我国 DDoS 攻击资源月度分析报告

（2019 年 10 月）

国家计算机网络应急技术处理协调中心

2019 年 10 月

目　录

一、引言

（一）攻击资源定义

本报告为 2019 年 10 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，境外控制端最多位于美国；得益于近期 DDoS 攻击资源的集中治理，境内控制端数量明显减少，其中位于河南省的数量最多，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广东省、浙江省、江苏省和山东省，其中大量肉鸡地址归属于电信运营商。2019 年以来监测到的持续活跃的肉鸡资源中，位于浙江省、江苏省、广东省和北京市占的比例最大。

3、本月被利用发起 Memcached 反射攻击境内反射服务器数量按省份统计排名前三名的省份是山东省、广东省和四川省；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、河南省和辽宁省；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、浙江省和吉林省；数量最多的归属运营商是联通。

4、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，2019 年以来被持续利用的跨域伪造流量来源路由器中，归属于福建省、安徽省和辽宁省路由器数量最多。

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，2019 年以来被持续利用的本地伪造流量来源路由器中，归属于四川省、福建省和江苏省路由器数量最多。

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，2019 年 10 月，利用肉鸡发起 DDoS 攻击的控制端有 388 个，其中，17 个控制端位于我国境内，371 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 37.2%，其次是荷兰和德国，如图 1 所示。

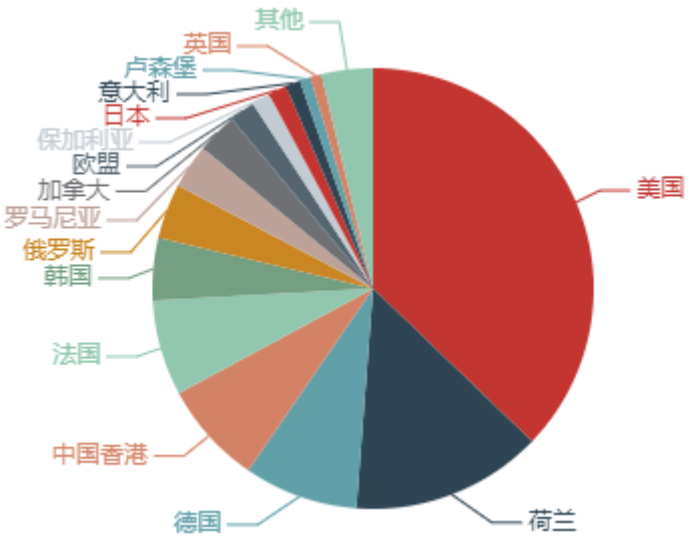

图 1 本月发起 DDoS 攻击的境外控制端数量按国家或地区分布

位于境内的控制端按省份统计，河南省占的比例最大，占 23.5%，其次是江苏省、四川省和浙江省；按运营商统计，电信占的比例最大，占 58.8%，移动占 35.3%，如图 2 所示。

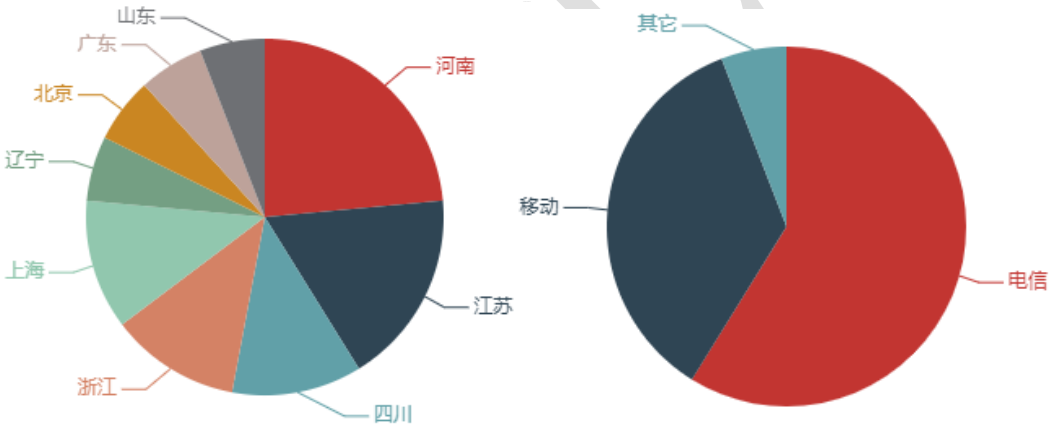

图 2 本月发起 DDoS 攻击的境内控制端数量按省份和运营商分布

本月发起攻击最多的境内控制端前二十名及归属如表 1 所示，位于河南省的地址最多。

表 1 本月发起攻击的境内控制端

控制端地址	归属省份	归属运营商或云服务商
103.XX.XX.143	上海市	电信
223.XX.XX.36	江苏省	移动
222.XX.XX.190	上海市	电信
101.XX.XX.194	北京市	BGP 多线
36.XX.XX.10	浙江省	电信
61.XX.XX.163	江苏省	电信
223.XX.XX.78	江苏省	移动
106.XX.XX.45	河南省	电信
47.XX.XX.210	山东省	阿里云
43.XX.XX.88	辽宁省	电信
1.XX.XX.240	河南省	电信
118.XX.XX.156	四川省	BGP 多线
118.XX.XX.197	四川省	BGP 多线
115.XX.XX.125	浙江省	电信
120.XX.XX.126	广东省	阿里云
123.XX.XX.162	河南省	电信
123.XX.XX.44	河南省	电信

2019 年至今监测到的控制端中，2.8%的控制端在本月仍处于活跃状态，共计 79 个，其中位于我国境内的控制端数量为 2 个，位于境外的控制端数量为 77 个。持续活跃的境内控制端及归属如表 2 所示。

表 2 2019 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
118.XX.XX.156	四川省	BGP 多线
47.XX.XX.210	山东省	阿里云

（二）肉鸡资源分析

根据 CNCERT 抽样监测数据，2019 年 10 月，共有 417,197 个境内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）。

这些境内肉鸡资源按省份统计，广东省占的比例最大，为

14.2%，其次是浙江省、江苏省和山东省；按运营商统计，电信占的比例最大，为 58.9%，联通占 28.1%，移动占 12.2%，如图 3 所示。

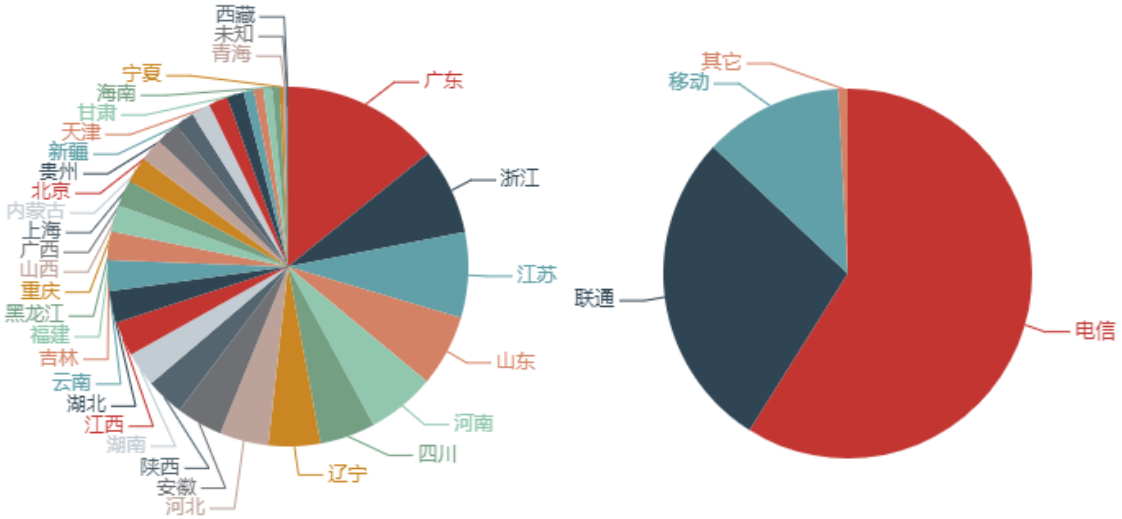

图 3 本月境内肉鸡地址数量按省份和运营商分布

本月参与攻击最多的境内肉鸡地址前二十名及归属如表 3 所示，位于辽宁省的地址最多。

表 3 本月参与攻击最多的境内肉鸡地址 TOP20

肉鸡地址	归属省份	归属运营商
59.XX.XX.110	山西省	电信
59.XX.XX.14	辽宁省	电信
218.XX.XX.21	安徽省	电信
59.XX.XX.14	辽宁省	电信
60.XX.XX.66	云南省	电信
60.XX.XX.12	安徽省	电信
220.XX.XX.26	浙江省	电信
36.XX.XX.91	安徽省	电信
114.XX.XX.177	江苏省	电信
117.XX.XX.201	江苏省	电信
118.XX.XX.204	湖南省	电信
59.XX.XX.113	辽宁省	电信
110.XX.XX.133	河北省	联通
115.XX.XX.217	浙江省	电信
183.XX.XX.194	浙江省	电信
1.XX.XX.154	黑龙江省	联通

116.XX.XX.97	内蒙古自治区	联通
123.XX.XX.158	辽宁省	电信
59.XX.XX.105	辽宁省	电信
113.XX.XX.221	黑龙江省	联通

2019 年至今监测到的肉鸡资源中，共计 6,436 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 4,176 个，位于境外的肉鸡数量为 2,260 个。2019 年至今持续活跃的境内肉鸡资源按省份统计，浙江省占的比例最大，占 20.2%，其次是江苏省、广东省和北京市；按运营商统计，电信占的比例最大，占 51.2%，移动占 24.5%，联通占 13.7%，如图 4 所示。

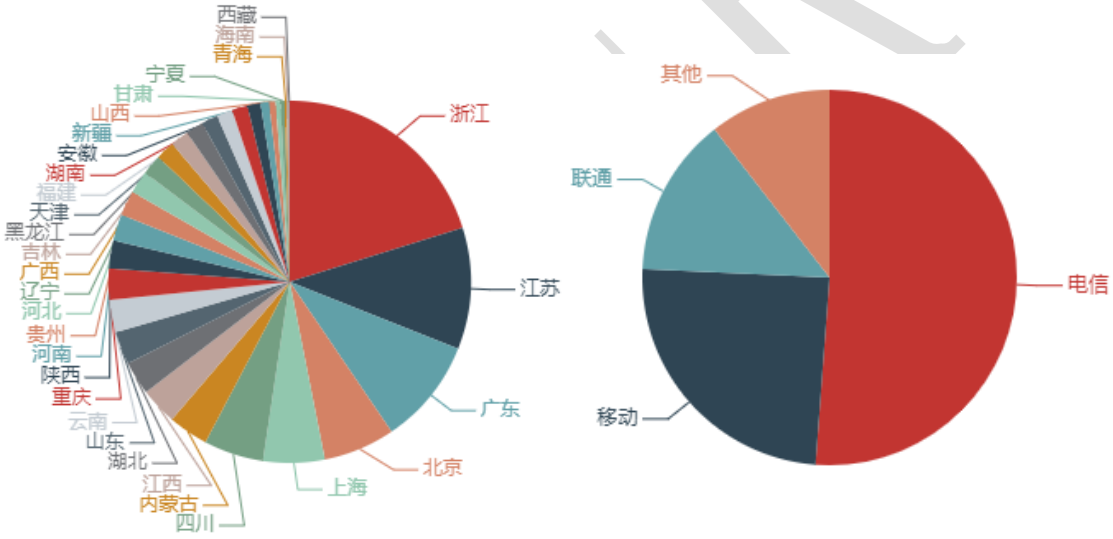

图 4 2019 年以来持续活跃的境内肉鸡数量按省份和运营商分布

（三）反射攻击资源分析

根据 CNCERT 抽样监测数据，2019 年 10 月，利用反射服务器发起的三类重点反射攻击共涉及 4,966,180 台反射服务器，其中境内反射服务器 3,292,020 台，境外反射服务器 1,674,160 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 24,482 台，占比 0.5%，其中境内反射服务器 23,160 台，境外反射服务器 1,322 台；利用 NTP 反射发起反射攻击的反射服务器有 3,862,682 台，占比 77.8%，其中境内反射服务器 2,428,575 台，境外反射服务器 1,434,107 台；利用 SSDP 反射发起反射攻击的反射服务器有 1,079,016 台，占比 21.7%，其中境内反射服务器 840,285 台，境外反射服务器 238,731 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，2019 年 10 月，利用 Memcached 服务器实施反射攻击的事件共涉及境内 23,160 台反射服务器，境外 1,322 台反射服务器。

本月境内反射服务器数量按省份统计，山东省占的比例最大，占 13.0%，其次是广东省、四川省和云南省；按归属运营商统计，电信占的比例最大，占 72.6%，移动占比 21.5%，联通占比 5.5%，如图 5 所示。

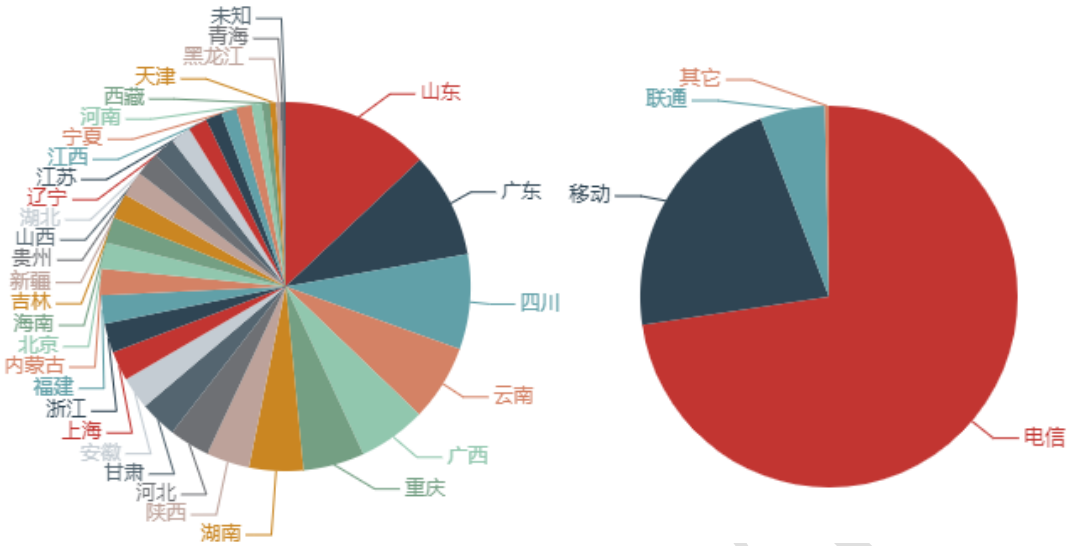

图 5 本月境内 Memcached 反射服务器数量按省份、运营商分布

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 16.2%，其次是中国香港、法国和德国，如图 6 所示。

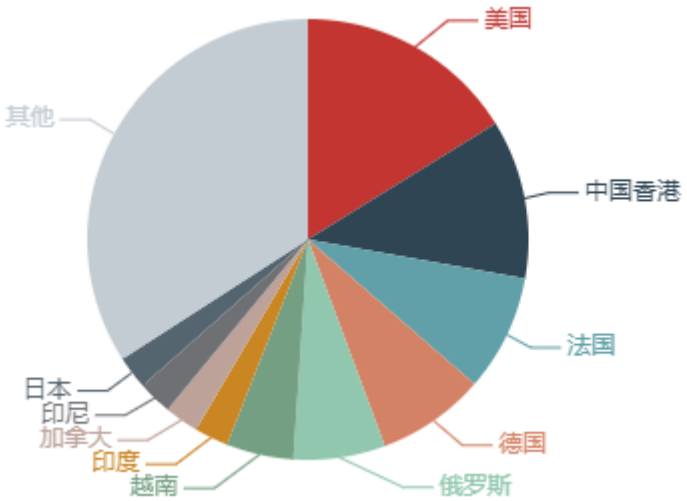

图 6 本月境外 Memcached 反射服务器数量按国家或地区分布

本月被利用发起 Memcached 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 4 所示，位于上海市的地址最多。

表 4 本月境内被利用发起 Memcached 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	归属运营商或云服务商
140.XX.XX.118	上海市	联通
106.XX.XX.142	北京市	电信
111.XX.XX.101	上海市	BGP 多线
118.XX.XX.151	上海市	BGP 多线
115.XX.XX.93	上海市	BGP 多线
115.XX.XX.193	上海市	BGP 多线
49.XX.XX.137	上海市	BGP 多线
49.XX.XX.236	上海市	BGP 多线
111.XX.XX.95	上海市	BGP 多线
117.XX.XX.51	甘肃省	移动
114.XX.XX.232	上海市	BGP 多线
129.XX.XX.228	上海市	BGP 多线
140.XX.XX.161	北京市	BGP 多线
106.XX.XX.230	北京市	电信
221.XX.XX.101	陕西省	联通
39.XX.XX.63	北京市	阿里云
221.XX.XX.103	陕西省	联通
120.XX.XX.166	上海市	移动
62.XX.XX.110	北京市	BGP 多线
106.XX.XX.18	北京市	电信
116.XX.XX.162	上海市	联通
182.XX.XX.188	云南省	电信
1.XX.XX.155	山西省	电信
118.XX.XX.217	上海市	BGP 多线
106.XX.XX.122	未知	BGP 多线
106.XX.XX.185	未知	BGP 多线
152.XX.XX.102	北京市	BGP 多线
116.XX.XX.127	北京市	BGP 多线
118.XX.XX.132	上海市	BGP 多线
49.XX.XX.22	上海市	BGP 多线

近两月被利用发起攻击的 Memcached 反射服务器中，共计 2,238 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，浙江省占的比例最大，占 16.4%，其次是山东省、广东省和江苏省；按运营商统计，

电信占的比例最大，占 42.1%，移动占 28.9%，联通占 14.5%，如图 7 所示。

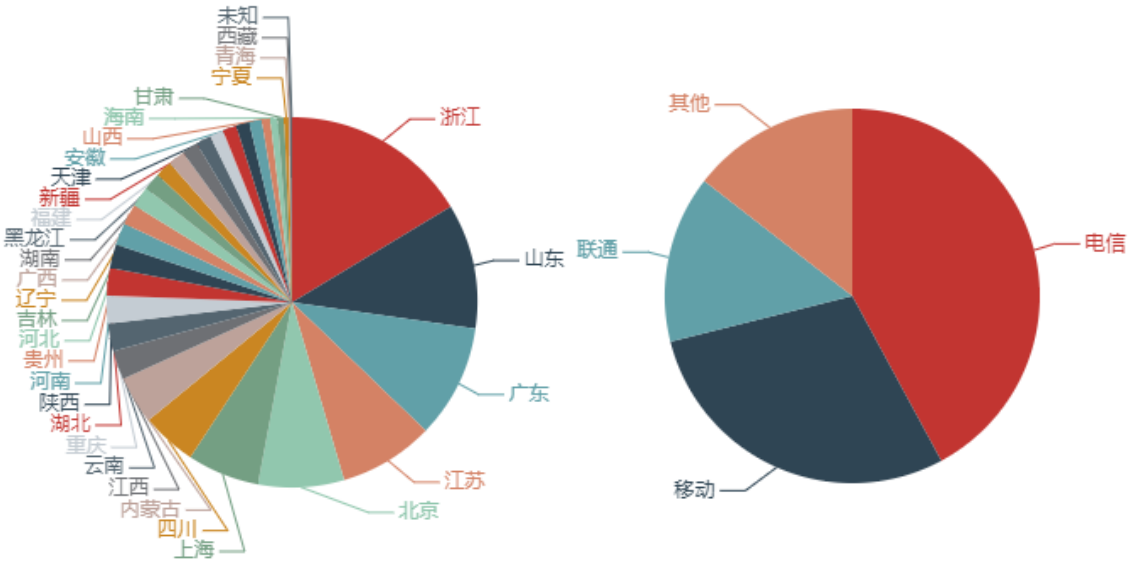

图 7 近两月被持续利用发起攻击的 Memcached 反射服务器数量按省份运营商分布

（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，2019 年 10 月，NTP 反射攻击事件共涉及我国境内 2,428,575 台反射服务器，境外 1,434,107 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 12.8%，其次是河南省、

辽宁省和河北省；按归属运营商统计，联通占的比例最大，占 67.5%，电信占比 28.3%，移动占比 2.9%，如图 8 所示。

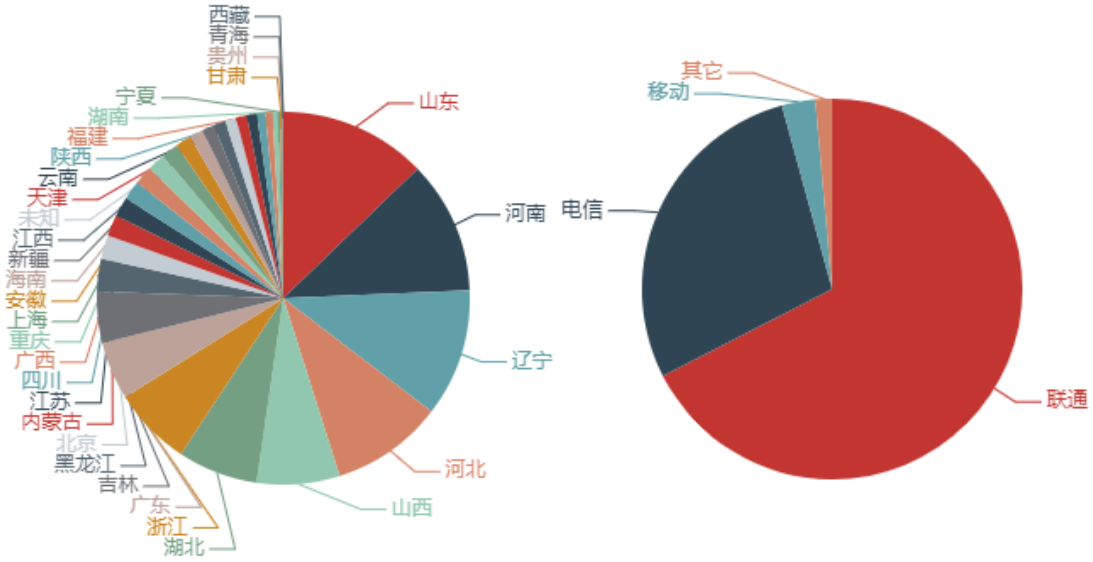

图 8 本月被利用发起 NTP 反射攻击的境内反射服务器数量按省份和运营商分布

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，越南占的比例最大，占 35.7%，其次是巴西、巴基斯坦和乌克兰，如图 9 所示。

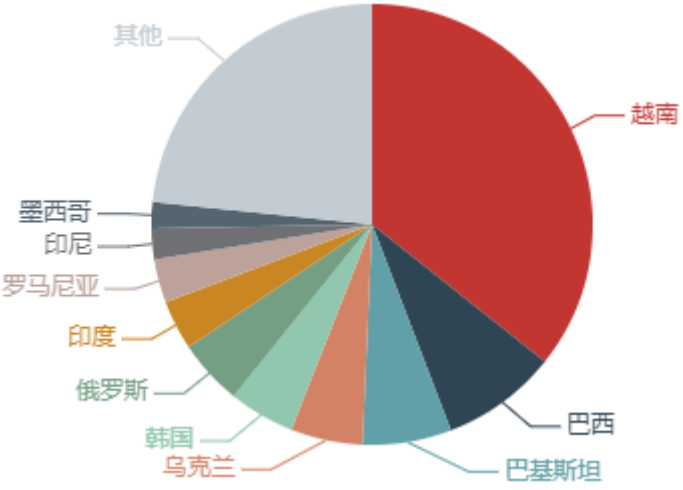

图 9 本月被利用发起 NTP 反射攻击的境外反射服务器数量按国家或地区分布

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，位于山东省的

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
220.XX.XX.229	云南省	电信
111.XX.XX.206	山西省	移动
223.XX.XX.173	山东省	移动
218.XX.XX.98	山东省	移动
111.XX.XX.215	山西省	移动
112.XX.XX.166	山东省	移动
112.XX.XX.92	山东省	移动
211.XX.XX.78	山西省	移动
120.XX.XX.99	安徽省	移动
183.XX.XX.70	山西省	移动
112.XX.XX.80	安徽省	移动
119.XX.XX.50	宁夏回族自治区	电信
222.XX.XX.110	山东省	BGP 多线
223.XX.XX.4	山东省	移动
112.XX.XX.252	山东省	移动
111.XX.XX.30	山西省	移动
223.XX.XX.3	山东省	移动
111.XX.XX.146	山西省	移动
122.XX.XX.226	吉林省	联通
211.XX.XX.36	山西省	移动
223.XX.XX.202	山东省	移动
59.XX.XX.2	山西省	电信
111.XX.XX.245	山西省	移动
223.XX.XX.242	山东省	移动
112.XX.XX.109	山东省	移动
122.XX.XX.20	吉林省	联通
111.XX.XX.217	山西省	移动
111.XX.XX.162	山东省	移动
112.XX.XX.251	山东省	移动
223.XX.XX.5	山东省	移动

近两月被持续利用发起攻击的 NTP 反射服务器中，共计 175,928 个在本月仍处于活跃状态，其中 92,669 个位于境内，83,259 个位于境外。持续活跃的 NTP 反射服务器按省份统计，河北省占的比例最大，占 18.1%，其次是湖北省、山东省和山

西省；按运营商统计，联通占的比例最大，占 44.3%，电信占 30.2%，移动占 22.8%，如图 10 所示。

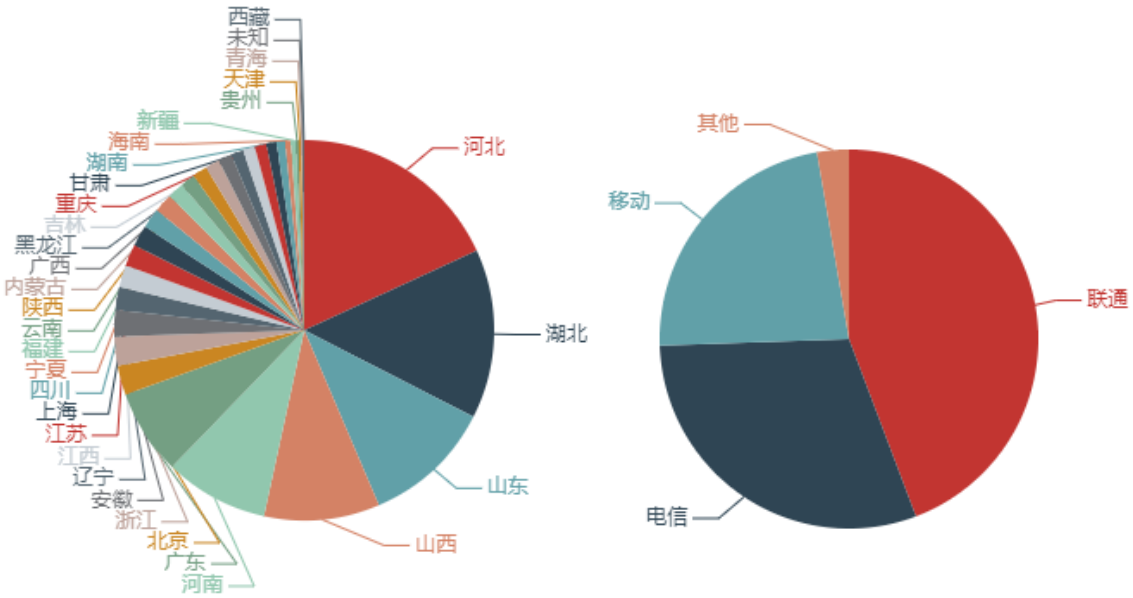

图 10 近两月被持续利用发起攻击的 NTP 反射服务器数量按省份和运营商分布

（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，2019 年 10 月，SSDP 反射攻击事件共涉及境内 840,285 台反射服务器，境外 238,731 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 24.2%，其次是浙江省、吉林省和广东省；按归属运营商统计，联通占的比例最大，占 64.8%，电信占比 33.6%，移动占比 0.7%，如图 11 所示。

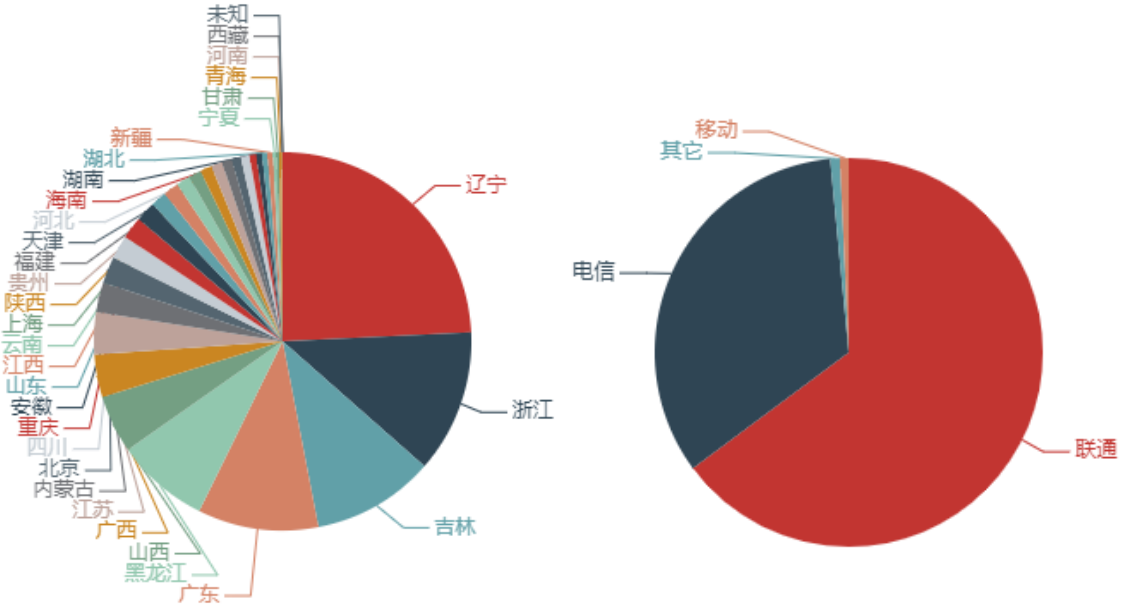

图 11 本月被利用发起 SSDP 反射攻击的境内反射服务器数量按省份和运营商分布

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，俄罗斯占的比例最大，占 16.9%，其次是美国、中国台湾和加拿大，如图 12 所示。

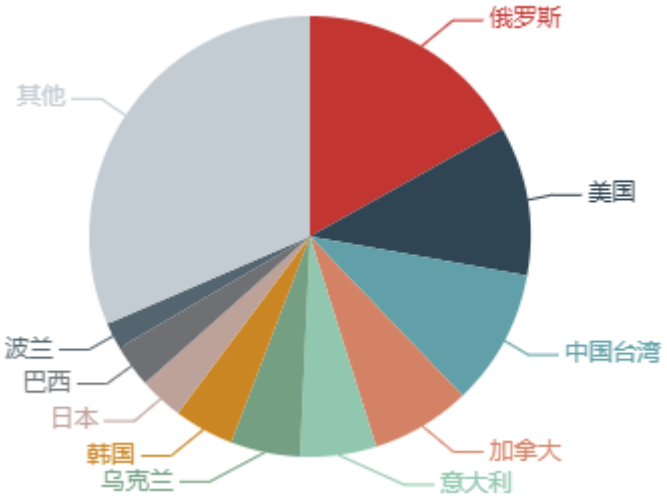

图 12 本月被利用发起 SSDP 反射攻击的境外反射服务器数量按国家或地区分布

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，位于湖南省和陕西省的地址最多。

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
116.XX.XX.222	上海市	电信
59.XX.XX.236	海南省	电信
112.XX.XX.249	安徽省	移动
116.XX.XX.140	上海市	电信
125.XX.XX.83	甘肃省	电信
180.XX.XX.10	上海市	电信
222.XX.XX.245	上海市	电信
58.XX.XX.66	上海市	联通
125.XX.XX.73	上海市	BGP 多线
218.XX.XX.163	湖南省	电信
59.XX.XX.242	山西省	电信
183.XX.XX.236	重庆市	电信
58.XX.XX.226	上海市	联通
183.XX.XX.166	重庆市	电信
222.XX.XX.182	重庆市	电信
222.XX.XX.88	湖南省	电信
117.XX.XX.134	上海市	移动
61.XX.XX.170	重庆市	电信
118.XX.XX.118	甘肃省	电信
220.XX.XX.20	湖南省	电信
61.XX.XX.126	宁夏回族自治区	电信
218.XX.XX.35	湖南省	电信
27.XX.XX.62	上海市	联通
58.XX.XX.154	上海市	联通
218.XX.XX.128	湖南省	电信
112.XX.XX.118	上海市	联通
140.XX.XX.50	上海市	联通
125.XX.XX.193	甘肃省	电信
113.XX.XX.14	广西壮族自治区	电信
116.XX.XX.33	广西壮族自治区	电信

近两月被持续利用发起攻击的 SSDP 反射服务器中，共计 200,092 个在本月仍处于活跃状态，其中 110,705 位于境内，

89,387 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 13.7%，其次是河北省、广东省和湖北省；按运营商统计，联通占的比例最大，占 52.2%，电信占 33.7%，移动占 12.2%，如图 13 所示。

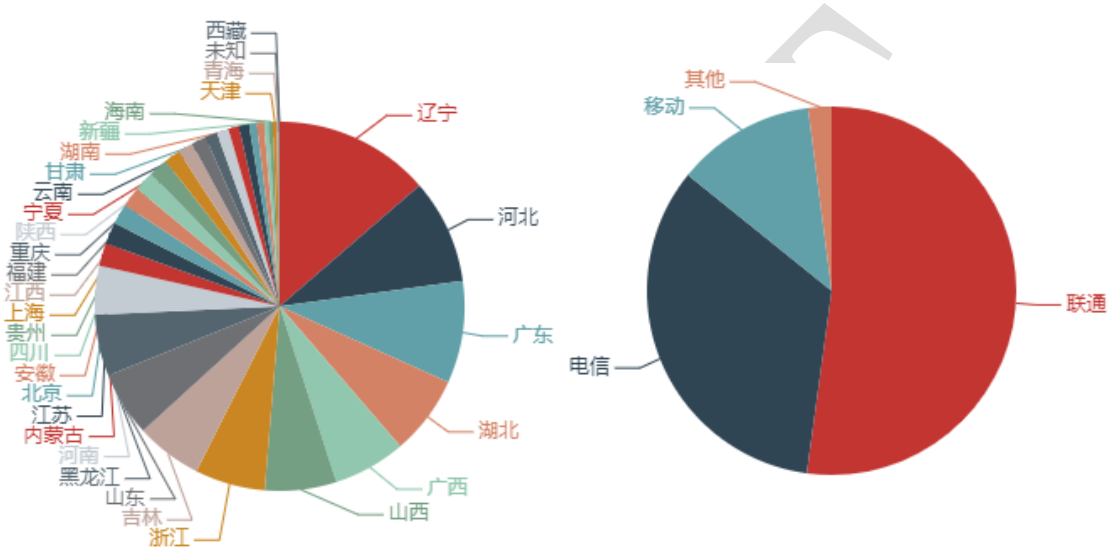

图 13 近两月被持续利用发起攻击的 SSDP 反射服务器数量按省份运营商分布

（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，2019 年 10 月，通过跨域伪造流量发起攻击的流量来源于 24 个路由器。根据参与攻击事件的数量统计，归属于北京市的路由器（202.XX.XX.61 和 202.XX.XX.60）参与的攻击事件数量最多，其次是归属于安徽省移动的路由器（120.XX.XX.247），如表 7 所示。

表 7 本月参与攻击的跨域伪造流量来源路由器

跨域伪造流量来源路由器	归属省份	归属运营商
202.XX.XX.61	北京市	待确认
202.XX.XX.60	北京市	待确认
120.XX.XX.247	安徽省	移动
218.XX.XX.221	福建省	移动
218.XX.XX.5	贵州省	移动
221.XX.XX.253	安徽省	移动
218.XX.XX.213	福建省	移动
218.XX.XX.212	福建省	移动
218.XX.XX.215	福建省	移动
218.XX.XX.214	福建省	移动
120.XX.XX.248	安徽省	移动
218.XX.XX.220	福建省	移动
202.XX.XX.116	天津市	待确认
218.XX.XX.4	贵州省	移动
202.XX.XX.118	天津市	待确认
202.XX.XX.222	四川省	待确认
202.XX.XX.223	四川省	待确认
58.XX.XX.248	湖北省	联通
111.XX.XX.1	青海省	移动
221.XX.XX.7	江苏省	移动
120.XX.XX.8	广东省	联通
202.XX.XX.52	辽宁省	待确认
202.XX.XX.180	辽宁省	待确认
120.XX.XX.8	广东省	联通

跨域伪造流量涉及路由器按省份分布统计，福建省占的比例最大，占 25.0%，其次是安徽省、辽宁省和贵州省；按路由器所属运营商统计，移动占的比例最大，占 43.3%，联通占比 10.0%，电信占比 3.3%，如图 14 所示。

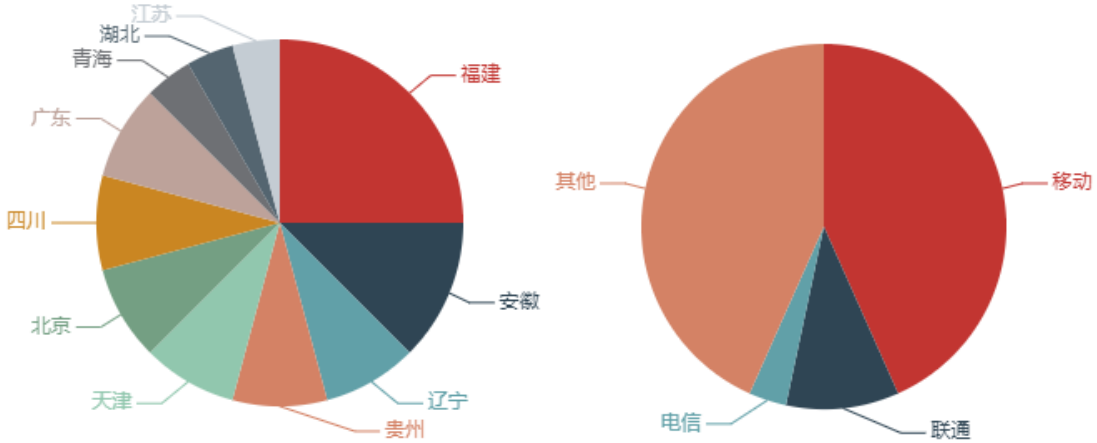

图 14 跨域伪造流量来源路由器数量按省份和运营商分布

2019 年以来被持续利用转发 DDoS 攻击的跨域伪造流量来源路由器中，监测发现有 8 个在本月仍活跃，存活率为 5.1%，分布在天津市、北京市、辽宁省和四川省，均归属电信运营商，如图 15 所示。

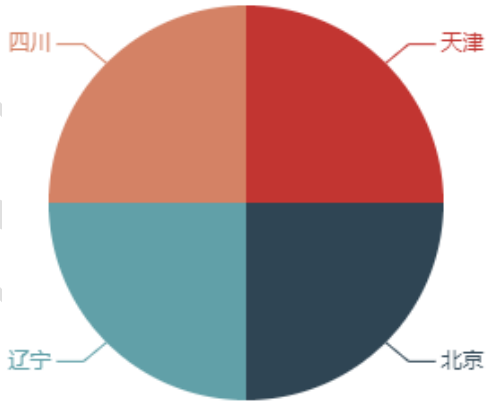

图 15 2019 年被持续利用转发跨域伪造攻击流量本月仍活跃路由器数量按省份分布

2.本地伪造流量来源路由器

根据 CNCERT 抽样监测数据，2019 年 10 月，通过本地伪造流量发起攻击的流量来源于 47 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（220.XX.XX.127 和 220.XX.XX.126）参与的攻击事件数量最多，其次是归属于

四川省电信的路由器（218.XX.XX.129），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
220.XX.XX.127	浙江省	电信
220.XX.XX.126	浙江省	电信
218.XX.XX.129	四川省	电信
202.XX.XX.136	浙江省	电信
202.XX.XX.137	浙江省	电信
218.XX.XX.130	四川省	电信
202.XX.XX.2	四川省	电信
202.XX.XX.65	四川省	电信
61.XX.XX.1	四川省	电信
61.XX.XX.2	浙江省	电信
61.XX.XX.1	浙江省	电信
61.XX.XX.220	浙江省	电信
218.XX.XX.224	福建省	移动
218.XX.XX.225	福建省	移动
218.XX.XX.204	福建省	移动
218.XX.XX.205	福建省	移动
221.XX.XX.189	广东省	移动
221.XX.XX.237	广东省	移动
61.XX.XX.255	江苏省	电信
221.XX.XX.229	广东省	移动
221.XX.XX.6	江苏省	电信
221.XX.XX.5	江苏省	电信
202.XX.XX.65	四川省	电信
202.XX.XX.64	四川省	电信
202.XX.XX.67	四川省	电信

本月本地伪造流量涉及路由器按省份分布，四川省占的比例最大，占 19.2%，其次是福建省、江苏省和广东省；按路由器所属运营商统计，电信占的比例最大，占 66.0%，移动占比 19.2%，联通占比 8.5%，如图 16 所示。

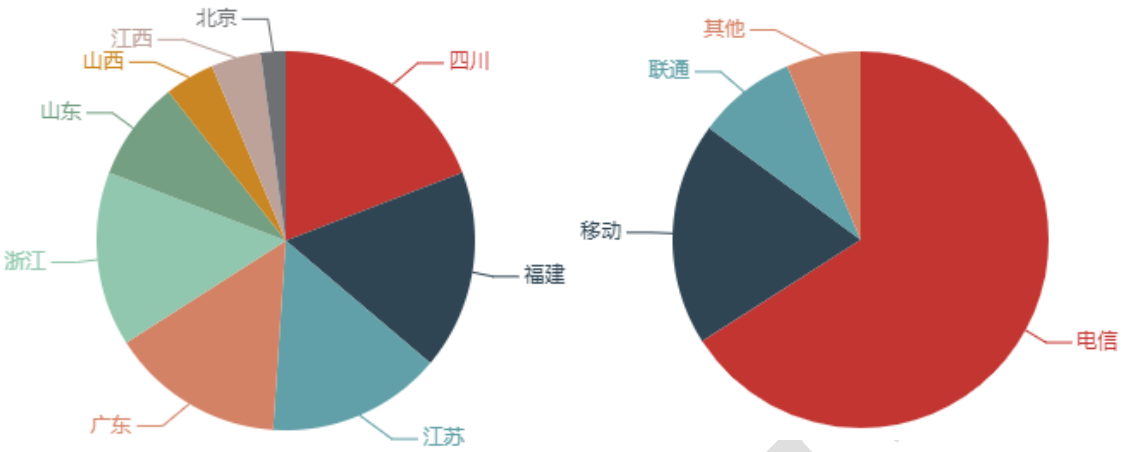

图 16 本月本地伪造流量来源路由器数量按省份和运营商分布

2019 年以来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 42 个在本月仍活跃，存活率为 7.3%。按省份统计，四川省占的比例最大，占 22.0%，其次是福建省、江苏省和浙江省；按路由器所属运营商统计，电信占的比例最大，占 58.2%，移动占比 14.6%，如图 17 所示。

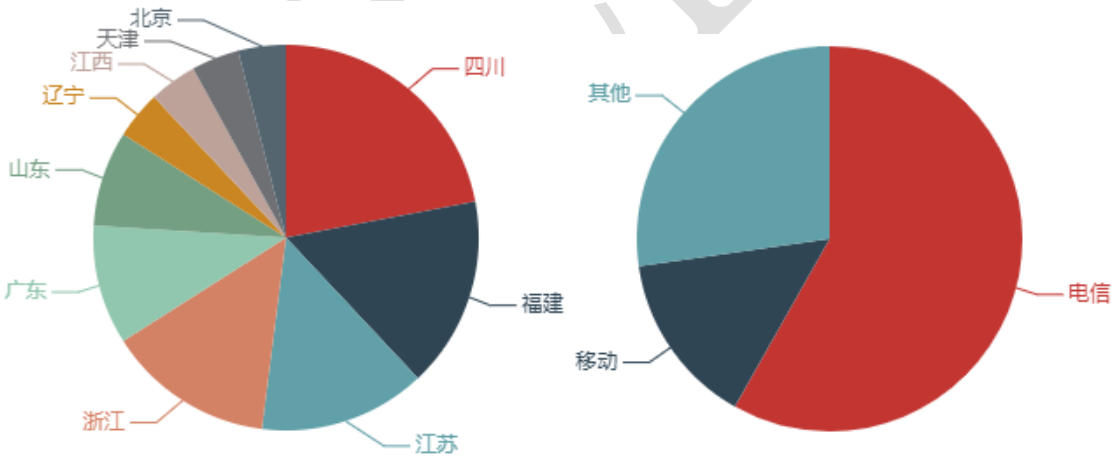

图 17 2019 年被持续利用且本月仍活跃的本地伪造流量来源路由器数量按省份运营商分布