我国 DDoS 攻击资源月度分析报告

(2019 年 3 月)

CNCERT

国家计算机网络应急技术处理协调中心

2019 年 4 月

目 录

CNCERT

一、引言

（一）攻击资源定义

本报告为 2019 年 3 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

除《企业家第一课》、《企业家功成堂》外，其他公众号分享本期资料的，均属于抄袭！

邀请各位读者朋友尊重劳动成果，关注搜索正版号：《企业家第一课》、《企业家功成堂》

谢谢观看！

企业家第一课，专注做最纯粹的知识共享平台

关注官方微信
获取更多干货

加入知识共享平台
一次付费 一年干货

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；境内控制端最多位于江苏省，其次是广东省、辽宁省和浙江省，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、江苏省、河南省和广东省，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，位于河南省、江苏省、福建省占的比例最大。

3、本月被利用发起 Memcached 反射攻击境内反射服务器数量按省份统计排名前三名的省份是河南省、广东省和山东省；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、河北省和湖北省；数量最多的归属运营商是移动。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，归属于天津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，归属于江苏省、北京市和天津市路由器数量最多。

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，2019 年以来被持续利用的本地伪造流量来源路由器中，归属于浙江省、江苏省、广东省和北京市路由器数量最多。

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 3 月，利用肉鸡发起 DDoS 攻击的控制端有 252 个，其中，26 个控制端位于我国境内，226 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 49.1%，其次是中国香港和法国，如图 1 所示。

CNCERT

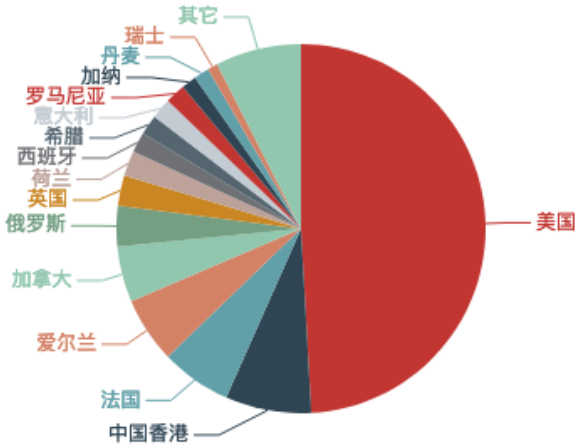

图 1 本月发起 DDoS 攻击的境外控制端数量按国家或地区分布

位于境内的控制端按省份统计，江苏省占的比例最大，占 19.2%，其次是广东省、辽宁省和浙江省；按运营商统计，电信占的比例最大，占 65.4%，联通占 15.4%，移动占 3.8%，如图 2 所示。

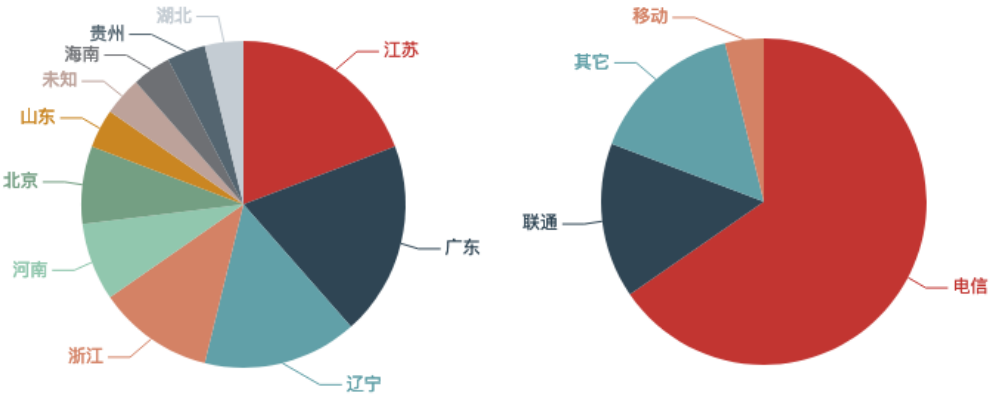

图 2 本月发起 DDoS 攻击的境内控制端数量按省份和运营商分布

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，主要位于广东省。

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
115.X.X.43	浙江省	电信
221.X.X.62	海南省	移动

42.X.X.222	辽宁省	电信
222.X.X.108	江苏省	电信
42.X.X.96	河南省	联通
58.X.X.158	江苏省	电信
101.X.X.25	浙江省	联通
183.X.X.26	广东省	电信
118.X.X.194	北京市	电信
120.X.X.114	浙江省	阿里云
101.X.X.113	广东省	阿里云
123.X.X.198	贵州省	电信
59.X.X.88	北京市	阿里云
61.X.X.82	江苏省	电信
122.X.X.135	河南省	联通
14.X.X.168	广东省	电信
59.X.X.237	辽宁省	电信
117.X.X.204	北京市	待确认
118.X.X.207	广东省	电信
118.X.X.156	广东省	电信

2019 年至今监测到的控制端中，25.2%的控制端在本月仍处于活跃状态，共计 49 个，其中位于我国境内的控制端数量为 4 个，位于境外的控制端数量为 45 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**
118.X.X.207	广东省	电信
120.X.X.114	浙江省	阿里云
118.X.X.156	广东省	电信
118.X.X.194	北京市	电信

（二）肉鸡资源分析

根据 CNCERT 抽样监测数据，2019 年 3 月，共有 204,299 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

12.5%，其次是江苏省、河南省和广东省；按运营商统计，电信占的比例最大，为 68.4%，联通占 20.7%，移动占 7.7%，如图 3 所示。

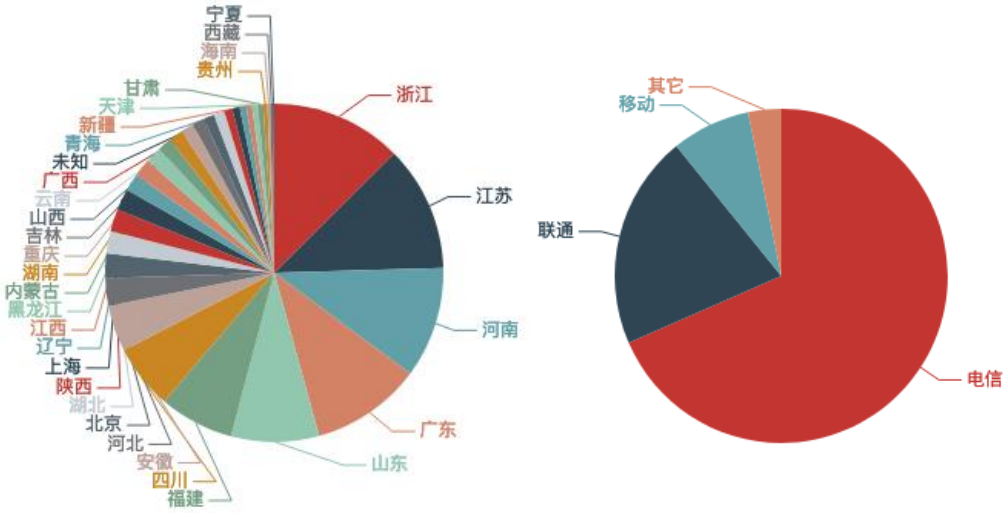

图 3 本月肉鸡地址数量按省份和运营商分布

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，位于浙江省的地址最多。

表 3 本月参与攻击最多的肉鸡地址 TOP20

肉鸡地址	归属省份	归属运营商或云服务商
36.X.X.125	内蒙古自治区	电信
122.X.X.10	湖北省	联通
103.X.X.3	天津市	电信
183.X.X.226	浙江省	电信
183.X.X.98	浙江省	电信
121.X.X.99	广西壮族自治区	联通
61.X.X.114	浙江省	电信
210.X.X.170	北京市	联通
183.X.X.86	浙江省	电信
140.X.X.138	北京市	腾讯云
59.X.X.240	辽宁省	电信
223.X.X.3	北京市	移动
58.X.X.118	湖北省	电信
140.X.X.29	北京市	联通
122.X.X.61	浙江省	电信
103.X.X.154	北京市	待确认
183.X.X.99	浙江省	电信

36.X.X.7	北京市	电信
118.X.X.31	天津市	电信
122.X.X.218	浙江省	电信

2019 年至今监测到的肉鸡资源中，共计 55,970 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 53,151 个，位于境外的肉鸡数量为 2,819 个。2019 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。

表 4 2019 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
36.X.X.125	内蒙古自治区	电信
122.X.X.10	湖北省	联通
113.X.X.16	陕西省	电信
218.X.X.249	广西壮族自治区	电信
14.X.X.41	广东省	电信
112.X.X.170	广东省	联通
58.X.X.131	广东省	联通
120.X.X.50	广东省	联通
14.X.X.241	广东省	电信
112.X.X.51	广东省	联通
113.X.X.167	湖北省	联通
119.X.X.89	广东省	电信
183.X.X.50	湖北省	联通
118.X.X.139	吉林省	联通
183.X.X.60	广东省	电信
120.X.X.229	宁夏回族自治区	移动
111.X.X.53	吉林省	移动
122.X.X.110	吉林省	联通
59.X.X.2	辽宁省	电信
117.X.X.17	江西省	电信

2019 年至今持续活跃的境内肉鸡资源按省份统计，河南省占的比例最大，占 23.3%，其次是江苏省、福建省和安徽省；按运营商统计，电信占的比例最大，占 82.6%，联通占 11.3%，移动占 2.6%，如图 4 所示。

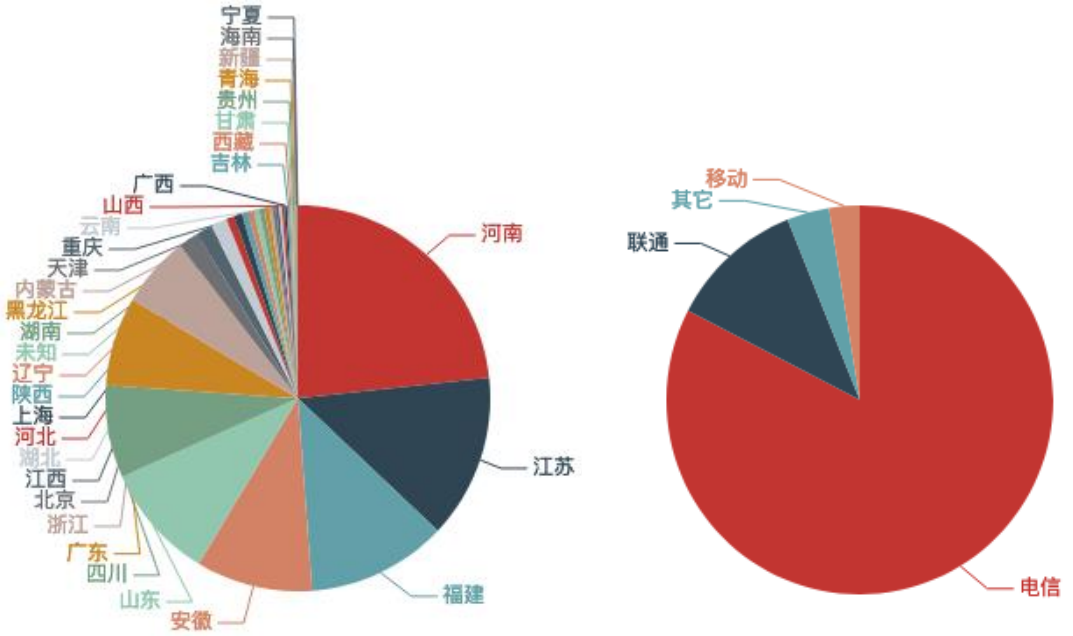

图 4 2019 年以来持续活跃的肉鸡数量按省份和运营商分布

（三）反射攻击资源分析

根据 CNCERT 抽样监测数据，2019 年 3 月，利用反射服务器发起的三类重点反射攻击共涉及 1,303,733 台反射服务器，其中境内反射服务器 946,672 台，境外反射服务器 357,061 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 10,203 台，占比 0.8%，其中境内反射服务器 7,096 台，境外反射服务器 3,107 台；利用 NTP 反射发起反射攻击的反射服务器有 573,453 台，占比 44.0%，其中境内反射服务器 394,888 台，境外反射服务器 178,565 台；利用 SSDP 反射发起反射攻击的反射服务器有 720,076 台，占比 55.2%，其中境内反射服务器 544,688 台，境外反射服务器 175,388 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 3 月，利用 Memcached 服务器实施反射攻击的事件共涉及境内 7,096 台反射服务器，境外 3,107 台反射服务器。

本月境内 Memcached 反射服务器数量按省份统计，河南省占的比例最大，占 28.9%，其次是广东省、山东省和浙江省；按归属运营商或云服务商统计，电信占的比例最大，占 50.0%，移动占比 21.6%，联通占比 17.1%，阿里云占比 6.8%，如图 5 所示。

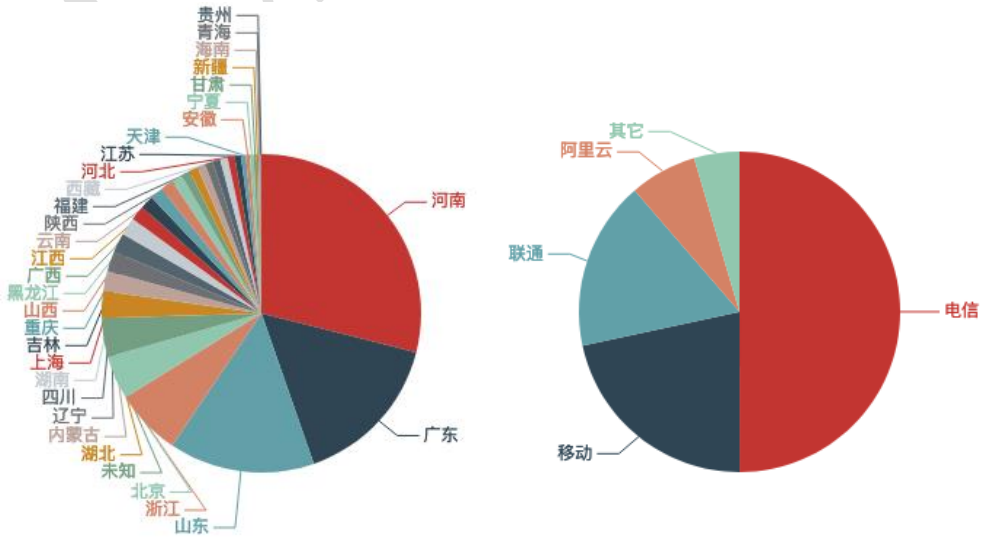

图 5 本月境内 Memcached 反射服务器数量按省份、运营商或云服务商分布

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 29.1%，其次是中国香港、俄罗斯和法国，如图 6 所示。

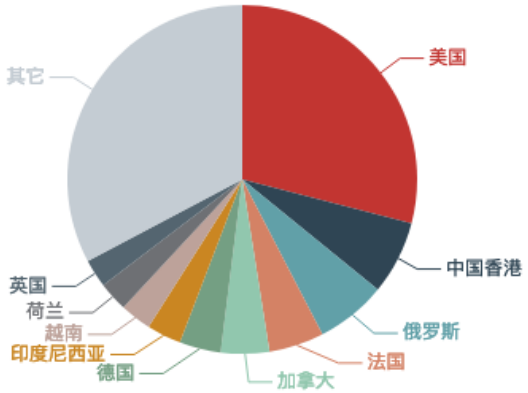

图 6 本月境外反射服务器数量按国家或地区分布

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 5 所示，位于广东省的地址最多。

表 5 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
115.X.X.149	浙江省	电信
113.X.X.112	广东省	电信
123.X.X.195	北京市	阿里云
182.X.X.75	北京市	阿里云
116.X.X.10	云南省	电信
222.X.X.246	湖南省	电信
123.X.X.233	北京市	阿里云
218.X.X.12	江西省	电信
182.X.X.200	广东省	电信
116.X.X.67	广东省	联通
123.X.X.153	北京市	阿里云
119.X.X.15	广东省	阿里云
118.X.X.156	浙江省	阿里云

123.X.X.237	北京市	阿里云
120.X.X.76	广东省	阿里云
123.X.X.174	北京市	阿里云
120.X.X.82	浙江省	阿里云
101.X.X.90	北京市	阿里云
112.X.X.12	广东省	阿里云
112.X.X.77	浙江省	电信
123.X.X.251	北京市	阿里云
123.X.X.6	北京市	阿里云
112.X.X.84	北京市	阿里云
120.X.X.62	广东省	阿里云
121.X.X.249	浙江省	电信
120.X.X.36	浙江省	阿里云
120.X.X.159	广东省	阿里云
121.X.X.37	浙江省	阿里云
123.X.X.128	北京市	阿里云
120.X.X.56	广东省	阿里云

近两月被利用发起攻击的 Memcached 反射服务器中，共计 3,031 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，广东省占的比例最大，占 23.4%，其次是山东省、浙江省、北京市和上海市；按运营商或云服务统计，电信占的比例最大，占 24.9%，阿里云占 24.4%，移动占 19.9%，联通占 19.7%，如图 7 所示。

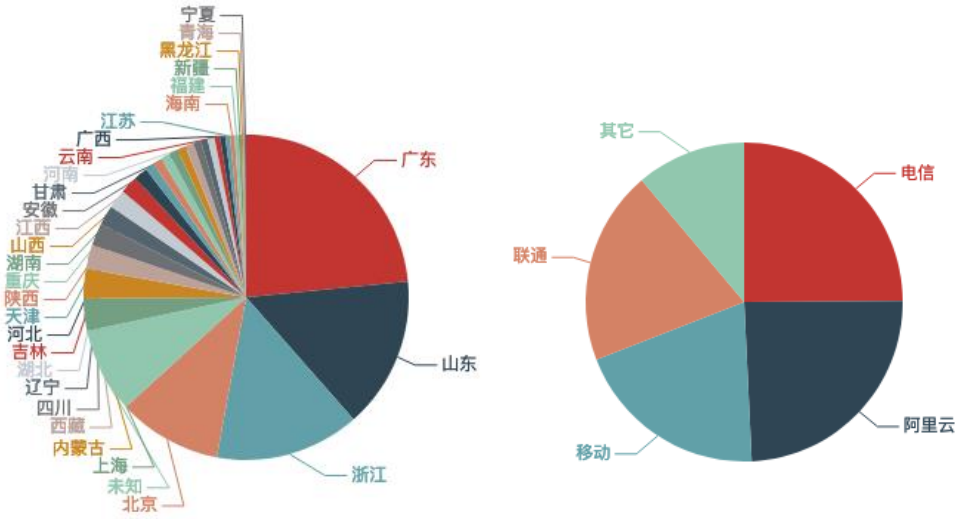

图 7 近两月被持续利用发起攻击的 Memcached 反射服务器数量按省份运营商或云服务商分布

（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，2019 年 3 月，NTP 反射攻击事件共涉及我国境内 394,888 台反射服务器，境外 178,565 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 28.0%，其次是河北省、湖北省和河南省；按归属运营商统计，移动占的比例最大，占 41.9%，联通占比 40.7%，电信占比 17.0%，如图 8 所示。

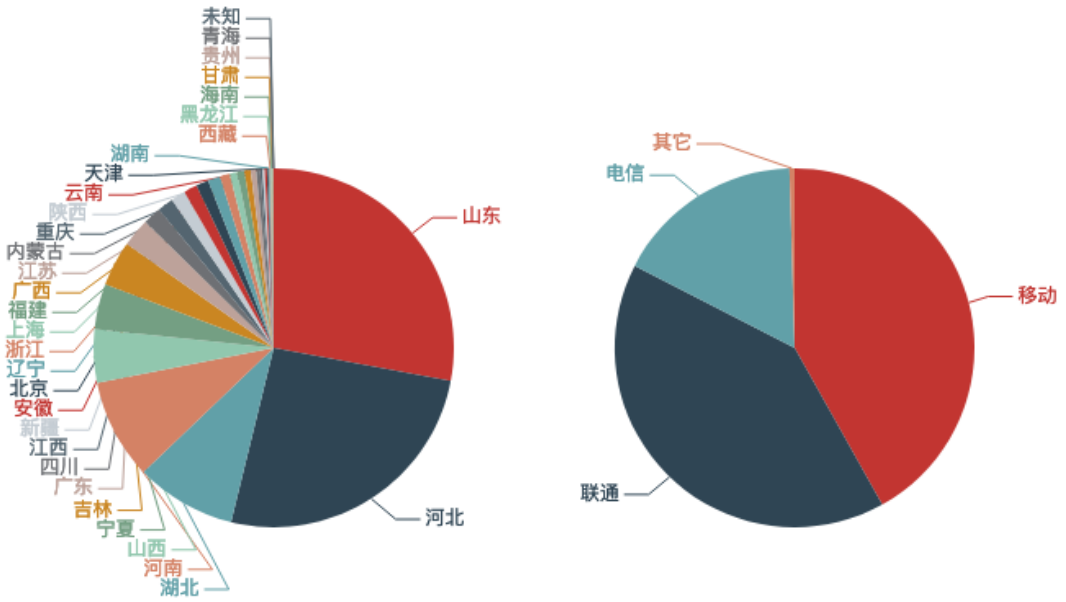

图 8 本月被利用发起 NTP 反射攻击的境内反射服务器数量按省份和运营商分布

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 50.4%，其次是澳大利亚、巴西和美国，如图 9 所示。

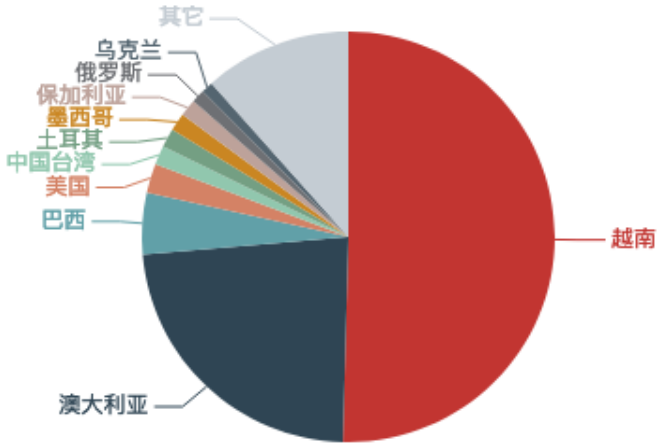

图 9 本月被利用发起 NTP 反射攻击的境外反射服务器数量按国家或地区分布

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 6 所示，位于山西省的地址最多。

表 6 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
111.X.X.70	山西省	移动
119.X.X.50	宁夏回族自治区	电信
211.X.X.146	山西省	移动
223.X.X.123	山东省	移动
120.X.X.149	广东省	移动
218.X.X.101	山东省	移动
111.X.X.206	山西省	移动
211.X.X.66	山西省	移动
111.X.X.245	山西省	移动
120.X.X.99	安徽省	移动
112.X.X.92	山东省	移动

211.X.X.85	山西省	移动
211.X.X.150	山西省	移动
211.X.X.234	山西省	移动
120.X.X.125	安徽省	移动
223.X.X.173	山东省	移动
183.X.X.29	山西省	移动
111.X.X.14	山西省	移动
112.X.X.58	山东省	移动
112.X.X.209	安徽省	移动
112.X.X.24	山东省	移动
183.X.X.235	山西省	移动
111.X.X.30	山西省	移动
111.X.X.21	山西省	移动
211.X.X.54	山西省	移动
120.X.X.28	安徽省	移动
112.X.X.197	安徽省	移动
112.X.X.254	安徽省	移动
111.X.X.217	山西省	移动
112.X.X.80	安徽省	移动

近两月被持续利用发起攻击的 NTP 反射服务器中，共计 256,756 个在本月仍处于活跃状态，其中 184,446 个位于境内，72,310 个位于境外。持续活跃的 NTP 反射服务器按省份统计，山东省占的比例最大，占 31.1%，其次是河北省、湖北省和河南省；按运营商统计，移动占的比例最大，占 45.8%，联通占 38.2%，电信占 15.5%，如图 10 所示。

CNCERT

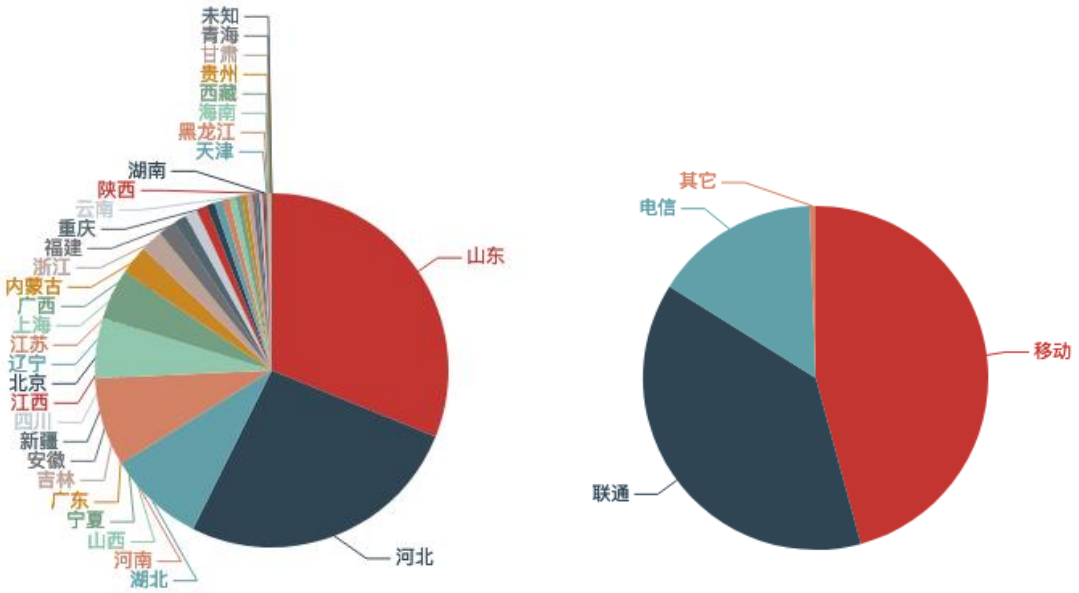

图 10 近两月被持续利用发起攻击的 NTP 反射服务器数量按省份运营商分布

（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，2019 年 3 月，SSDP 反射攻击事件共涉及境内 544,688 台反射服务器，境外 175, 388 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 23.1%，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

63.5%，电信占比 35.0%，移动占比 1.1%，如图 11 所示。

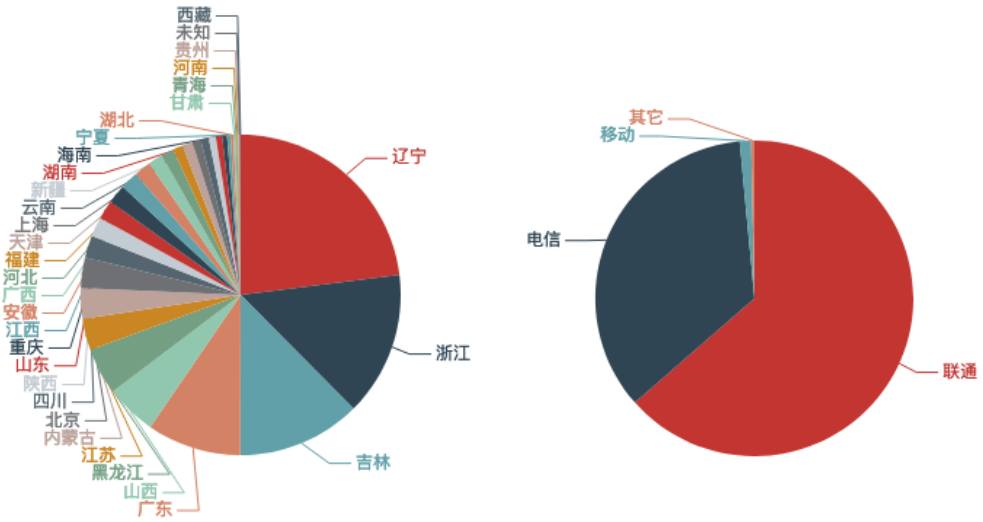

图 11 本月被利用发起 SSDP 反射攻击的境内反射服务器数量按省份和运营商分布

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 19.1%，其次是美国、加拿大和中国台湾，如图 12 所示。

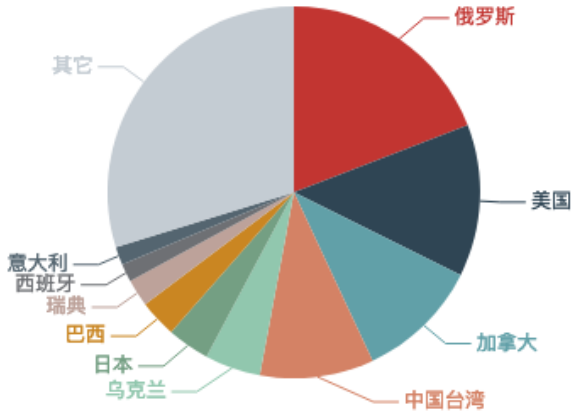

图 12 本月被利用发起 SSDP 反射攻击的境外反射服务器数量按国家或地区分布

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 7 所示，位于广东省的地址最多。

表 7 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
113.X.X.59	广东省	电信
220.X.X.215	云南省	电信
219.X.X.126	陕西省	电信
113.X.X.150	广东省	电信
60.X.X.213	云南省	电信
113.X.X.134	广东省	电信
222.X.X.46	重庆市	电信
113.X.X.9	广东省	电信
222.X.X.78	陕西省	电信
60.X.X.65	云南省	电信
60.X.X.206	云南省	电信
61.X.X.66	广东省	电信
222.X.X.209	云南省	电信
124.X.X.102	吉林省	电信
218.X.X.188	广东省	电信
219.X.X.76	陕西省	电信
121.X.X.189	广东省	电信
222.X.X.231	重庆市	电信
222.X.X.69	重庆市	电信
219.X.X.164	陕西省	电信
119.X.X.162	广东省	电信
124.X.X.194	陕西省	电信
61.X.X.44	陕西省	电信
61.X.X.98	陕西省	电信
125.X.X.54	四川省	电信
110.X.X.50	新疆维吾尔自治区	电信
220.X.X.118	云南省	电信
222.X.X.130	重庆市	电信
222.X.X.198	重庆市	电信
119.X.X.226	广东省	电信

近两月被持续利用发起攻击的 SSDP 反射服务器中，共计 171,579 个在本月仍处于活跃状态，其中 73,793 位于境内，97,786 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 16.2%，其次是浙江省、广东省和吉林省；按运营商统计，联通占的比例最大，占 54.1%，电信占 40.1%，移动占 4.8%，如图 13 所

示。

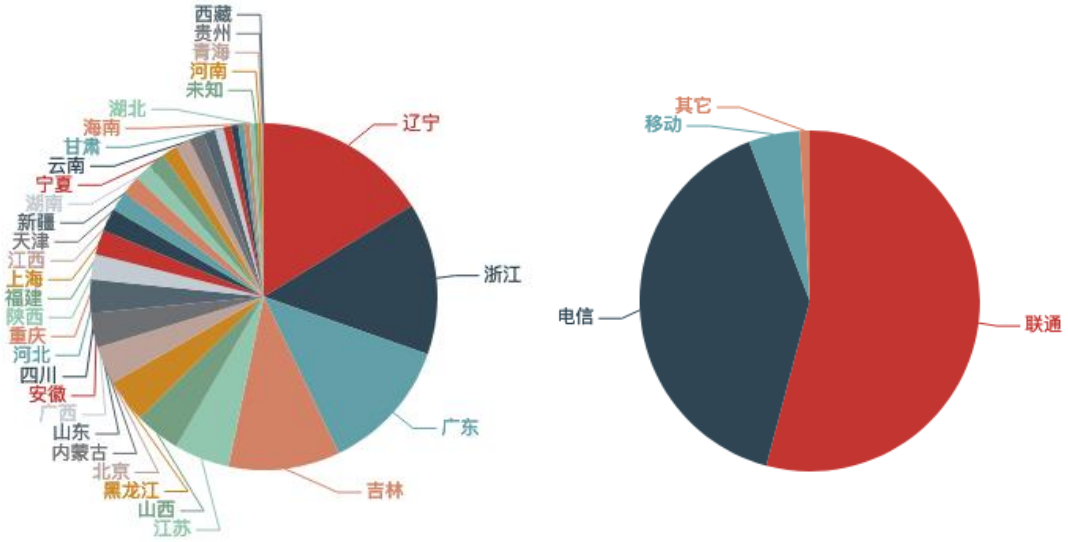

图 13 近两月被持续利用发起攻击的 SSDP 反射服务器数量按省份运营商分布

（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 3 月，通过跨域伪造流量发起攻击的流量来源于 85 个路由器。根据参与攻击事件的数量统计，归属于天津市的路由器（202.X.X.118）参与的攻击事件数量最多，其次是归属于北京市电信的路由器（220.X.X.243、220.X.X.253、219.X.X.70），如表 8 所示。

表 8 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
202.X.X.118	天津市	待确认
220.X.X.243	北京市	电信
220.X.X.253	北京市	电信
219.X.X.70	北京市	电信
202.X.X.116	天津市	待确认
221.X.X.254	新疆维吾尔自治区	联通
218.X.X.2	云南省	电信
218.X.X.1	云南省	电信
221.X.X.1	天津市	电信

221.X.X.2	天津市	电信
117.X.X.2	天津市	联通
117.X.X.1	天津市	联通
218.X.X.138	湖北省	联通
202.X.X.222	集团	电信
202.X.X.223	集团	电信
202.X.X.192	江苏省	待确认
202.X.X.193	江苏省	待确认
221.X.X.191	广东省	移动
202.X.X.205	重庆市	电信
202.X.X.204	重庆市	电信
211.X.X.4	湖南省	移动
211.X.X.3	湖南省	移动
221.X.X.229	广东省	移动
202.X.X.136	浙江省	电信
202.X.X.137	浙江省	电信

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 16.5%，其次是江苏省和广东省；按路由器所属运营商统计，电信占的比例最大，占 41.4%，移动占比 25.3%，联通占比 16.1%，如图 14 所示。

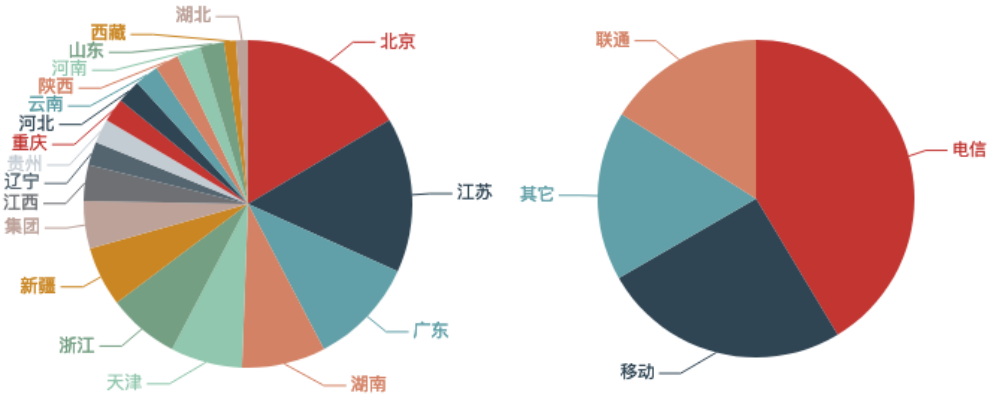

图 14 跨域伪造流量来源路由器数量按省份和运营商分布

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 59 个在本月仍活跃，存活率为 44.7%。按省份分布统计，江苏省占的比例最大，占 22.0%，

其次是北京市和天津市；按路由器所属运营商统计，电信占的比例最大，占 39.3%，移动占比 24.6%，联通占比 14.8%，如图 15 所示。

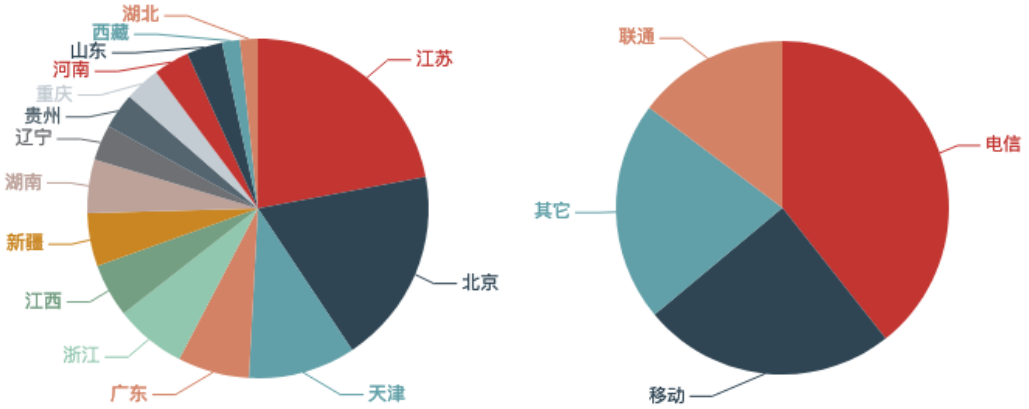

图 15 2019 年被持续利用转发跨域伪造攻击流量本月仍活跃路由器数量按省份和运营商分布

2. 本地伪造流量来源路由器

根据 CNCERT 抽样监测数据，2019 年 3 月，通过本地伪造流量发起攻击的流量来源于 184 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.4、61.X.X.8）参与的攻击事件数量最多，其次是归属于浙江省移动的路由器（211.X.X.225、211.X.X.224），如表 9 所示。

表 9 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.4	浙江省	电信
61.X.X.8	浙江省	电信
211.X.X.225	江西省	移动
211.X.X.224	江西省	移动
220.X.X.126	浙江省	电信
220.X.X.127	浙江省	电信
211.X.X.3	浙江省	移动
202.X.X.136	浙江省	电信
202.X.X.137	浙江省	电信
202.X.X.161	浙江省	电信
202.X.X.160	浙江省	电信

211.X.X.8	浙江省	移动
59.X.X.1	广东省	电信
119.X.X.9	广东省	电信
218.X.X.129	四川省	电信
118.X.X.168	四川省	电信
118.X.X.169	四川省	电信
202.X.X.64	四川省	电信
202.X.X.65	四川省	电信
211.X.X.2	浙江省	移动
183.X.X.254	广东省	电信
221.X.X.1	云南省	联通
183.X.X.254	广东省	电信
183.X.X.254	广东省	电信
218.X.X.2	云南省	电信

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 16.3%，其次是浙江省、广东省和内蒙古自治区；按路由器所属运营商统计，电信占的比例最大，占 43.2%，移动占比 27.0%，联通占比 14.6%，如图 16 所示。

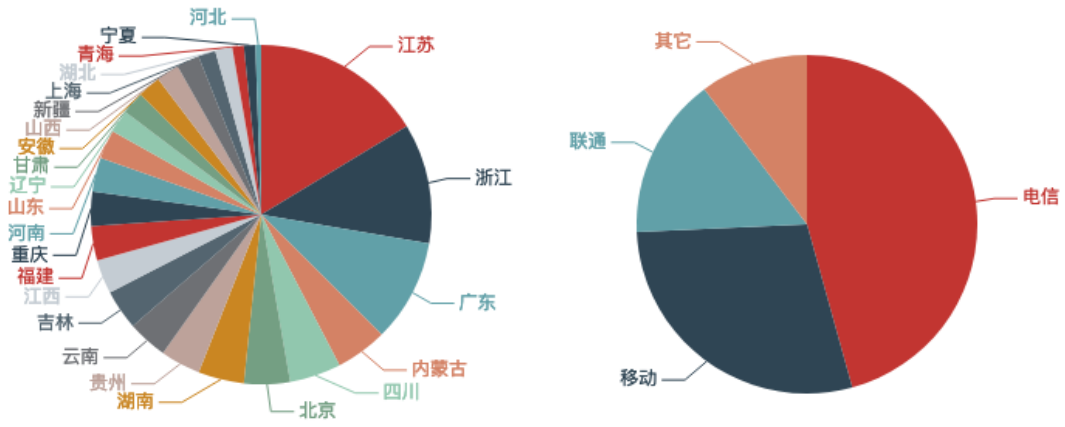

图 16 本月本地伪造流量来源路由器数量按省份和运营商分布

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 113 个在本月仍活跃，存活率为 51.1%。按省份统计，浙江省占的比例最大，占 18.6%，其次是江苏省、广东省和北京市；按路由器所属运营商统计，电信占的比例最

大，占 60.5%，移动占比 21.9%，联通占比 5.3%，如图 17 所示。

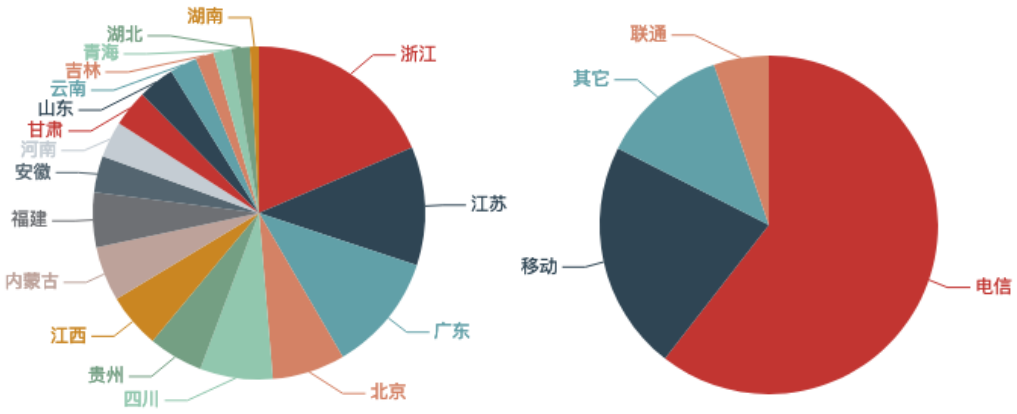

图 17 2019 年被持续利用且本月仍活跃的本地伪造流量来源路由器数量按省份运营商分布

CNCERT