我国境内云网络安全态势报告

(2018 年 11-12 月)

国家计算机网络应急技术处理协调中心

2019 年 1 月

目 录

一、 引言

近年来，云作为互联网基础设施在我国迅速发展，越来越多的企业（包括初创企业、小型企业、甚至传统企业以及党政机关等）和业务场景向云端逐步迁移。在云服务使用过程中，云服务商和云用户对云的可用性和可靠性关注较多，但对云的安全性（即避免危害云的网络攻击）和可控性（即避免利用云发起网络攻击）关注较少。

在本报告中，CNCERT 从安全性和可控性两个方面对 20 家我国主流云服务提供商的境内云网络安全事件进行跟踪监测，并对境内云网络安全态势进行综合评估分析，帮助云服务商和云用户及时掌握当前的云网络安全状态，以便采取相应的安全防护措施。

根据 CNCERT 监测数据，2018 年 11-12 月，在安全性方面，虽然境内云 IP 感染木马或僵尸网络的概率较低，但是由于云上承载的服务越来越多、越来越重要，在其他攻击上境内云则成为攻击的重灾区；在可控性方面，大部分境内云的可控性差于境内平均水平，由于云服务获得的便捷性和低成本，越来越多黑客倾向于利用云主机进行网络攻击。因此，云服务商和云用户应加大对网络安全的重视和投入，分工协作构建网络安全纵深检测防御体系，保障云的安全性和可控性，共同维护网络空间安全。

二、 监测范围说明

本报告监测的 20 家我国主流云服务商包括：阿里云、中国电信、腾讯云、中国联通、世纪互联、亚马逊云、微软云、华为云、美团云、网宿科技、蓝汛、UCloud、网易云、京东云、百度云、中国移动、金山云、奇虎 360、首都在线、鹏博士。

报告监测范围覆盖了 20 家主流云服务商的境内公有云、私有云和混合云的云服务器、云数据库、云存储、云主机、CDN（Content Distribution Network，内容分发网络）以及 IDC（Internet Data Center，互联网数据中心）使用的公网 IP，如包括中国电信、中国联通、中国移动各省 IDC 使用的公网 IP。20 家主流云服务商境外云以及 IDC 使用的公网 IP 不在监测范围内。

本报告监测的 20 家我国主流云服务商的境内云使用的 IP 数 2600 余万个，占境内全部 IP 数的 7.7%。其中，阿里云、中国电信、腾讯云使用 IP 数位居前三，分别占比 46.3%、17.5%、12.8%，如图 2-1 所示。

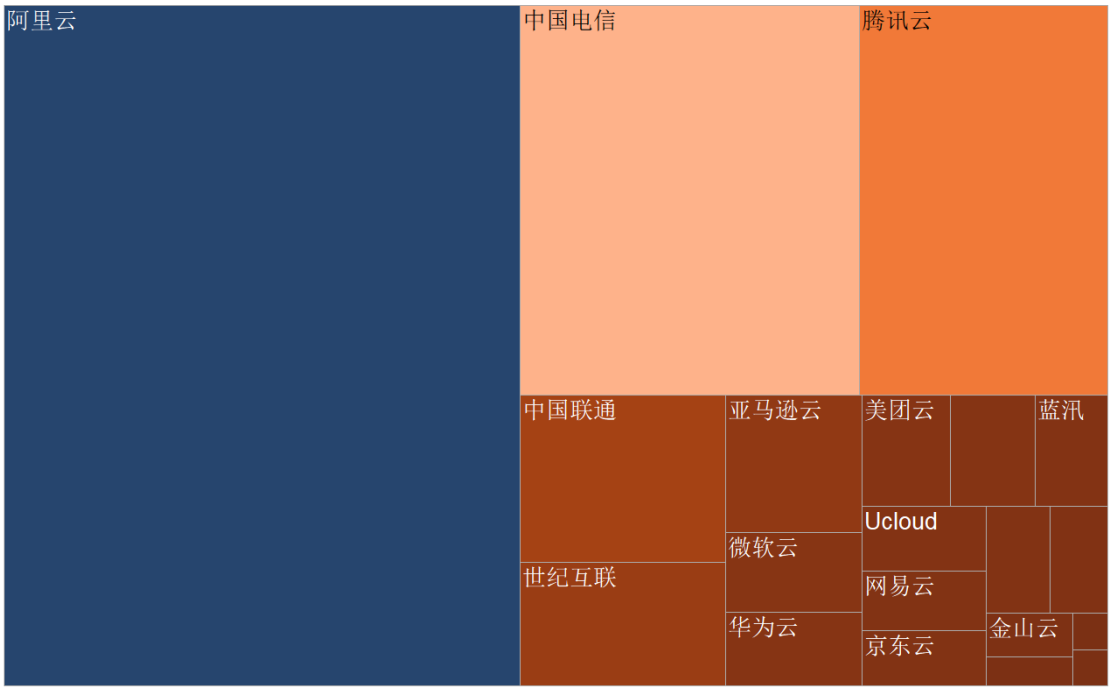

图 2-1 云服务商境内云使用 IP 数分布

三、 云安全性分析

本节对危害云的网络攻击事件进行监测和分析，监测事件包括针对云的 DDoS 攻击（Distributed Denial-of-Service attact，分布式拒绝服务攻击）、后门攻击、网页篡改、木马或僵尸网络感染等高危事件。

根据 CNCERT 监测数据，2018 年 11-12 月，20 家境内云遭受 DDoS 攻击次数占境内目标被攻击次数的 69.2%；被植入后门占境内被植入后门的 51.6%；被篡改网页占境内被篡改网页的 58.3%；受木马或僵尸网络控制的 IP 占境内全部受木马或僵尸网络控制的 IP 的 1.3%。而 20 家境内云使用的 IP 数仅占境内全部 IP 数的 7.7%。

虽然境内云 IP 感染木马或僵尸网络的概率较低，但是

在其他攻击上境内云则成为攻击的重灾区，其被攻击事件占境内被攻击事件比例相对较高。一方面因为云上承载服务越来越重要，使得针对云的攻击日益增多；另一方面相比传统企业，云用户对网络安全防护重视不够。

（一）DDoS 攻击分析

DDoS 攻击是指利用分布式的客户端，向服务提供者发送大量看似合法的请求，消耗或占用大量资源，从而使服务器无法处理合法的请求。在本报告中，一次 DDoS 攻击是指不同的攻击资源针对固定目标的单个 DDoS 攻击，攻击周期时长不超过 24 小时；如果相同的攻击目标被相同的攻击资源所攻击，但持续时间超过 24 小时或更多，则被认为是两次攻击。

根据 CNCERT 监测数据，2018 年 11-12 月，20 家境内云遭受 DDoS 攻击 27702 次，遭受攻击 IP 数 12049；全部境内目标被 DDoS 攻击 40047 次，遭受攻击 IP 数 18185；20 家境内云被攻击 IP 占境内被攻击 IP 的 66.3%，20 家境内云遭受攻击次数占境内目标被攻击次数的 69.2%。

遭受 DDoS 攻击次数较多的前五家云服务商分别是中国电信（39%）、阿里云（39%）、腾讯云（15%）、中国联通（3%）、百度云（2%），如图 3-1 所示。

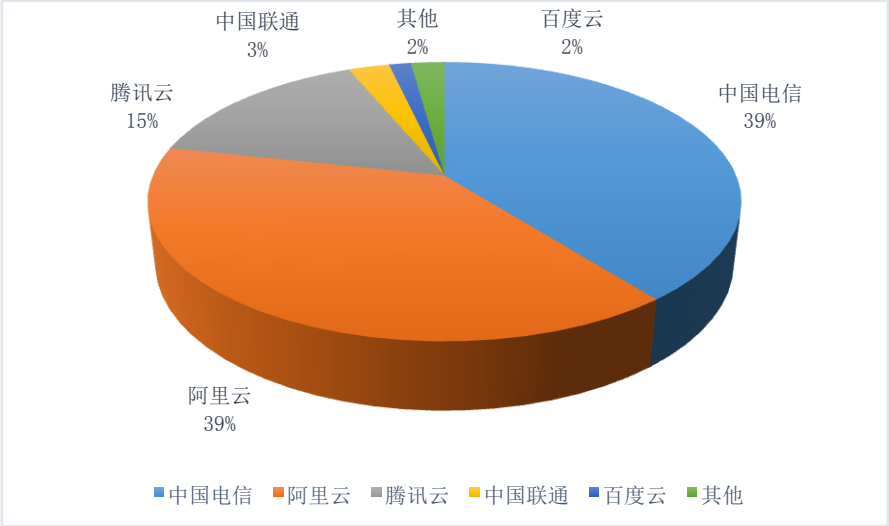

图 3-1 2018 年 11-12 月云服务商遭受 DDoS 攻击次数分布图

遭受 DDoS 攻击的 IP 分布如图 3-2 所示，其中中国电信的 IP 数最多，占比 37%，其次为阿里云 36%、腾讯云 18%、中国联通 3%、百度云 3%。

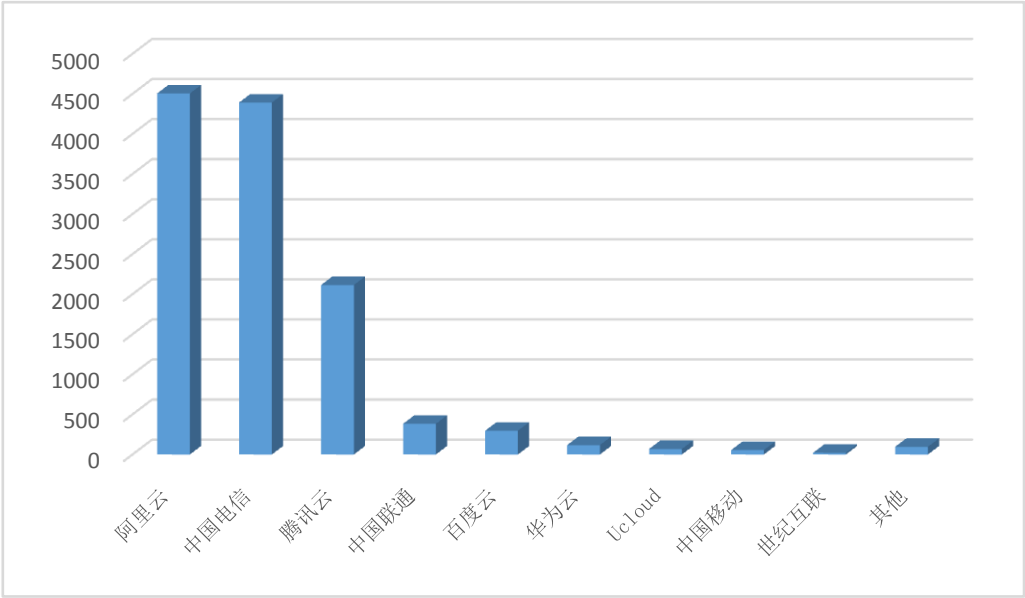

图 3-2 2018 年 11-12 月云服务商遭受 DDoS 攻击目标 IP 数分布图

被攻击最多的目标 IP 地址 TOP 20 列表如表 3-1 所示，前 20 个攻击目标 IP 均被持续攻击，前 3 个攻击目标 IP 被持续攻击了两个月。被攻击较多的前 20 个 IP 主要归属云服务商分别是中国电信（13 个）和阿里云（7 个）。

表 3-1 被攻击较多的目标 IP 地址 TOP 20

攻击目标 IP	攻击次数	归属省份	归属云服务商
47.X.X.90	61	北京	阿里云
144.X.X.181	61	青岛	中国电信
14.X.X.128	61	佛山	中国电信
183.X.X.2	58	东莞	中国电信
59.X.X.222	58	福州	中国电信
27.X.X.110	58	福州	中国电信
47.X.X.210	54	青岛	阿里云
183.X.X.66	53	佛山	中国电信
59.X.X.88	53	北京	阿里云
14.X.X.190	50	东莞	中国电信
183.X.X.142	50	东莞	中国电信
120.X.X.114	50	深圳	阿里云
39.X.X.43	49	北京	阿里云
122.X.X.178	46	金华	中国电信
47.X.X.117	46	上海	阿里云
14.X.X.61	43	东莞	中国电信
120.X.X.201	42	深圳	阿里云
125.X.X.117	42	佛山	中国电信
125.X.X.198	42	内江	中国电信
14.X.X.135	42	东莞	中国电信

（二）后门攻击分析

后门攻击是指黑客在网站的特定目录中上传远程控制页面，网站服务器被黑客通过该页面秘密远程控制。在本报告中，一次后门攻击是指云上服务器被植入一个新的网站后门，网站后门被更新修改则不认为是新的攻击。

根据 CNCERT 监测数据，2018 年 11-12 月，20 家境内云的 2541 个 IP 被植入网站后门 4676 个；境内共计 4673 个 IP 累计被植入网站后门 9056 个；20 家境内云被植入后门 IP 占境内被植入后门 IP 的 54.4%，20 家境内云被植入后门占境内被植入后门的 51.6%。

阿里云和中国电信被植入后门数较多，分别占 49%和 31%，其次是腾讯云 7%、百度云 3%、中国联通 2%、世纪互联 2%和鹏博士 2%，如图 3-3 所示。

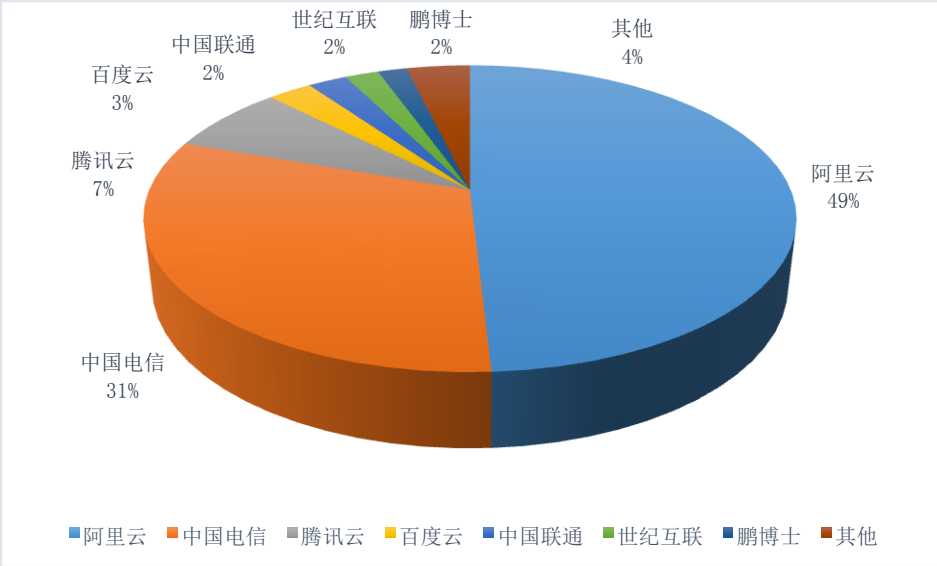

图 3-3 2018 年 11-12 月云服务商被植入网站后门数分布图

被植入网站后门的 IP 分布如图 3-4 所示，其中阿里云和中国电信的 IP 数较多，占比之和达到了 80%，分别为 52%和 28%，其次是腾讯云 7%，中国联通 3%。

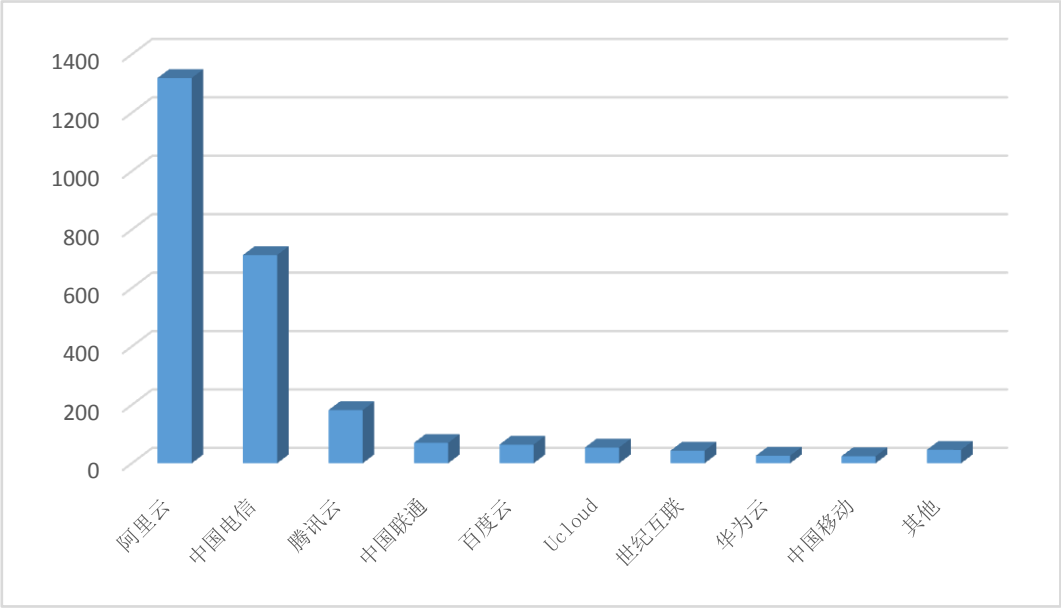

图 3-4 2018 年 11-12 月云服务商被放置后门 IP 数分布图

被植入网站后门的 IP 地址 TOP 20 列表如表 3-2 所示。云上 IP 被植入网站后门的数量分布差异较大，被植入网站后门数最多的一个 IP 来自阿里云，数量达到 140 个；其次是两个来自阿里云和一个来自鹏博士的 IP，被植入网站后门数量分别为 48、45 和 43 个；其余 IP 被植入网站后门数量均未超过 30 个。被植入网站后门较多的前 20 个 IP 主要归属云服务商分别是阿里云（9 个）和中国电信（7 个）、鹏博士（2 个）、百度云（1 个）、世纪互联（1 个）。

表 3-2 被放置网站后门的 IP 列表 TOP 20

攻击目标 IP	被植入网站后门数	归属省份	归属云服务商
47.X.X.31	140	山东	阿里云
118.X.X.214	48	浙江	阿里云
219.X.X.21	45	北京	鹏博士
39.X.X.195	43	广东	阿里云
120.X.X.50	29	广东	阿里云
119.X.X.44	25	广东	中国电信
118.X.X.104	22	四川	中国电信
219.X.X.108	22	北京	鹏博士
182.X.X.95	21	北京	阿里云
39.X.X.55	20	北京	阿里云
223.X.X.82	19	浙江	阿里云
139.X.X.235	17	上海	阿里云
119.X.X.184	17	湖北	中国电信
180.X.X.250	16	北京	百度云
61.X.X.117	15	四川	中国电信
118.X.X.73	15	四川	中国电信
120.X.X.186	14	北京	世纪互联
60.X.X.53	14	安徽	中国电信
118.X.X.78	14	浙江	阿里云
150.X.X.206	14	山东	中国电信

（三）网页篡改分析

网页篡改是指恶意破坏或更改网页内容，使网站无法正

常工作或出现黑客插入的非正常网页内容。在本报告中，一次网页篡改攻击是指黑客对一个网页的篡改，如果黑客多次修改同一网页则只被认为是一次攻击。

根据 CNCERT 监测数据，2018 年 11-12 月，20 家境内云 441 个网页遭到恶意篡改、遭受篡改的 IP 数达到 374 个；境内共计 757 个网页遭到恶意篡改、遭受篡改的 IP 数达到 610 个；20 家境内云被篡改 IP 占境内被篡改 IP 的 61.3%，20 家境内云被篡改网页占境内被篡改网页的 58.3%。

中国电信、阿里云和世纪互联被篡改网页数较多，分别占比 55%、29%、9%；其次是腾讯云、中国联通、百度云，均占比 2%，如图 3-5 所示。

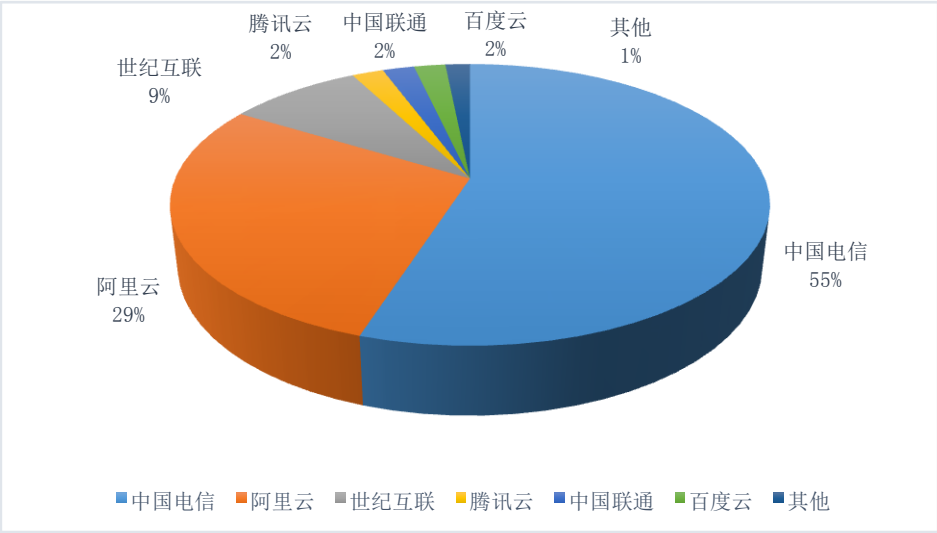

图 3-5 2018 年 11-12 月云服务商被篡改网页数分布图

被篡改网页的 IP 分布如图 3-6 所示，其中中国电信和阿里云被篡改网页 IP 数较多，占比之和超过了 80%，分别为 51%和 33%，其次是世纪互联 7%，中国联通 2%，百度云 2%，腾讯云 2%。

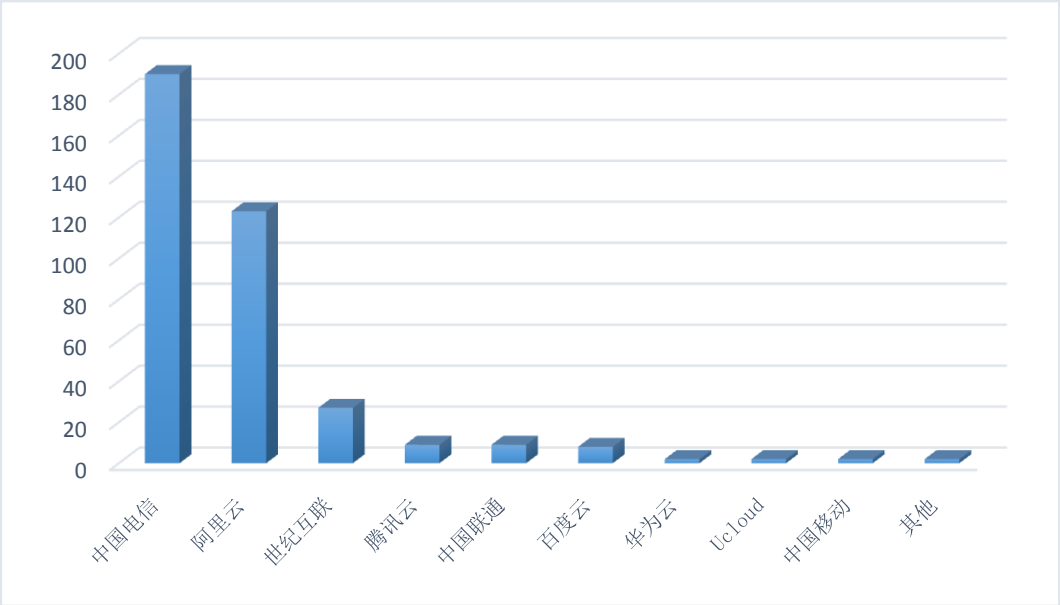

图 3-6 2018 年 11-12 月云服务商被篡改网页 IP 数分布图

被篡改网页的 IP 地址 TOP 20 列表如表 3-3 所示。云中网页被篡改较多的前 20 个 IP 中，每个 IP 被篡改网页数量分布相对稳定，被篡改网页数量在 2-7 次范围内。被篡改网页较多的前 20 个 IP 主要归属云服务商分别是中国电信（17 个）、世纪互联（3 个）。

表 3-3 被篡改网页的 IP 列表 TOP 20

攻击目标 IP	被篡改网页数	归属省份	归属云服务商
222.X.X.86	7	上海	中国电信
58.X.X.210	6	江苏	中国电信
120.X.X.158	6	北京	世纪互联
221.X.X.113	6	天津	中国电信
120.X.X.46	5	北京	世纪互联
219.X.X.158	5	河北	中国电信
36.X.X.5	5	陕西	中国电信
221.X.X.111	3	天津	中国电信
120.X.X.196	3	北京	世纪互联
117.X.X.239	3	陕西	中国电信
61.X.X.125	3	上海	中国电信
61.X.X.91	3	上海	中国电信
61.X.X.31	3	江苏	中国电信
125.X.X.19	2	陕西	中国电信
125.X.X.202	2	福建	中国电信

115.X.X.215	2	浙江	中国电信
122.X.X.66	2	浙江	中国电信
183.X.X.237	2	广东	中国电信
115.X.X.120	2	浙江	中国电信
122.X.X.141	2	浙江	中国电信

（四）木马或僵尸网络受控事件分析

木马是指由攻击者安装在受害者计算机上秘密运行并用于窃取信息及远程控制的程序。僵尸网络是指由攻击者通过控制服务器控制的受害计算机群。木马和僵尸网络对网络信息安全造成危害和威胁，是造成个人隐私泄露、失泄密、垃圾邮件和大规模拒绝服务攻击的重要原因。木马或僵尸网络受控事件是指用户计算机被植入僵尸木马程序被恶意远程控制。在本报告中，一起木马或僵尸网络事件是指云上主机被植入僵尸木马程序后被恶意远程控制，远程控制端的变化则不被认为是新的事件。

根据 CNCERT 监测数据，2018 年 11-12 月，20 家境内云的 16412 个 IP 对应主机被木马或僵尸程序控制，全部境内受木马或僵尸程序控制的 IP 达到 1227213 个，20 家境内云受控 IP 占境内受控 IP 的 1.3%。

受控 IP 数较多的前五家云服务商分别是中国电信（35%）、腾讯云（27%）、阿里云（20%）、中国联通（6%）、UCloud（3%），如图 3-7 所示。

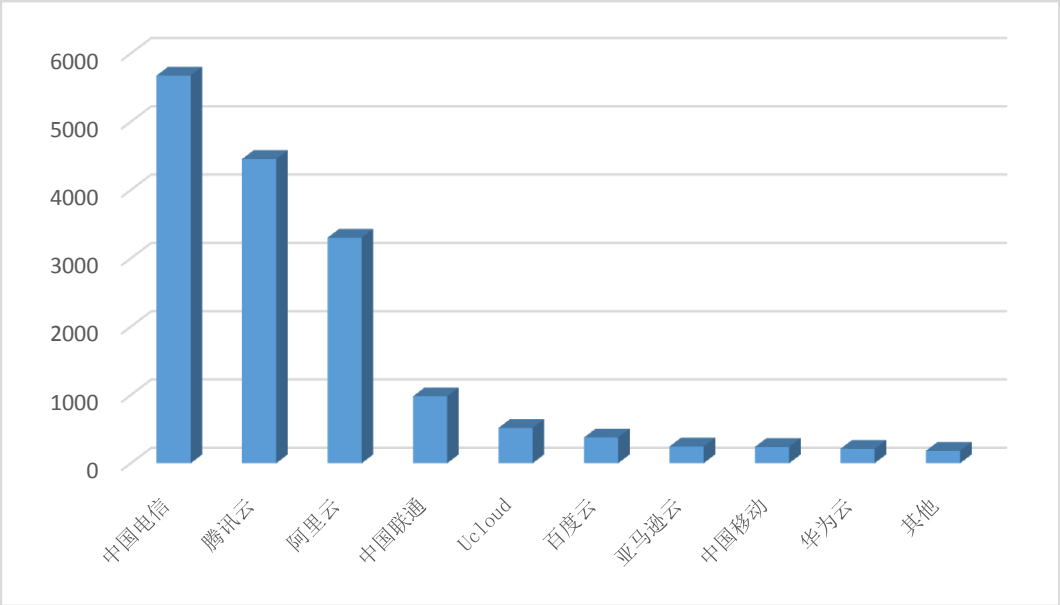

图 3-7 2018 年 11-12 月云服务商受控 IP 数分布图

云主机通常 24 小时在线，可持续接受控制端命令，受控危害更大。连接控制端次数较多的受控 IP 地址 TOP 20 如表 3-4 所示。TOP 20 列表中的每个 IP 与控制端通信次数十分频繁，次数达到 10^6~10^7 级别。连接控制端次数较多的 TOP 20 受控 IP 主要归属云服务商分别是腾讯云（10 个）、阿里云（7 个）、中国联通（2 个）、中国电信（1 个）。

表 3-4 连接控制端次数最多的 IP 地址 TOP 20

受控 IP	与控制端通信次数	归属省份	归属云服务商
193. X. X. 113	6589378	广东	腾讯云
193. X. X. 86	5411809	广东	腾讯云
120. X. X. 78	3385348	广东	阿里云
61. X. X. 170	2640902	北京	中国联通
123. X. X. 169	2317076	广东	腾讯云
121. X. X. 94	2146154	浙江	阿里云
112. X. X. 180	1928515	广东	阿里云
121. X. X. 43	1903425	浙江	阿里云
134. X. X. 145	1874993	广东	腾讯云
118. X. X. 147	1608751	四川	腾讯云
203. X. X. 39	1497317	广东	腾讯云
120. X. X. 172	1489373	浙江	阿里云
132. X. X. 139	1396679	四川	腾讯云

120.X.X.130	1369240	广东	阿里云
101.X.X.227	1352280	浙江	中国联通
134.X.X.239	1166188	广东	腾讯云
139.X.X.13	1011418	上海	阿里云
58.X.X.50	951975	江苏	中国电信
118.X.X.18	870766	上海	腾讯云
129.X.X.184	854505	四川	腾讯云

四、 云可控性分析

本节对利用云发起网络攻击的事件进行监测和分析，监测事件包括利用云发起或参与的 DDoS 攻击、植入网站后门、网页挂马、控制木马或僵尸程序等高危事件。

根据 CNCERT 监测数据，2018 年 11-12 月，黑客利用 20 家境内云 IP 参与了 80.1%针对境内目标的 DDoS 攻击；对外植入网站后门数占境内 IP 对外植入网站后门数的 39.4%；承载恶意代码种类占境内网站承载恶意代码种类的 53.7%；木马或僵尸网络控制端 IP 控制的肉鸡 IP 数占境内控制端 IP 控制的肉鸡 IP 数的 59%。

越来越多黑客利用云主机作为跳板机或控制端进行网络攻击，一方面是因为云服务使用便捷性、可靠性、低成本、高带宽、高性能，另一方面是因为云网络流量复杂便于黑客隐藏真实身份。因此，云服务商和云用户除了应加强自身安全防护体系建设外，应加强内部审计以避免云被用于对外发起攻击。

（一）发起或参与 DDoS 攻击分析

利用云发起 DDoS 攻击是指利用云主机作为 DDoS 僵尸网络或 DDoS 攻击平台的控制服务器，直接控制肉鸡或发包机发起网络攻击；利用云参与 DDoS 攻击是指利用云主机作为肉鸡或发包机，受控对外打出直接攻击流量、反射攻击发起流量，因为云主机可具有高性能和高带宽，如果借助反射放大攻击方式，单机就可轻松发动峰值超 1Gbps 的流量。本报告中，多个控制端被用于针对相同目标的 DDoS 攻击，被认为发起一次 DDoS 攻击；多个肉鸡被用于针对相同目标的 DDoS 攻击，被认为参与一次 DDoS 攻击。虽然当前越来越多的黑客为了隐匿身份、躲避溯源等原因，选择将攻击控制端部署在境外，但仍有不少控制端部署于境内。

根据 CNCERT 监测数据，2018 年 11-12 月，黑客利用 20 家境内云的 11688 个 IP 作为攻击控制端或肉鸡对 13715 个境内攻击目标 IP 进行 DDoS 攻击 32058 次；全部境内 18185 个攻击目标被 DDoS 攻击 40047 次；黑客利用 20 家境内云 IP 参与对境内 75.4%攻击目标 IP 的 DDoS 攻击，参与对境内目标 80.1%的 DDoS 攻击。

20 家境内云的 392 个 IP 作为攻击控制端对 2610 个境内攻击目标 IP 发起 DDoS 攻击 5543 次。作为控制端发起攻击较多的两家云服务商分别为中国电信和阿里云，中国电信占比 61%，阿里云占比 26%，明显高于其他厂商，如图 4-1 所

示。

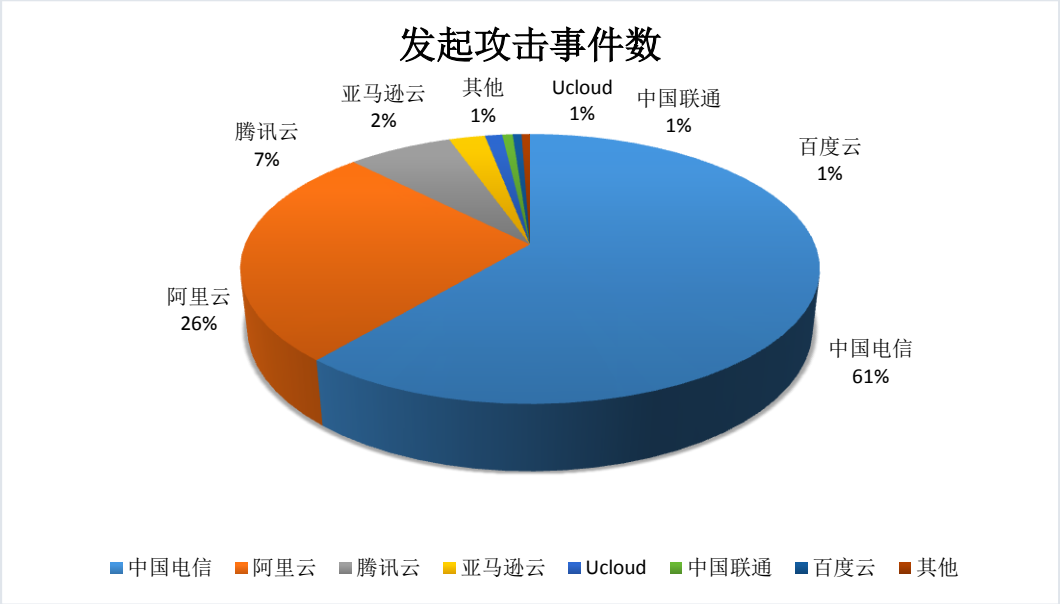

图 4-1 2018 年 11-12 月云服务商发起攻击事件数分布图

发起 DDoS 攻击的控制端 IP 分布如图 4-2 所示，发起攻击的控制 IP 数较多的前五家分别是：中国电信 43%、阿里云 19%、腾讯云 14%、UCloud 12%及中国联通 7%。

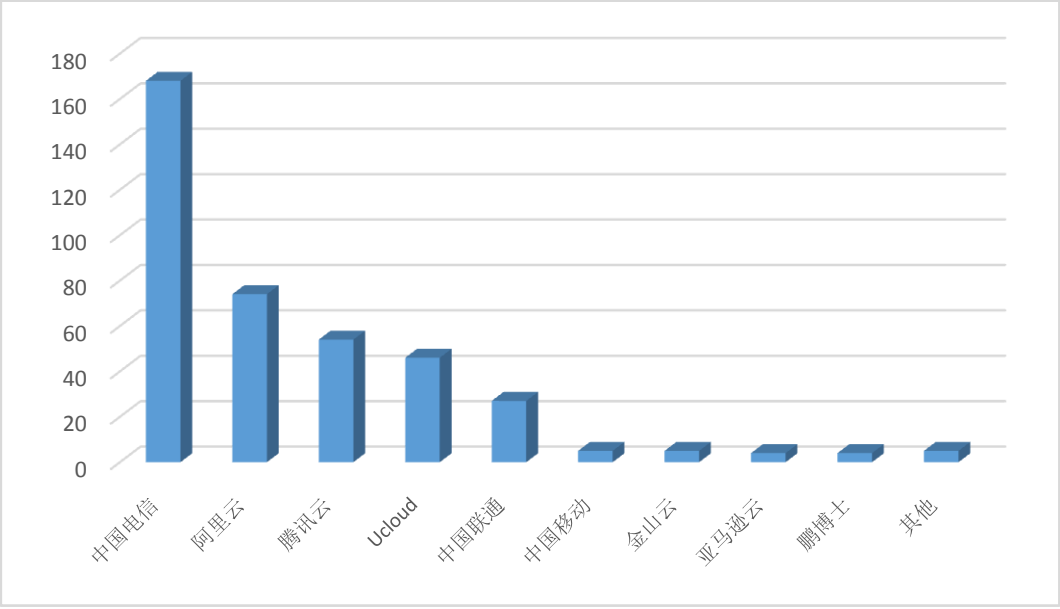

图 4-2 2018 年 11-12 月云服务商攻击控制端 IP 数分布图

发起 DDoS 攻击较多的控制端 IP 地址 TOP 20 列表如表 4-2 所示，发起 DDoS 攻击较多的 IP 为来自中国电信的一个位

于广东的 IP，其攻击次数为 3010 次，平均每天发起攻击超过 50 次。日均攻击次数超过 2 起的控制端 IP 有 16 个。发起 DDoS 攻击较多的控制端 IP 所归属的云服务商分别为中国电信（12 个）、阿里云（6 个）、腾讯云（2 个）。

表 4-1 发起 DDoS 攻击较多的控制端 IP 地址 TOP 20

控制端 IP	DDoS 攻击次数	归属省份	归属云服务商
183.X.X.24	3010	广东	中国电信
47.X.X.112	1987	上海	阿里云
59.X.X.88	1655	北京	阿里云
47.X.X.210	1206	山东	阿里云
58.X.X.241	731	江苏	中国电信
120.X.X.114	437	广东	阿里云
27.X.X.234	409	福建	中国电信
222.X.X.16	181	江苏	中国电信
183.X.X.57	172	广东	中国电信
116.X.X.5	165	湖北	中国电信
119.X.X.162	164	广东	中国电信
222.X.X.7	150	江苏	中国电信
221.X.X.64	144	江苏	中国电信
61.X.X.154	142	江苏	中国电信
58.X.X.8	133	江苏	中国电信
150.X.X.205	120	山东	中国电信
121.X.X.62	119	浙江	阿里云
119.X.X.225	109	四川	腾讯云
47.X.X.99	103	山东	阿里云
94.X.X.146	93	重庆	腾讯云

因为云主机的高性能、高带宽以及 24 小时在线的特点，境内云主机被大量利用参与 DDoS 攻击。20 家境内云的 11296 个 IP 作为肉鸡对 12139 个境内攻击目标 IP 进行 DDoS 攻击 28348 次。中国电信、阿里云、中国联通、腾讯云、百度云参与攻击次数较高，均超过了 20000 次，如图 4-3。

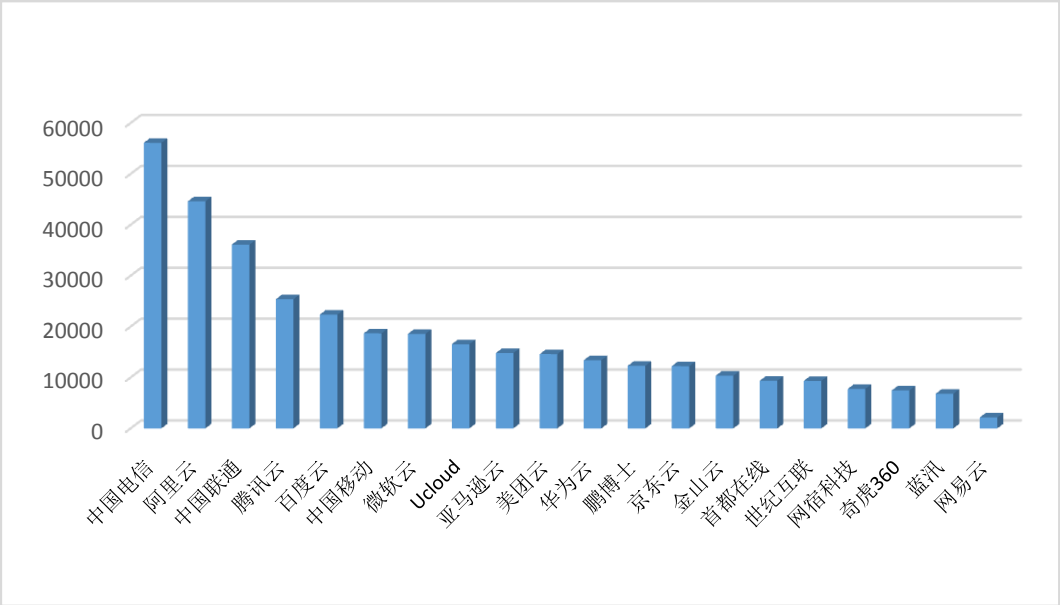

图 4-3 2018 年 11-12 月云服务商参与攻击事件数分布图

参与攻击的肉鸡 IP 分布如图 4-4 所示，数量较多的前三家云服务商为腾讯云 44%、中国电信 22%及阿里云 16%。腾讯云参与攻击肉鸡 IP 数量最多，远高于排在第二位中国电信。

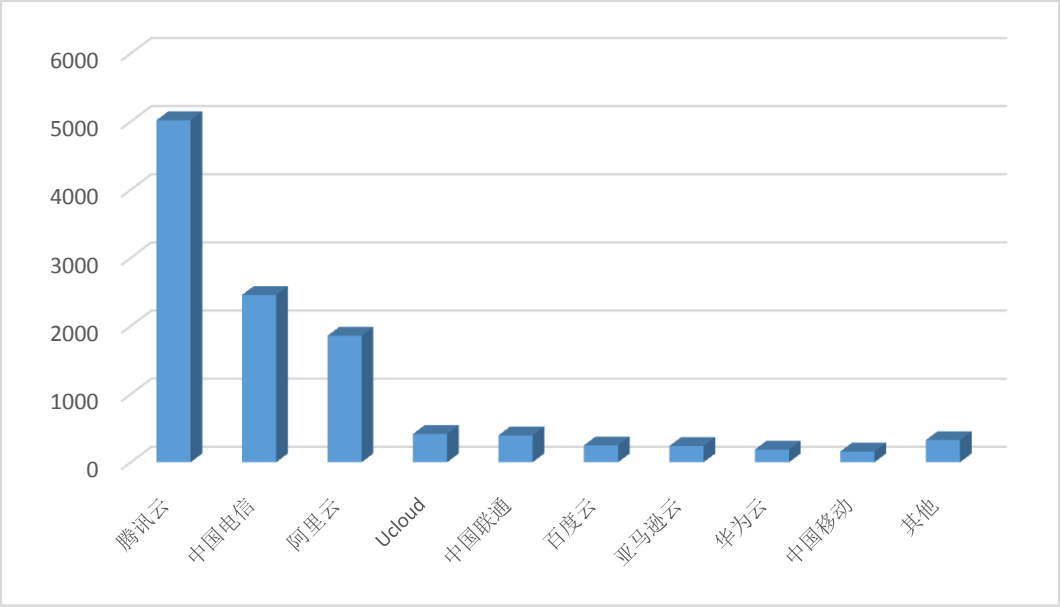

图 4-4 2018 年 11-12 月云服务商控制参与攻击肉鸡 IP 数分布图

参与 DDoS 攻击较多的肉鸡 IP 地址 TOP 20 列表如表 4-2 所示，TOP 20 中攻击次数在 20000 以上的有 4 个 IP，所属

的云服务商均为阿里云。参与 DDoS 攻击较多的 TOP 20 肉鸡 IP 所属云服务商包括腾讯云（10 个）、中国电信（3 个）、阿里云（5 个）、微软云（1 个）、亚马逊云（1 个）。

表 4-2 参与 DDoS 攻击较多的肉鸡 IP 地址 TOP 20

肉鸡 IP	DDoS 攻击次数	归属省份	归属云服务商
39.X.X.75	26070	广东	阿里云
139.X.X.13	23879	上海	阿里云
47.X.X.208	23440	浙江	阿里云
39.X.X.100	20976	北京	阿里云
36.X.X.67	15504	北京	中国电信
36.X.X.66	13802	北京	中国电信
42.X.X.38	12570	上海	微软云
123.X.X.13	11460	广东	腾讯云
118.X.X.126	11400	四川	腾讯云
52.X.X.31	11309	宁夏	亚马逊云
59.X.X.150	11227	广东	中国电信
118.X.X.180	11208	上海	腾讯云
122.X.X.17	11116	广东	腾讯云
118.X.X.184	11085	重庆	腾讯云
120.X.X.250	11023	浙江	阿里云
188.X.X.116	10979	天津	腾讯云
154.X.X.84	10894	北京	腾讯云
140.X.X.182	10876	北京	腾讯云
58.X.X.45	10868	北京	腾讯云
139.X.X.249	10865	天津	腾讯云

（二）发起后门攻击分析

利用云发起后门攻击是指利用云主机作为直接攻击机向外植入网站后门。

根据 CNCERT 监测数据，2018 年 11-12 月，黑客利用 20 家境内云的 1377 个 IP 对外植入 4298 个网站后门；利用全部境内 6179 个 IP 对外植入网站后门 10917 个；20 家境内云攻击 IP 占境内攻击 IP 的 22.3%，20 家境内云植入网站后门

数占境内 IP 植入网站后门数的 39.4%。

中国电信、阿里云、网宿科技被利用对外植入网站后门数较高，分别占比 33%、20%和 17%，如图 4-5 所示。

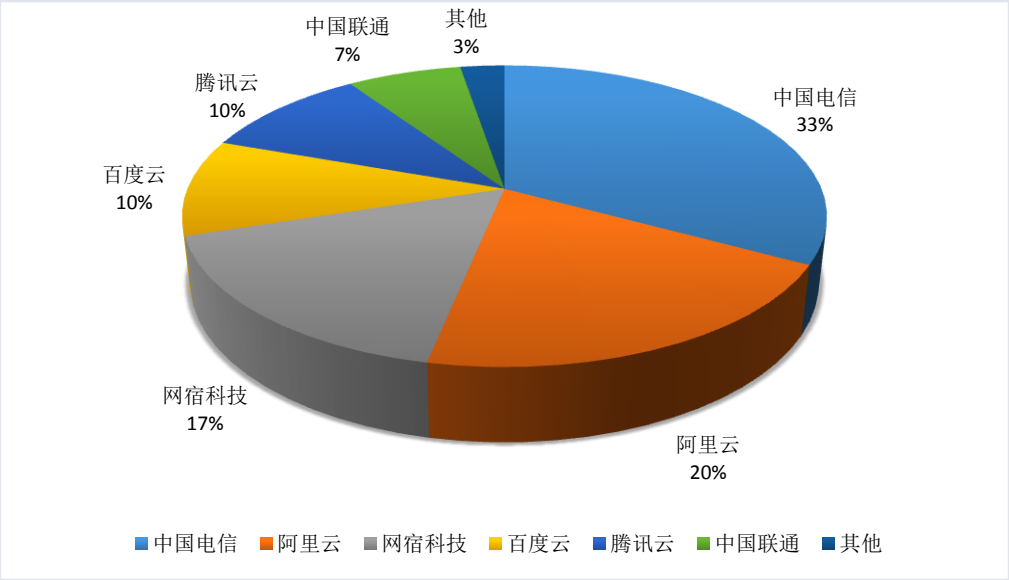

图 4-5 2018 年 11-12 月云服务商植入网站后门数分布图

对外植入网站后门的 IP 分布如图 4-6 所示，植入网站后门 IP 数较多的前五家服务商中，中国电信和网宿科技所占的比例均为 29%，随后是阿里云和腾讯云均占比 15%，中国联通 7%。

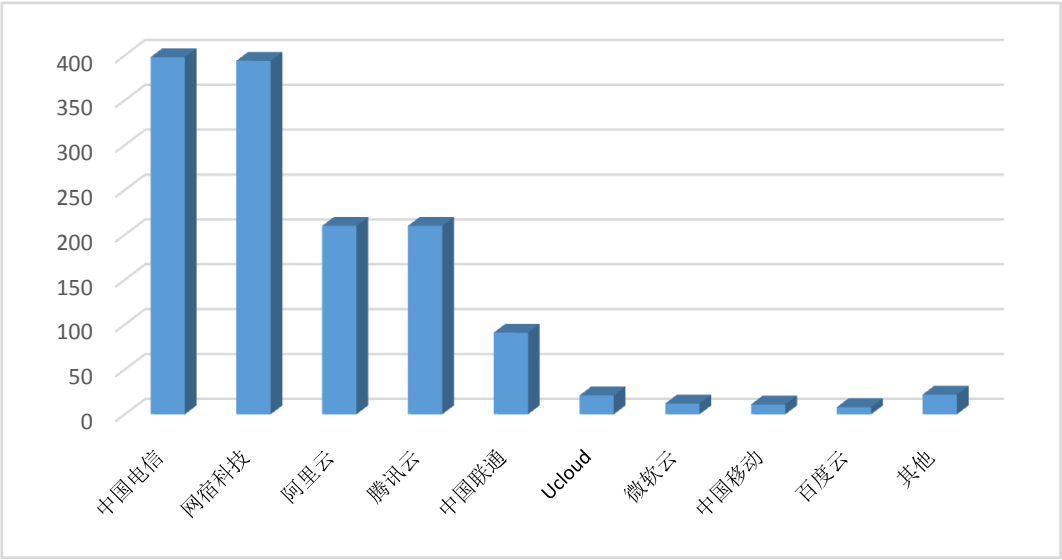

图 4-6 2018 年 11-12 月云服务商植入网站后门 IP 数分布图

对外植入网站后门较多的 IP 地址 TOP 20 列表如表 4-3 所示。植入网站后门数较多的四个 IP 均来自阿里云，植入网站后门数量均达到 600 个以上，分别为：655 个、644 个、641 个和 608 个。对外植入网站后门较多的前 20 个 IP 主要归属云服务商分别是阿里云（11 个）、中国电信（7 个）、百度云（2 个）。

表 4-3 放置网站后门的 IP 列表 TOP 20

攻击 IP	植入网站后门数	归属省份	归属云服务商
116.X.X.89	655	浙江	阿里云
120.X.X.189	644	浙江	阿里云
120.X.X.127	641	浙江	阿里云
115.X.X.234	608	山东	阿里云
61.X.X.252	596	江苏	中国电信
114.X.X.183	591	浙江	阿里云
115.X.X.214	589	山东	阿里云
114.X.X.24	526	上海	中国电信
101.X.X.1	526	北京	阿里云
58.X.X.163	497	江苏	中国电信
123.X.X.250	492	北京	阿里云
115.X.X.23	482	山东	阿里云
180.X.X.16	458	北京	百度云
180.X.X.64	440	北京	百度云
61.X.X.159	438	上海	中国电信
112.X.X.6	413	北京	阿里云
61.X.X.145	295	上海	中国电信
61.X.X.240	223	江苏	中国电信
120.X.X.140	216	广东	阿里云
60.X.X.86	210	浙江	中国电信

（三）网站放马分析

网站放马是指在网站中植入恶意代码，用户访问该网站后感染恶意代码从而达到运行具有入侵性或破坏性的程序、破坏被感染电脑数据的安全性和完整性的目的。在本报告中，

网站放马是指云上网站承载了恶意代码。

根据 CNCERT 监测数据，2018 年 11-12 月，20 家境内云的 3499 个 IP 被用于承载放马网站，承载放马网站数 40810 个，承载了 1312 种恶意代码；境内共计 15168 个 IP 被用于承载放马网站，承载放马网站数 182879 个，承载了 2444 种恶意代码；20 家境内云放马网站 IP 占境内放马网站 IP 的 23.1%，20 家境内云承载放马网站占境内承载放马网站的 22.3%；20 家境内云承载恶意代码种类占境内网站承载恶意代码种类的 53.7%。

放马网站分布如图 4-7，中国电信以 70%的比重占据最高比例，阿里云、中国联通放马网站数在总体中的比重分别为 17%和 10%。

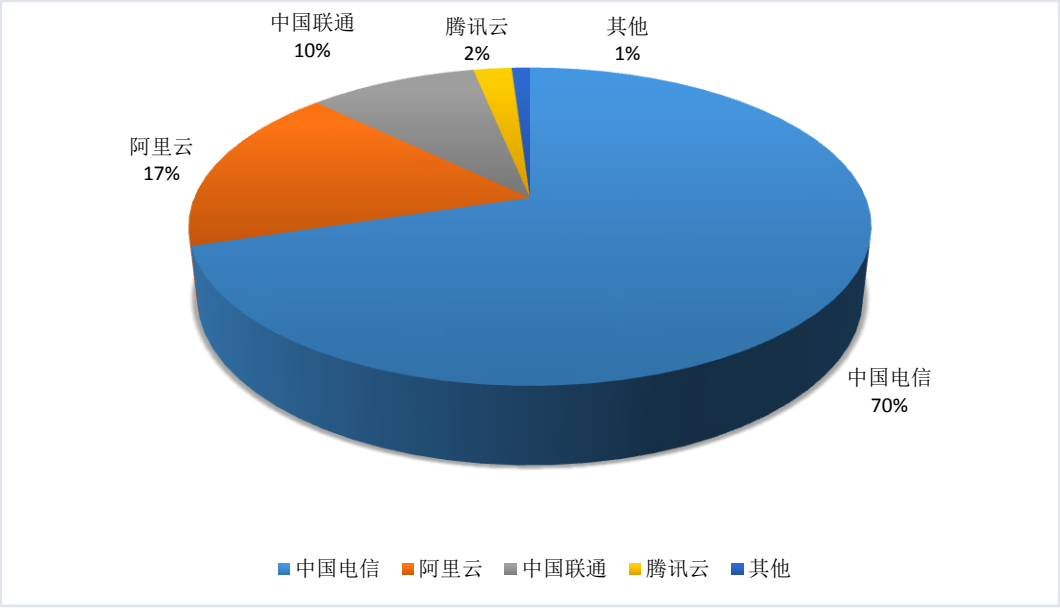

图 4-7 2018 年 11-12 月云服务商放马网站数分布图

放马网站的 IP 分布如图 4-8 所示，中国电信所占的比

例也最大为 62%，其次是中国联通 16%、阿里云 12%。

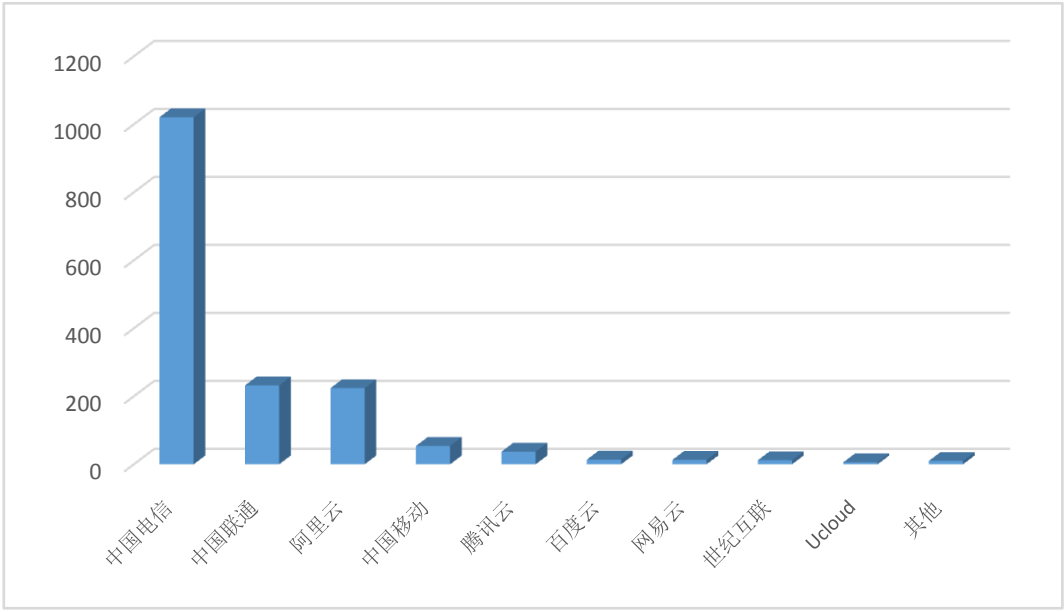

图 4-8 2018 年 11-12 月云服务商放马 IP 数分布图

放置恶意代码种类分布如图 4-9 所示，放置恶意代码种类较多的云服务商分别为中国电信、阿里云和中国联通，其放置恶意代码的种类所占比例分别为 51%、15%和 13%。

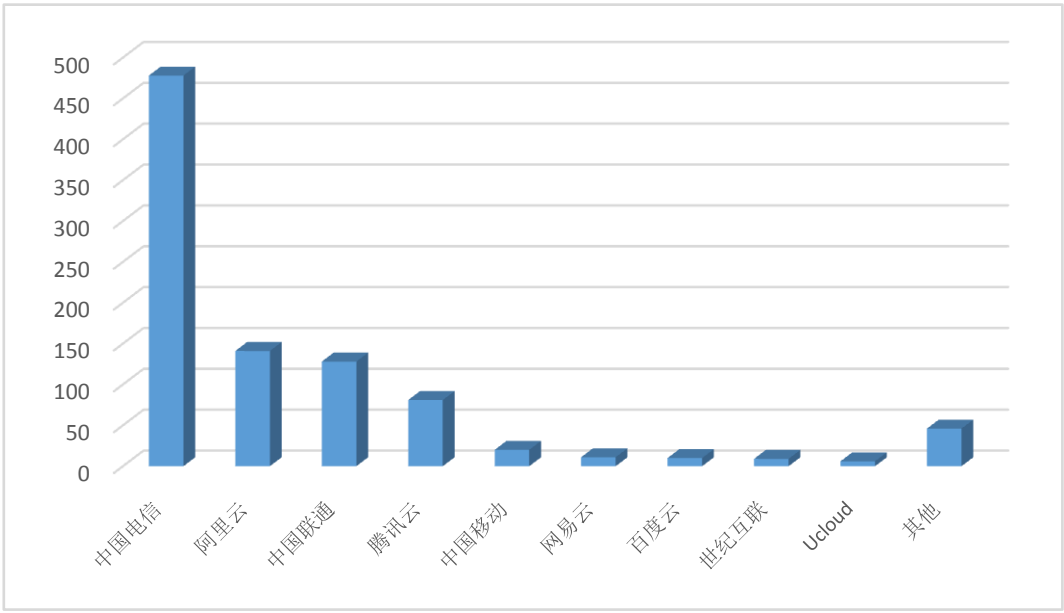

图 4-9 2018 年 11-12 月云服务商放置恶意代码种类分布图

承载放马网站最多的 IP 地址 TOP 20 列表如表 4-4 所示，中国电信的一个 IP 承载放马网站数达到了 9454，但是承载

的恶意代码种类仅 2 个。承载放马网站较多的前 20 个 IP 地址所属的云服务商包括中国电信（12 个）、阿里云（5 个）、中国联通（2 个）、腾讯云（1 个）。

表 4-4 承载放马网站较多的 IP 地址 TOP 20

放马 IP	放马网站数	放置恶意代码数	归属省份	归属云服务商
202.X.X.137	9454	2	浙江	中国电信
113.X.X.45	2188	1	广东	中国电信
101.X.X.49	2170	2	浙江	中国联通
219.X.X.144	2033	1	山东	中国电信
124.X.X.42	1892	1	湖南	中国电信
120.X.X.37	1345	1	广东	阿里云
115.X.X.167	1225	2	山东	阿里云
180.X.X.239	1105	2	江苏	中国电信
115.X.X.35	1080	2	浙江	阿里云
120.X.X.32	1028	1	广东	阿里云
150.X.X.231	634	1	山东	中国电信
101.X.X.129	450	1	北京	阿里云
61.X.X.166	416	1	江苏	中国电信
42.X.X.239	384	1	河南	中国联通
222.X.X.135	373	1	江苏	中国电信
122.X.X.6	371	60	浙江	中国电信
122.X.X.212	368	1	广东	腾讯云
61.X.X.185	348	51	江苏	中国电信
113.X.X.53	346	1	广东	中国电信
113.X.X.51	340	1	广东	中国电信

承载恶意代码种类较多的 IP 地址 TOP 20 列表如表 4-5 所示，其中中国电信 12 个、中国联通 7 个、腾讯云 1 个；承载恶意代码数量最多的 IP 归属于腾讯云，承载的恶意代码高达 86 种。

表 4-5 放置恶意代码数量 TOP 20 的网页放马 IP 列表

放马 IP	放马网站数	放置恶意代码数	归属省份	归属云服务商
203.X.X.179	147	86	广东	腾讯云
218.X.X.74	233	68	江苏	中国电信
122.X.X.6	371	60	浙江	中国电信
122.X.X.37	180	57	浙江	中国电信

61.X.X.185	348	51	江苏	中国电信
58.X.X.35	211	48	江苏	中国电信
222.X.X.62	223	44	江苏	中国电信
221.X.X.38	51	36	山西	中国联通
121.X.X.65	55	35	河北	中国联通
59.X.X.140	243	35	江西	中国电信
118.X.X.144	70	34	四川	中国电信
222.X.X.207	74	34	广西	中国电信
221.X.X.20	54	33	山西	中国联通
121.X.X.195	47	32	河北	中国联通
122.X.X.14	142	32	浙江	中国电信
221.X.X.22	48	31	山西	中国联通
61.X.X.189	87	30	江苏	中国电信
221.X.X.36	47	29	山西	中国联通
220.X.X.107	45	29	天津	中国联通
183.X.X.163	57	26	广东	中国电信

（四）木马或僵尸网络控制事件分析

利用云控制木马或僵尸网络是指利用云主机作为木马或僵尸程序的控制端，窃取受害者信息或远程控制受害者计算机等。

根据 CNCERT 监测数据，2018 年 11-12 月，20 家境内云的 1367 个 IP 被用作木马或僵尸网络控制端，控制了 489680 个肉鸡 IP;境内全部木马或僵尸网络控制端达到 4589 个，控制了 830641 个肉鸡 IP；20 家境内云控制端 IP 占境内控制端 IP 的 29.8%，20 家境内云控制端 IP 控制的肉鸡 IP 数占境内全部控制端 IP 控制的肉鸡 IP 数的 59%。

控制端控制的 IP 数分布如图 4-10 所示，中国电信控制的 IP 数所占比例最大，达到了 96%。

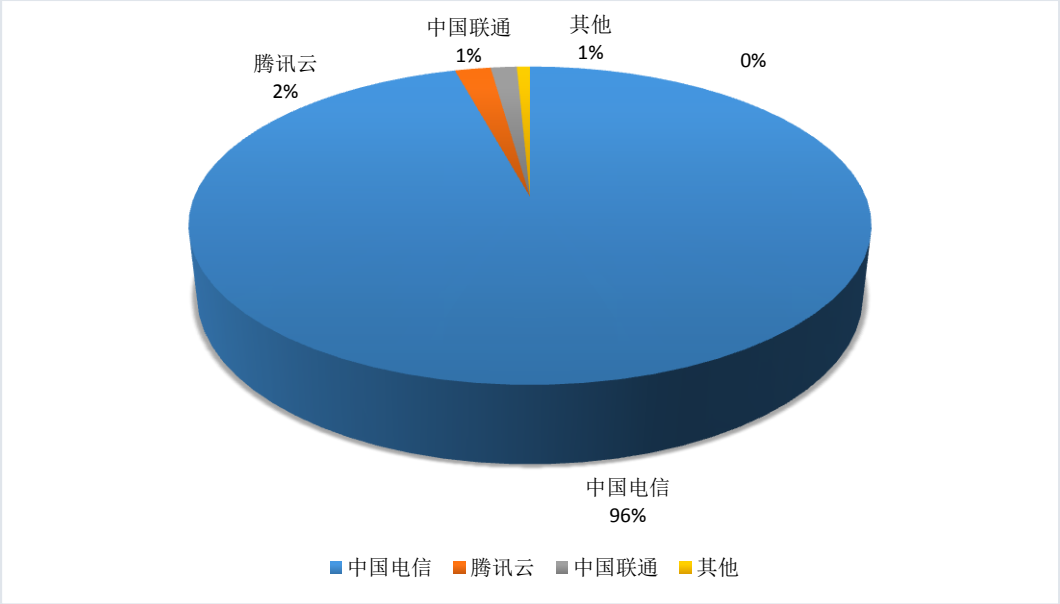

图 4-10 2018 年 11-12 月云服务商控制端控制的 IP 数分布图

控制端 IP 分布如图 4-11 所示，中国电信所占比例最大为 59%，其次为阿里云 14%、百度云 7%、腾讯云 7%、中国联通 5%。

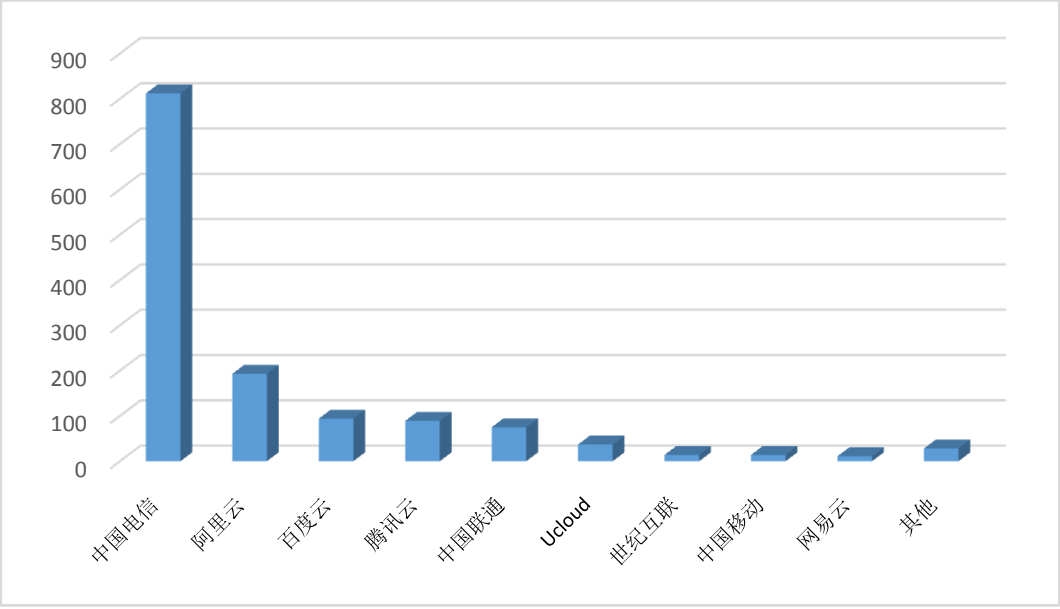

图 4-11 2018 年 11-12 月云服务商控制端 IP 数分布图

控制肉鸡最多的控制端 IP 地址 TOP 20 列表如表 4-6 所示，IP 主要集中在江苏、浙江地区，所属的云服务商均为中国电信。

表 4-6 控制肉鸡最多的控制端 IP 地址 TOP 20

控制端 IP	控制肉鸡 IP 数	与肉鸡通信次数	归属省份	归属云服务商
115.X.X.147	109692	7824194	浙江	中国电信
115.X.X.210	102135	5098457	浙江	中国电信
183.X.X.207	101995	5775107	浙江	中国电信
115.X.X.155	101236	5884527	浙江	中国电信
115.X.X.164	97858	4408780	浙江	中国电信
58.X.X.183	71992	47086241	江苏	中国电信
115.X.X.182	59306	2201124	浙江	中国电信
183.X.X.233	58895	4199914	浙江	中国电信
222.X.X.151	55275	10270059	江苏	中国电信
58.X.X.85	54552	74801829	江苏	中国电信
115.X.X.132	44535	7168466	浙江	中国电信
58.X.X.95	42922	26729296	江苏	中国电信
115.X.X.144	38692	9544876	浙江	中国电信
183.X.X.40	37244	1786309	浙江	中国电信
222.X.X.139	32495	5191596	江苏	中国电信
58.X.X.182	26474	16170513	江苏	中国电信
222.X.X.128	26022	11924828	江苏	中国电信
58.X.X.96	23768	31189948	江苏	中国电信
183.X.X.229	20955	2158958	浙江	中国电信
115.X.X.160	19892	771133	浙江	中国电信

五、 云网络安全态势分析

本节汇总分析监测发现的各类网络安全事件，建立网络安全态势指数模型，对 20 家境内云的网络安全态势进行评估分析，帮助云服务商和云用户掌握当前的网络安全状态，以便其针对各类网络威胁采取适当预防措施，使系统免受攻击和破坏，使网络安全得到充分保护。

网络安全态势指数总分值 100 分，包括安全性和可控性两个一级指标，因安全性和可控性同样重要，所以二者分值相同；安全性指标包括拒绝服务攻击、后门攻击、网页篡改、木马或僵尸网络受控事件 4 个二级指标；可控性指标包括发

起或参与拒绝服务攻击、发起网站后门攻击、网站放马事件、木马或僵尸网络控制事件 4 个二级指标。

根据二级指标的事件平均发生概率计算二级指标值，再逐级加权求和获得百分制的网络安全态势指数。因此，网络安全态势指数为:

$$E_i = \sum_k w_k \frac{\max_j(x_{jk}) - x_{ik}}{\max_j(x_{jk}) - \min_j(x_{jk})}$$

其中，w_k为二级指标k的权重，x_{ik}为二级指标k的攻击事件发生概率（即第i个云服务商二级指标k攻击事件数/第i个云服务商的 IP 总数）。网络安全态势指数分值越高表示各类安全事件平均发生概率越低，网络安全性和可控性越好。

根据 CNCERT 监测数据，2018 年 11-12 月，20 家境内云网络安全态势指数排名如表 5-1 所示，其中境内代表境内平均网络安全态势指数。

表 5-2 各云服务商境内云网络安全态势指数排名

排名	公司名	网络安全性指数	网络可控性指数	网络安全态势指数
1	网易云	99.0	98.4	98.7
2	蓝汛	98.0	97.9	97.9
3	美团云	99.6	96.1	97.8
4	亚马逊云	97.2	97.8	97.5
5	微软云	96.6	95.4	96.0
6	京东云	97.1	94.3	95.7
7	奇虎 360	99.1	92.2	95.6
8	金山云	94.9	92.7	93.8
9	华为云	87.5	96.3	91.9
10	阿里云	81.4	96.6	89.0
11	世纪互联	77.8	98.7	88.2
12	网宿科技	99.5	72.9	86.2
13	首都在线	90.6	81.7	86.1

14	腾讯云	74.9	96.1	85.5
--	境内	72.4	97.0	84.7
15	Ucloud	77.4	90.5	84.0
16	中国移动	76.4	88.6	82.5
17	中国联通	83.1	80.0	81.5
18	鹏博士	59.9	74.2	67.1
19	百度云	46.4	68.8	57.6
20	中国电信	37.2	45.3	41.2

从安全性指数来看，除鹏博士、百度云、中国电信外，大部分境内云的安全性均优于境内平均水平，这主要是由于境内云 IP 感染木马或僵尸网络的概率较低，但是在其他攻击上境内云则成为攻击的重灾区，这主要是由于云上承载的服务越来越多、越来越重要。从可控性指数来看，除世纪互联、网易云、蓝汛、亚马逊云外，大部分境内云的可控性均差于境内平均水平，说明越来越多黑客倾向于利用云主机进行网络攻击。

当前，云网络安全形势不容乐观，随着更多企业和业务场景向云平台迁移，则情况会更加严峻。根据“谁运营，谁负责”的网络政策，云网络安全维护是云服务商和云用户的共同责任，只是根据其服务类型（基础设施即服务 IaaS、平台即服务 PaaS、软件即服务 SaaS）的不同而职责分工略有不同。因此，云服务商和云用户应加大对网络安全的重视和投入，除做好及时更新软硬件漏洞、避免使用弱口令、关闭不必要服务等常规防护措施外，还应通过分工协作构建网络安全纵深检测防御体系，保障云的安全性和可控性，共同维护网络空间安全。