

# A Growing Mongo Problem

Ming Chow

Email: [mchow@cs.tufts.edu](mailto:mchow@cs.tufts.edu)

Twitter: [@0xmchow](https://twitter.com/0xmchow)

# MongoDB Use in the Present

- News websites. Examples: Business Insider (<http://www.businessinsider.com/>), The Guardian UK (<http://www.slideshare.net/tackers/why-we-chose-mongodb-for-guardiancouk>)
- Massively Multiplayer Online Games (MMORPGs): EA's FIFA Online 3 (<http://www.mongodb.com/blog/post/ea-scores-mongodb-based-fifa-online-3>)
- Countless companies including Adobe, Craigslist, Dropbox, eBay, MetLife (<http://www.mongodb.com/mongodb-scale>)

# MongoDB Use in the Future

- The Internet of Things (IoT)
  - Embedded devices
  - For real-time data from sensors, connected devices
  - References:
    - <http://www.mongodb.com/use-cases/internet-of-things>
    - <http://www.usatoday.com/story/tech/2014/07/01/mongodb-oracle-battle-of-the-databases-google-internet-of-things/11305863/>
    - <http://blogs.wsj.com/cio/2014/06/24/expect-internet-of-things-to-bring-new-data-demands-mongodb-ceo/>

# Why Target MongoDBs?

- For the *enormous* amount of data stored.
- Naive developers and administrators => they hardly care about security; defaults are almost never changed
  - Learning curve of using MongoDB is low
- 10Gen is oblivious to security issues: "*...We were on with...the MongoDB guys talking about the security of the platform, and...it was really clear that they just didn't care, because their customers weren't asking for it.*" - Rich Mogull, Security Weekly Podcast Episode 345

# The Reality of MongoDB and Security: It Is That Bad

- “Just walk in”
- No authentication out-of-the-box
- Lots of blind trust
  - User input
  - Connections from other computers
- No encryption used for data or for transmission of data from server to client by default

# On SHODAN

The screenshot shows a web browser window with two tabs: "SHODAN - Computer Search" and "A Growing Mongo Problem". The address bar shows the URL "www.shodanhq.com/search?q=mongodb". The page features a navigation menu with links for "Shodan", "Exploits", "Scanhub", "Maps", "Blog", and "Membership". Below the navigation is a search bar containing the text "mongodb" and a "Search" button. The main content area is divided into three columns:

- Services:** A table listing various services and their counts.

Service	Count
MongoDB	25,991
SMTP	12
HTTP	2
VNC	1
SMB	1
- Top Countries:** A table listing the top countries and their counts.

Country	Count
United States	10,065
China	5,478
Russian Federation	1,146
Germany	975
France	546
- 83.98.138.135:** A detailed entry for a specific IP address, including the organization name "Reasonnet IP Networks B.V.", the date it was added ("05.08.2014"), and a small flag icon. To the right of this entry is a section titled "MongoDB Server Information" containing a JSON object with various metrics and server details.

```
{
  "metrics": {
    "getLastError": {
      "wtime": {
        "num": 0,
        "totalMillis": 0
      },
      "wtimeouts": 0
    },
    "queryExecutor": {
      "scanned": 10887074067
    },
    "record": {
```

# On SHODAN (continued)

The screenshot shows a web browser window with the URL `www.shodanhq.com/search?q=mongo`. The page features a navigation bar with links to Shodan, Exploits, Scanhub, Maps, Blog, and Membership. Below the navigation bar is a search bar containing the text 'mongo' and a 'Search' button. The main content area displays search results for 'mongo', organized into three columns: Services, Top Countries, and a list of specific IP addresses with their associated hostnames and details.

Like living on the edge?

Shodan Exploits Scanhub Maps Blog Membership

SHODAN mongo Search

Services			
<a href="#">MongoDB Web Interface</a>	8,550	<b>74.91.20.66</b>	HTTP/1.0 401
<a href="#">MongoDB</a>	610	<b>DataShack, LC</b>	WWW-Authenticate: Digest realm="mongo",
<a href="#">Finger</a>	21	Added on 10.10.2014	Content-Type: text/plain;charset=utf-8
<a href="#">SMTP</a>	17	Kansas City	Connection: close
<a href="#">NetBIOS</a>	7		Content-Length: 12

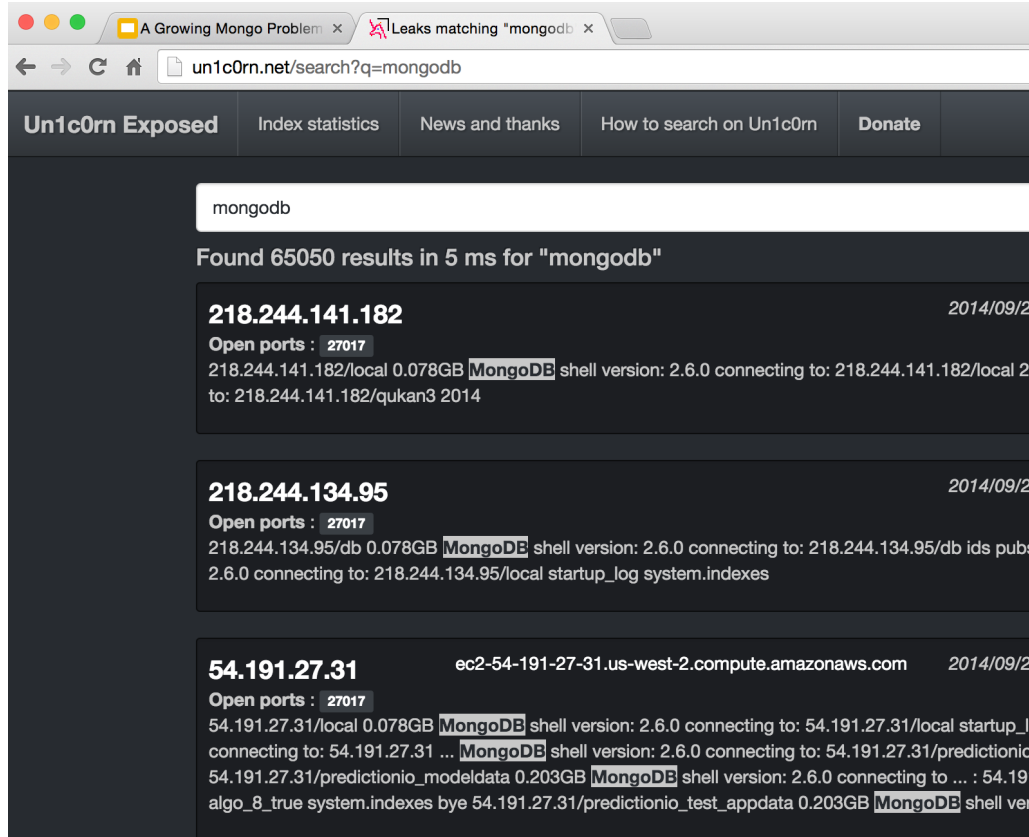
  

Top Countries			
<a href="#">United States</a>	4,571	<b>84.16.67.141</b>	HTTP/1.0 401
<a href="#">Russian Federation</a>	874	<b>Infomaniak Network SA</b>	WWW-Authenticate: Digest realm="mongo",
<a href="#">China</a>	849	Added on 10.10.2014	Content-Type: text/plain;charset=utf-8
<a href="#">Germany</a>	348		Connection: close
<a href="#">France</a>	298	ice13.infomaniak.ch	Content-Length: 12

<b>50.56.220.58</b>	HTTP/1.0 401
<b>Rackspace Hosting</b>	WWW-Authenticate: Digest realm="mongo",
Added on 10.10.2014	Content-Type: text/plain;charset=utf-8
San Antonio	
50.56.220.58.static.cloud.ipn.com	

# On Project Un1c0rn (<http://un1c0rn.net/>)



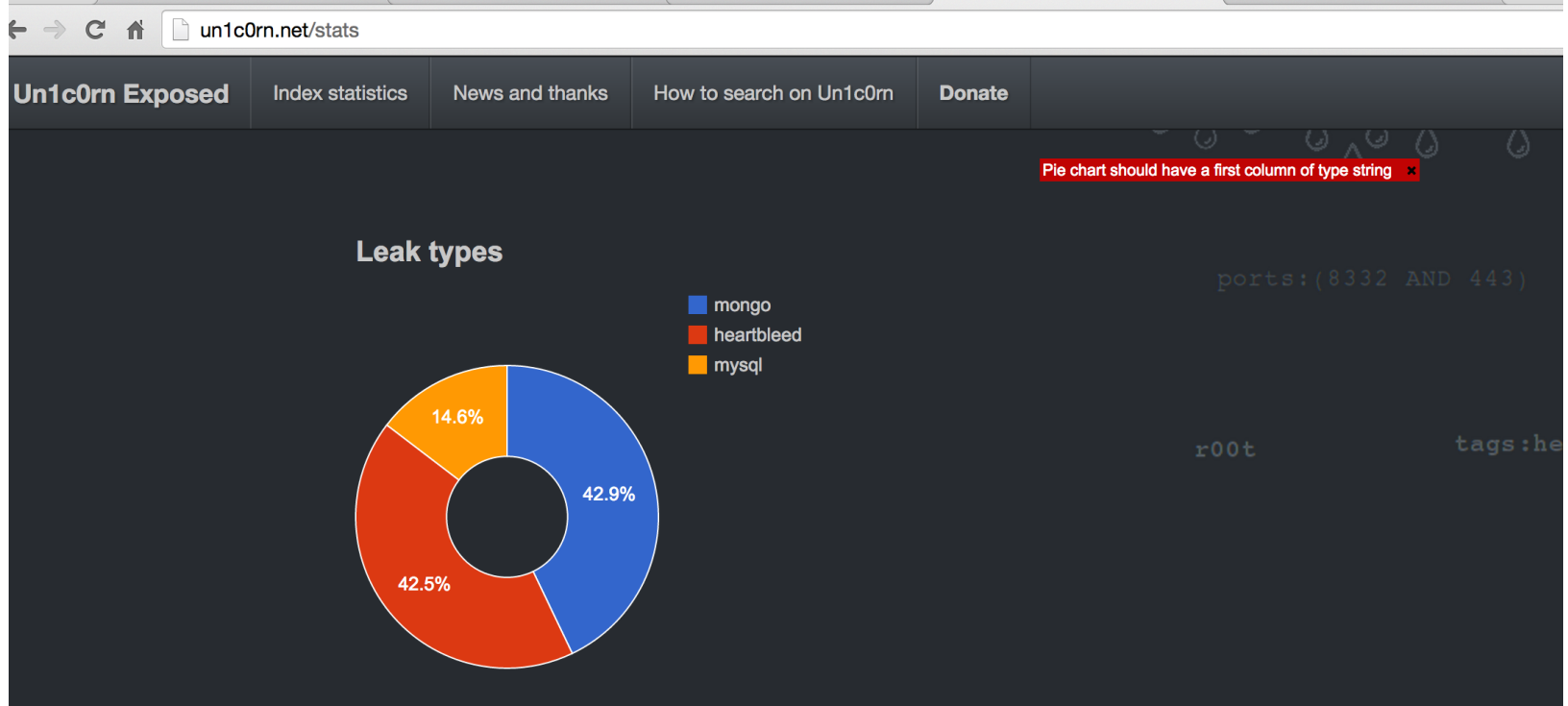
The screenshot shows a web browser window with two tabs: "A Growing Mongo Problem" and "Leaks matching 'mongodb'". The address bar shows the URL `un1c0rn.net/search?q=mongodb`. The page has a dark theme and a navigation bar with links: "Un1c0rn Exposed", "Index statistics", "News and thanks", "How to search on Un1c0rn", and "Donate".

The search results for "mongodb" are displayed as follows:

- Search Query:** mongodb
- Found 65050 results in 5 ms for "mongodb"**
- 218.244.141.182** (2014/09/2)
  - Open ports : 27017
  - 218.244.141.182/local 0.078GB MongoDB shell version: 2.6.0 connecting to: 218.244.141.182/local 2 to: 218.244.141.182/qukan3 2014
- 218.244.134.95** (2014/09/2)
  - Open ports : 27017
  - 218.244.134.95/db 0.078GB MongoDB shell version: 2.6.0 connecting to: 218.244.134.95/db ids pub 2.6.0 connecting to: 218.244.134.95/local startup\_log system.indexes
- 54.191.27.31** (2014/09/2) `ec2-54-191-27-31.us-west-2.compute.amazonaws.com`
  - Open ports : 27017
  - 54.191.27.31/local 0.078GB MongoDB shell version: 2.6.0 connecting to: 54.191.27.31/local startup\_ connecting to: 54.191.27.31 ... MongoDB shell version: 2.6.0 connecting to: 54.191.27.31/predictionio 54.191.27.31/predictionio\_modeldata 0.203GB MongoDB shell version: 2.6.0 connecting to ... : 54.19 algo\_8\_true system.indexes bye 54.191.27.31/predictionio\_test\_appdata 0.203GB MongoDB shell ver



# On Project Un1c0rn (continued)



# On the Application Side, Injection Attacks

1. **Query:** creating unsafe queries via string concatenation
2. **Schema:** inserting a record into a schema that does not exist will automatically create the new schema
3. **JavaScript:** `$where`, `db.eval()` take in JavaScript functions as parameters
4. **Request:** insert associative arrays in GET requests.  
See <https://gist.github.com/mchow01/49f8979829f1c488d922>

# Russell Butturini's NoSQLMap

- <http://www.nosqlmap.net/>
- Automates injection attacks and exploit default configuration
- Supports MongoDB and now also CouchDB
- Notable features on MongoDB:
  - Database enumeration and cloning attacks
  - Extracts database names, users, and password hashes
  - Scans subnets or IP lists for MongoDB databases with default access and enumerating versions
  - Dictionary and brute force password cracking of recovered MongoDB hashes

```
1-Set target host/IP (Current: [REDACTED])
2-Set web app port (Current: 80)
3-Set App Path (Current: Not Set)
4-Toggle HTTPS (Current: OFF)
5-Set MongoDB Port (Current : 27017)
6-Set HTTP Request Method (GET/POST) (Current: GET)
7-Set my local MongoDB/Shell IP (Current: Not Set)
8-Set shell listener port (Current: Not Set)
9-Toggle Verbose Mode: (Current: ON)
0-Load options file
a-Load options from saved Burp request
b-Save options file
x-Back to main menu
Select an option: x
```

```
=====
NoSQLMap
=====
```

```
NoSQLMap-v0.5
nosqlmap@gmail.com
```

```
1-Set options
2-NoSQL DB Access Attacks
3-NoSQL Web App attacks
4-Scan for Anonymous MongoDB Access
5-Change Platform (Current: MongoDB)
x-Exit
Select an option: 2
DB Access attacks (MongoDB)
```

```
=====
Checking to see if credentials are needed...
Successful access with no credentials!
```

# Now What?

- What I underestimated: the flexibility and scaling of MongoDB.
- With the growing concerns of security of the “Internet of Things”, this only adds fuel to the fire.
- The future is ripe for attackers.

# References

- Chow, M. “Abusing NoSQL Databases” DEF CON 21, Las Vegas, NV  
<https://www.defcon.org/images/defcon-21/dc-21-presentations/Chow/DEFCON-21-Chow-Abusing-NoSQL-Databases.pdf>
- Butterini, R. “Making Mongo Cry: NoSQL for Penetration Testers” DerbyCon 2014, Louisville, KY <http://slideplayer.us/slide/2510942/>, Video: <http://www.irongeek.com/i.php?page=videos/derbycon4/t408-making-mongo-cry-attacking-nosql-for-pen-testers-russell-butturini>