
SH3LLCON
Security Hell Conference
mongoDB
Document
•RavenDB
• MongoDB
• CouchDB
• Cloudant
•DynamoDB
• Redis-to-go
Graph
• InfiniteGraph
• DEX
• Neo4j
•OrientDB
•NuvolaBase
"_id" : ObjectId("506c734adbd7
"bd" : "-2208932970",
"cd" : 1349183839,
"em" : "unesco@gmail.com",
"hhid" : ObjectId("506ae95f053b045
"ia" : 1,
"id" : "2",
"ll" : 1349183839,
"nm" : "UNESCO",
"pl" : "",
"pt" : "",
"pw" : "50b8a347f1c7
"ty" : "nGGnRYx0p03
"ud" : 3,
1349183839
LOL
sh3llcon
By s4ur0n

MONGOL OL

Whoami

```
class PedroC:
    def __init__(self):
        self.name = 'Pedro Candel'
        self.email = 's4ur0n@navajanegra.com'
        self.nickname = '@NN2ed_s4ur0n'
        self.role = 'Security Researcher'
        self.interest = [ 'Reversing', 'Malware', 'Offensive Security' ]
        self.member_of = [ 'NavajaNegra', 'mlw.re', 'OWASP' ]
```

mlw.re

NAVAJA NEGRA CONFERENCE
ALBACETE

OWASP
Open Web Application Security Project
Madrid Chapter

SH3LLCON
Security Hell Conference

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**

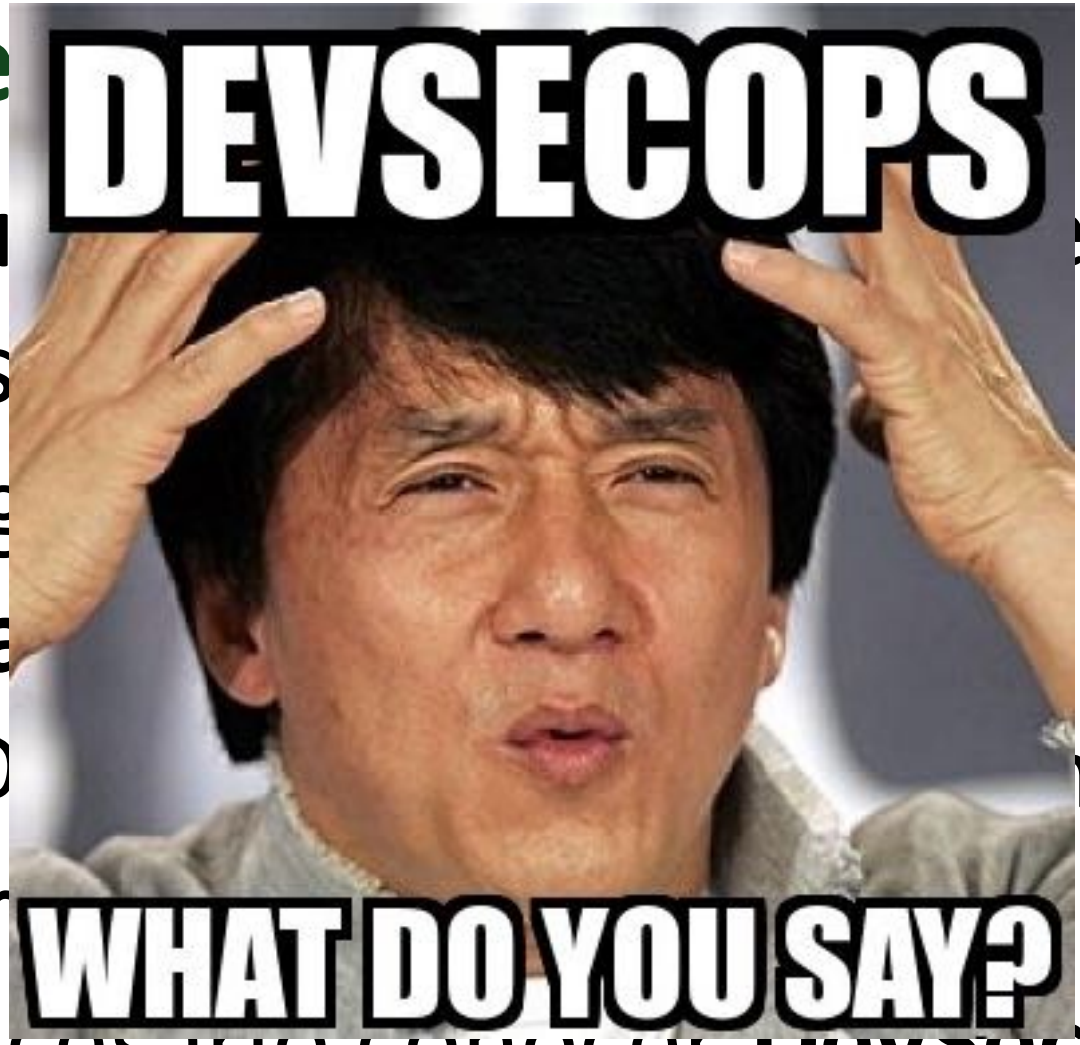
MONGOL

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@ … s, 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

- Descargar de https://www.mongodb.org/downloads#production la última versión (Current Stable Release: 3.2.1)
- Tip: This distribution **does not include SSL encryption**

Instalación de MongoDB

```
wget
https://fastdl.mongodb.org/osx
/mongodb-osx-x86_64-3.2.0.tgz
tar -zxvf mongodb-osx-x86_64-
3.2.0.tgz
cd mongodb-osx-x86_64-
3.2.0/bin
```

Instalación de MongoDB

```
./mongod
MongoDB starting : pid=21757
port=27017 dbpath=/data/db 64-
bit host=MAWILIN
mkdir -p ./data/db
./mongod --dbpath ./data/db
waiting for connections on
port 27017
```

Instalación de MongoDB

```
netstat –an | grep 27017
tcp4  0 0 *.27017 *.* LISTEN
```

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

Instalación de MongoDB

```
./mongod [--help]
./mongod --port 26116
```

Cliente:

```
./mongo
```

Uso de MongoDB

- Operaciones de consulta
- Operaciones de actualización de datos CRUD (Create, Read, Update, Delete)
- Manejo de índices
- Consultas de agregación (Map-Reduce y Aggregation Framework)

Administración de MongoDB

- **Alta disponibilidad** con **réplicas**:
  - **Servidor principal**: el único que acepta modificación o inserción de datos. Mantiene un log denominado **oplog**

Administración de MongoDB

- **Servidor(es) secundario(s):** se pueden usar para consultar datos, pero nunca para hacer modificaciones directamente sobre ellos
- **Servidores con prioridad 0**
- **Servidor oculto (hidden)**

Administración de MongoDB

- **Servidor retardado (delayed)**
- **Árbitro**
- **Oplog**

- Consultas sobre la réplica:

```
db.getReplicationInfo()
```

Administración de MongoDB

- Podemos consultarlos con la **consola web** incorporada de MondoDB
- **Añadir 1000** al puerto por defecto donde escucha
- Es necesario añadir **–rest** a mongod para habilitar todas las funciones para acceder por API REST

Administración de MongoDB

```
./mongod --dbpath ./data/db
–rest
http://localhost:28017/
```

Administración de MongoDB

- **OpLog**:
  - MongoDB es capaz de replicarse entre servers de forma eficiente y transparente
  - Estos se comunican entre si para mantener los datos del conjunto de réplicas siempre actualizados

Administración de MongoDB

```
use local
db.oplog.rs.find().pretty();
rs.status()
```

Administración de MongoDB

- **Fragmentación (Sharding)**:
  - El sharding es una herramienta muy útil para balancear la carga de datos entre servidores
  - La elección de la clave por la que se realizará el sharding (shard key) es muy importante

Administración de MongoDB

- En MongoDB, el tamaño de las particiones no se mide en número de documentos, si no en MB
- Por defecto un shard tiene un tamaño máximo de 64 MB, aunque es algo que podemos configurar

Administración de MongoDB

- **GridFS**:
  - Es una abstracción de un sistema de ficheros para MongoDB
  - Empleado para guardar contenido generado por los usuarios
  - Separación en chunks de 256 KB

Administración de MongoDB

- Permite guardar documentos mayores de 16 MB
- No restringe las limitaciones de los sistemas de ficheros

Administración de MongoDB

- Implementado con 2 colecciones

```
show collections;
fs.chunks
fs.files
system.indexes
```

MONGOL

SH3LLCON
Security Hell Conference

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

MONGOL OL

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

SH3LLCON
Security Hell Conference

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
S      3969790205 hosts [1 port/host]
       0.16% 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

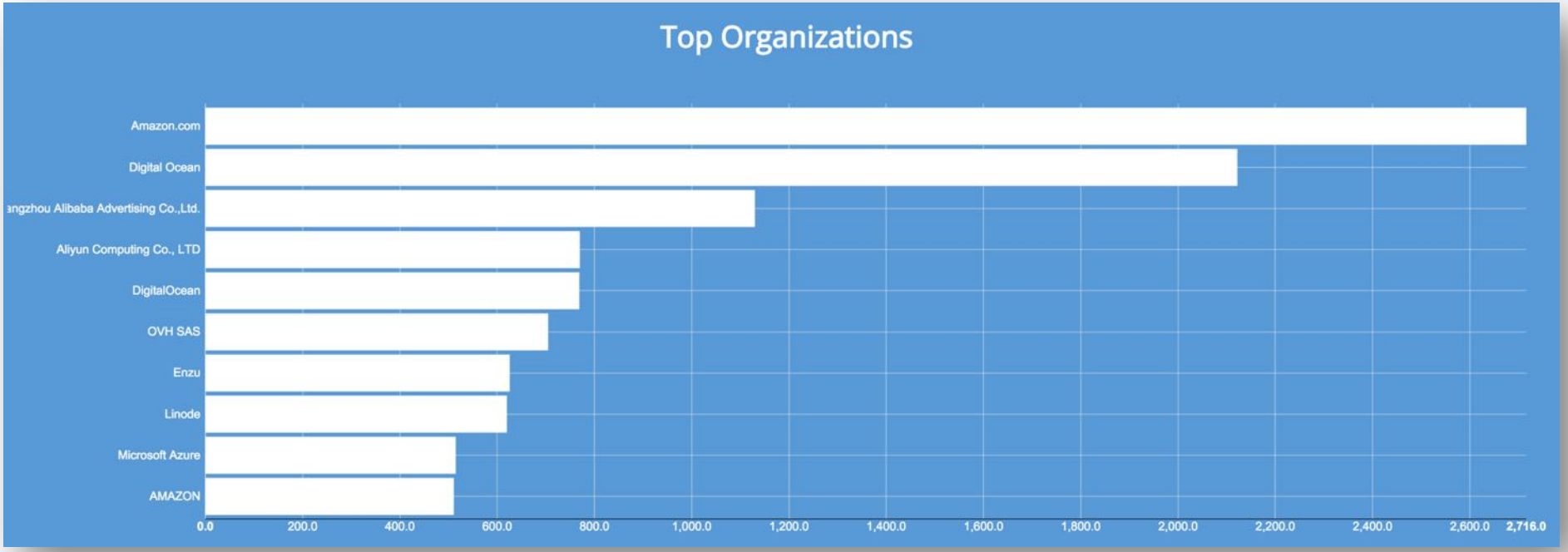
Distribución por Países

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

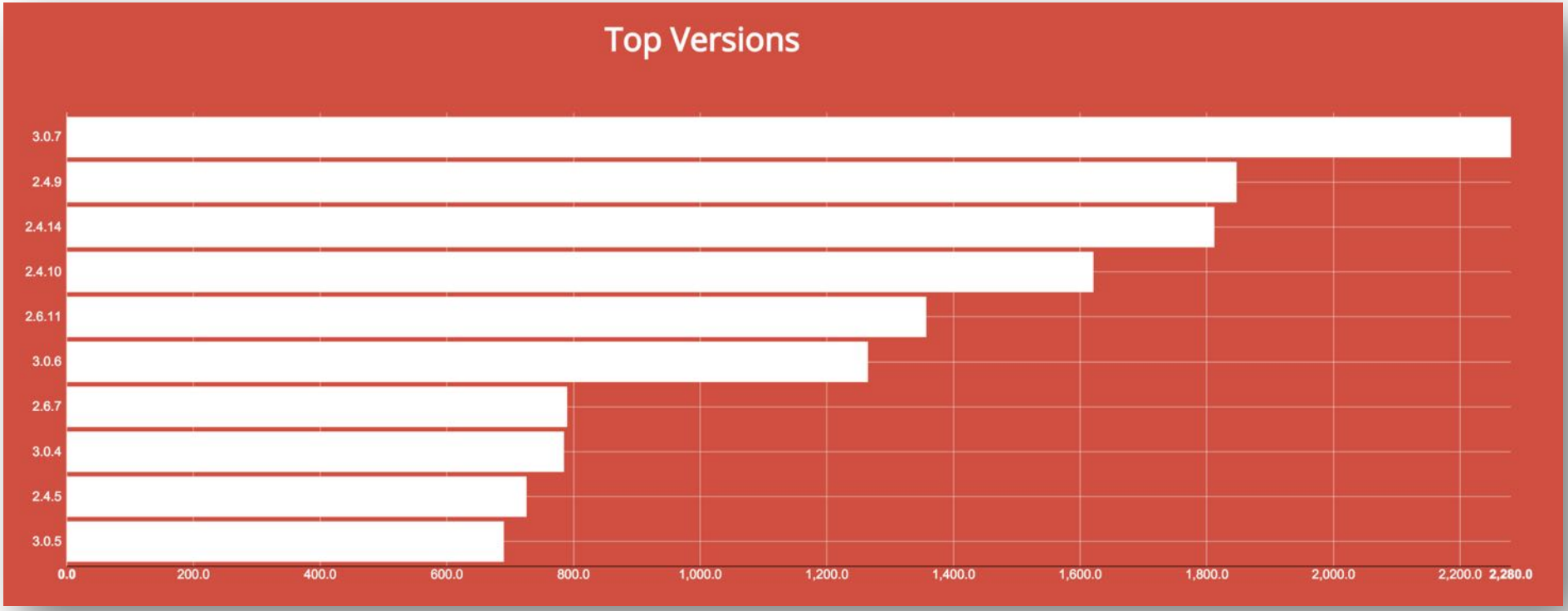
MONGOLOL

Organizaciones (ISPs)



MONGOL

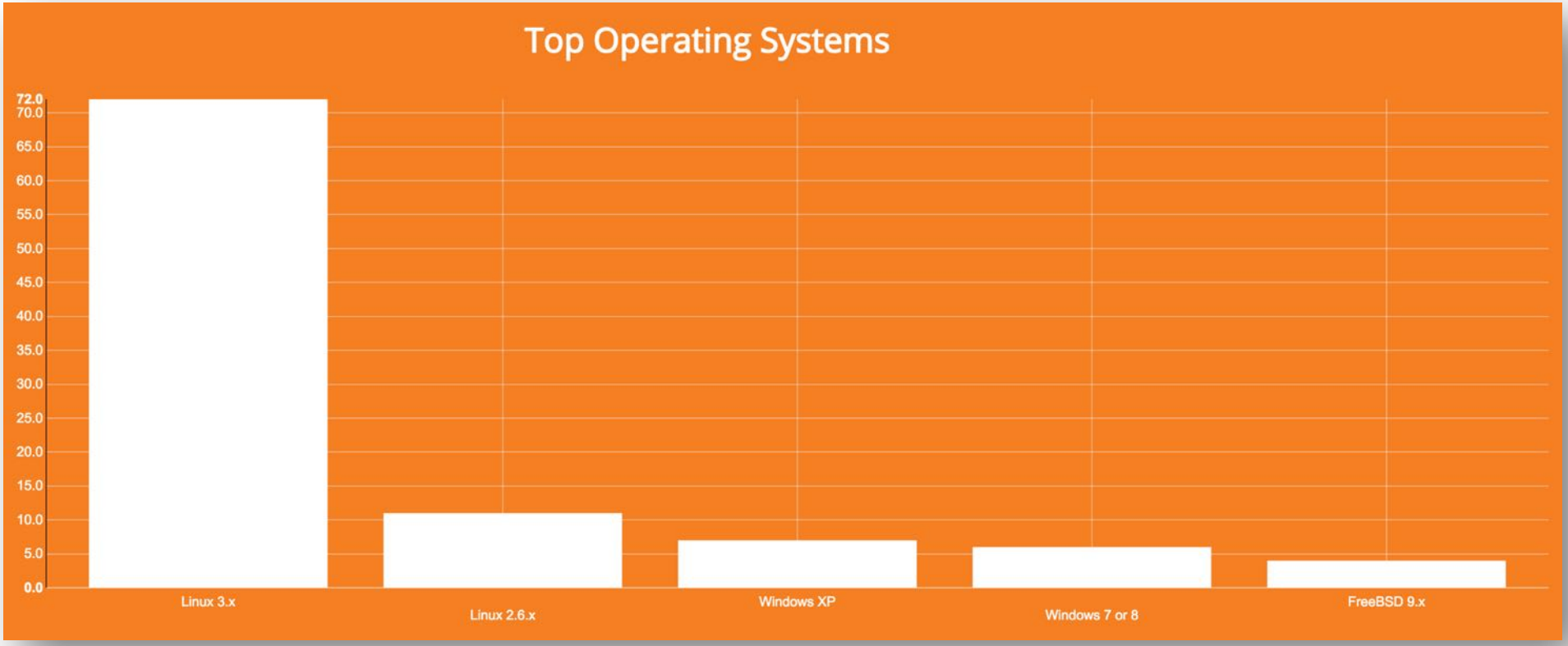
Versiones



MONGOLOL

Dominios

Sistema Operativo de servidor



MONGOL

SH3LLCON
Security Hell Conference

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)

Otras investigaciones

- Online Gaming site **Slingo** (2,5 Millones de cuentas)
- **iFit** (570.000 usuarios)

MONGOLOL

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)

MONGOL

SH3LLCON
Security Hell Conference

Spain

MONGOL

España

Censored ☹

MONGOL

España

Censored ☹

MONGOLOL

Golismeando datos

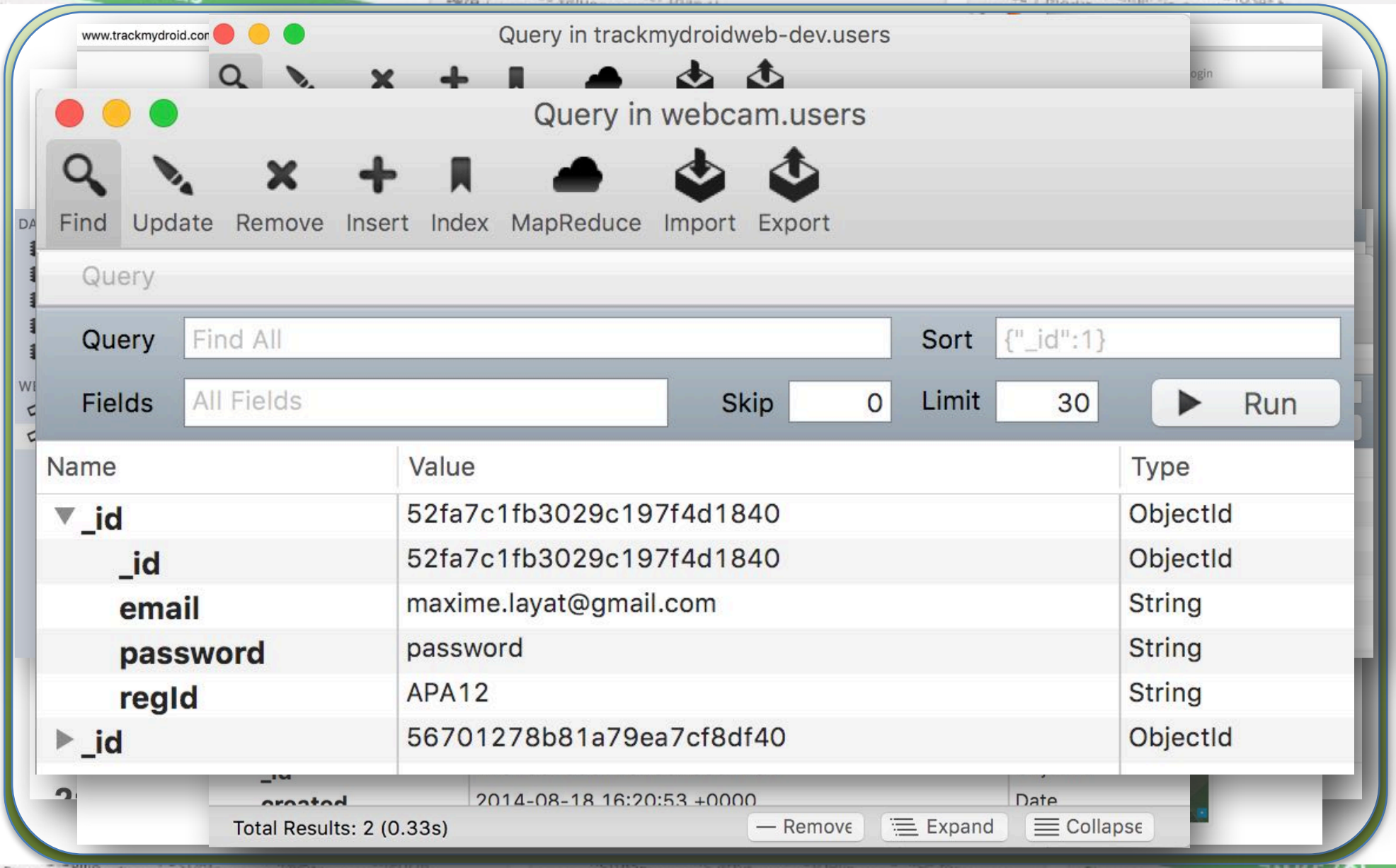
Censored ☹

MONGOL

SH3LLCON
Security Hell Conference

EU

MONGOL

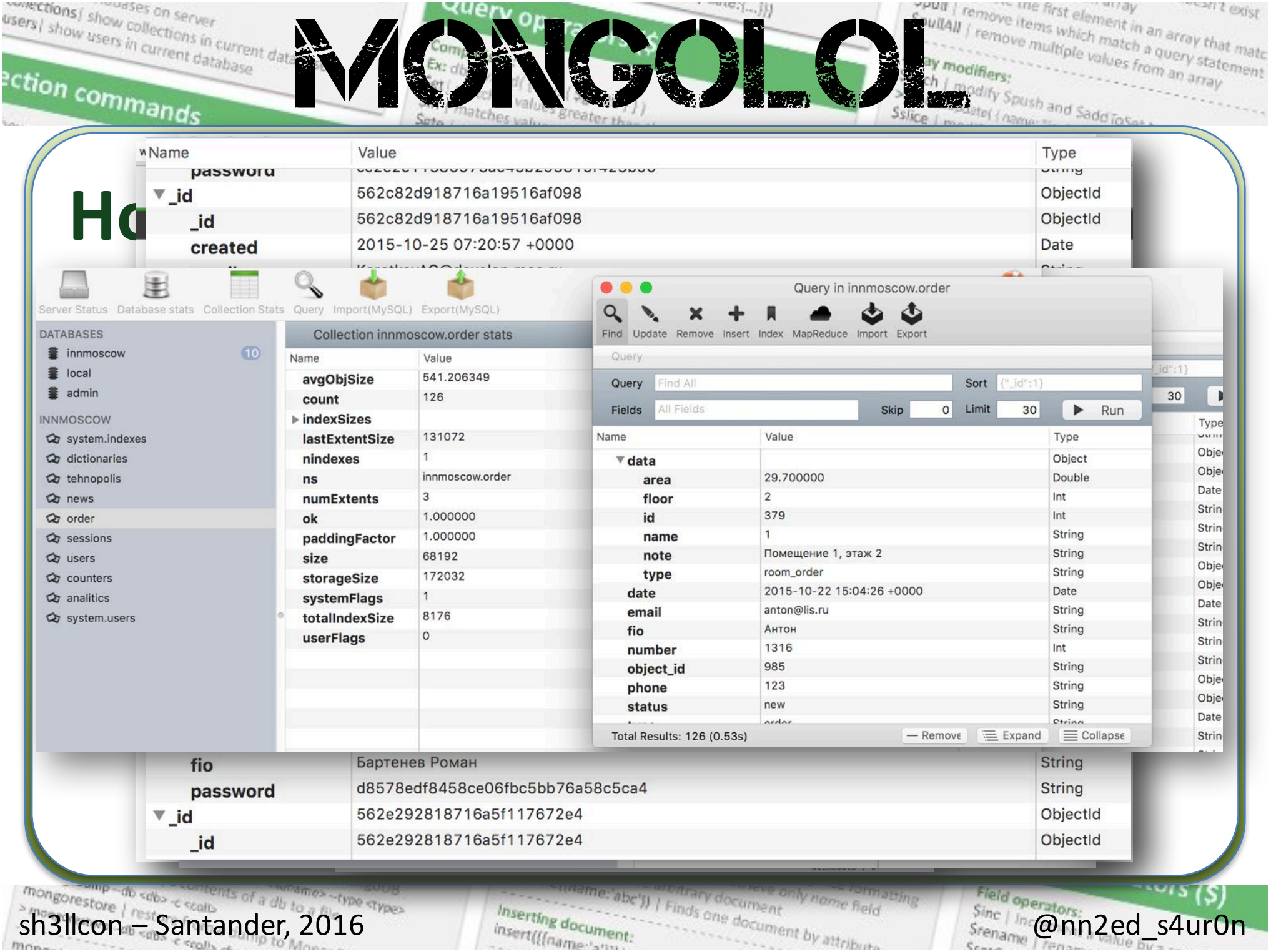

Query in trackmydroidweb-dev.users
Query in webcam.users
Find
Update
Remove
Insert
Index
MapReduce
Import
Export
Query
Query
Find All
Sort
{"_id":1}
Fields
All Fields
Skip
0
Limit
30
Run
Name
Value
Type
_id
52fa7c1fb3029c197f4d1840
ObjectId
_id
52fa7c1fb3029c197f4d1840
ObjectId
email
maxime.layat@gmail.com
String
password
password
String
regId
APA12
String
_id
56701278b81a79ea7cf8df40
ObjectId
2014-08-18 16:20:53 +0000
Date
Total Results: 2 (0.33s)
Remove
Expand
Collapse

MONGOL

SH3LLCON
Security Hell Conference

Из России с любовью

MONGOL

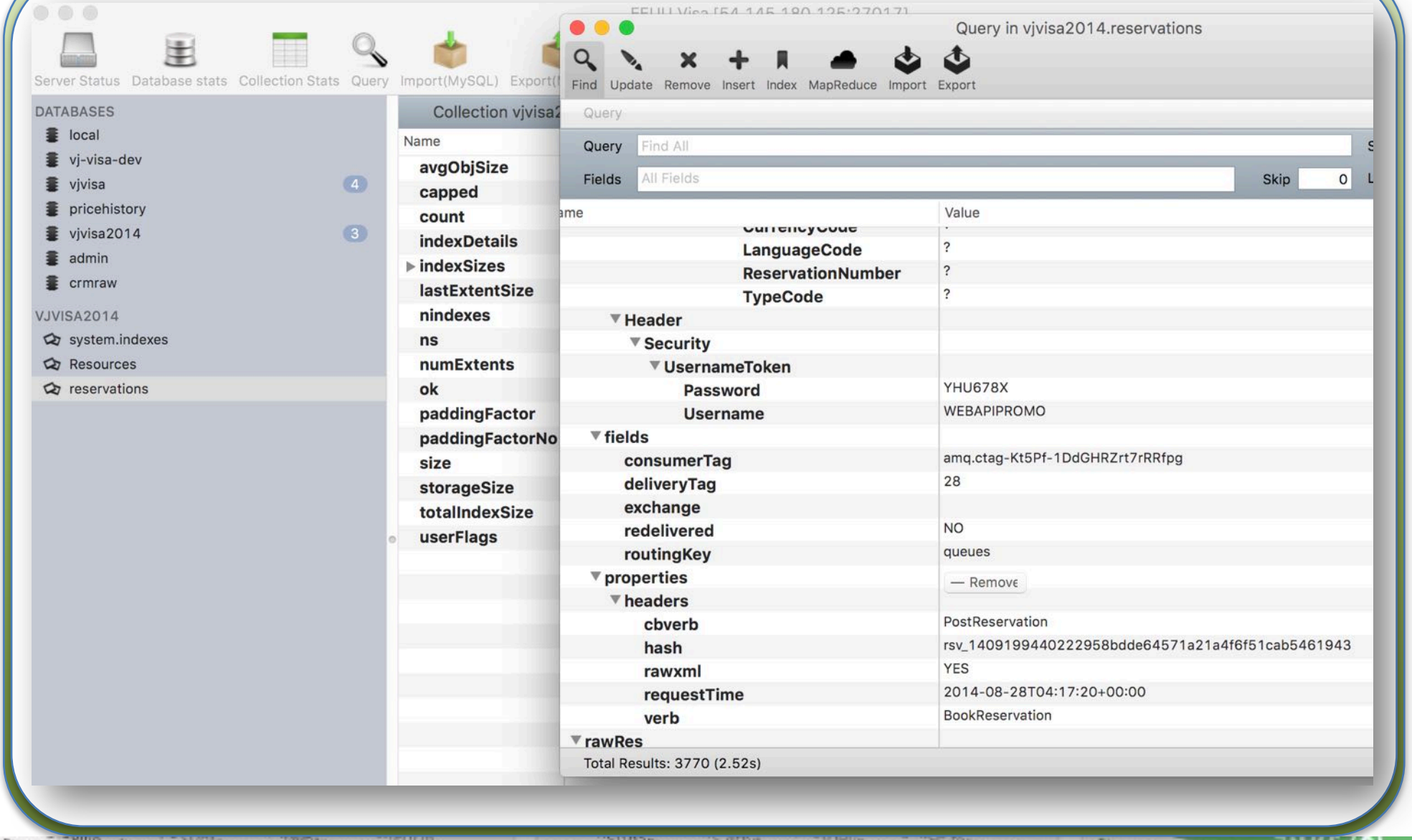

Server Status
Database stats
Collection Stats
Query
Import(MySQL)
Export(MySQL)
DATABASES
innmoscow
local
admin
INNMOSCOW
system.indexes
dictionaries
tehnopolis
news
order
sessions
users
counters
analitics
system.users
Collection innmoscow.order stats
Name
Value
avgObjSize 541.206349
count 126
indexSizes
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
Query Find All
Sort {"_id":1}
Fields All Fields
Skip 0
Limit 30
Run
Name
Value
Type
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
password
_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

MONGOL

SH3LLCON
Security Hell Conference

USA

MONGOL

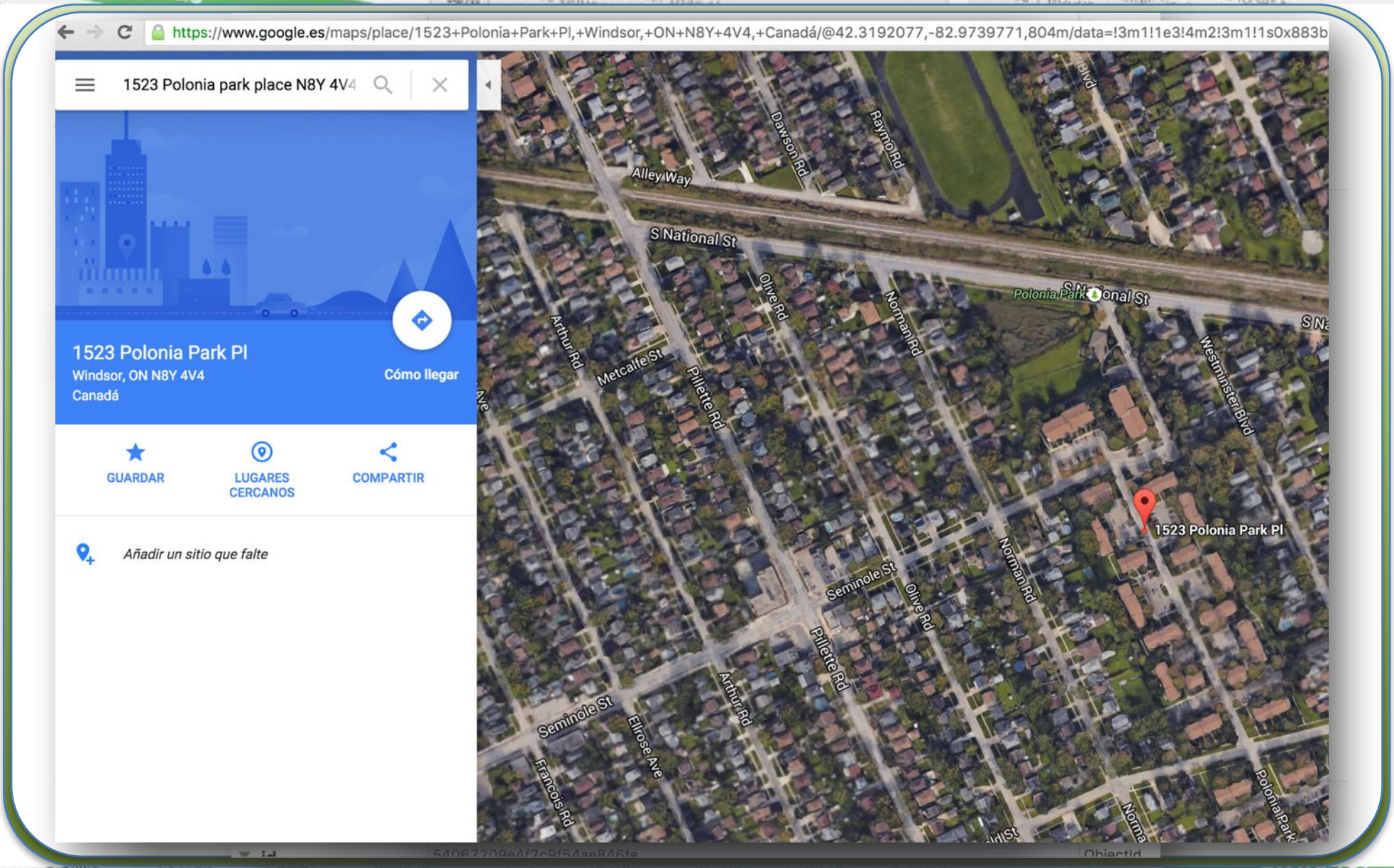

Server Status
Database stats
Collection Stats
Query
Import(MySQL)
DATABASES
local
vj-visa-dev
vjvisa
4
pricehistory
vjvisa2014
3
admin
crmraw
VJVISA2014
system.indexes
Resources
reservations
Collection vjvisa2
Name
avgObjSize
capped
count
indexDetails
indexSizes
lastExtentSize
nindexes
ns
numExtents
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)

MONGOL

SH3LLCON
Security Hell Conference

CANADA

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
Raymond Rd
S National St
Olive Rd
Norman Rd
Arthur Rd
Metcalfe St
Pillette Rd
Westminster Blvd
Polonia Park
1523 Polonia Park Pl
Seminole St
Ellrose Ave
Francois Rd

MONGOLOL

SH3LLCON
Security Hell Conference

```
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

MONGOLOL

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

Automatización de tareas

MONGOL

SH3LLCON
Security Hell Conference

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

SH3LLCON
Security Hell Conference

¿Preguntas?

MONGOL OL

SH3LLCON Security Hell Conference

Underground CON

Free with Open Bar

Stay tuned next Monday

sh3llcon
Security Hell Conference

Muchas gracias

@NN2ed_s4ur0n

s4ur0n@navajanegra.com