Meow: 针对未授权访问数据库的攻击事件

0x01 背景

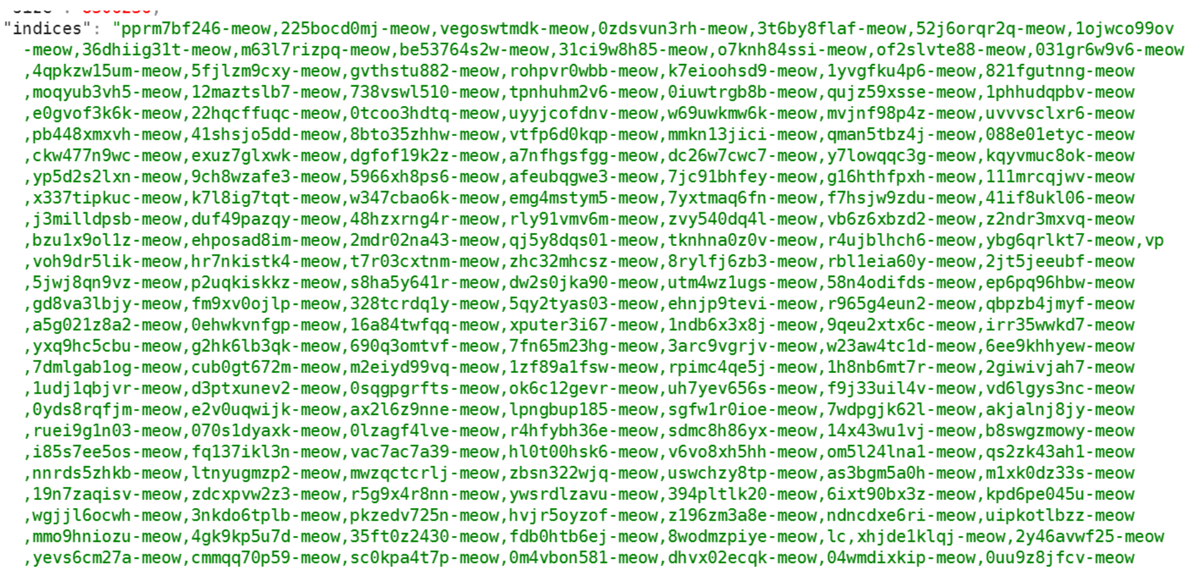
7月16日vpnmentor报道了一则关于ES信息泄漏的事件，一家香港的VPN提供商将自己的ES暴露在互联网上，造成超过2000万用户日志泄露。这是距离此次Meow攻击互联网上为授权数据库最近的一次关于ES泄漏的事件。

7月22日 BleepinComputer（@BleepinComputer）报道了有关Meow的攻击活动，称超过1800多个数据库被攻击。

0x02 数据

Meow 此次针对网络中未授权访问数据库进行攻击，主要目标对象为MonogDB、ElasticSearch数据库。

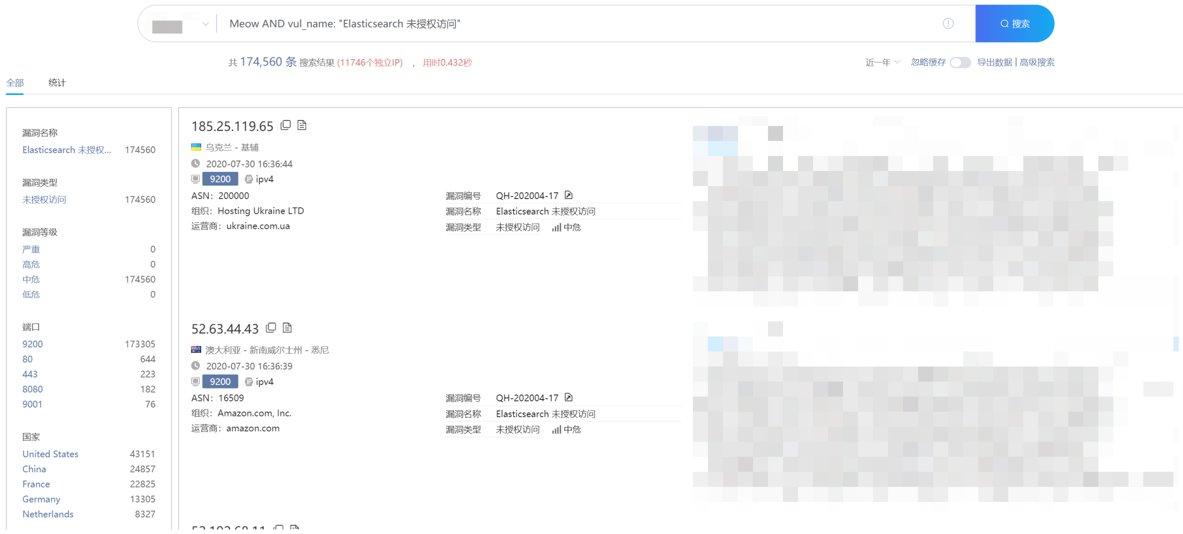
被攻击后特征为：清空数据库，并留下`Meow`字样，但没有任何钱包地址和勒索的字样。



```
"indices": "pprm7bf246-meow,225bocd0mj-meow,vegoswtmdk-meow,0zdsvun3rh-meow,3t6by8flaf-meow,52j6orqr2q-meow,1ojwco99ov
  -meow,36dhiig31t-meow,m63l7rizpq-meow,be53764s2w-meow,31ci9w8h85-meow,o7knh84ssi-meow,of2slvte88-meow,031gr6w9v6-meow
  ,4qpkzw15um-meow,5fjlzm9cxy-meow,gvthstu882-meow,rohpvr0wbb-meow,k7eioohsd9-meow,1yvgfku4p6-meow,821fgutnng-meow
  ,moqyub3vh5-meow,12maztslb7-meow,738vswl510-meow,tpnhuhm2v6-meow,0iuwtrgb8b-meow,qujz59xsse-meow,1phhudqpbv-meow
  ,e0gvof3k6k-meow,22hqcffuqc-meow,0tcoo3hdtq-meow,uyyjcofdnv-meow,w69uwkmw6k-meow,mvjnf98p4z-meow,uvvvsclxr6-meow
  ,pb448xmxvh-meow,41shsjo5dd-meow,8bto35zhhw-meow,vtfp6d0kqp-meow,mmkn13jici-meow,qman5tbz4j-meow,088e01etyc-meow
  ,ckw477n9wc-meow,exuz7glxwk-meow,dgfof19k2z-meow,a7nfhgsfgg-meow,dc26w7cwc7-meow,y7lowqqc3g-meow,kqyvmuc8ok-meow
  ,yp5d2s2lxn-meow,9ch8wzafe3-meow,5966xh8ps6-meow,afeubqgwe3-meow,7jc91bhfey-meow,g16hthfpxh-meow,111mrcqjwv-meow
  ,x337tipkuc-meow,k7l8ig7tqt-meow,w347cbao6k-meow,emg4mstym5-meow,7yxtmaq6fn-meow,f7hsjw9zdu-meow,41if8ukl06-meow
  ,j3milldpsb-meow,duf49pazqy-meow,48hzxrng4r-meow,rly91vmv6m-meow,zvy540dq4l-meow,vb6z6xbzd2-meow,z2ndr3mxvq-meow
  ,bzu1x9ol1z-meow,ehposad8im-meow,2mdr02na43-meow,qj5y8dqs01-meow,tknhna0z0v-meow,r4ujblhch6-meow,ybg6qrlkt7-meow,vp
  ,voh9dr5lik-meow,hr7nkistk4-meow,t7r03cxtnm-meow,zhc32mhcsz-meow,8rylfj6zb3-meow,rbl1eia60y-meow,2jt5jeeubf-meow
  ,5jwj8qn9vz-meow,p2uqkiskkz-meow,s8ha5y641r-meow,dw2s0jka90-meow,utm4wz1ugs-meow,58n4odifds-meow,ep6pq96hbw-meow
  ,gd8va3lbjy-meow,fm9xv0ojlp-meow,328tcrdq1y-meow,5qy2tyas03-meow,ehnjp9tevi-meow,r965g4eun2-meow,qbpzb4jmyf-meow
  ,a5g021z8a2-meow,0ehwkvnfgp-meow,16a84twfqq-meow,xputer3i67-meow,1ndb6x3x8j-meow,9qeu2xtx6c-meow,irr35wwkd7-meow
  ,yxq9hc5cbu-meow,g2hk6lb3qk-meow,690q3omtvf-meow,7fn65m23hg-meow,3arc9vgrjv-meow,w23aw4tc1d-meow,6ee9khhyew-meow
  ,7dmlgab1og-meow,cub0gt672m-meow,m2eiyd99vq-meow,1zf89a1fsw-meow,rpimc4qe5j-meow,1h8nb6mt7r-meow,2giwivjah7-meow
  ,1udj1qbjvr-meow,d3ptxunev2-meow,0sqgpgrfts-meow,ok6c12gevr-meow,uh7yev656s-meow,f9j33uil4v-meow,vd6lgys3nc-meow
  ,0yds8rqfjm-meow,e2v0uqwijk-meow,ax2l6z9nne-meow,lpngbup185-meow,sgfw1r0ioe-meow,7wdpgjk62l-meow,akjalnj8jy-meow
  ,ruei9g1n03-meow,070s1dyaxk-meow,0lzagf4lve-meow,r4hfybh36e-meow,sdmc8h86yx-meow,14x43wu1vj-meow,b8swgzmowy-meow
  ,i85s7ee5os-meow,fq137ikl3n-meow,vac7ac7a39-meow,hl0t00hsk6-meow,v6vo8xh5hh-meow,om5l24lna1-meow,qs2zk43ah1-meow
  ,nnrds5zhkb-meow,ltnyugmzp2-meow,mwzqctcrlj-meow,zbsn322wjq-meow,uswchzy8tp-meow,as3bgm5a0h-meow,m1xk0dz33s-meow
  ,19n7zaqisv-meow,zdcxpvw2z3-meow,r5g9x4r8nn-meow,ywsrdlzavu-meow,394pltlk20-meow,6ixt90bx3z-meow,kpd6pe045u-meow
  ,wgjjl6ocwh-meow,3nkdo6tplb-meow,pkzedv725n-meow,hvjr5oyzof-meow,z196zm3a8e-meow,ndncdxe6ri-meow,uipkotlbzz-meow
  ,mmo9hniozu-meow,4gk9kp5u7d-meow,35ft0z2430-meow,fdb0htb6ej-meow,8wodmzpiye-meow,lc,xhjde1klqj-meow,2y46avwf25-meow
  ,yevs6cm27a-meow,cmmqq70p59-meow,sc0kpa4t7p-meow,0m4vbon581-meow,dhvx02ecqk-meow,04wmdixkip-meow,0uu9z8jfcv-meow
```

1. Elasticsearch数据库被攻击情况

通过Quake发现Meow相关攻击行为在7月21日出现。当前Quake累计记录了174,560条有关Meow的攻击，其中涉及独立IP数量11746个。



Meow AND vul_name: "Elasticsearch 未授权访问"

搜索

共 174,560 条 搜索结果 (11746个独立IP) ， 用时0.432秒

近一年 忽略缓存 导出数据 | 高级搜索

全部 统计

漏洞名称

Elasticsearch 未授权...	174560

漏洞类型

未授权访问	174560

漏洞等级

严重	0
高危	0
中危	174560
低危	0

端口

9200	173305
80	644
443	223
8080	182
9001	76

国家

United States	43151
China	24857
France	22825
Germany	13305
Netherlands	8327

185.25.119.65

乌克兰 - 基辅

2020-07-30 16:36:44

9200 ipv4

ASN：200000

组织：Hosting Ukraine LTD

运营商：ukraine.com.ua

漏洞编号 QH-202004-17

漏洞名称 Elasticsearch 未授权访问

漏洞类型 未授权访问 中危

52.63.44.43

澳大利亚 - 新南威尔士州 - 悉尼

2020-07-30 16:36:39

9200 ipv4

ASN：16509

组织：Amazon.com, Inc.

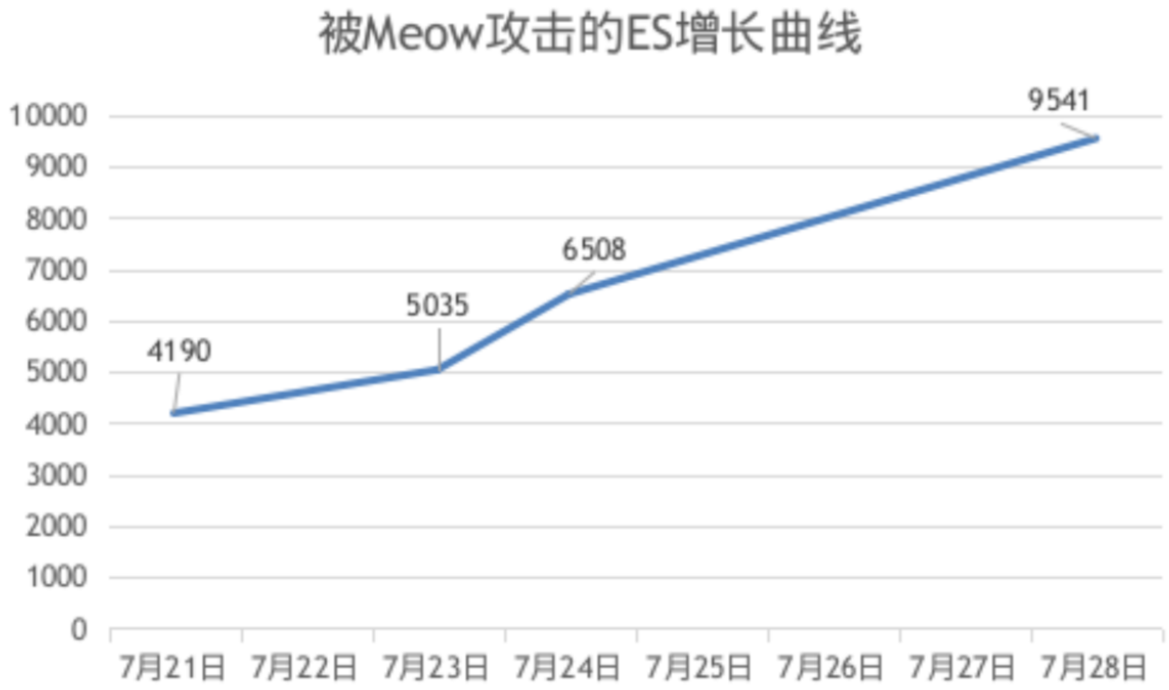
运营商：amazon.com

漏洞编号 QH-202004-17

漏洞名称 Elasticsearch 未授权访问

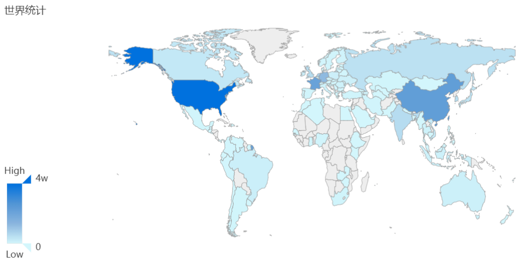
漏洞类型 未授权访问 中危

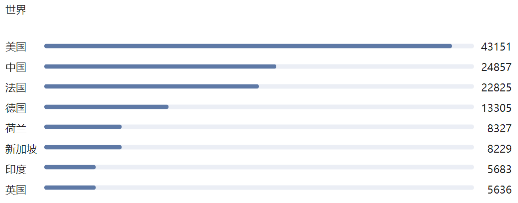
结合最近针对Elasticsearch的扫描数据可以得到，Meow针对ES的攻击增长曲线。可见被攻击的ES数量仍然存在上升趋势。



1.1 全球情况

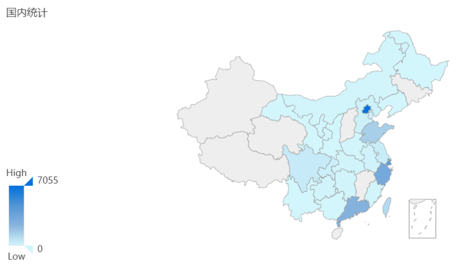
该攻击行为针对ElasticSearch数据库的攻击全球态势如下：

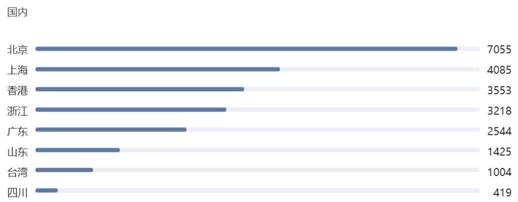




注:图中数量为累计记录

1.2 国内情况

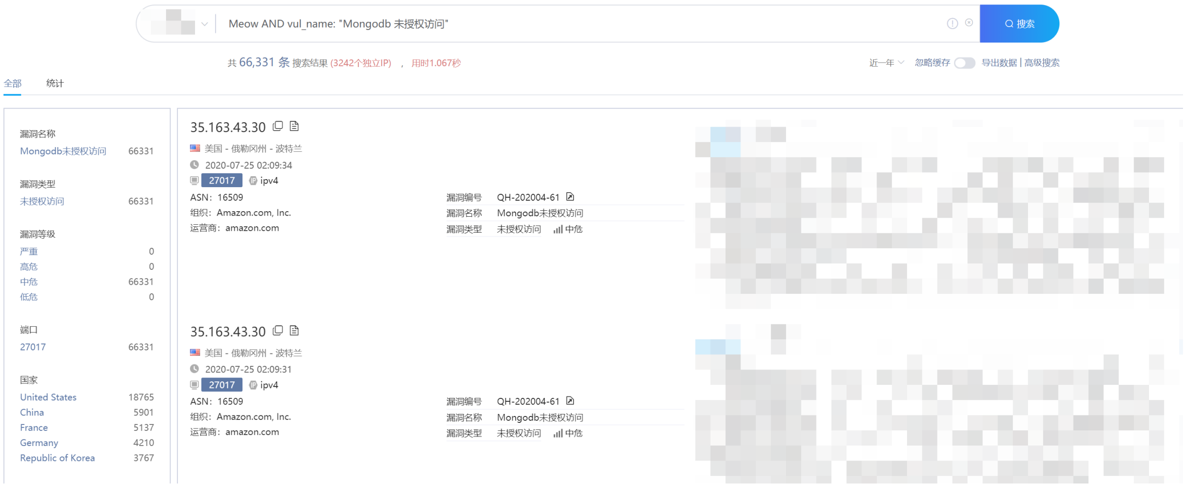




注:图中数量为累计记录

2. MongoDB数据库被攻击情况

该数据库Mongodb 的情况如图，Quake记录了66,331条攻击记录。独立IP为3242个。



[redacted] Meow AND vul_name: "Mongodb 未授权访问"

共 66,331 条 搜索结果 (3242个独立IP) ， 用时1.067秒

漏洞名称
Mongodb未授权访问 66331

漏洞类型
未授权访问 66331

漏洞等级
严重 0
高危 0
中危 66331
低危 0

端口
27017 66331

国家
United States 18765
China 5901
France 5137
Germany 4210
Republic of Korea 3767

35.163.43.30
美国 - 俄勒冈州 - 波特兰
2020-07-25 02:09:34
27017 ipv4
ASN：16509
组织：Amazon.com, Inc.
运营商：amazon.com

漏洞编号 QH-202004-61
漏洞名称 Mongodb未授权访问
漏洞类型 未授权访问 中危

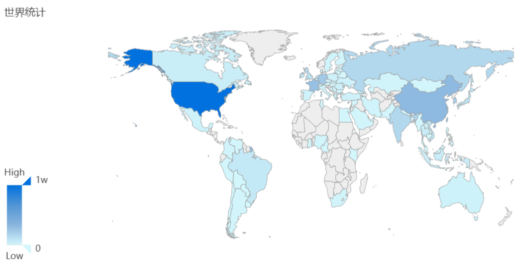
[redacted]

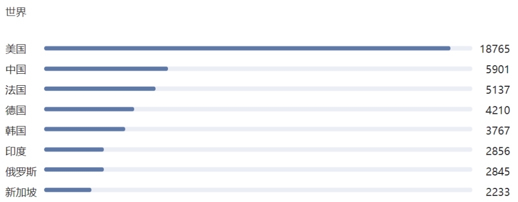
35.163.43.30
美国 - 俄勒冈州 - 波特兰
2020-07-25 02:09:31
27017 ipv4
ASN：16509
组织：Amazon.com, Inc.
运营商：amazon.com

漏洞编号 QH-202004-61
漏洞名称 Mongodb未授权访问
漏洞类型 未授权访问 中危

[redacted]

2.1 全球情况

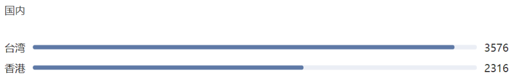




2.2 国内情况

国内Quake记录了5,901条被攻击记录，其中独立IP为331个，主要分布在香港和台湾。

国内统计
High
3576
Low
0

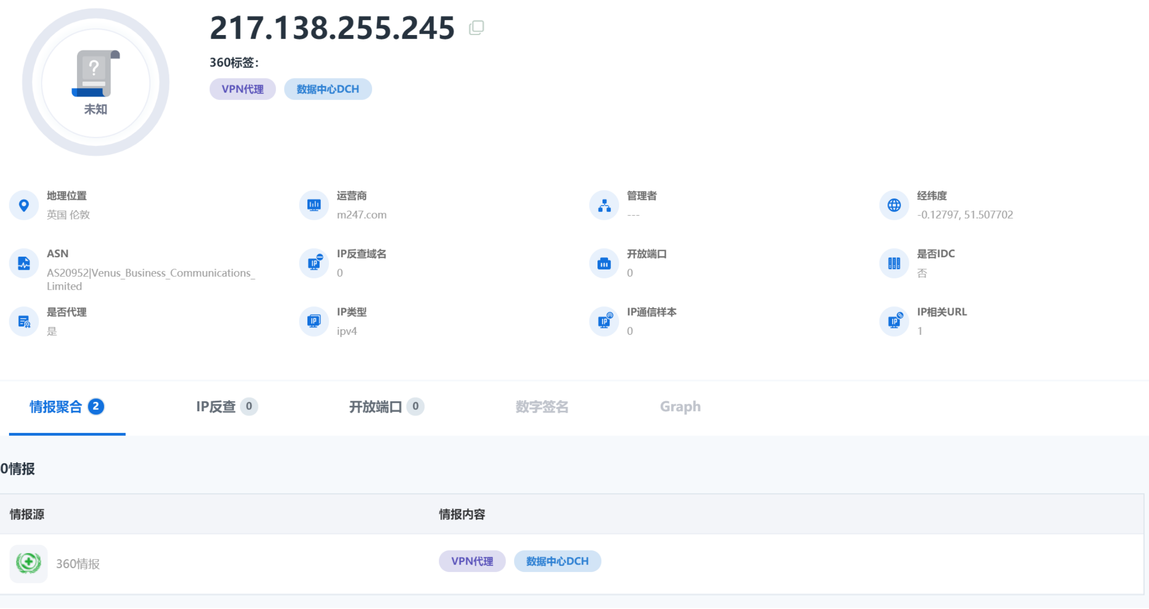


0x03 相关IoC

IP地址

```
217.138.255.245
```

通过360 TI威胁情报云溯源发现该IP为一个VPN设备：



217.138.255.245

360标签：VPN代理 数据中心DCH

未知

地理位置 英国 伦敦

运营商 m247.com

管理者 ---

经纬度 -0.12797, 51.507702

ASN AS20952|Venus_Business_Communications_Limited

IP反查域名 0

开放端口 0

是否IDC 否

是否代理 是

IP类型 ipv4

IP通信样本 0

IP相关URL 1

360情报

情报源	情报内容
360情报	VPN代理 数据中心DCH

0x04 结论

1. Meow该攻击组织（行为）活动目的尚不明确，可以持续关注类似攻击行为和组织；
2. 通过长期监测发现，互联网中仍存在大量数据库存在未授权访问情况；该情况持续已久，360CERT于2017年就曾发布过相关报告：MongoDB勒索事件现状调查报告
3. 用户可以针对使用我们系统对上述相关数据库进行检索和持续关注，相关检索语法为 `app:"ElasticSearch数据库"` 和 `app:"Mongodb数据库"`

0x05 参考链接

- https://www.vpnmentor.com/blog/report-free-vpns-leak/#Timeline-of-Discovery-and-Owner-Reaction
- https://www.hackread.com/vpn-firm-zero-logs-policy-leaks-20-million-user-logs/
- https://www.bleepingcomputer.com/news/security/new-meow-attack-has-wiped-over-1-800-unsecured-databases/