我国 DDoS 攻击资源月度分析报告

(2018 年 8 月)

国家计算机网络应急技术处理协调中心

2018 年 8 月

目 录

一、引言

（一）攻击资源定义

本报告为 2018 年 8 月份的 DDoS 攻击资源月度分析报告。围绕互联网环境威胁治理问题，基于 CNCERT 监测的 DDoS 攻击事件数据进行抽样分析，重点对“DDoS 攻击是从哪些网络资源上发起的”这个问题进行分析。主要分析的攻击资源包括:

1、 控制端资源，指用来控制大量的僵尸主机节点向攻击目标发起 DDoS 攻击的木马或僵尸网络控制端。

2、 肉鸡资源，指被控制端利用，向攻击目标发起 DDoS 攻击的僵尸主机节点。

3、 反射服务器资源，指能够被黑客利用发起反射攻击的服务器、主机等设施，它们提供的网络服务中，如果存在某些网络服务，不需要进行认证并且具有放大效果，又在互联网上大量部署（如 DNS 服务器，NTP 服务器等），它们就可能成为被利用发起 DDoS 攻击的网络资源。

4、 跨域伪造流量来源路由器，是指转发了大量任意伪造 IP 攻击流量的路由器。由于我国要求运营商在接入网上进行源地址验证，因此跨域伪造流量的存在，说明该路由器或其下路由器的源地址验证配置可能存在缺陷，且该路由器下的网络中存在发动 DDoS 攻击的设备。

5、 本地伪造流量来源路由器，是指转发了大量伪造本区

域 IP 攻击流量的路由器。说明该路由器下的网络中存在发动 DDoS 攻击的设备。

在本报告中，一次 DDoS 攻击事件是指在经验攻击周期内，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，但间隔为 24 小时或更多，则该事件被认为是两次攻击。此外，DDoS 攻击资源及攻击目标地址均指其 IP 地址，它们的地理位置由它的 IP 地址定位得到。

（二）本月重点关注情况

1、本月利用肉鸡发起 DDoS 攻击的控制端中，境外控制端接近一半位于美国；境内控制端最多位于江苏省，其次是浙江省、河南省和广东省，按归属运营商统计，电信占的比例最大。

2、本月参与攻击较多的肉鸡地址主要位于浙江省、山东省、江苏省和广东省，其中大量肉鸡地址归属于电信运营商。2018 年以来监测到的持续活跃的肉鸡资源中，位于江苏省、山东省、广东省占的比例最大。

3、本月被利用发起 Memcached 反射攻击境内反射服务器数量相比上月有明显下降，按省份统计排名前三名的省份是西藏自治区、四川省和广东省；数量最多的归属运营商是电信。被利用发起 NTP 反射攻击的境内反射服务器数量按省份统计排名前三名的省份是山东省、湖北省和河南省；数量最多的归

属运营商是联通。被利用发起 SSDP 反射攻击的境内反射服务器数量按省份统计排名前三名的省份是辽宁省、江苏省和浙江省；数量最多的归属运营商是联通。

4、近两月，跨域伪造流量来源路由器数量有较明显的下降。本月转发伪造跨域攻击流量的路由器中，归属于北京市的路由器参与的攻击事件数量最多，2018 年以来被持续利用的跨域伪造流量来源路由器中，归属于北京市、浙江省和上海市路由器数量最多。

5、本月转发伪造本地攻击流量的路由器中，归属于浙江省电信的路由器参与的攻击事件数量最多，2018 年以来被持续利用的本地伪造流量来源路由器中，归属于江苏省、山东省、河南省和湖南省路由器数量最多。

二、DDoS 攻击资源分析

（一）控制端资源分析

根据 CNCERT 抽样监测数据，2018 年 8 月，利用肉鸡发起 DDoS 攻击的控制端有 367 个，其中，48 个控制端位于我国境内，319 个控制端位于境外。

位于境外的控制端按国家或地区分布，美国占的比例最大，占 37.6%，其次是加拿大和丹麦，如图 1 所示。

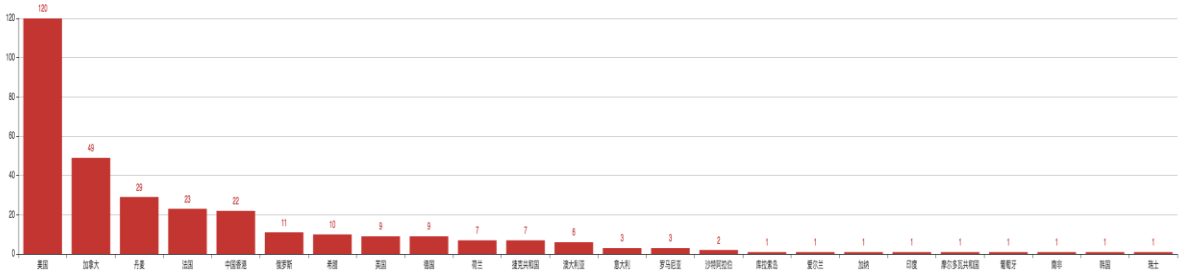

图 1 本月发起 DDoS 攻击的境外控制端数量按国家或地区分布

位于境内的控制端按省份统计，江苏省占的比例最大，占 35.7%，其次是浙江省、河南省和广东省；按运营商统计，电信占的比例最大，占 72.9%，联通占 18.8%，如图 2 所示。

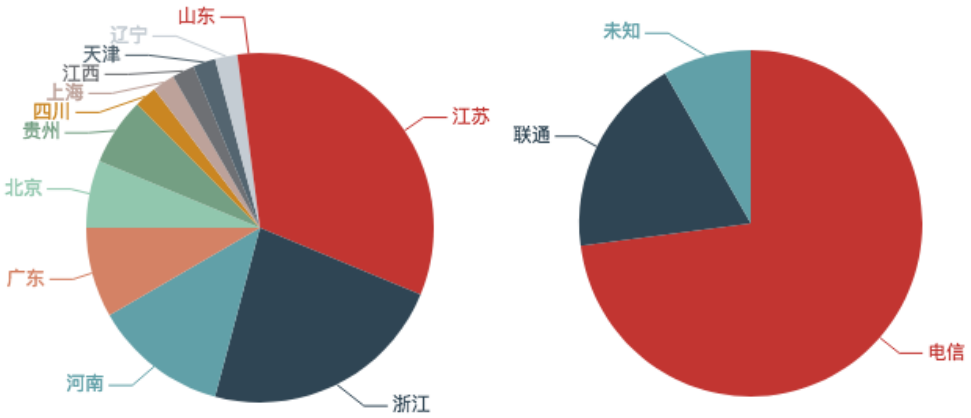

图 2 本月发起 DDoS 攻击的境内控制端数量按省份和运营商分布

发起攻击最多的境内控制端前二十名及归属如表 1 所示，主要位于江苏省。

表 1 本月发起攻击最多的境内控制端 TOP20

控制端地址	归属省份	归属运营商或云服务商
222. X. X. 232	江苏省	电信
183. X. X. 90	浙江省	电信
58. X. X. 158	江苏省	电信
114. X. X. 188	北京市	电信
120. X. X. 134	浙江省	阿里云
58. X. X. 93	江苏省	电信
123. X. X. 188	贵州省	电信

58.X.X.29	江苏省	电信
125.X.X.3	广东省	电信
222.X.X.216	江苏省	电信
116.X.X.222	河南省	联通
183.X.X.92	广东省	电信
111.X.X.186	江西省	电信
115.X.X.164	浙江省	电信
42.X.X.114	河南省	联通
222.X.X.34	江苏省	电信
58.X.X.169	江苏省	电信
58.X.X.51	江苏省	电信
58.X.X.5	江苏省	电信
118.X.X.61	天津市	电信

2018 年 1 月至今监测到的控制端中，7.4%的控制端在本月仍处于活跃状态，共计 77 个，其中位于我国境内的控制端数量为 6 个，位于境外的控制端数量为 71 个。持续活跃的境内控制端及归属如表 2 所示。

表 2 2018 年以来持续活跃发起 DDOS 攻击的境内控制端

控制端地址	**归属省份**	**归属运营商或云服务商**
211.X.X.89	四川省	电信
222.X.X.34	江苏省	电信
222.X.X.232	江苏省	电信
119.X.X.116	广东省	电信
139.X.X.51	上海市	阿里云
118.X.X.50	广东省	电信

（二）肉鸡资源分析

根据 CNCERT 抽样监测数据，2018 年 8 月，共有 141,704 个肉鸡地址参与真实地址攻击(包含真实地址攻击与其它攻击的混合攻击)。

这些肉鸡资源按省份统计，浙江省占的比例最大，为 15.4%，其次是山东省、江苏省和广东省；按运营商统计，电

信占的比例最大，为 52.9%，联通占 37.6%，移动占 6.6%，如图 3 所示。

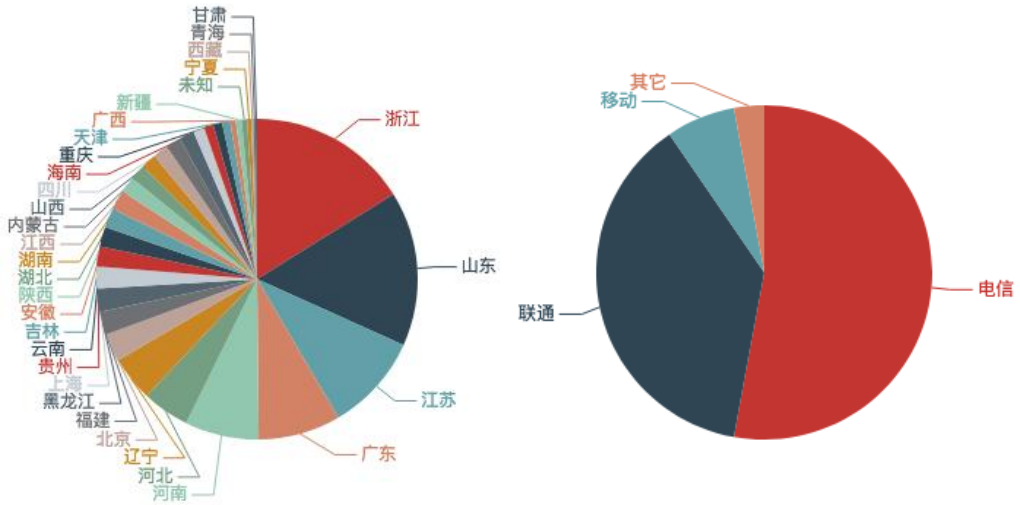

图 3 本月肉鸡地址数量按省份和运营商分布

本月参与攻击最多的肉鸡地址前二十名及归属如表 3 所示，位于新疆维吾尔自治区和河南省的地址最多。

表 3 本月参与攻击最多的肉鸡地址 TOP20

肉鸡地址	归属省份	归属运营商
61.X.X.28	甘肃省	电信
60.X.X.174	新疆维吾尔族自治区	联通
61.X.X.114	河南省	联通
61.X.X.66	青海省	电信
139.X.X.208	北京市	待确认
118.X.X.186	甘肃省	电信
175.X.X.131	湖南省	电信
58.X.X.114	湖南省	联通
112.X.X.146	安徽省	联通
222.X.X.242	贵州省	电信
61.X.X.243	内蒙古自治区	联通
112.X.X.234	江苏省	联通
219.X.X.97	黑龙江省	电信
114.X.X.253	北京市	待确认
221.X.X.129	内蒙古自治区	联通
202.X.X.138	新疆维吾尔族自治区	电信
111.X.X.69	河南省	移动
218.X.X.182	河南省	联通
111.X.X.34	北京市	联通

106.X.X.223	新疆维吾尔族自治区	电信

2018 年 1 月至今监测到的肉鸡资源中，共计 22,627 个肉鸡在本月仍处于活跃状态，其中位于我国境内的肉鸡数量为 18,935 个，位于境外的肉鸡数量为 3,692 个。2018 年 1 月至今被利用发起 DDoS 攻击最多的肉鸡 TOP20 及归属如表 4 所示，此持续活跃的肉鸡列表数据与上月保持未变。

表 4 2018 年以来被利用发起 DDoS 攻击数量排名 TOP20,且在本月持续活跃的肉鸡地址

肉鸡地址	归属省份	归属运营商
61.X.X.28	甘肃省	电信
60.X.X.174	新疆维吾尔族自治区	联通
61.X.X.114	河南省	联通
61.X.X.66	青海省	电信
139.X.X.208	北京市	待确认
118.X.X.186	甘肃省	电信
175.X.X.131	湖南省	电信
58.X.X.114	湖南省	联通
112.X.X.146	安徽省	联通
222.X.X.242	贵州省	电信
61.X.X.243	内蒙古自治区	联通
112.X.X.234	江苏省	联通
219.X.X.97	黑龙江省	电信
114.X.X.253	北京市	待确认
221.X.X.129	内蒙古自治区	联通
202.X.X.138	新疆维吾尔族自治区	电信
111.X.X.69	河南省	移动
218.X.X.182	河南省	联通
111.X.X.34	北京市	联通
106.X.X.223	新疆维吾尔族自治区	电信

2018 年 1 月至今持续活跃的境内肉鸡资源按省份统计，江苏省占的比例最大，占 17.6%，其次是山东省、广东省和浙江省；按运营商统计，电信占的比例最大，占 57.2%，联通占 24.6%，移动占 11.0%，如图 4 所示。

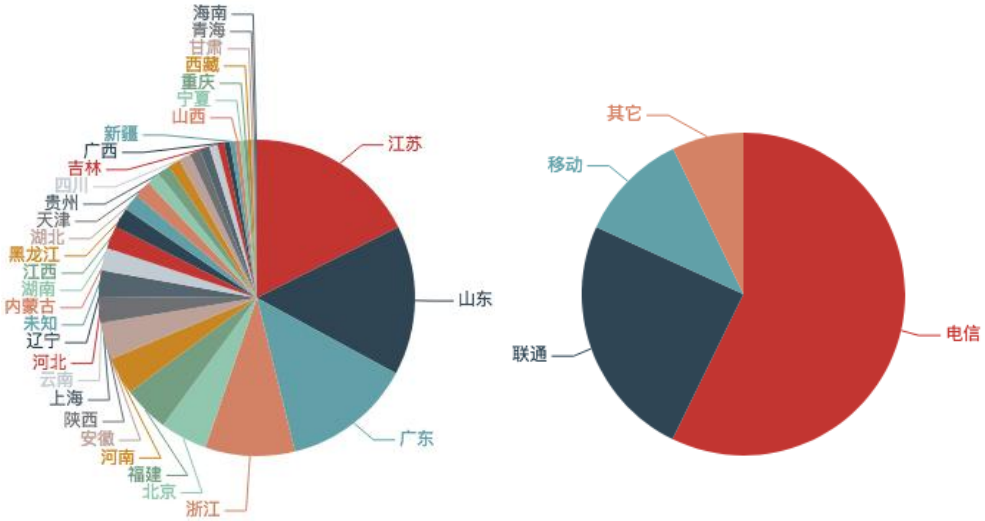

图 4 2018 年以来持续活跃的肉鸡数量按省份和运营商分布

（三）反射攻击资源分析

根据 CNCERT 抽样监测数据，2018 年 8 月，利用反射服务器发起的三类重点反射攻击共涉及 3,089,618 台反射服务器，其中境内反射服务器 2,874,263 台，境外反射服务器 215,355 台。反射攻击所利用 Memcached 反射服务器发起反射攻击的反射服务器有 9,660 台，占比 0.3%，其中境内反射服务器 9,542 台，境外反射服务器 118 台；利用 NTP 反射发起反射攻击的反射服务器有 803,446 台，占比 26.0%，其中境内反射服务器 682,916 台，境外反射服务器 120,530 台；利用 SSDP 反射发起反射攻击的反射服务器有 2,276,512 台，占比 73.7%，其中境内反射服务器 2,181,805 台，境外反射服务器 94,707 台。

（1）Memcached 反射服务器资源

Memcached 反射攻击利用了在互联网上暴露的大批量 Memcached 服务器（一种分布式缓存系统）存在的认证和设计缺陷，攻击者通过向 Memcached 服务器 IP 地址的默认端口 11211 发送伪造受害者 IP 地址的特定指令 UDP 数据包，使 Memcached 服务器向受害者 IP 地址返回比请求数据包大数倍的数据，从而进行反射攻击。

根据 CNCERT 抽样监测数据，2018 年 8 月，利用 Memcached 服务器实施反射攻击的事件共涉及境内 9,542 台反射服务器，境外 118 台反射服务器。本月被利用的 Memcached 服务器数量相比上月有明显下降。

本月境内反射服务器数量按省份统计，西藏自治区占的比例最大，占 15.6%，其次是四川省、广东省和河北省；按归属运营商或云服务商统计，电信占的比例最大，占 71.1%，移动占比 20.8%，联通占比 7.7%，如图 5 所示。

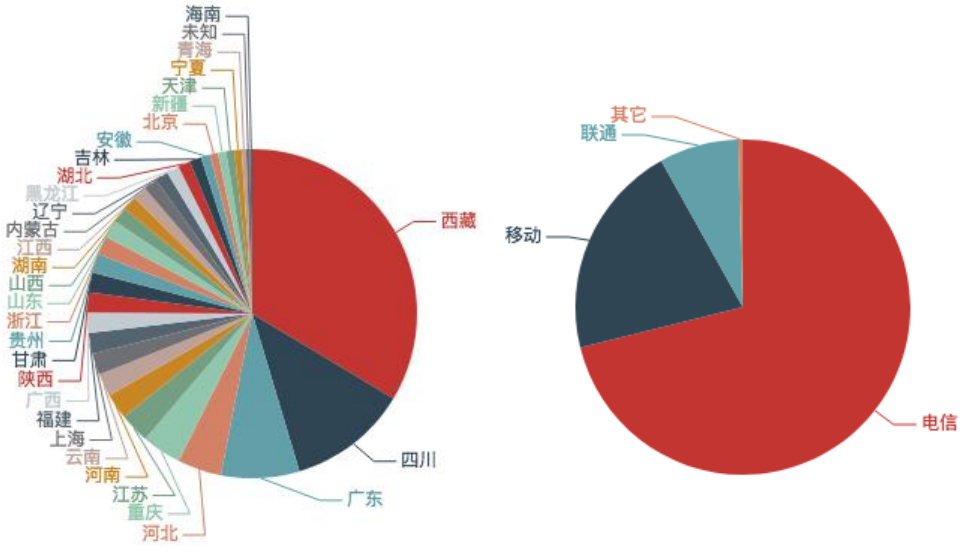

图 5 本月境内 Memcached 反射服务器数量按省份、运营商或云服务商分布

本月境外反射服务器数量按国家或地区统计，美国占的比例最大，占 83.2%，其次是印度尼西亚、俄罗斯和新加坡，如图 6 所示。

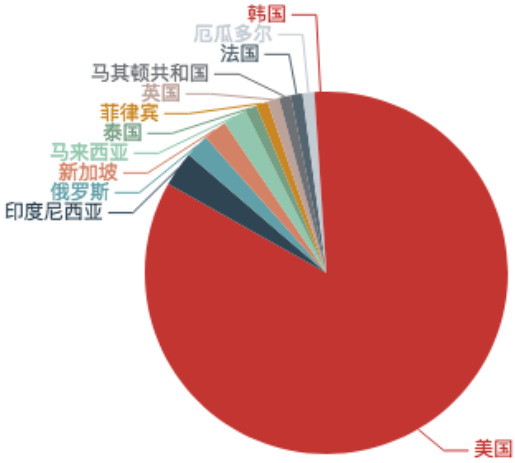

图 6 本月境外反射服务器数量按国家或地区分布

本月境内发起反射攻击事件数量 TOP100 中目前仍存活的 Memcached 服务器为位于西藏自治区的服务器（202.X.X.217）。

近两月被利用发起攻击的 Memcached 反射服务器中，共计 119 个在本月仍处于活跃状态。近两月被持续利用发起攻击的 Memcached 反射服务器按省份统计，西藏自治区占的比例最大，占 30.3%，其次是广东省、上海市和四川省；按运营商或云服务统计，电信占的比例最大，占 59.7%，移动占 25.2%，联通占 10.9%，如图 7 所示。

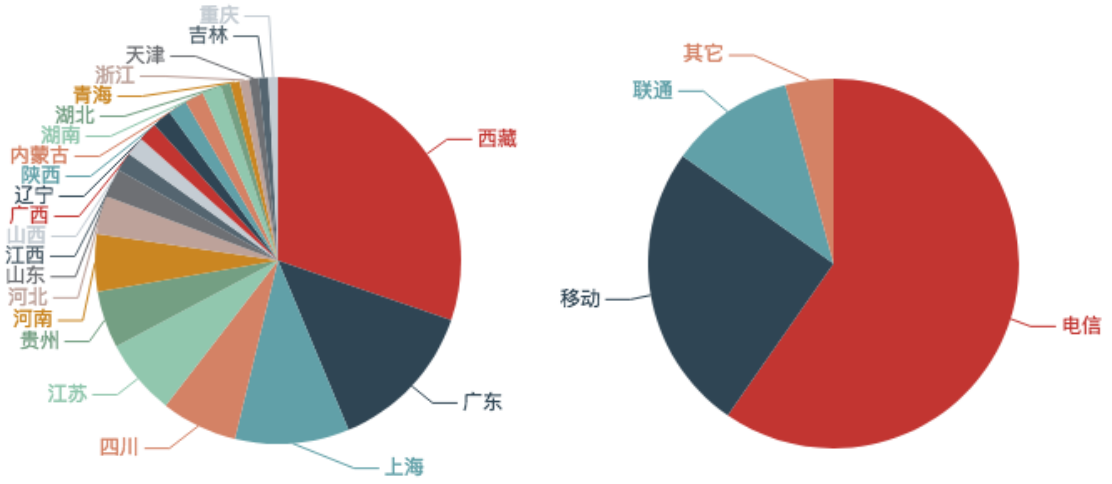

图 7 近两月被持续利用发起攻击的 Memcached 反射服务器数量按省份运营商或云服务商分布

（2）NTP 反射服务器资源

NTP 反射攻击利用了 NTP（一种通过互联网服务于计算机时钟同步的协议）服务器存在的协议脆弱性，攻击者通过向 NTP 服务器 IP 地址的默认端口 123 发送伪造受害者 IP 地址的 Monlist 指令数据包，使 NTP 服务器向受害者 IP 地址反射返回比原始数据包大数倍的数据，从而进行反射攻击。

根据 CNCERT 抽样监测数据，2018 年 8 月，NTP 反射攻击事件共涉及我国境内 682,916 台反射服务器，境外 120,530 台反射服务器。

本月被利用发起 NTP 反射攻击的境内反射服务器数量按省份统计，山东省占的比例最大，占 24.4%，其次是湖北省、河南省和河北省；按归属运营商统计，联通占的比例最大，占 40.1%，移动占比 39.3%，电信占比 20.4%，如图 8 所示。

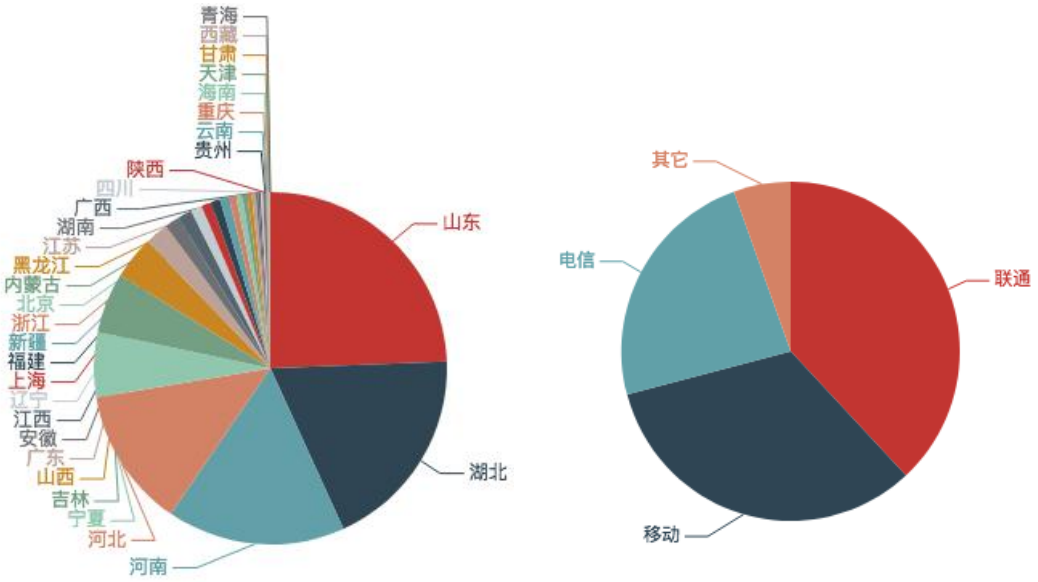

图 8 本月被利用发起 NTP 反射攻击的境内反射服务器数量按省份和运营商分布

本月被利用发起 NTP 反射攻击的境外反射服务器数量按国家或地区统计，澳大利亚占的比例最大，占 74.7%，其次是美国、巴基斯坦和印度，如图 9 所示。

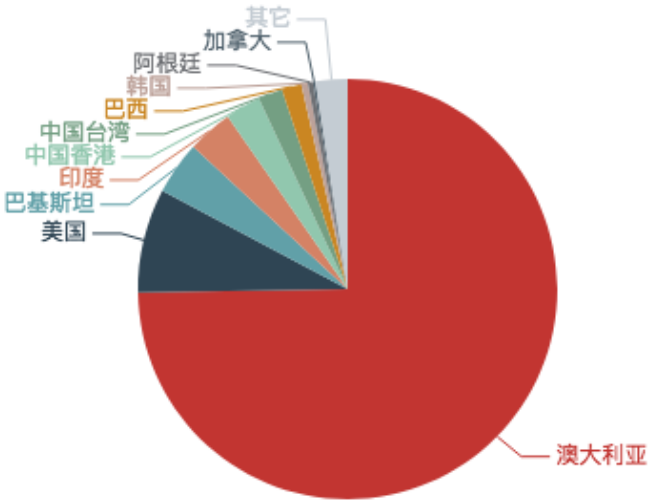

图 9 本月被利用发起 NTP 反射攻击的境外反射服务器数量按国家或地区分布

本月被利用发起 NTP 反射攻击的境内反射服务器按被利用发起攻击数量排名 TOP30 及归属如表 5 所示，位于山西省的地址最多。

表 5 本月境内被利用发起 NTP 反射攻击的反射服务器按涉事件数量 TOP30

反射服务器地址	归属省份	归属运营商
222.X.X.199	宁夏回族自治区	电信
183.X.X.11	山西省	移动
211.X.X.85	山西省	移动
111.X.X.245	山西省	移动
183.X.X.196	山西省	移动
183.X.X.235	山西省	移动
183.X.X.85	山西省	移动
111.X.X.203	山西省	移动
111.X.X.70	山西省	移动
183.X.X.219	山西省	移动
211.X.X.154	山西省	移动
183.X.X.174	山西省	移动
183.X.X.195	山西省	移动
183.X.X.115	山西省	移动
183.X.X.80	山西省	移动
183.X.X.10	山西省	移动
111.X.X.211	山西省	移动
111.X.X.6	宁夏回族自治区	电信
218.X.X.169	贵州省	移动
61.X.X.226	宁夏回族自治区	电信
211.X.X.114	山西省	移动
183.X.X.218	山西省	移动
111.X.X.208	山西省	移动
119.X.X.140	宁夏回族自治区	电信
211.X.X.180	山西省	移动
183.X.X.92	山西省	移动
183.X.X.173	山西省	移动
183.X.X.203	山西省	移动
183.X.X.52	山西省	移动
123.X.X.206	湖北省	移动

近两月被持续利用发起攻击的 NTP 反射服务器中，共计 241,806 个在本月仍处于活跃状态，其中 211,714 个位于境内，30,092 个位于境外。持续活跃的 NTP 反射服务器按省份统计，湖北省占的比例最大，占 47.3%，其次是山东省、河北省和河南省；按运营商统计，联通占的比例最大，占 48.3%，移动占

31.2%，电信占 20.1%，如图 10 所示。

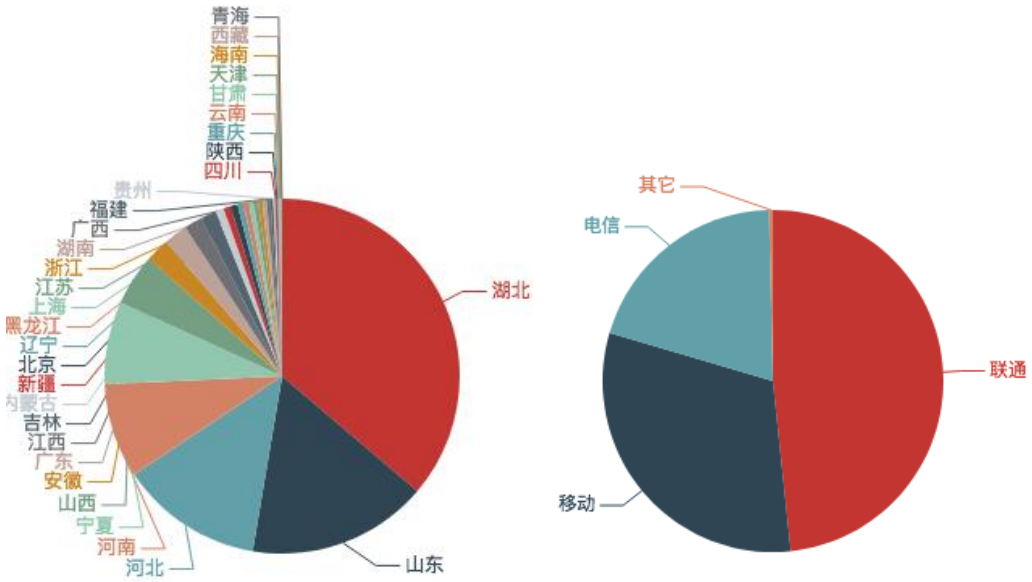

图 10 近两月被持续利用发起攻击的 NTP 反射服务器数量按省份运营商分布

（3）SSDP 反射服务器资源

SSDP 反射攻击利用了 SSDP（一种应用层协议，是构成通用即插即用(UPnP)技术的核心协议之一）服务器存在的协议脆弱性，攻击者通过向 SSDP 服务器 IP 地址的默认端口 1900 发送伪造受害者 IP 地址的查询请求，使 SSDP 服务器向受害者 IP 地址反射返回比原始数据包大数倍的应答数据包，从而进行反射攻击。

根据 CNCERT 抽样监测数据，2018 年 8 月，SSDP 反射攻击事件共涉及境内 2,181,805 台反射服务器，境外 94,707 台反射服务器。

本月被利用发起 SSDP 反射攻击的境内反射服务器数量按省份统计，辽宁省占的比例最大，占 20.5%，其次是江苏省、

浙江省和广东省；按归属运营商统计，联通占的比例最大，占 53.7%，电信占比 43.3%，移动占比 2.7%，如图 11 所示。

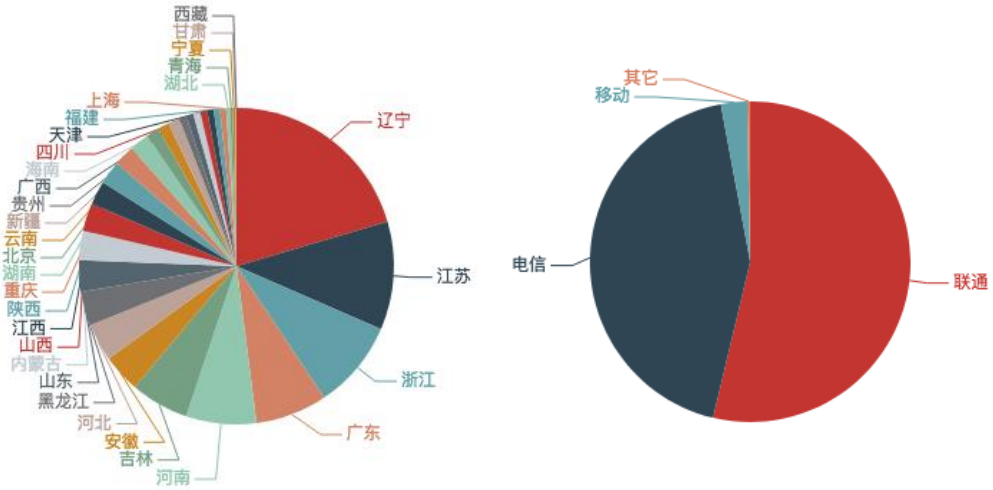

图 11 本月被利用发起 SSDP 反射攻击的境内反射服务器数量按省份和运营商分布

本月被利用发起 SSDP 反射攻击的境外反射服务器数量按国家或地区统计，美国占的比例最大，占 29.9%，其次是中国台湾、加拿大和韩国，如图 12 所示。

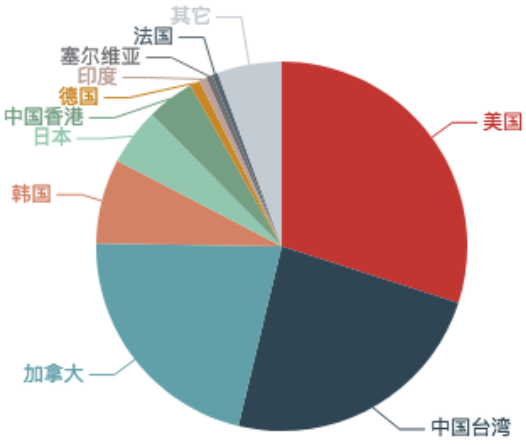

图 12 本月被利用发起 SSDP 反射攻击的境外反射服务器数量按国家或地区或地区分布

本月被利用发起 SSDP 反射攻击的境内反射服务器按被利用发起攻击数量排名 TOP30 的反射服务器及归属如表 6 所示，位于黑龙江省的地址最多。

表 6 本月境内被利用发起 SSDP 反射攻击事件数量中排名 TOP30 的反射服务器

反射服务器地址	归属省份	归属运营商
218.X.X.30	新疆维吾尔族自治区	移动
218.X.X.70	新疆维吾尔族自治区	移动
218.X.X.90	宁夏回族自治区	电信
111.X.X.2	黑龙江省	移动
59.X.X.198	山西省	电信
111.X.X.69	宁夏回族自治区	移动
218.X.X.156	宁夏回族自治区	移动
61.X.X.118	陕西省	电信
117.X.X.196	新疆维吾尔族自治区	移动
222.X.X.209	云南省	电信
111.X.X.6	黑龙江省	移动
111.X.X.5	湖北省	移动
112.X.X.50	云南省	电信
111.X.X.25	黑龙江省	移动
117.X.X.249	新疆维吾尔族自治区	移动
117.X.X.98	新疆维吾尔族自治区	移动
113.X.X.118	陕西省	电信
111.X.X.139	黑龙江省	移动
111.X.X.75	黑龙江省	移动
111.X.X.215	黑龙江省	移动
119.X.X.178	宁夏回族自治区	电信
111.X.X.125	黑龙江省	移动
111.X.X.127	黑龙江省	移动
111.X.X.157	黑龙江省	移动
112.X.X.3	云南省	电信
111.X.X.108	黑龙江省	移动
111.X.X.178	黑龙江省	移动
120.X.X.234	新疆维吾尔族自治区	电信
113.X.X.22	陕西省	电信
219.X.X.126	陕西省	电信

近两月被持续利用发起攻击的 SSDP 反射服务器中，共计 546,364 个在本月仍处于活跃状态，其中 490,173 个位于境内，56,191 个位于境外。近两月持续活跃的参与大量攻击事件的 SSDP 反射服务器按省份统计，辽宁省占的比例最大，占 26.2%，其次是江苏省、浙江省和广东省；按运营商统计，联通占的比

例最大，占 59.1%，电信占 37.4%，移动占 3.2%，如图 13 所示。

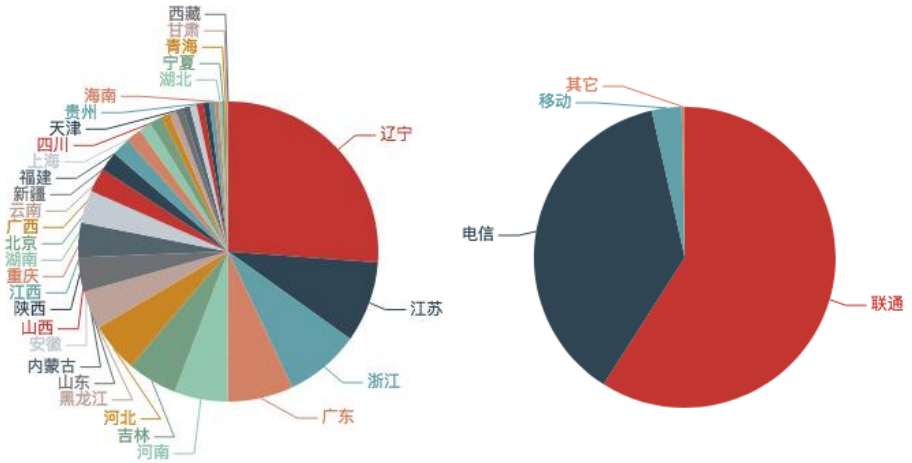

图 13 近两月被持续利用发起攻击的 SSDP 反射服务器数量按省份运营商分布

（四）发起伪造流量的路由器分析

1. 跨域伪造流量来源路由器

根据 CNCERT 抽样监测数据，2018 年 8 月，通过跨域伪造流量发起攻击的流量来源于 91 个路由器。近两月，跨域伪造流量来源路由器数量有较明显的下降。根据参与攻击事件的数量统计，归属于北京市的路由器（150.X.X.1、150.X.X.2）参与的攻击事件数量最多，其次是归属于上海市电信（124.X.X.250）的路由器，如表 7 所示。

表 7 本月参与攻击最多的跨域伪造流量来源路由器 TOP25

跨域伪造流量来源路由器	归属省份	归属运营商
150.X.X.1	北京市	待确认
150.X.X.2	北京市	待确认
124.X.X.250	上海市	电信
218.X.X.101	内蒙古自治区	联通
140.X.X.1	北京市	待确认
140.X.X.2	北京市	待确认
124.X.X.1	上海市	电信

202. X. X. 24	上海市	电信
202. X. X. 118	天津市	待确认
222. X. X. 200	北京市	待确认
202. X. X. 17	上海市	电信
219. X. X. 70	北京市	电信
202. X. X. 23	上海市	电信
202. X. X. 21	上海市	电信
202. X. X. 116	天津市	待确认
124. X. X. 202	上海市	电信
124. X. X. 201	上海市	电信
222. X. X. 180	上海市	电信
202. X. X. 137	浙江省	电信
150. X. X. 1	北京市	待确认
150. X. X. 2	北京市	待确认
118. X. X. 168	四川省	电信
221. X. X. 1	天津市	电信
118. X. X. 169	四川省	电信
202. X. X. 222	四川省	待确认

跨域伪造流量涉及路由器按省份分布统计，北京市占的比例最大，占 31.9%，其次是浙江省和上海市；按路由器所属运营商统计，电信占的比例最大，占 33.0%，移动占比 20.9%，联通占比 16.5%，如图 14 所示。

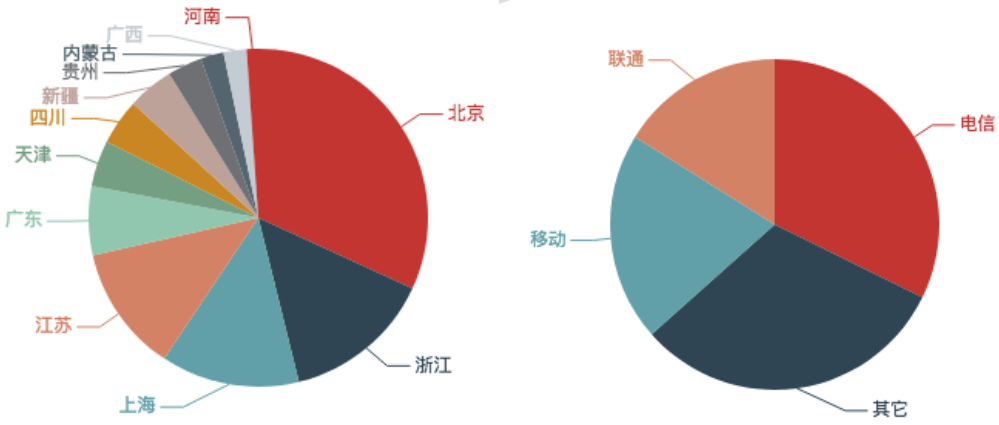

图 14 跨域伪造流量来源路由器数量按省份和运营商分布

2018 年度被持续利用转发 DDoS 攻击的跨域伪造流量来源路由器中，监测发现有 66 个在本月仍活跃，存活率为 16.7%。

按省份分布统计，北京市占的比例最大，占 31.8%，其次是浙江省和上海市；按路由器所属运营商统计，电信占的比例最大，占 36.8%，移动占比 23.5%，联通占比 22.1%，如图 15 所示。

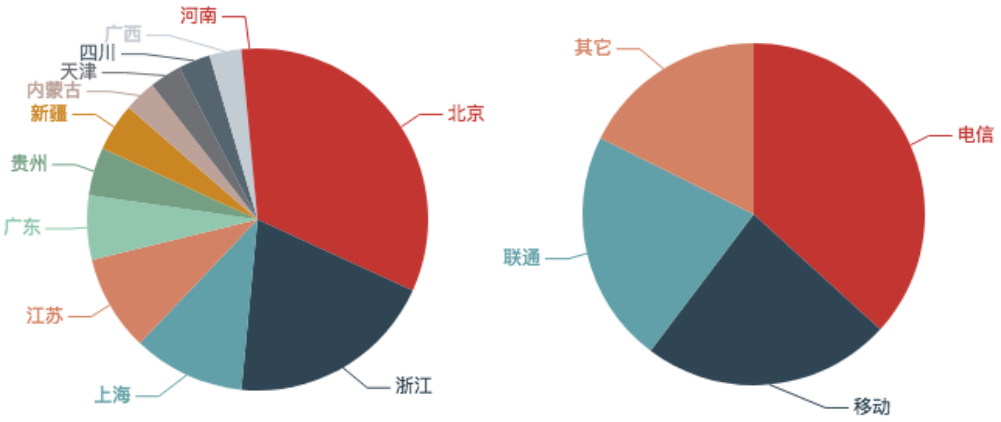

图 15 2018 年被持续利用转发跨域伪造攻击流量本月仍活跃路由器数量按省份和运营商分布

2. 本地伪造流量来源路由器

根据 CNCERT 抽样监测数据，2018 年 8 月，通过本地伪造流量发起攻击的流量来源于 189 个路由器。根据参与攻击事件的数量统计，归属于浙江省电信的路由器（61.X.X.8、61.X.X.4、220.X.X.127、220.X.X.126、202.X.X.136）参与的攻击事件数量最多，其次是归属于贵州省移动的路由器（211.X.X.9），如表 8 所示。

表 8 本月参与攻击最多的本地伪造流量来源路由器 TOP25

本地伪造流量来源路由器	归属省份	归属运营商
61.X.X.8	浙江省	电信
61.X.X.4	浙江省	电信
220.X.X.127	浙江省	电信
220.X.X.126	浙江省	电信
202.X.X.136	浙江省	电信
211.X.X.9	贵州省	移动
202.X.X.137	浙江省	电信
211.X.X.10	贵州省	移动
211.X.X.19	贵州省	移动

211. X. X. 20	贵州省	移动
118. X. X. 168	四川省	电信
118. X. X. 169	四川省	电信
202. X. X. 204	宁夏回族自治区	电信
202. X. X. 205	宁夏回族自治区	电信
202. X. X. 200	宁夏回族自治区	待确认
202. X. X. 202	宁夏回族自治区	待确认
218. X. X. 130	四川省	电信
218. X. X. 129	四川省	电信
202. X. X. 167	山东省	电信
202. X. X. 165	山东省	电信
124. X. X. 122	陕西省	电信
220. X. X. 253	北京市	电信
220. X. X. 243	北京市	电信
140. X. X. 2	山东省	待确认
140. X. X. 1	山东省	待确认

本月本地伪造流量涉及路由器按省份分布，江苏省占的比例最大，占 10.7%，其次是山东省、河南省和湖南省；按路由器所属运营商统计，电信占的比例最大，占 47.4%，移动占比 24.5%，联通占比 13.8%，如图 16 所示。

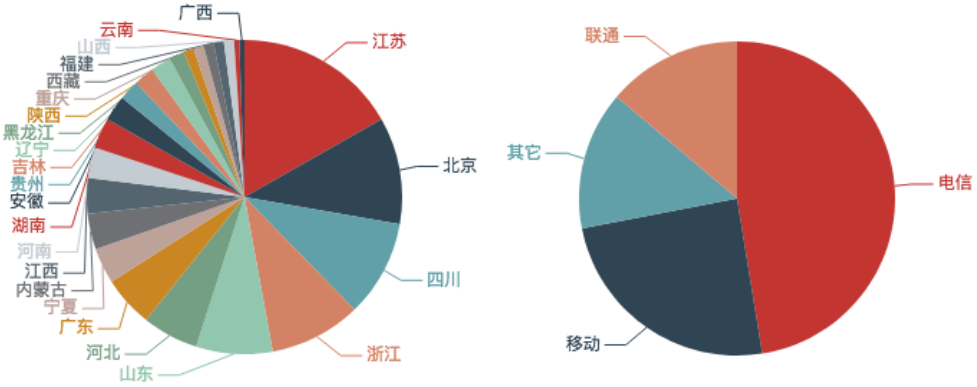

图 16 本地伪造流量来源路由器数量按省份和运营商分布

2018 年被持续利用转发本地伪造流量 DDoS 攻击的路由器中，监测发现有 153 个在本月仍活跃，存活率为 19.0%。按省份统计，江苏省占的比例最大，占 16.8%，其次是浙江省、北京市和四川省；按路由器所属运营商统计，电信占的比例最

大，占 54.4%，移动占比 28.8%，联通占比 12.5%，如图 17 所示。

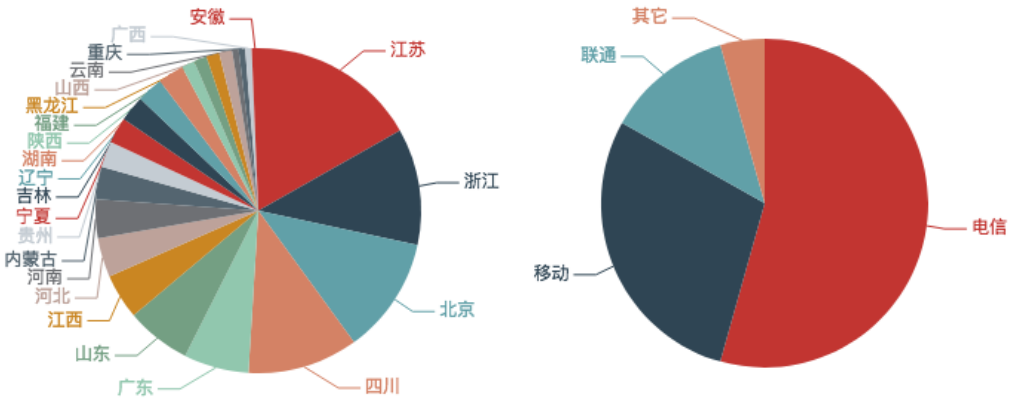

图 17 2018 年被持续利用且本月仍活跃的本地伪造流量来源路由器数量按省份运营商分布