor de base de datos orientado a documentos del tipo **NoSQL** (Not Only SQL) multiplataforma
- Desde 2009 inicialmente desarrollado por 10gen
- Más de **9 millones de descargas**

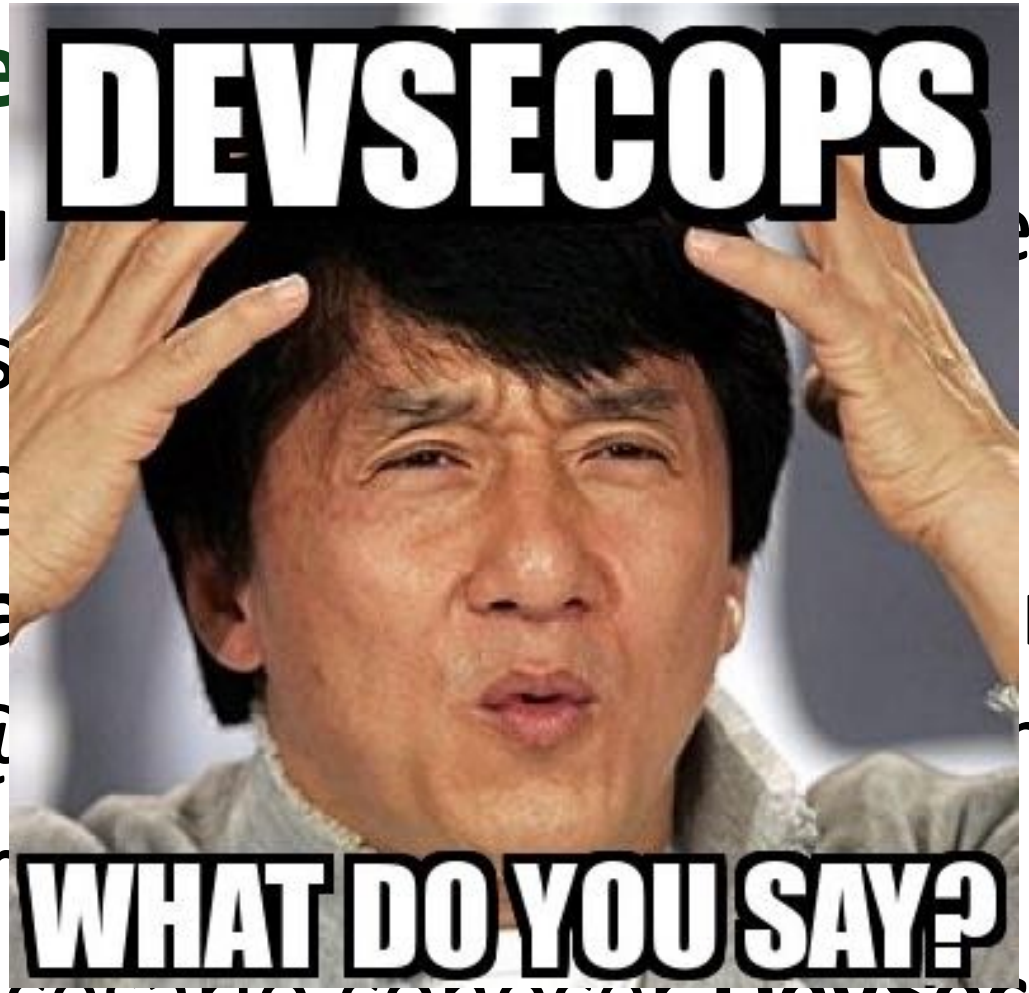
MONGOLOL

Características generales

- **No usan SQL** ya que **no son bases de datos relacionales**
- **No se necesitan estructuras fijas** (tablas, columnas etc.)
- En general **no soportan ACID** (Atomicity, Consistency, Isolation y Durability)

MONGOLOL

Caracte



- Lo qu de datos
- Mong **muy de moda** rollo
- Tod@ ns, desar
- Es necesario conocer **DevSecOps**

Características generales

- MongoDB guarda los documentos en **BSON** (implementación binaria del JSON)
- Los documentos se guardan en **colecciones**, que podrían asemejarse a las tablas que conocemos de los sistemas relacionales

Características generales

- La diferencia principal es que los documentos no tienen porque tener los **mismos campos** e incluso los **tipos de datos pueden ser diferentes**
- No existe un **esquema** definido

Características generales

- En definitiva MongoDB es un sistema **mucho más flexible**
- Como **no hay restricciones**, la lógica principal para controlar la integridad de los datos, **recaerá en la aplicación**

Instalación de MongoDB

- MongoDB **no requiere** de ningún proceso de instalación
- Para ejecutar una instancia **con los valores por defecto**, tampoco se necesita configuración
- Todo reside con la **ejecución del binario** del demonio

MONGOLOL

Disclaimer

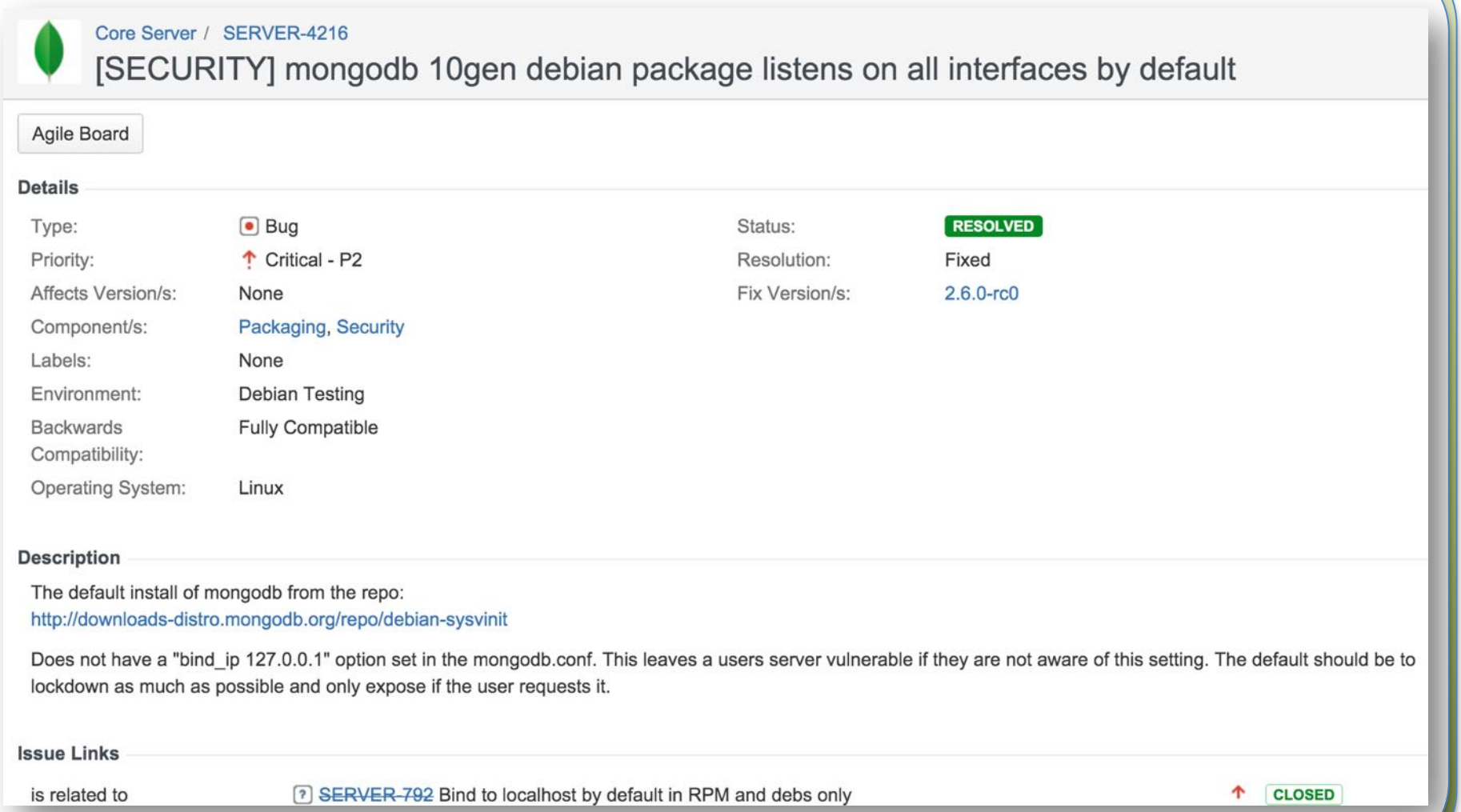
MONGOLOL

No se trata de una vulnerabilidad, simplemente se trata de una mala o débil práctica de configuración [de seguridad] cuando queda expuesta la IP pública de un servidor **sin filtrado y/o protección** permitiendo el acceso por defecto **sin autenticación**

MONGOLOL

Otros sistemas de Bases de Datos como Redis, Memcached, ElasticSearch, CouchDB, Riak, Cassandra, etc...
también se encuentran expuestos sin autenticación o con credenciales por defecto

MONGOLOL



Core Server / SERVER-4216

[SECURITY] mongodb 10gen debian package listens on all interfaces by default

Agile Board

Details

Type:	Bug	Status:	RESOLVED
Priority:	Critical - P2	Resolution:	Fixed
Affects Version/s:	None	Fix Version/s:	2.6.0-rc0
Component/s:	Packaging, Security		
Labels:	None		
Environment:	Debian Testing		
Backwards Compatibility:	Fully Compatible		
Operating System:	Linux		

Description

The default install of mongodb from the repo:
http://downloads-distro.mongodb.org/repo/debian-sysvinit

Does not have a "bind_ip 127.0.0.1" option set in the mongodb.conf. This leaves a users server vulnerable if they are not aware of this setting. The default should be to lockdown as much as possible and only expose if the user requests it.

Issue Links

is related to SERVER-792 Bind to localhost by default in RPM and debs only CLOSED

MONGOLOL

Searching

MONGOLOL

Búsqueda de instancias

- Escan

```
root@dronpimpon:~# masscan -p27017 0.0.0.0/0 --banners --rate 1500000 --excludefile exclude.conf -oG mongos.txt
exclude.conf: excluding 122 ranges from file

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2016-01-05 19:21:33 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
3969790205 hosts [1 port/host]
 16% done,   6:59:55 remaining, found=3409
```

MONGOLOL

Búsqueda de instancias

- Internet Mapping Project, Bell Labs/ Lumeta, 1998+
- IPv4 Census 2003-2006
- EFF SSL Observatory 2014
- Internet Census 2012 (the botnet)
- RIPE Atlas (slightly different)
- Critical.IO, 2012-2013

MONGOLOL

Búsqueda de instancias

- University of Michigan (
- Shadow

El nuevo delito de acceso ilícito a datos o programas informáticos (art. 197.3 Código Penal)

Con la publicación en el BOE de la Ley Orgánica 5/2010, de 22 de junio, en vigor desde el 23 de diciembre del año 2010, se reformaba la Ley Orgánica 10/1995 que aprobó el vigente Código Penal. Tres han sido los delitos informáticos afectados por esta reforma: la intrusión informática (art. 197.3 CP), la estafa informática (art. 248 CP) y los daños informáticos (art. 264 CP).

Búsqueda de instancias

- Shodan

MONGOLOL

Global

SHODAN port:27017

Exploits | Maps | Like 16

TOP COUNTRIES

United States	14,204
China	8,720
France	1,911
Netherlands	1,857
Singapore	1,671

TOP ORGANIZATIONS

Amazon.com	4,769
Digital Ocean	3,275
Hangzhou Alibaba Advertising Co....	2,648
Aliyun Computing Co., LTD	1,569
OVH SAS	1,030

TOP OPERATING SYSTEMS

Linux 3.x	31
Windows 7 or 8	6
Linux 2.6.x	5
Windows XP	2
FreeBSD 9.x	1

TOP PRODUCTS

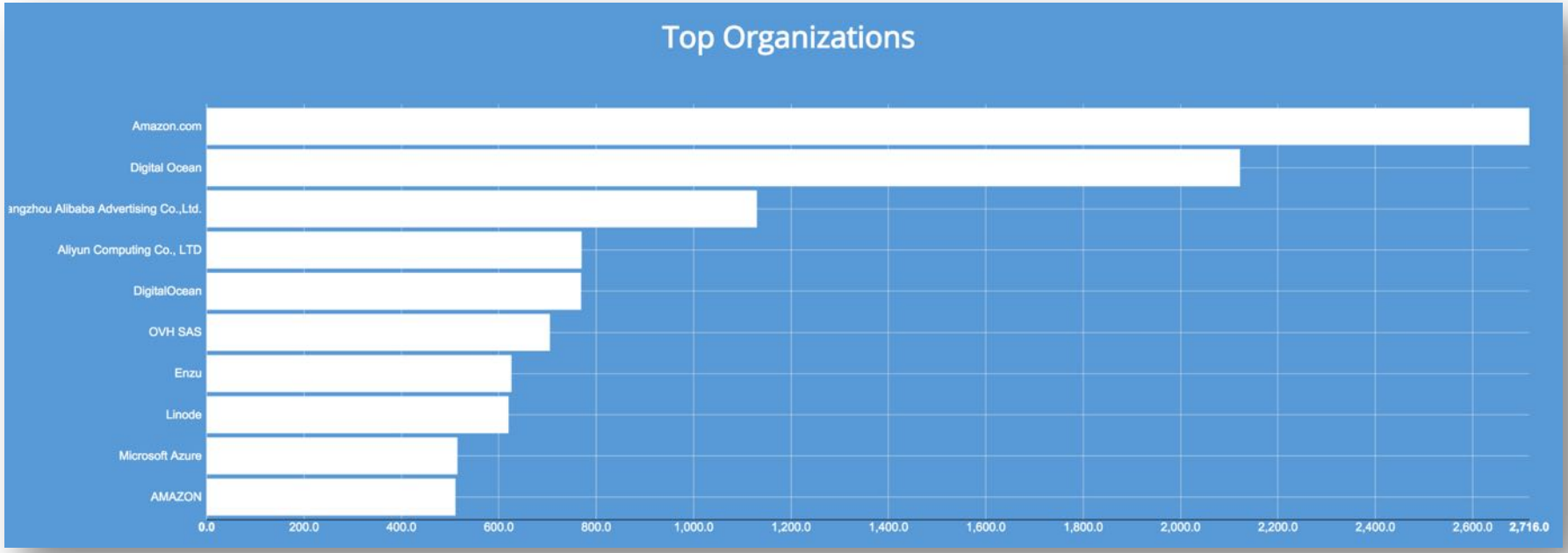
MongoDB	41,512

Distribución por Países

Top Countries

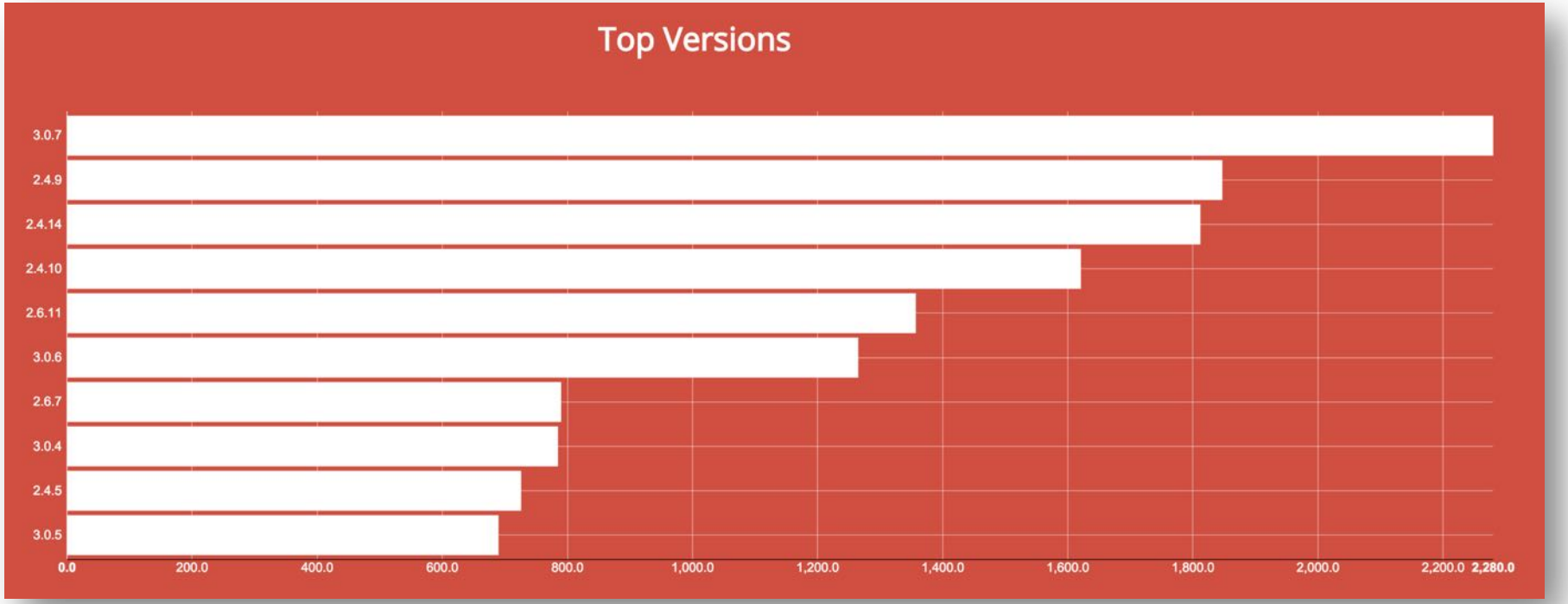
1.	United States	9,908
2.	China	4,567
3.	Netherlands	1,114
4.	France	1,100
5.	Germany	900
6.	Singapore	880
7.	United Kingdom	739
8.	Japan	689
9.	Russian Federation	572
10.	Canada	517

Organizaciones (ISPs)



MONGOLOL

Versiones

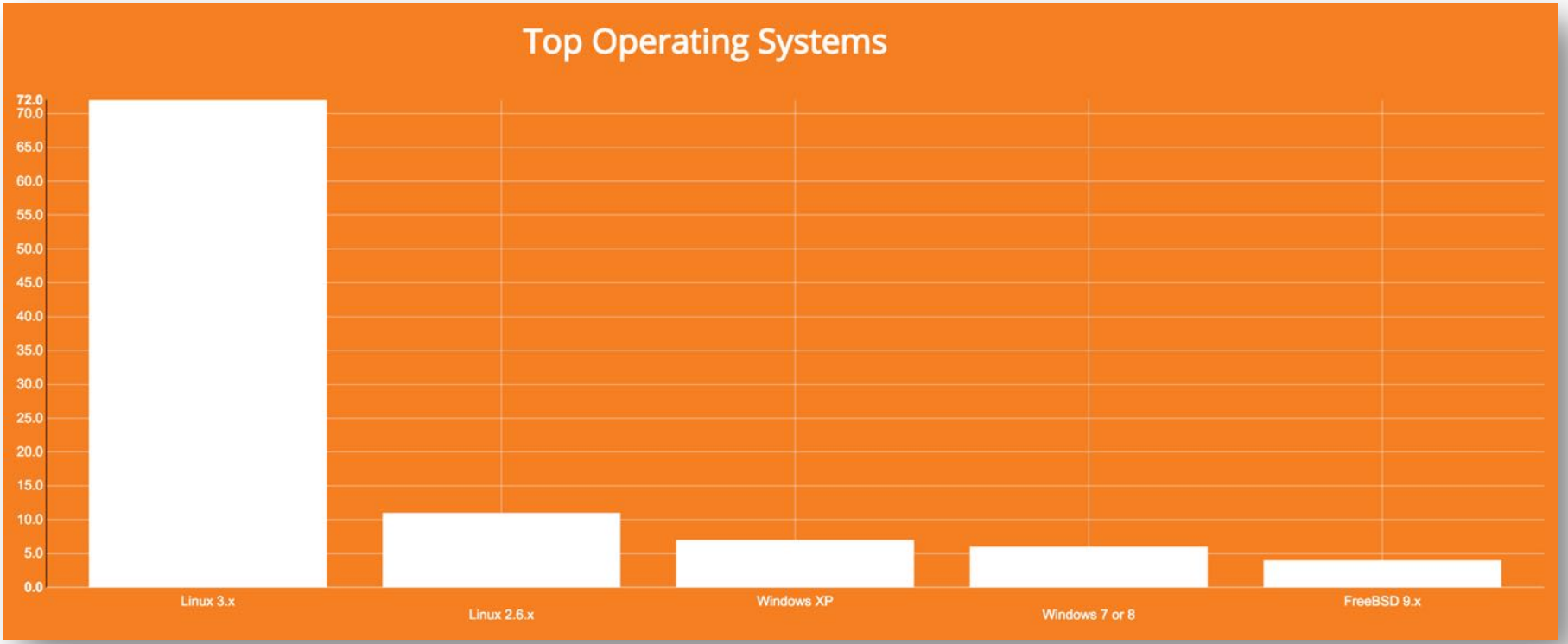


MONGOLOL

Dominios

MONGOLOL

Sistema Operativo de servidor



MONGOLOL

Data breach

Otras investigaciones

- **30.000 instancias** con aproximadamente 600 TB (595,2 TB) de datos expuestos (**Datos en Julio de 2015**)
- **Chris Vickery** reportó reportó 25 millones de cuentas expuestas en bases de datos sin seguridad

Otras investigaciones

- Aproximadamente 13 millones de cuentas asociadas a **MacKeeper** y sus desarrolladores Kromtech Alliance
- **Hello Kitty** (3,3 Millones de cuentas)
- Video Chat **OkHello** (2,6 Millones de cuentas)

MONGOLOL

Otra

- O
  M

Hack
Cust

By Eduard Kovacs or

LinkedIn G+1

Hackers report

Personal info of

Apr 22 2016

Posted by Dissent at 7:13 am

In today's installment of "Epic Info
due to a misconfigured databas
Amazon, and why it wasn't pro

Last week, MacKeeper Sec
another misconfigured Mo
citizens.

Vickery, who has blogged about this


```
{
  "_id" : ObjectId("[redacted]"),
  "CONSECUTIVO_ALFABETICO_POR_SECCION" : [redacted],
  "CLAVE_ELECTOR" : "[redacted]",
  "FOLIO_NACIONAL" : [redacted],
  "OCR" : NumberLong("[redacted]"),
  "APELLIDO_PATERNO" : "[redacted]",
  "APELLIDO_MATERNO" : "[redacted]",
  "NOMBRE" : "[redacted]",
  "FECHA_NACIMIENTO" : [redacted],
  "LUGAR_NACIMIENTO" : [redacted],
  "SEXO" : [redacted],
  "OCUPACION" : [redacted],
  "CALLE" : "[redacted]",
  "NUM_EXTERIOR" : [redacted],
  "NUM_INTERIOR" : [redacted],
  "COLONIA" : [redacted],
  "CODIGO_POSTAL" : [redacted],
  "TIEMPO_RESIDENCIA" : [redacted],
  "ENTIDAD" : [redacted],
  "DISTRITO" : [redacted],
  "MUNICIPIO" : [redacted],
  "SECCION" : [redacted],
  "LOCALIDAD" : [redacted]
```


izon Enterprise

ATED)

Add comments

tion details exposed online
f Mexico, who uploaded it to

covered yet
ta from 93,424,710 Mexican

een cap of an individual's record:

s can also acquire sets
on on vulnerabilities in

There have been many
abases exposed a large
incidents over the past period where misconfigured
number of records of sensitive information.

Información expuesta

- Nombres
- Direcciones de correo electrónico
- Códigos postales
- Direcciones IP
- Usuarios
- Contraseñas
- …

Colecciones más usuales

- local
- admin
- db
- test
- config
- mydb
- …

Resultados muy pobres

- GridFS (fs.chunks)

MONGOLOL

Spain

MONGOLOL

Esp

- F ...iones
  d... ...n a
  se... ...5 al
  G... ...la
  G...
- Inv... ...os
  "ce... ...Disclosure

TÍTULO X

Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio

CAPÍTULO PRIMERO

Del descubrimiento y revelación de secretos

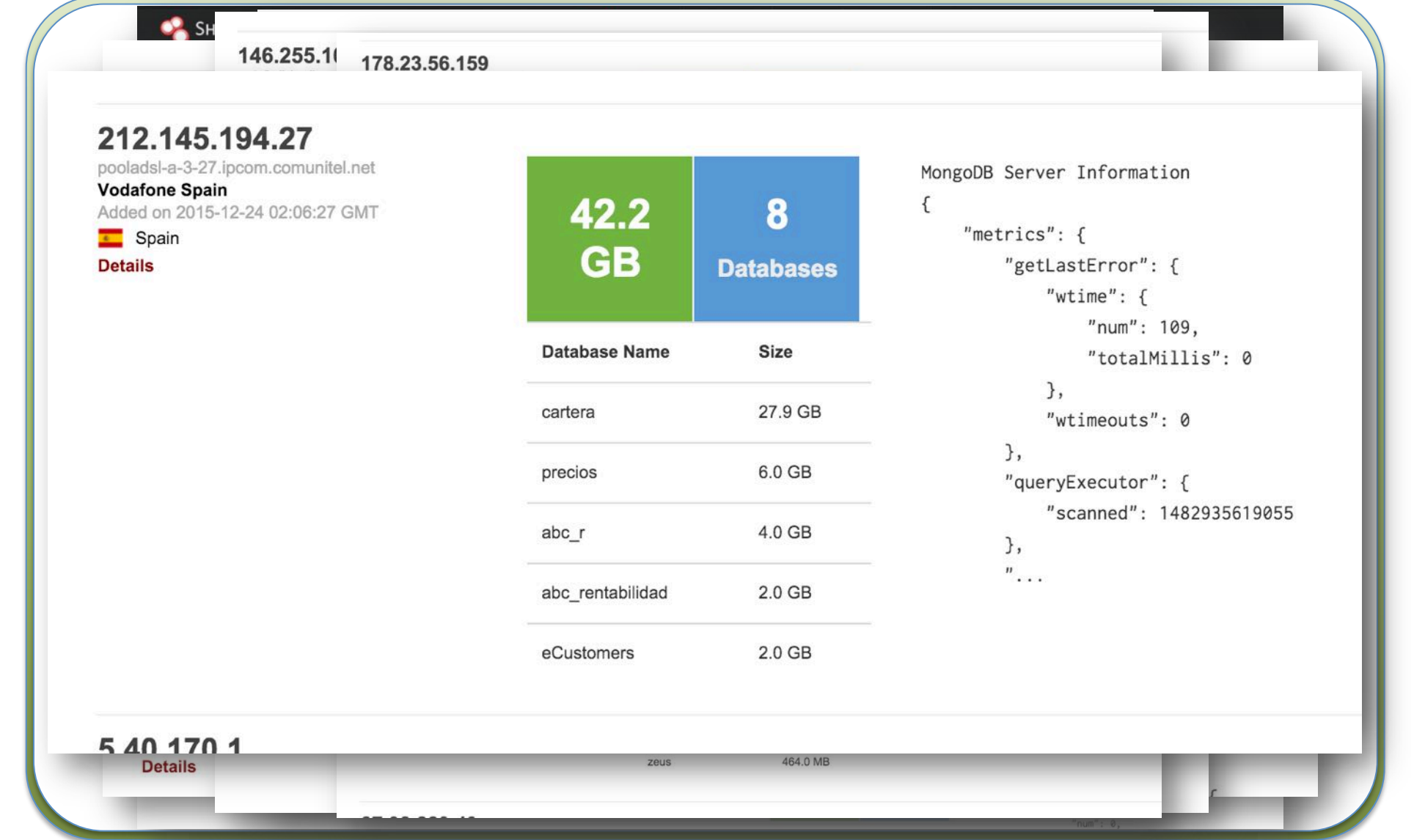
Artículo 197

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

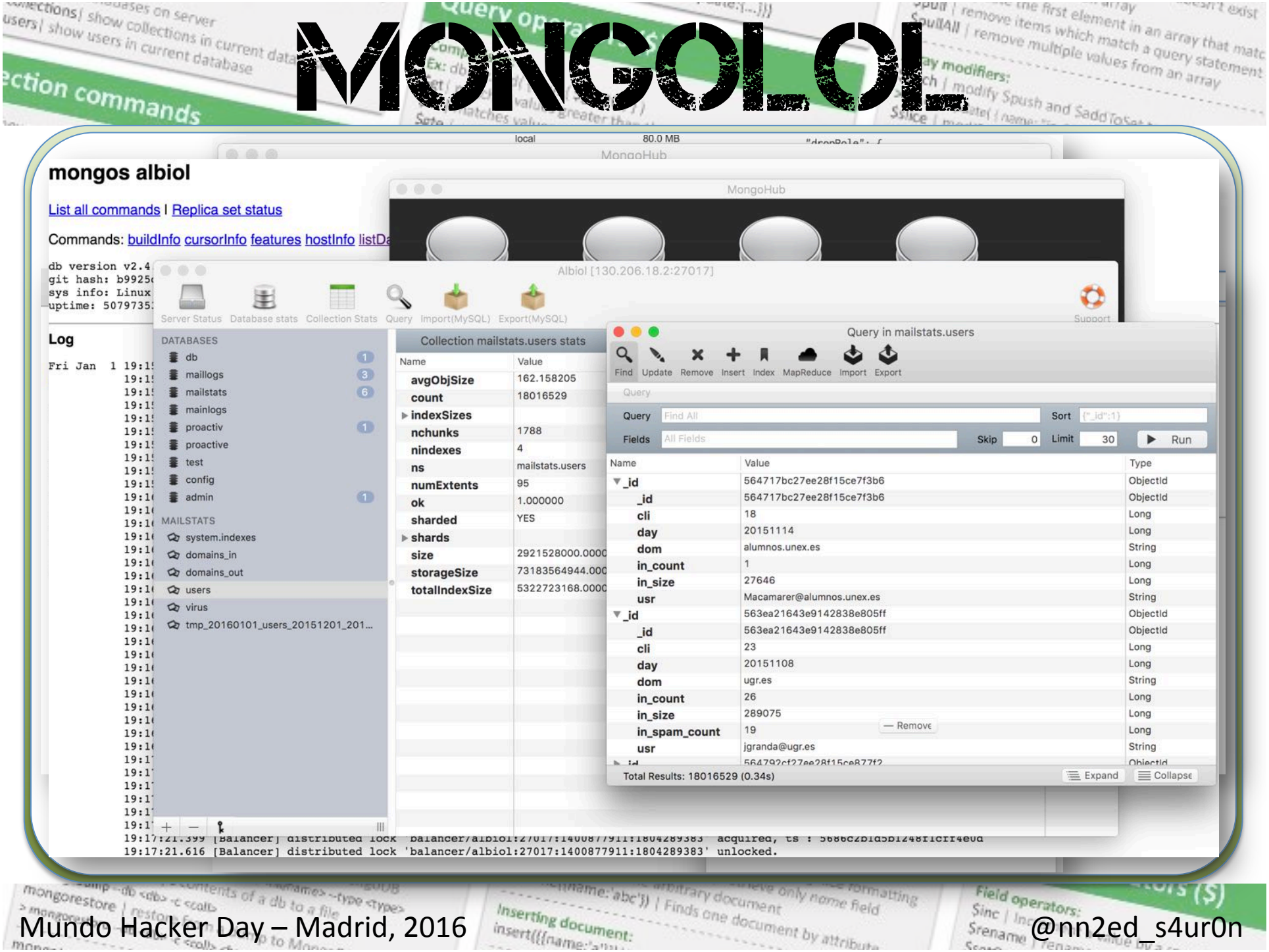
2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

MONGOLOL


146.255.1(
178.23.56.159
212.145.194.27
pooladsl-a-3-27.ipcom.comunitel.net
Vodafone Spain
Added on 2015-12-24 02:06:27 GMT
Spain
Details
42.2 GB
8 Databases
Database Name
Size
cartera
27.9 GB
precios
6.0 GB
abc_r
4.0 GB
abc_rentabilidad
2.0 GB
eCustomers
2.0 GB
MongoDB Server Information
{
"metrics": {
"getLastError": {
"wtime": {
"num": 109,
"totalMillis": 0
},
"wtimeouts": 0
},
"queryExecutor": {
"scanned": 1482935619055
},
"...
5.40.170.1
Details
zeus
464.0 MB

MONGOLOL


mongos albiol
List all commands | Replica set status
Commands: buildInfo cursorInfo features hostInfo
Log
MongoHub
Albiol [130.206.18.2:27017]
Server Status
Database stats
Collection Stats
Query
Import(MySQL)
Export(MySQL)
Support
DATABASES
db
maillogs
mailstats
mainlogs
proactiv
proactive
test
config
admin
MAILSTATS
system.indexes
domains_in
domains_out
users
virus
tmp_20160101_users_20151201_201...
Collection mailstats.users stats
Name
Value
avgObjSize 162.158205
count 18016529
indexSizes
nchunks 1788
nindexes 4
ns mailstats.users
numExtents 95
ok 1.000000
sharded YES
shards
size 2921528000.0000
storageSize 73183564944.000
totalIndexSize 5322723168.0000
Query in mailstats.users
Find
Update
Remove
Insert
Index
MapReduce
Import
Export
Query
Query Find All
Sort {"_id":1}
Fields All Fields
Skip 0
Limit 30
Run
Name
Value
Type
_id 564717bc27ee28f15ce7f3b6 ObjectId
_id 564717bc27ee28f15ce7f3b6 ObjectId
cli 18 Long
day 20151114 Long
dom alumnos.unex.es String
in_count 1 Long
in_size 27646 Long
usr Macamarer@alumnos.unex.es String
_id 563ea21643e9142838e805ff ObjectId
_id 563ea21643e9142838e805ff ObjectId
cli 23 Long
day 20151108 Long
dom ugr.es String
in_count 26 Long
in_size 289075 Long
in_spam_count 19 Long
usr jgranda@ugr.es String
Remove
Total Results: 18016529 (0.34s)
Expand
Collapse
19:17:21.616 [Balancer] distributed lock 'balancer/albiol:27017:1400877911:1804289383' unlocked.

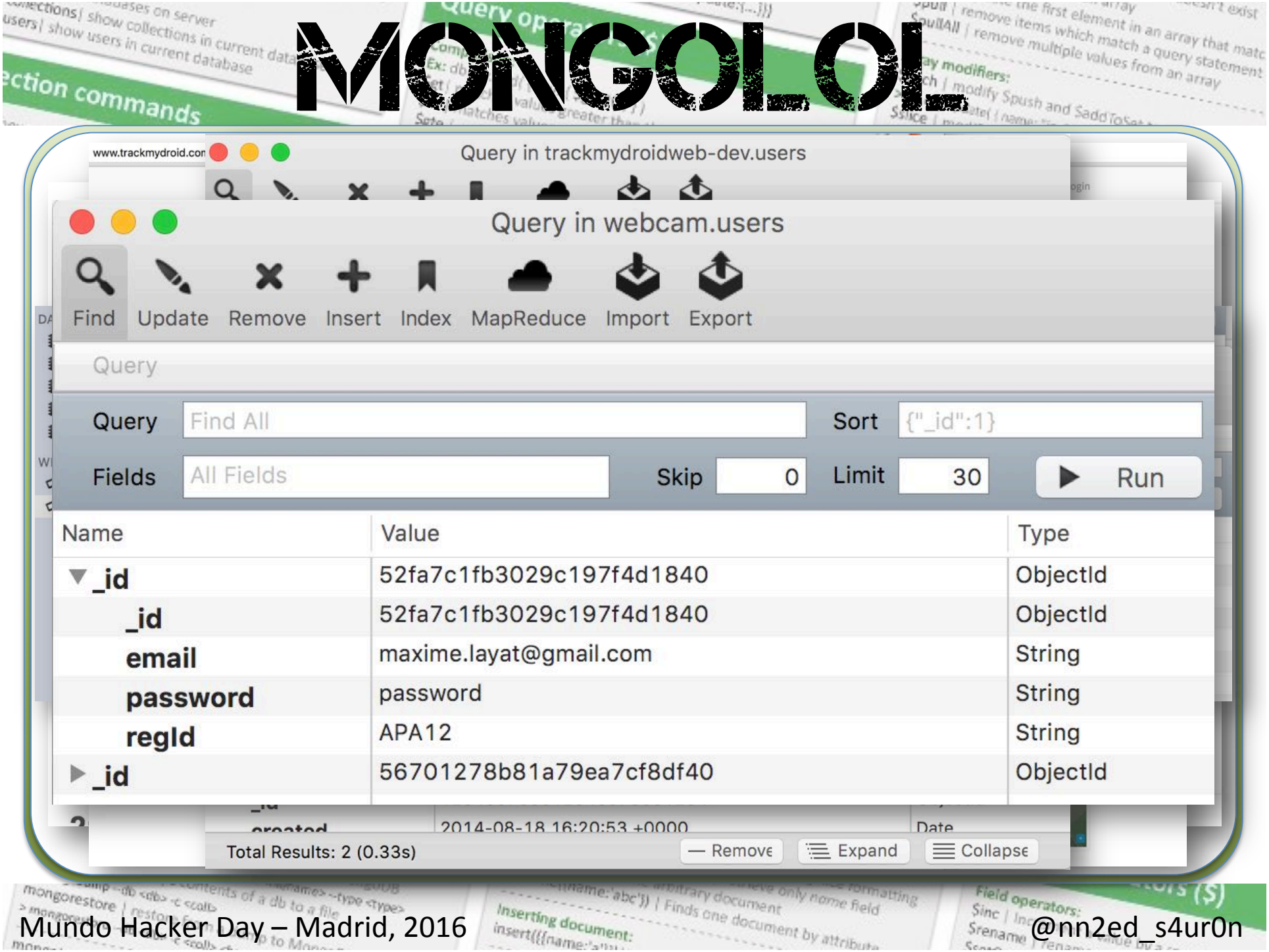
MONGOLOL


SHODAN
port:27017 country:es
Exploits
Maps
Share Search
TOP COUNTRIES
Spain
222
TOP CITIES

MONGOLOL

Europe

MONGOLOL


Query in trackmydroidweb-dev.users
Query in webcam.users
Find
Update
Remove
Insert
Index
MapReduce
Import
Export
Query
Query
Find All
Sort
{"_id":1}
Fields
All Fields
Skip
0
Limit
30
Run
Name
Value
Type
_id
52fa7c1fb3029c197f4d1840
ObjectId
_id
52fa7c1fb3029c197f4d1840
ObjectId
email
maxime.layat@gmail.com
String
password
password
String
regId
APA12
String
_id
56701278b81a79ea7cf8df40
ObjectId
Total Results: 2 (0.33s)
Remove
Expand
Collapse

MONGOL_OL

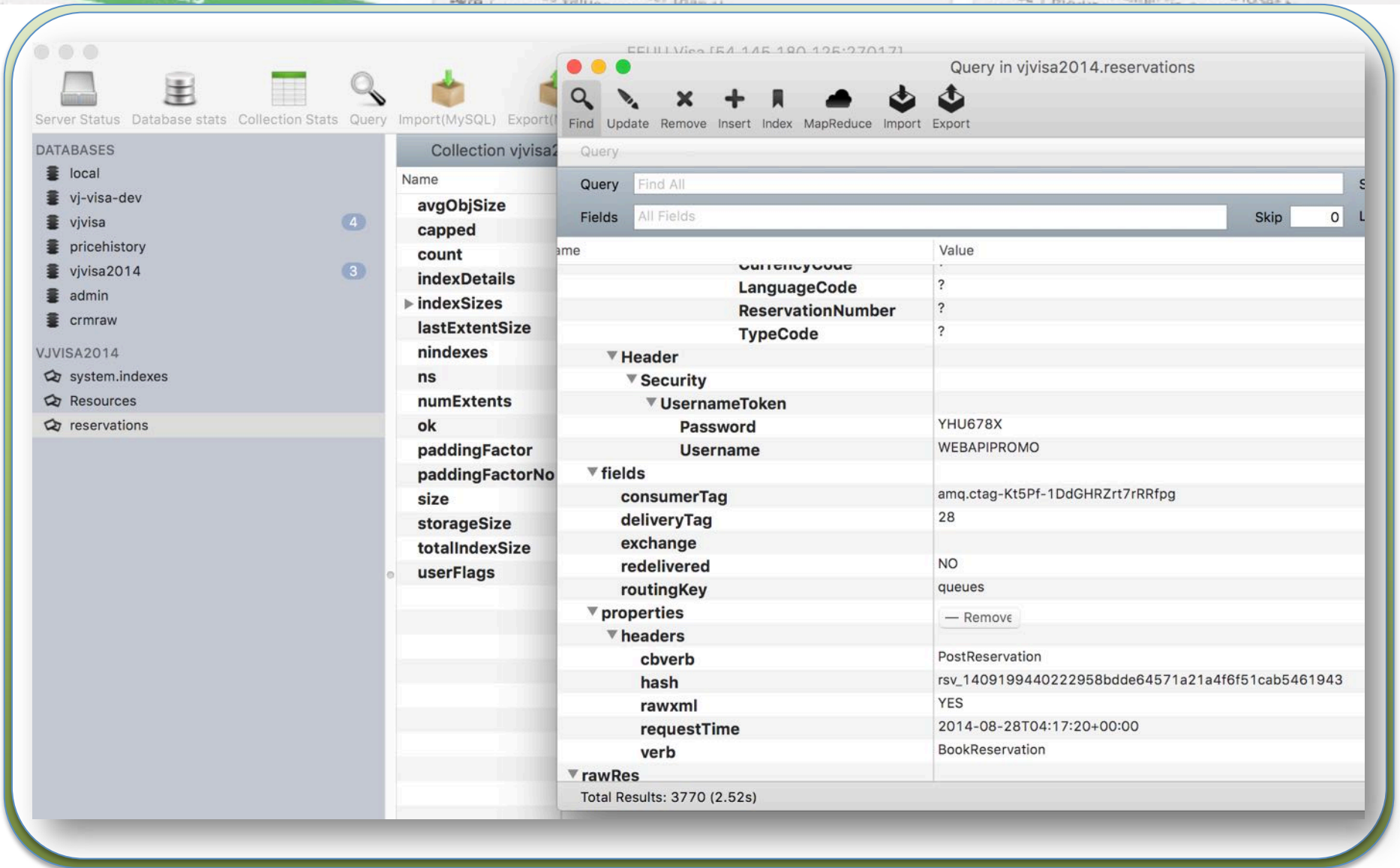
Из России с любовью

MONGOLOL


Server Status
Database stats
Collection Stats
Query
Import(MySQL)
Export(MySQL)
DATABASES
innmoscow
local
admin
INNMOSCOW
system.indexes
dictionaries
tehnopolis
news
order
sessions
users
counters
analitics
system.users
Collection innmoscow.order stats
Name
Value
avgObjSize 541.206349
count 126
indexSizes
lastExtentSize 131072
nindexes 1
ns innmoscow.order
numExtents 3
ok 1.000000
paddingFactor 1.000000
size 68192
storageSize 172032
systemFlags 1
totalIndexSize 8176
userFlags 0
Query in innmoscow.order
Find
Update
Remove
Insert
Index
MapReduce
Import
Export
Query
Find All
Sort
Fields
All Fields
Skip 0
Limit 30
Run
data Object
area 29.700000 Double
floor 2 Int
id 379 Int
name 1 String
note Помещение 1, этаж 2 String
type room_order String
date 2015-10-22 15:04:26 +0000 Date
email anton@lis.ru String
fio Антон String
number 1316 Int
object_id 985 String
phone 123 String
status new String
Total Results: 126 (0.53s)
Remove
Expand
Collapse
Name
Value
Type
_id 562c82d918716a19516af098 ObjectId
_id 562c82d918716a19516af098 ObjectId
created 2015-10-25 07:20:57 +0000 Date
fio Бартенев Роман String
password d8578edf8458ce06fbc5bb76a58c5ca4 String
_id 562e292818716a5f117672e4 ObjectId
_id 562e292818716a5f117672e4 ObjectId

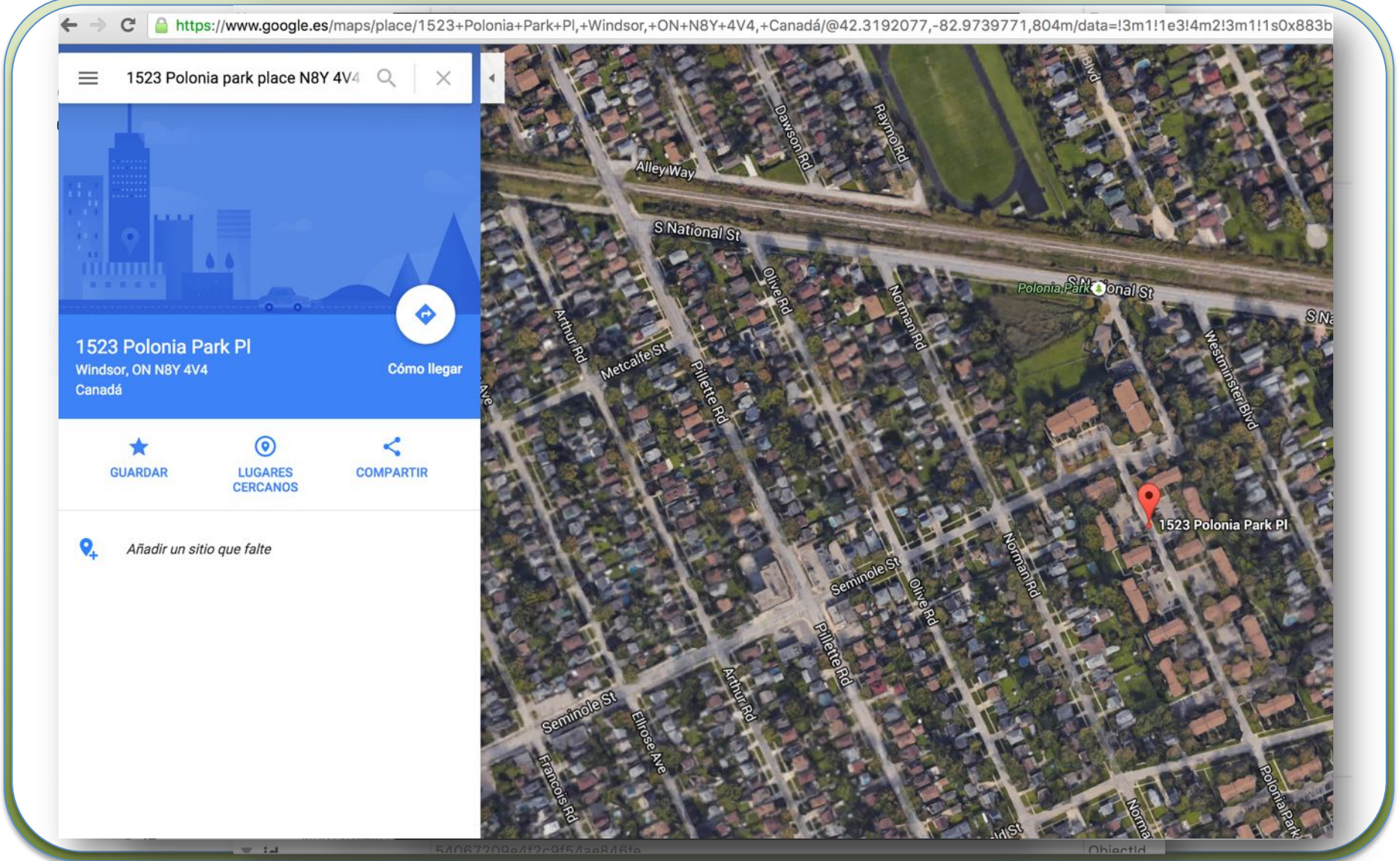
MONGOLOL

MONGOLOL


Server Status
Database stats
Collection Stats
Query
Import(MySQL)
DATABASES
local
vj-visa-dev
vjvisa
4
pricehistory
vjvisa2014
3
admin
crmraw
VJVISA2014
system.indexes
Resources
reservations
Collection vjvisa2
Name
avgObjSize
capped
count
indexDetails
indexSizes
lastExtentSize
nindexes
ns
numExtents
ok
paddingFactor
paddingFactorNo
size
storageSize
totalIndexSize
userFlags
Query in vjvisa2014.reservations
Find
Update
Remove
Insert
Index
MapReduce
Import
Export
Query
Query
Find All
Fields
All Fields
Skip
0
Value
LanguageCode
?
ReservationNumber
?
TypeCode
?
Header
Security
UsernameToken
Password
YHU678X
Username
WEBAPIPROMO
fields
consumerTag
amq.ctag-Kt5Pf-1DdGHRZrt7rRRfpg
deliveryTag
28
exchange
redelivered
NO
routingKey
queues
properties
— Remove
headers
cbverb
PostReservation
hash
rsv_1409199440222958bdde64571a21a4f6f51cab5461943
rawxml
YES
requestTime
2014-08-28T04:17:20+00:00
verb
BookReservation
rawRes
Total Results: 3770 (2.52s)

MONGOLOL

MONGOLOL

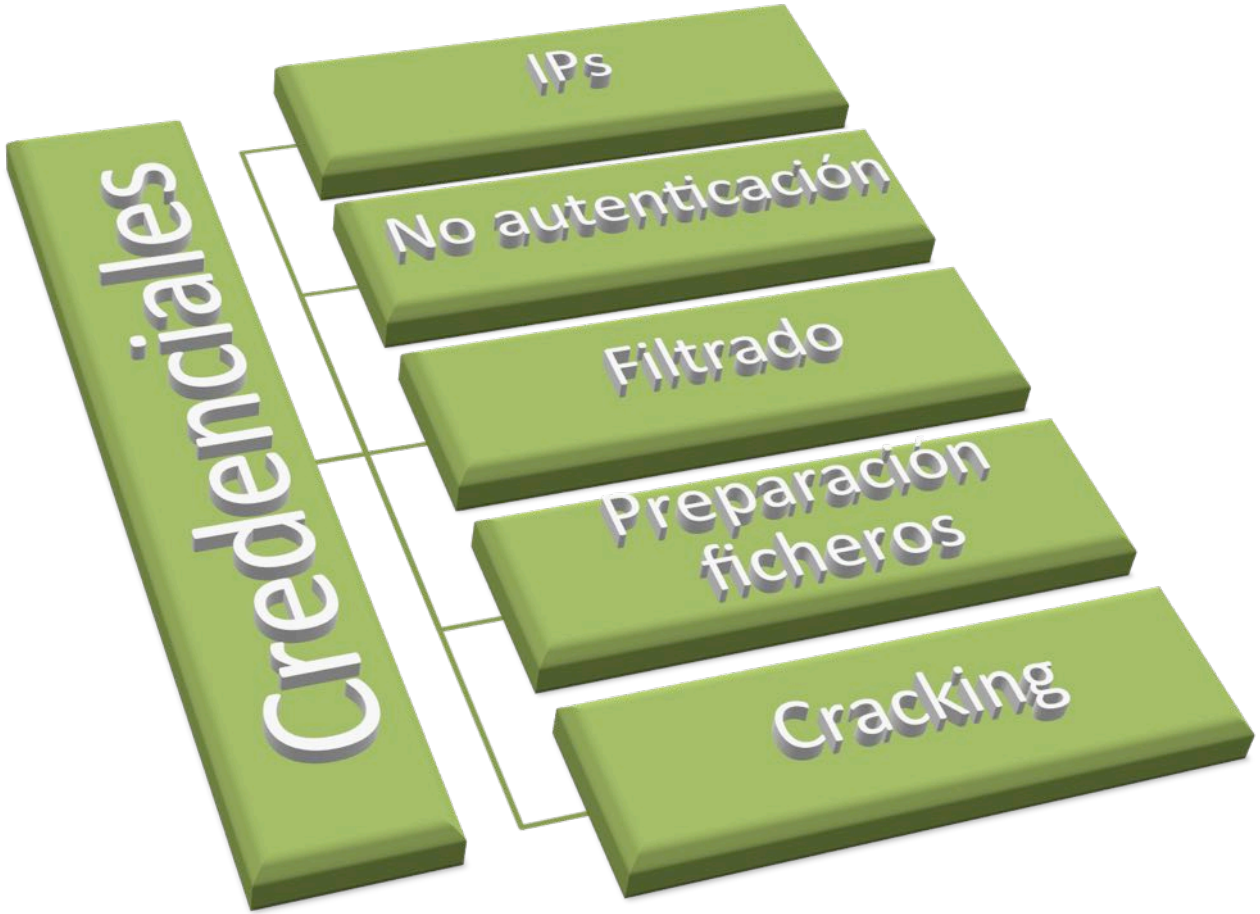

https://www.google.es/maps/place/1523+Polonia+Park+Pl,+Windsor,+ON+N8Y+4V4,+Canadá/@42.3192077,-82.9739771,804m/data=!3m1!1e3!4m2!3m1!1s0x883b
1523 Polonia park place N8Y 4V4
1523 Polonia Park Pl
Windsor, ON N8Y 4V4
Canadá
Cómo llegar
GUARDAR
LUGARES CERCANOS
COMPARTIR
Añadir un sitio que falte
Alley Way
Dawson Rd
Raymo Rd
S National St
Olive Rd
Norman Rd
Arthur Rd
Metcalfe St
Pillette Rd
Westminster Blvd
Seminole St
Ellrose Ave
Francois Rd
Polonia Park Pl

MONGOLOL

```
db.mongolol.find()
{
    "_id" : ObjectId("61f521e737945d314bc4ab01"),
    "name" :  "God",
    "mode" : [  {
            ' name" : "automatic",
           "status" : "on”  }, ]
}
```

MONGOLOL

Automatización de tareas



Automatización de tareas

- Masscan
- https://github.com/robertdavidgraham/masscan

```
masscan –p 27017 0.0.0.0/0 \
--excludefile \ data/
exclude.conf
```

Automatización de tareas

- Shodan
- https://www.shodan.io/data

```
ls -l shodan-export.json
-rw-r-----  1 s4ur0n  staff
384397431  2 ene 21:38 shodan-
export.json
```

Automatización de tareas

- Filtrado de Ips

Automatización de tareas

- Acceso no autenticado
- NoSQLMap
- https://github.com/tcstool/NoSQLMap

Automatización de tareas

- Filtrado de credenciales
- Reconocimiento de hashes/ codificaciones empleadas
- https://github.com/blackthorne/Codetective
- http://www.onlinehashcrack.com/
- …

Automatización de tareas

- Diccionarios de datos
- https://github.com/danielmiessler/SecLists

Automatización de tareas

- Hashcat
- oclHashcat (OpenCL & CUDA)
- http://hashcat.net/oclhashcat/

MONGOLOL

Security

Seguridad en MongoDB

- MongoDB **no viene** con demasiadas medidas de seguridad **por defecto**
- Con sólo **8 líneas** podemos realizar:
  - ✓ Autenticación de usuarios
  - ✓ Sólo se permiten conexiones desde la ip indicada (en este caso la ip local)

Seguridad en MongoDB

- ✓ Se cambia el puerto por defecto al que deseemos
- ✓ Se deshabilita cualquier acceso vía http tanto a la parte de administración como a la API Rest

Seguridad en MongoDB

/etc/mongod.conf

```
security:
   authorization: "enabled"
net:
   bindIp: 127.0.0.1
   port: 26116
http:
   enabled: false
   RESTInterfaceEnabled: false
```

Seguridad en MongoDB

- Creación de usuarios:

```
use admin
db.createUser({
   user:  "s4ur0n",
   pwd:   "p4$$w0rd",
   roles:[ {role:"userAdminAnyDatabase",
            db: "admin" } ]
   })
```

Seguridad en MongoDB

- Tutoriales de Seguridad disponibles en https://docs.mongodb.org/manual/administration/security/
- Habilitación del control de acceso
- Mecanismos de autenticación (x.509, Kerberos, SASL con LDAP)
- Usuarios y Roles

Seguridad en MongoDB

- Seguridad de red: TLS/SSL, FIPS (Federal Information Processing Standard) y Firewall
- Cifrado
- Auditoría y registro (--auditDestination syslog|console)

MONGOLOL

¿Preguntas?

Muchas gracias

@NN2ed_s4ur0n

s4ur0n@s4ur0n.com