公有云威胁情报

公有云网络安全威胁情报（202110）：趋势及典型案例分析

Rugang Chen
Nov 25, 2021 • 10 min read

1 概述

云计算服务价格低廉，部署快捷方便，但存在安全风险。黑客可以用虚假信息购买，或入侵他人机器获得云资源，用这些资源窃取、勒索原有用户的数据，或用于发起DDoS攻击、发送垃圾和钓鱼邮件、虚拟货币挖矿、刷单、违法代理和传播僵尸网络木马等其他恶意行为。

360网络安全研究院 Anglerfish蜜罐（以下简称“蜜罐系统”）通过模拟仿真技术伪装成针对互联网、物联网以及工业互联网的指纹特征、应用协议、应用程序和漏洞，捕获并分析网络扫描和网络攻击行为。在2021年10月，我们共监测到来自全球58253个云服务器IP共计9213万次的网络扫描和攻击，其中发现云上网站“某市供排水总公司”持续地对外发起网络攻击行为。

2 云服务器攻击总体情况

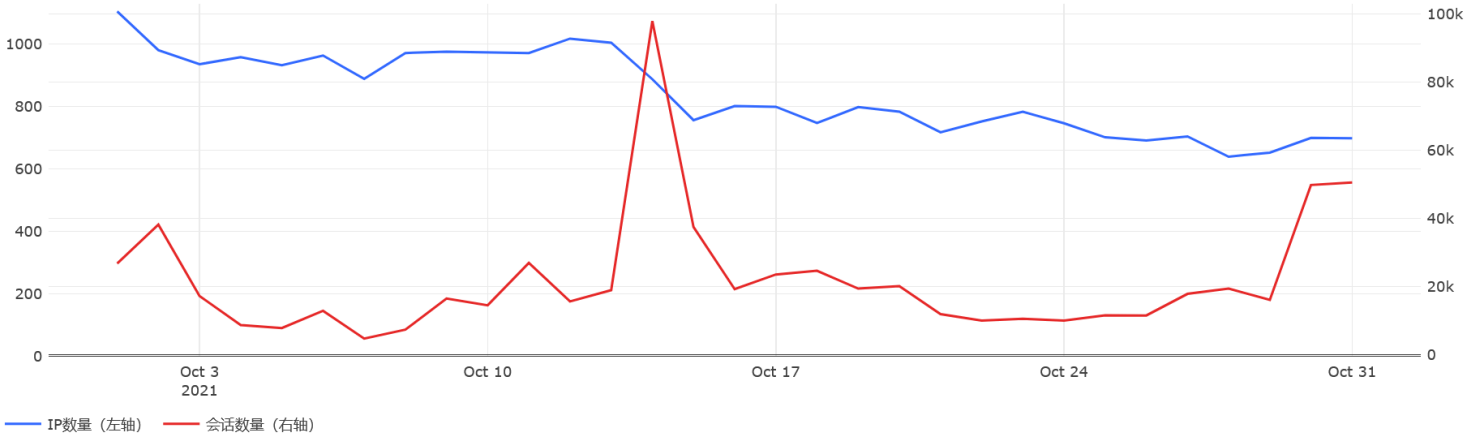
由于IPv4地址和网络端口数量是有限的，黑客通过购买或入侵获取云服务器资源后，会扫描互联网IP地址，确定攻击目标。公网上的蜜罐系统模拟成相关设备和应用程序后，就有可能被黑客攻击。因此，蜜罐系统可以用于监测互联网上包括利用云服务器发起攻击在内的各类网络攻击行为。

我们的数据来源除了蜜罐系统搜集到的网络五元组、网络数据包和恶意软件样本信息外，还包括一个覆盖国内外十几家主流厂商的云服务器IP段列表。

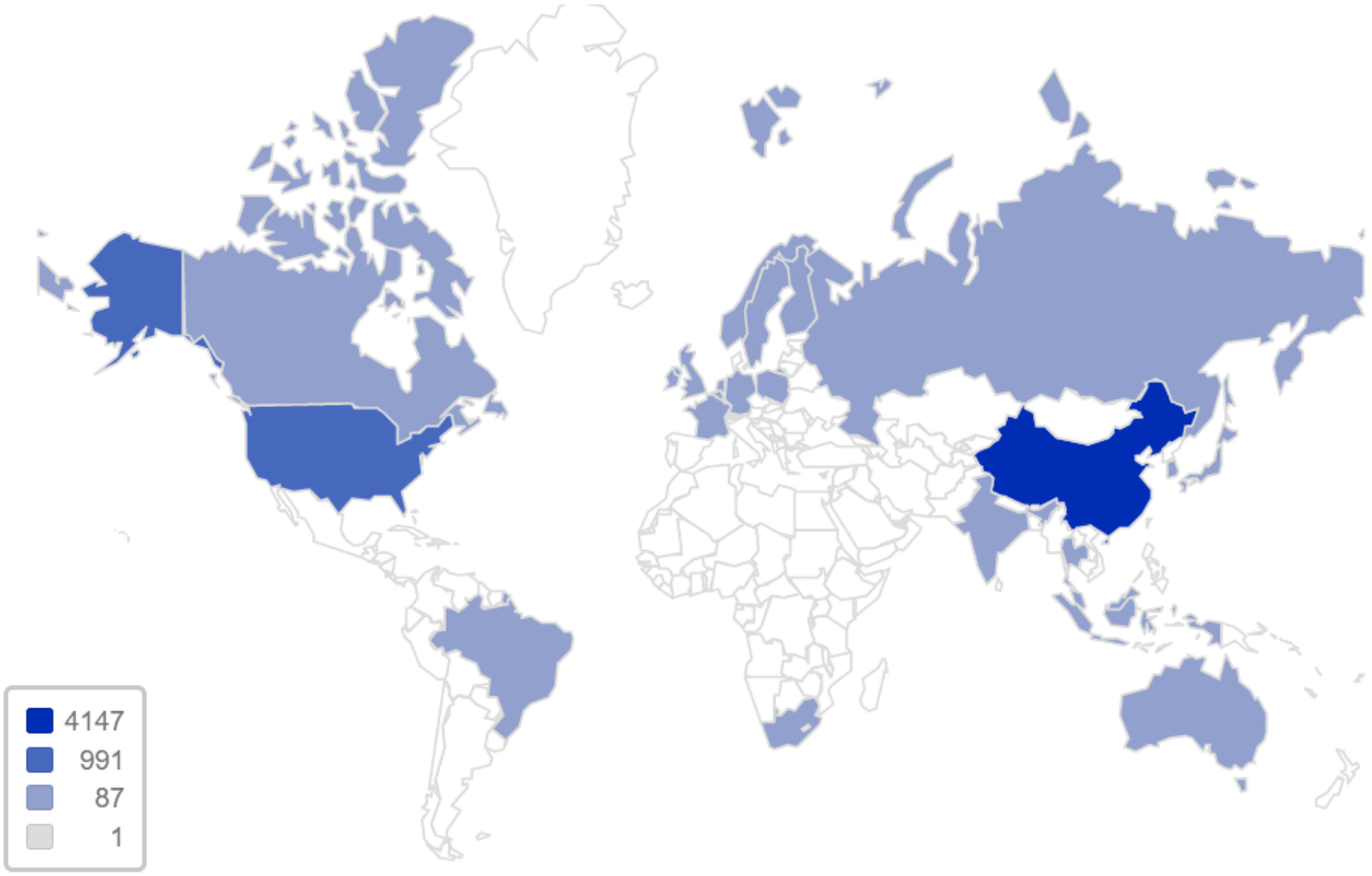
云服务器攻击源IP的时间趋势和空间分布

从时间趋势上看，在10月份的大多数时间里，蜜罐系统每天发现具有攻击行为的云服务器IP地址600~1000个，攻击会话数1万条左右。

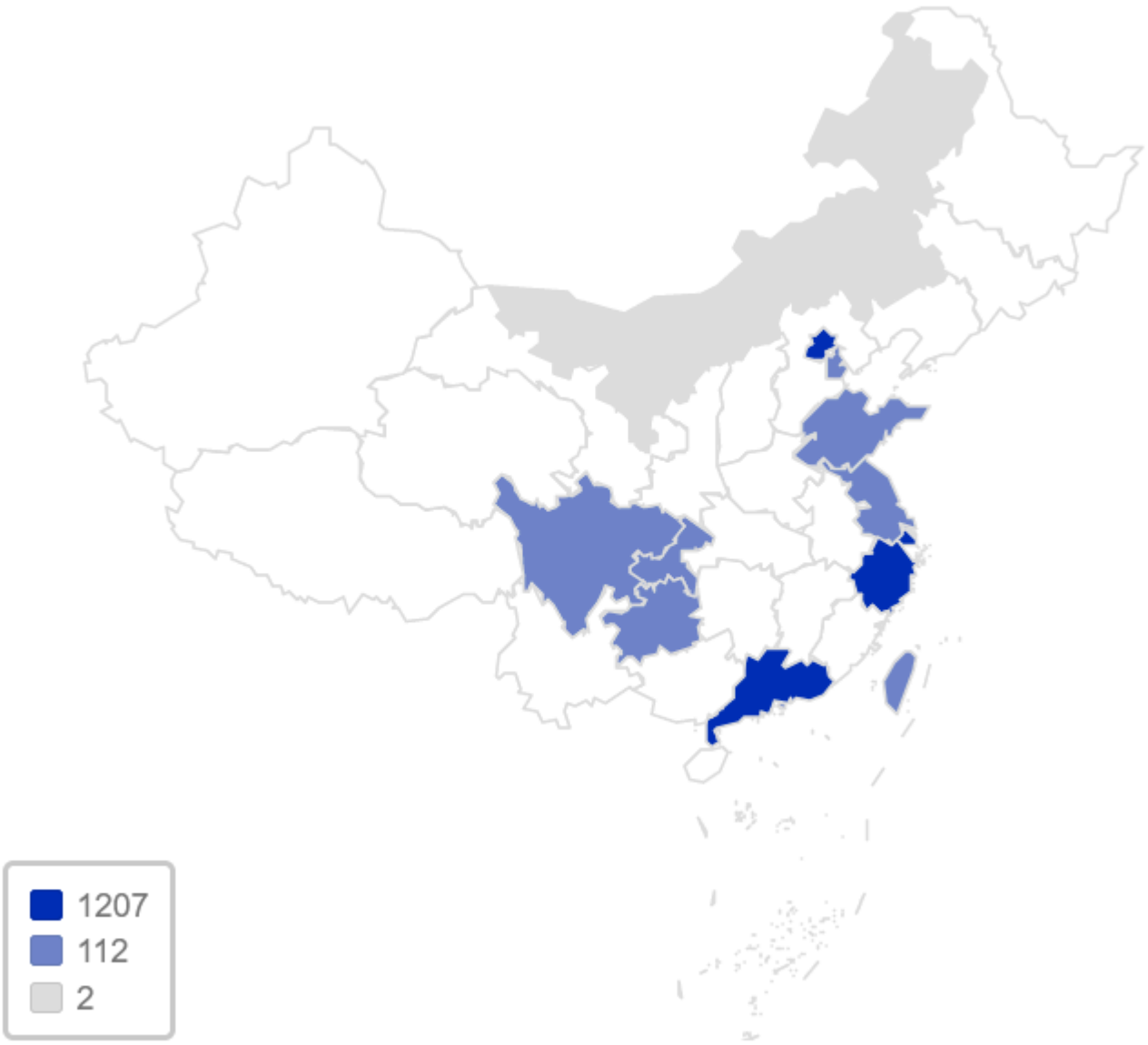
在10月14日、30日和31日，会话数出现了高于稳定范围的突增，其中IP地址为51.141.*.*的云服务器在多个端口利用MikroTik路由器设备的CVE-2018-14847漏洞进行攻击引起了10月14日会话数的突增，IP地址为143.198.*.*的云服务器发起的Telnet暴力破解引起了10月30日和31日的会话数的突增。



从地理位置上看，云服务器攻击源IP在亚洲、欧洲和北美洲较多，而在非洲、南美洲较少。中国和美国是攻击源IP数量最多的两个国家。



位于中国的云服务器攻击源IP分布在华北地区、东南沿海地区和西南地区，集中在北京、上海、广东、浙江等互联网和云计算行业较为发达的地区。



3 云服务器上的恶意行为

使用云产品进行攻击

使用云产品进行的攻击行为类型包括DDoS攻击、WEB攻击、密码爆破攻击，传播木马病毒、僵尸网络的C2服务器等。

在密码爆破攻击方面，10月份我们共监测到**854**个云服务器源IP发起了约**25.7**万次的密码爆破攻击，其中对Telnet协议的爆破攻击最为常见。

下表提供了10月份爆破攻击次数最多的10个云服务器的IP地址。

IP地址	协议/端口	次数
143.198.*.*	Telnet/TCP23	80,714
35.204.*.*	Telnet/TCP23, TCP2323	19,466
137.184. *.*	Telnet/TCP23, TCP2323	16,709
161.35. *.*	Telnet/TCP23	7,461
139.162. *.*	Telnet/TCP23, TCP2323	7,340
192.81. *.*	Telnet/TCP23, TCP2323	5,138
167.99. *.*	Telnet/TCP23	5,123
143.198. *.*	Telnet/TCP23, TCP2323	4,633
174.138. *.*	Telnet/TCP23, TCP2323	4,553
137.184. *.*	Telnet/TCP23, TCP2323	3,807

此外，我们发现一个IP地址为**47.92.*.***的云服务器在10月份发起了306次FTP爆破攻击。我们还发现该服务器上架设了一个网站，所有者是**某市供排水总公司**。我们对该案例进行了详细分析，具体内容请见第4节。

在传播木马病毒、僵尸网络等恶意程序方面，10月份我们共监测到**3324**个云计算IP地址传播了**157种恶意软件约88.2万次**。

云服务器攻击者最流行的恶意软件家族类型包括了木马下载器（TrojanDownloader）、恶意挖矿软件（CoinMiner）、Tsunami僵尸网络程序等。在整个10月份，有近3000个云服务器IP发起了近27万次会话以传播恶意挖矿软件。恶意挖矿软件已经成为当前云服务器恶意软件中最主要突出的问题。

下表是传播恶意软件最活跃的10个IP。

IP地址	传播次数	恶意软件家族
152.136. *.*	22,986	5
81.70. *.*	18,495	4
101.35. *.*	13,444	6
180.76. *.*	12,336	5
42.193. *.*	11,948	4
106.12. *.*	11,432	4
118.195.*.*	9,934	4
121.4. *.*	8,482	6
118.195. *.*	8,293	4
106.13. *.*	7,543	4

下表是传播恶意软件家族种类最为广泛的10个IP。IP传播的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	传播次数	恶意软件家族
47.103. *.*	1,246	12
82.156*.*	194	12
39.99. *.*	160	12
82.157. *.*	703	12
1.15. *.*	544	11
1.13. *.*	105	11
35.225. *.*	756	10
52.131. *.*	2,946	10
81.70. *.*	764	10
101.34. *.*	780	10

下面是恶意软件的下载URL中提取的下载服务器的IP/域名，建议屏蔽：

域名/IP地址	源IP数量	恶意软件家族	下载次数
oracle.zzhreceive.top	1,782	9	263,116
112.253.11.38	1,415	1	28,160
194.87.139.103	772	3	52,833
45.133.203.192	735	3	42,745
py2web.store	691	1	20,528
crypto.htxreceive.top	202	5	238,266
194.145.227.21	64	1	143
199.19.226.117	36	1	434
185.243.56.167	27	3	1,240
45.9.148.37	24	4	239

卸载云主机安全产品

主流的云厂商在提供云服务的同时提供配套的免费或收费的主机安全产品。在开始进攻其他云服务器时，黑客通常首先会尝试卸载目标主机上预装的安全产品，以避免后续攻击过程被发现和阻止。

以下是发送卸载云主机安全产品的恶意软件次数最多的10个IP。

IP地址	恶意软件家族	传播次数
121.4. *.*	28	6,912
101.35*.*	29	6,624
106.12. *.*	25	5,841
52.131. *.*	40	5,309
1.117. *.*	21	4,588
180.76. *.*	21	4,222
101.35. *.*	22	4,123
106.13. *.*	23	3,910
49.232. *.*	24	3,778
1.15. *.*	23	3,618

执行卸载主机安全产品行为的软件和脚本主要通过以下这些IP/域名下载。

域名/IP地址	源IP数量	下载次数	恶意软件数
oracle.zzhreceive.top	1,136	181,556	74
112.253.11.38	1,128	19,307	7
45.133.203.192	869	136,761	114
py2web.store	769	45,032	8
194.87.139.103	763	110,061	10
194.145.227.21	168	727	18
103.209.103.16	13	116	11
154.66.240.59	8	3,537	8
86.105.195.120	3	416	10

这些恶意软件的下载服务器主要分布在欧洲和美国。

漏洞的扫描和攻击

大多数云服务器攻击者倾向于使用热门应用程序的旧漏洞。我们发现，排除掉暴力破解后，云服务器攻击者最喜欢使用Redis漏洞。此外，NVR、DVR、网络摄像头等安防设备和路由器设备的漏洞也是云服务器漏洞攻击的主要目标。

被云服务器攻击者攻击最多的程序是Redis，其他包括MikroTik、GoAhead、DLink、ATLASSIAN等厂商的设备和程序也是主要的被攻击目标。

以下是利用的漏洞种类最多的10个IP。

IP地址	攻击次数	漏洞数量
193.122.*.*	68,021	20
188.166. *.*	25	9
139.59. *.*	45	9
128.199. *.*	36	9
47.245. *.*	41	9
130.61. *.*	14	8
139.224. *.*	21	8
140.238. *.*	23	8
121.37. *.*	8	7
124.70. *.*	7	7

4 案例分析

在对云服务器密码爆破攻击行为的分析中，一个IP地址为**47.92.*.***的云主机引起了我们的兴趣。其特点包括：该IP地址同时提供了**某市供排水公司**官网服务；该IP地址对外发起了大量攻击；该IP地址可能存在公民信息泄漏隐患。

该网站可能存储了大量的公民个人身份信息和水费账户信息。考虑到黑客入侵后可能获得了系统全部权限，上述公民信息有泄漏隐患。

这个IP在10月份有2天较为活跃，分别是在10月1日和28日，活跃时间主要在北京时间晚上20~24点（图中为UTC时间，北京时间需要+8小时）。

该IP主要访问21和2121的FTP端口，以及一些接近60000的高端口，其中21和2121端口的Payload是FTP的控制命令，高端口的Payload是样本文件的数据。该IP在21和2121端口上进行FTP服务器弱密码爆破，爆破成功后在被动模式下通过接近60000的随机端口上传Photo.scr、AV.scr和Video.lnk三个文件。

以下是其中一条FTP暴力破解的控制Payload，可以看出从密码爆破到发送恶意文件的完整攻击过程：

USER admin
PASS 123qwe!@#
PWD
CWD /
PASV
STOR //Photo.scr
PASV
PASV
STOR //AV.scr
PASV
PASV
STOR //Video.lnk
PASV
TYPE A
PASV

5 防护建议

对上述典型案例中涉及的IP地址，我们建议其域名拥有者与平台提供者协商，同时雇佣第三方独立安全公司对其网站安全做全面审计。如有必要，可以考虑将公民隐私相关信息的存储位置，放置在更加远离公网访问界面的位置。

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。

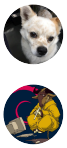
公有云网络安全威胁情报(202204)

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 →

Background On October 27, 2021, our Botmon system ided an attacker attacking Edgewater Networks' devices via CVE-2017-6079 with a relatively unique mount file system command in its payload, which had our attention, and after analysis, we confirmed that this was a brand new botnet, and based on it'



Nov 30, 2021 · 14 min read

Specter Botnet is 'taking over' Top Legit DNS Domains By Using ClouDNS Service

Abstract In order to reduce the possible impact of false positives, it is pretty common practice for security industry to whitelist the top Alexa domains such as www.google.com, www.apple.com, www.qq.com, www.alipay.com. And we have seen various machine learning detection models that bypass

Nov 18, 2021 · 6 min read