MongoDB 勒索事件现状调查报告

目录

i. 事件背景

2016 年底至 2017 年初，互联网爆发了针对 MongoDB 的勒索事件，国内外新闻都有大范围的报道。

黑客利用了 Mongodb 未授权访问漏洞，批量的对可操作的数据库进行了“删库”操作，并留下自己的联系方式，以此要挟用户使用比特币支付赎金换回数据。

相关报道如下：
http://www.top-news.top/news-12640670.html
https://www.toppn.com/view/184696.html

ii. 调查的起因

近日 360CERT 通过在外部署的探针发现，某 C 段地址的 27017 端口短时间内被大量扫描。360CERT 遂立即对该事件进行跟进，发现该 C 段地址有数台存在未授权访问的 Mongodb 服务器。

通过初步检测发现该 C 段 Mongodb 服务器发现均存在名为“WRITE_ME”、“REQUEST_YOUR_DATA”、“CONTACTME”等数据库 （如图 1，图 2，图 3）。通过数据库内留下的信息判断，黑客将用户数据删除后索要 0.1 至 1 个比特币。

```
> show dbs
WRITE_ME  0.203GB
admin     (empty)
> use WRITE_ME
switched to db WRITE_ME
> show collections
WRITE_ME
system.indexes
> db.WRITE_ME.find()
{ "_id" : ObjectId("5927dbb9b164759986d13d3b"), "email" : "request@firemail.cc",
 "btc_wallet" : "1GCgiza9buq4WdEtrsRjbvZMcbnnvCsZwH", "note" : "Your DB is in sa
fety and backed up (check logs). To restore send 0.2 BTC and email with your ser
ver ip or domain name. Each 24 hours we erase all data." }
>
```

图 1：勒索者留下的数据库“WRITE_ME”

```
> show dbs
REQUEST_YOUR_DATA  0.203GB
admin              (empty)
test               (empty)
> use REQUEST_YOUR_DATA
switched to db REQUEST_YOUR_DATA
> db.REQUEST_YOUR_DATA.find()
{ "_id" : ObjectId("593cfc5169f02e8a2a110596"), "email" : "request@tfwno.gf", "b
tc_wallet" : "1JjNwP7kXyvP38xbFhxbmebHAZFvnfXHt8", "note" : "Your DB is in safet
y and backed up (check logs). To restore send 0.1 BTC and email with your server
 ip or domain name. Each 24 hours we erase all data." }
>
```

图 2：勒索者留下的数据库“REQUEST_YOUR_DATA”

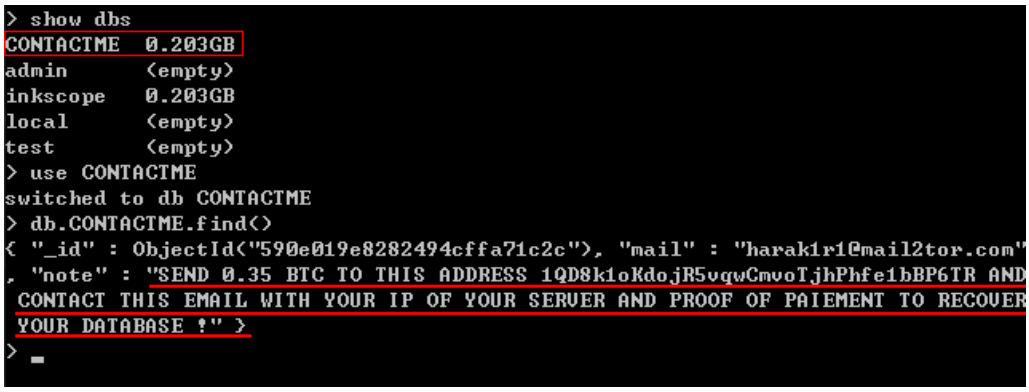

图 3：勒索者留下的数据库“CONTACTME”

由此判断当前互联网上任然存在着大量未授权访问的 Mongodb 服务器，已经被黑客删除了数据，并以此进行勒索。

iii. 全网扫描数据分析

针对全网扫描后发现，有 52313 个 IP 地址开放了 27017 端口。

进一步对上述 IP 地址进一步扫描后发现有 5538 个 Mongodb 服务器仍存在未授权访问漏洞，其中 4279 个已经发现勒索者信息（如图 4）。

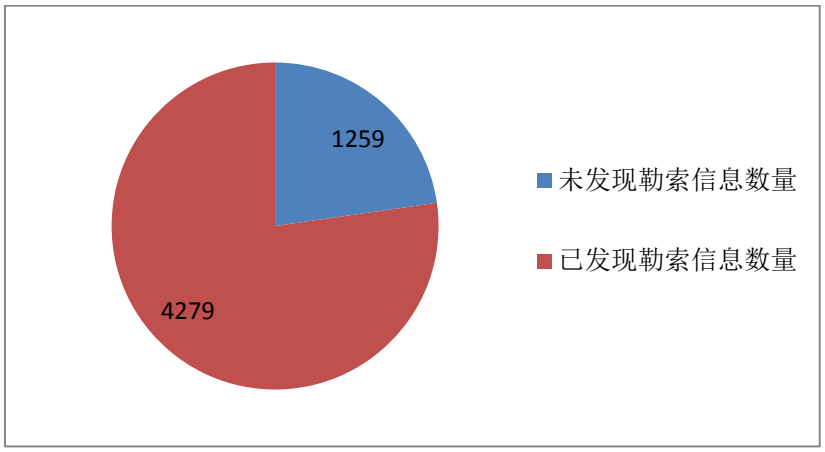

图 4：未授权访问的 Mongodb 服务器被勒索情况

1. TOP10 勒索者邮箱

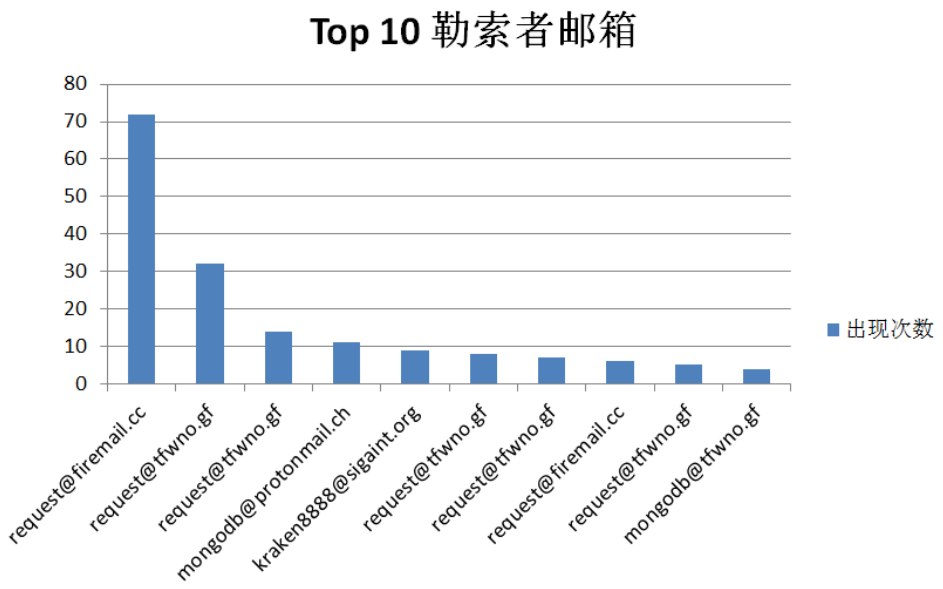

图 5：Top 10 勒索者邮箱

上述“勒索者邮箱”是指在未授权访问的 Mongodb 中，勒索者在其留下的电子邮箱（如图 5）。

2. TOP10 攻击日期

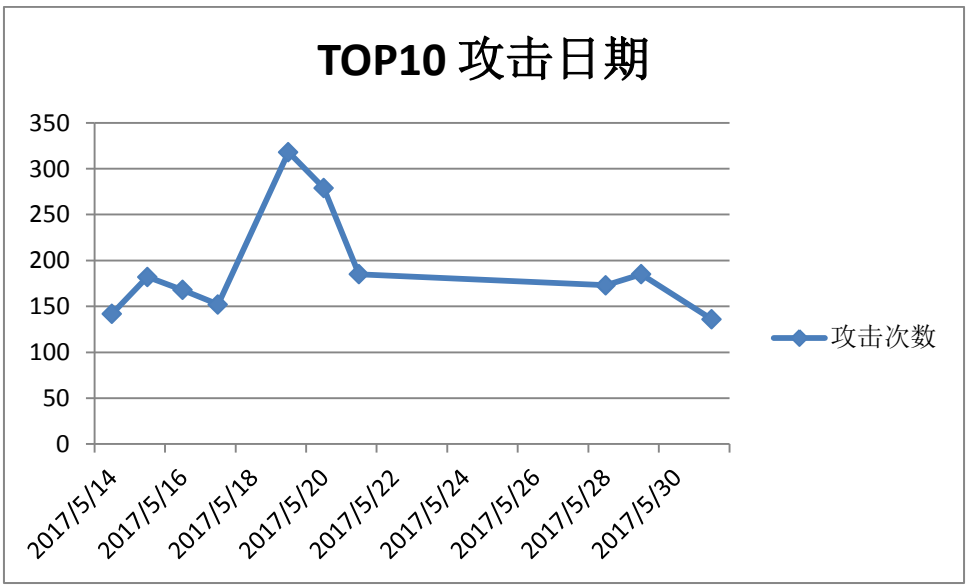

图 6：TOP10 攻击日期

上述“攻击日期”是指在未授权访问的 Mongodb 中，勒索者在添加勒索信息时的操作日期（如图 6）。

通过 360 NetworkScan Mon 平台可以看出在 2017 年 5 月 16 日左右，互联网产生了大量针对 27017 端口的扫描数量（如图 7，图 8）。

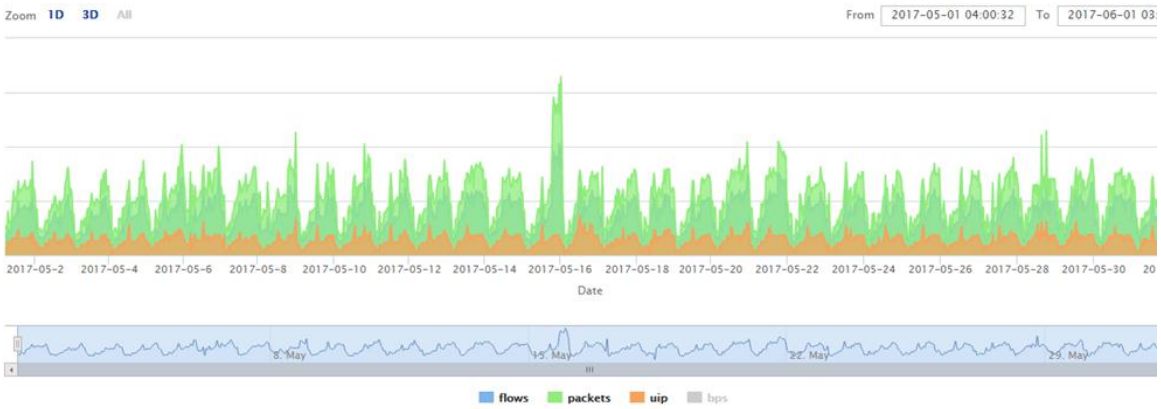

图 7：360NetworkScan Mon 系统针对 27017 端口监控结果

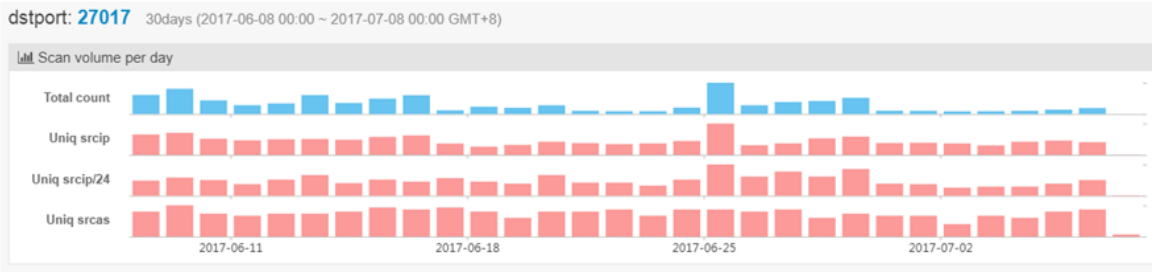

图 8：360NetworkScan Mon 系统针对 27017 端口监控结果

3. TOP10 勒索者数据库使用名称

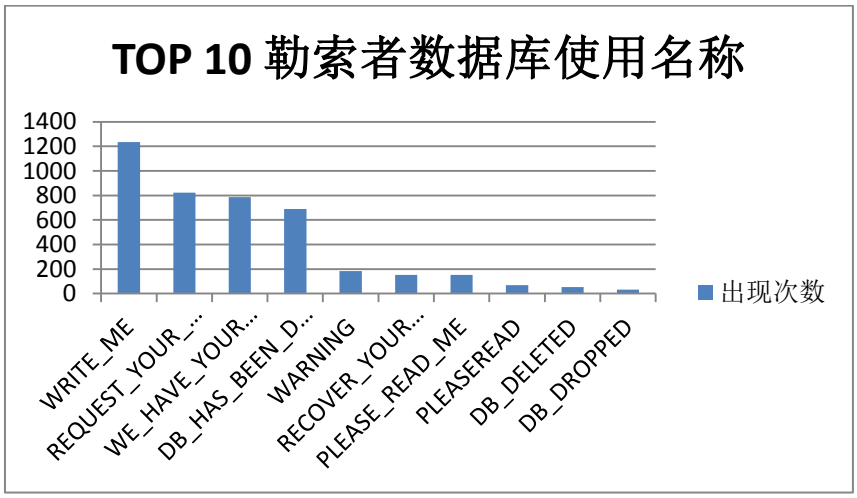

图 9：TOP 10 勒索者数据库使用名称

上述“勒索者数据库使用名称”是指在未授权访问的 MongoDB 中，勒索者在添加勒索信息时的创建的数据库名称（如图 9）。

如果某个 MongoDB 中出现上述名称的数据库，那很有可能已经被勒索者攻击。

4. TOP10 数据库数量

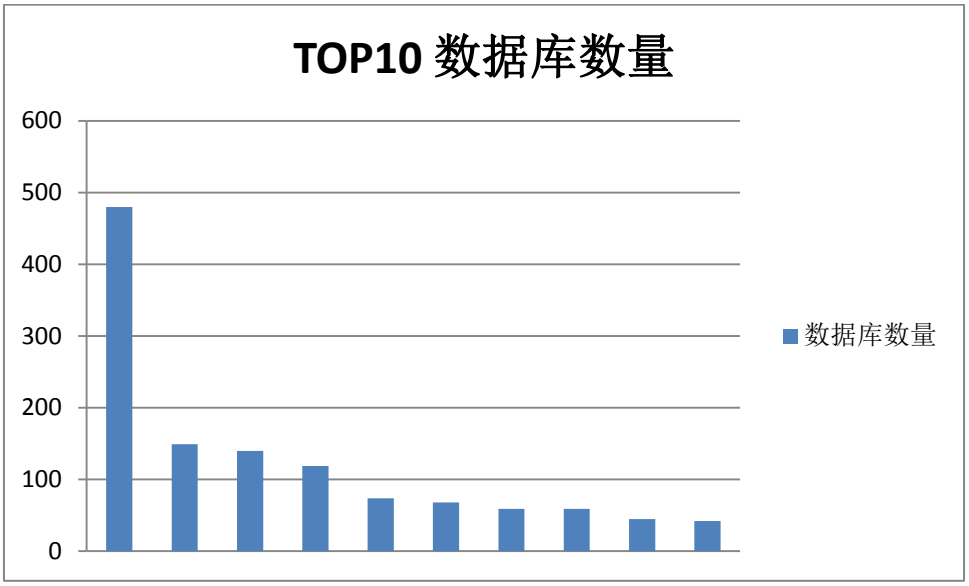

图 10：TOP10 数据库数量

上述“数据库数量”是指存在未授权访问的 MongoDB 服务器中数据库的数量（为保护用户数据，对应的 IP 地址已被隐藏）。

可以看出上述 MongoDB 服务器拥有大量数据，但是存在极大的安全隐患。

iv. 漏洞影响面

在 5538 个存在未授权访问漏洞的 MongoDB 服务器中，属于中国的 IP 数量为 1180。比例达到了 21%。其中根据 IP 物理地址进行归属划分，列出了 TOP20 的物理地址归属（如下表 1）。

IP 物理地址归属	数量
中国,浙江,杭州	123
中国,北京,北京	97
中国,山东,青岛	74
中国,广东,深圳	72
中国,广东,广州	46
中国,上海,上海	44
中国,北京,北京	37
中国,上海,上海	37
中国,上海,上海	27
中国,北京,北京	26
中国,北京,北京	20
中国,广东,广州	19
中国,浙江,杭州	14
中国,香港	14
中国,北京,北京	14
中国,天津,天津	14
中国,台湾	14
中国,北京,北京	12
中国,上海,上海	11
中国,北京,北京	11

表 1：TOP20 物理地址归属

v. 修复建议

1. 修改默认端口或将 MongoDB 部署在内部网络中。
   修改默认的 MongoDB 端口(默认为：TCP 27017)为其他端口。
2. 开启 MongoDB 授权

```
> use admin
> db.createUser(
{
   user: "root",
   pwd: "YOUR PASSWORD",
   roles:
   [
    {
      role: "userAdminAnyDatabase",
      db: "admin"
    }
   ]
 }
)
```

3. 使用 SSL 加密功能
4. 使用--bind_ip 选项
   该选项可以限制监听接口 IP， 当在启动 MongoDB 的时候，使用 -bind_ip 192.168.0.1 表示启动 ip 地址绑定，数据库实例将只监听 192.168.0.1 的请求。
5. 开启日志审计功能
   审计功能可以用来记录用户对数据库的所有相关操作。
6. 做好数据备份的策略，以防万一

vi. 总结

针对 MongoDB 的勒索在 2016 年底就开始了，但是时至今日仍然有大量的未授权访问机存在，同样其他一些基础的互联网应用也存在类似问题，这个问题值得我们关注。

随着勒索软件的流行，随着虚拟货币的增值，黑客通过网络攻击进行获利提供了变现渠道，越来越多的正面暴力攻击正在变得常态化，希望各个厂商、开发者能够重视此类问题，不要造成不必要的损失。

最后，感谢 360 信息安全部和 360 网络安全研究院提供的数据支撑。