我国 DDoS 攻击资源月度
及 2018 年上半年治理情况分析报告

（2018 年 6 月）

国家计算机网络应急技术处理协调中心

2018 年 6 月

目 录

一、引言

（一）攻击资源定义

本报告为 2018 年 6 月份的 DDoS 攻击资源月度分析及半年治理情况分析报告。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）重点关注情况

1、本月利用肉鸡发起 DDoS 攻击的控制端中，境外控制端近一半位于美国；境内控制端最多位于北京市，其次是浙江省、河南省和贵州省，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北京市、贵州省、四川省和云南省，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，位于山东省、上海市、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按省份统计排名前三名的省份是山东省、广东省和北京市，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广东省、山东省和甘肃省；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、江苏省和河南省；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，归属于新疆维吾尔自治区移动的某路由器参与的攻击事件数量最多；北京市、江苏省和山东省的跨域伪造来源路由器数量最多。

5、本月转发伪造本地攻击流量的路由器中，归属于山西省电信的某路由器参与的攻击事件数量最多；江苏省、山西省、陕西省和广东省的本地伪造流量来源路由器数量最多。

6、经过半年来针对我国境内的攻击资源的专项治理工作，境内控制端、肉鸡等资源的月活跃数量较 2017 年有了较明显的下降趋势；境内控制端、跨域伪造流量来源路由器、本地伪造流量来源路由器等资源近三个月每月的新增率、消亡率相比 2017 年月度平均数值有一定程度的上升，意味着资源变化速度加快，可被利用的资源稳定性降低；境内反射服务器资源每月的新增率、消亡率相比 2017 年月度平均数值，新增率变化不明显、消亡率呈现一定程度的下降，意味着可利用的资源数量逐步减少。

二、DDoS 攻击资源月度分析

（一）控制端资源分析

根据 CNCERT 抽样监测数据，2018 年 6 月，利用肉鸡发起

DDoS 攻击的控制端有 277 个，其中，28 个控制端位于我国境内，249 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 42.6%，其次是法国和中国香港，如图 1 所示。

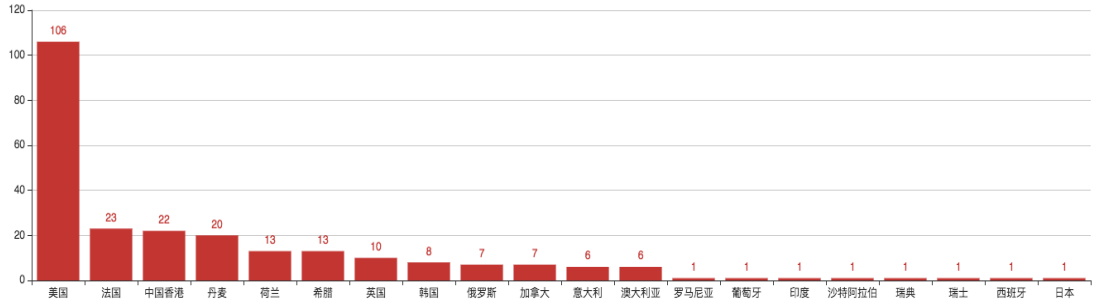

图 1 本月发起 DDoS 攻击的境外控制端数量按国家或地区分布

位于境内的控制端按省份统计，北京市占的比例最大，占 28.6%，其次是浙江省、河南省和贵州省；按运营商统计，电信占的比例最大，占 53.6%，联通占 14.3%，如图 2 所示。

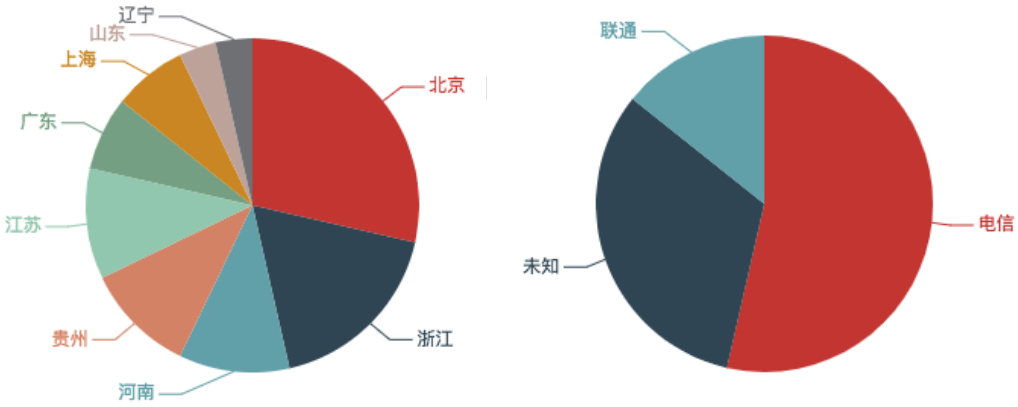

图 2 本月发起 DDoS 攻击的境内控制端数量按省份和运营商分布

发起攻击最多的境内控制端前二十名及归属如表 1 所示，主要位于江苏省和浙江省。

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

123.X.X.143	贵州省	电信
222.X.X.88	江苏省	电信
123.X.X.28	贵州省	电信
118.X.X.50	广东省	电信
115.X.X.105	浙江省	电信
42.X.X.152	河南省	联通
14.X.X.241	广东省	电信
114.X.X.150	北京市	电信
139.X.X.51	上海市	阿里云
61.X.X.112	江苏省	电信
119.X.X.73	山东省	联通
42.X.X.198	河南省	联通
123.X.X.85	贵州省	电信
42.X.X.193	河南省	联通
118.X.X.246	辽宁省	腾讯云
122.X.X.165	浙江省	电信
115.X.X.74	浙江省	电信
115.X.X.191	浙江省	电信
182.X.X.227	上海市	腾讯云
114.X.X.239	北京市	电信

2018 年 1 月至今监测到的控制端中，4.7%的控制端在本月仍处于活跃状态，共计 69 个，其中位于我国境内的控制端数量为 33 个，位于境外的控制端数量为 36 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**
14.X.X.173	云南省	联通
211.X.X.156	湖北省	联通
218.X.X.30	黑龙江省	联通
121.X.X.62	浙江省	电信
42.X.X.104	辽宁省	联通
113.X.X.35	广东省	电信
115.X.X.39	浙江省	电信
220.X.X.164	天津市	联通
123.X.X.169	山东省	联通
61.X.X.60	河南省	联通
117.X.X.110	陕西省	电信
183.X.X.75	浙江省	电信

183.X.X.19	浙江省	电信
139.X.X.174	吉林省	联通
115.X.X.206	浙江省	电信
117.X.X.199	陕西省	电信
222.X.X.48	江苏省	电信
111.X.X.158	北京市	联通
27.X.X.34	山东省	联通
111.X.X.159	北京市	联通
123.X.X.153	山东省	联通
117.X.X.112	江西省	电信
101.X.X.195	北京市	电信
61.X.X.89	河南省	联通
111.X.X.196	江西省	电信
117.X.X.207	陕西省	电信
117.X.X.107	江西省	电信
113.X.X.149	重庆市	联通
175.X.X.203	湖南省	电信
121.X.X.108	河北省	联通
61.X.X.201	江苏省	电信
183.X.X.41	浙江省	电信
183.X.X.35	浙江省	电信

2018 年 1 月至今持续活跃的境内控制端按省份统计，浙江省所占比例最大，为 21.2%；按运营商统计，电信占的比例最大，为 54.5%，联通占 45.5%，如图 3 所示。

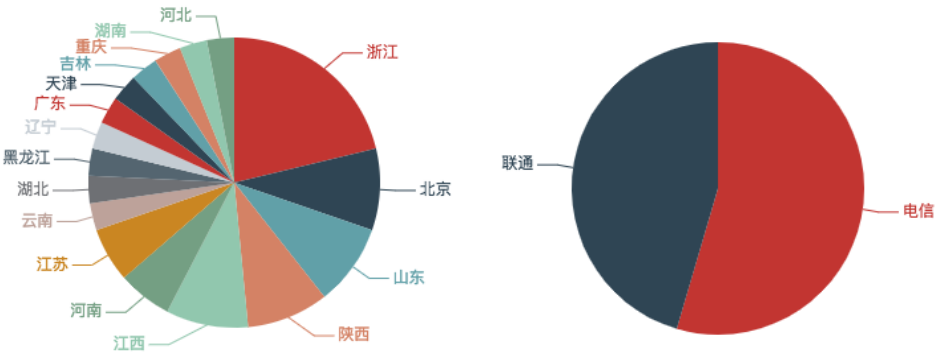

图 3 2018 年以来持续活跃发起 DDoS 攻击的境内控制端数量按省份和运营商分布

（二）肉鸡资源分析

根据 CNCERT 抽样监测数据，2018 年 6 月，共有 117,690

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，北京市占的比例最大，为 7.9%，其次是贵州省、四川省和云南省；按运营商统计，电信占的比例最大，为 54.0%，联通占 25.7%，移动占 17.5%，如图 4 所示。

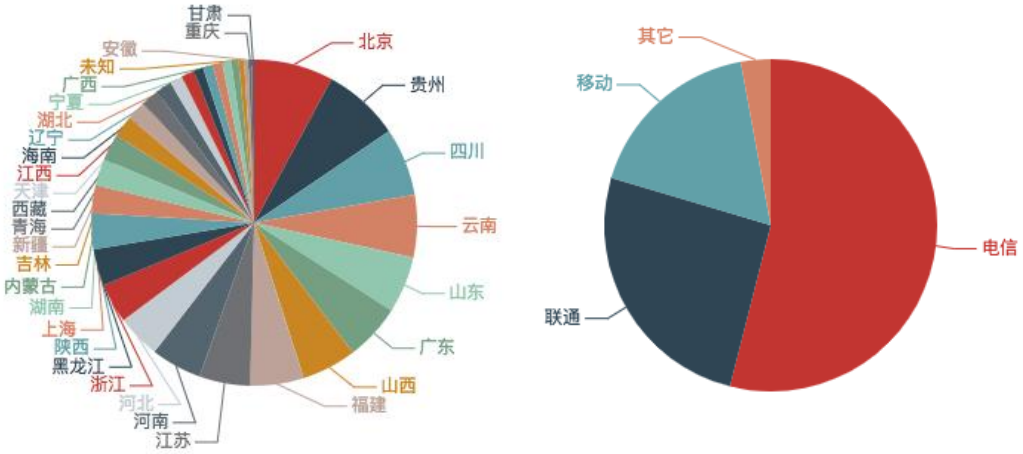

图 4 本月肉鸡地址数量按省份和运营商分布

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，位于山西省的地址最多。

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
58.X.X.148	山东省	电信
124.X.X.2	山西省	联通
123.X.X.32	内蒙古自治区	电信
122.X.X.199	河南省	联通
183.X.X.66	山西省	移动
111.X.X.2	山西省	移动
58.X.X.12	山东省	电信
60.X.X.211	山西省	联通
106.X.X.223	新疆维吾尔族自治区	电信
124.X.X.2	河南省	联通
118.X.X.101	四川省	电信
112.X.X.146	安徽省	联通

111.X.X.53	吉林省	移动
114.X.X.253	北京市	待确认
116.X.X.243	河南省	联通
125.X.X.214	北京市	联通
119.X.X.110	宁夏回族自治区	电信
39.X.X.51	江西省	移动
61.X.X.114	河南省	联通
114.X.X.11	北京市	联通

2018 年 1 月至今监测到的肉鸡资源中，共计 14,451 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 11,620 个，位于境外的肉鸡数量为 2,831 个。2018 年 1 月至今被持续利用发起 DDoS 攻击最多的肉鸡 TOP20 及归属如表 4 所示，位于山西省的地址最多。

表 42018 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**
58.X.X.148	山东省	电信
124.X.X.2	山西省	联通
123.X.X.32	内蒙古自治区	电信
122.X.X.199	河南省	联通
183.X.X.66	山西省	移动
111.X.X.2	山西省	移动
60.X.X.211	山西省	联通
106.X.X.223	新疆维吾尔族自治区	电信
124.X.X.2	河南省	联通
118.X.X.101	四川省	电信
112.X.X.146	安徽省	联通
111.X.X.53	吉林省	移动
114.X.X.253	北京市	待确认
116.X.X.243	河南省	联通
39.X.X.51	江西省	移动
61.X.X.114	河南省	联通
114.X.X.11	北京市	联通
183.X.X.15	北京市	待确认
122.X.X.13	河南省	电信
61.X.X.28	甘肃省	电信

2018 年 1 月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 11.6%，其次是山东省、四川省和广东省；按运营商统计，电信占的比例最大，占 63.1%，联通占 15.2%，移动占 12.4%，如图 5 所示。

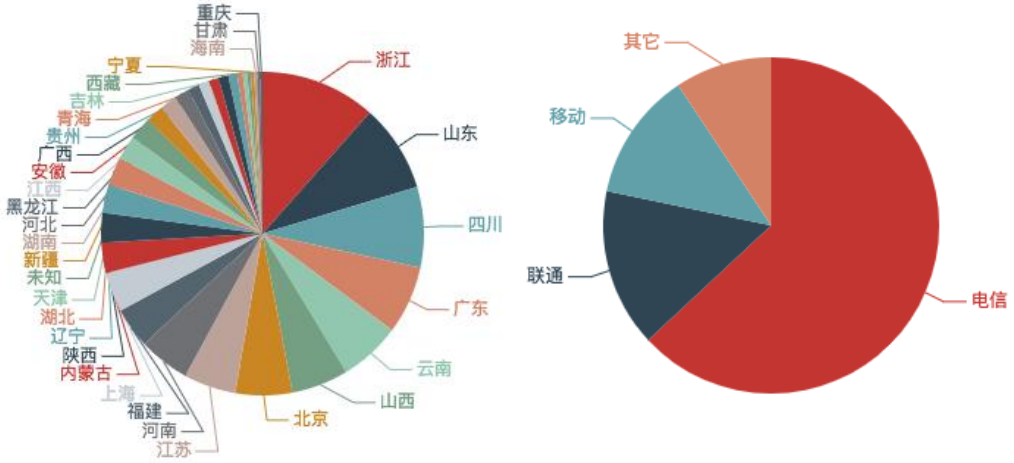

图 5 2018 年以来持续活跃的肉鸡数量按省份和运营商分布

（三）反射攻击资源分析

根据 CNCERT 抽样监测数据，2018 年 6 月，利用反射服务器发起的三类重点反射攻击共涉及 3,689,197 台反射服务器，其中境内反射服务器 3,451,932 台，境外反射服务器 237,265 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 16,055 台，占比 0.4%，其中境内反射服务器 13,410 台，境外反射服务器 2,645 台；利用 NTP 反射发起反射攻击的反射服务器有 772,835 台，占比 20.9%，其中境内反射服务器 754,496 台，境外反射服务器 18,339 台；利用 SSDP 反射发起反射攻击的反射服务器有 2,900,307 台，占比 78.6%，其中境

内反射服务器 2,684,026 台，境外反射服务器 216,281 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 6 月，利用 Memcached 服务器实施反射攻击的事件共涉及境内 13,410 台反射服务器，境外 2,645 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 15.3%，其次是广东省、北京市和浙江省；按归属运营商或云服务商统计，电信占的比例最大，占 36.7%，移动占比 25.9%，联通占比 20.6%，阿里云占比 8.4%，如图 6 所示。

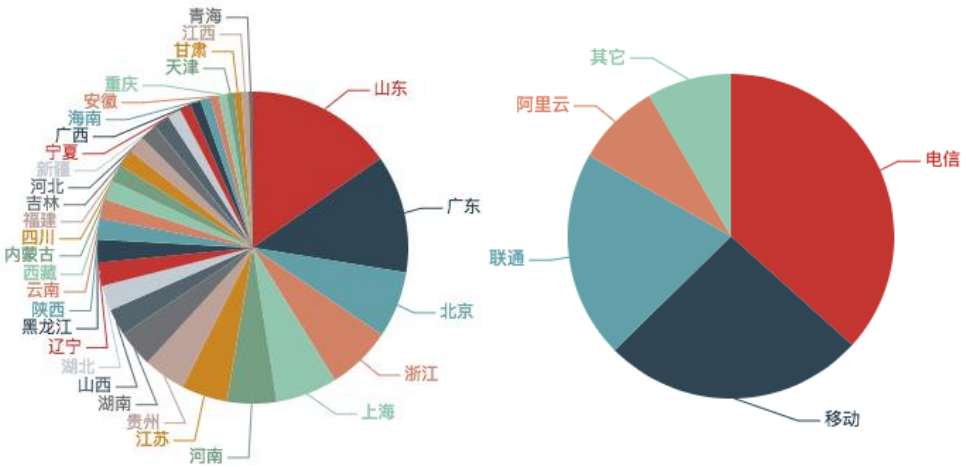

图 6 本月境内 Memcached 反射服务器数量按省份、运营商或云服务商分布

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 37.5%，其次是中国香港、加拿大和法国，如图 7 所示。

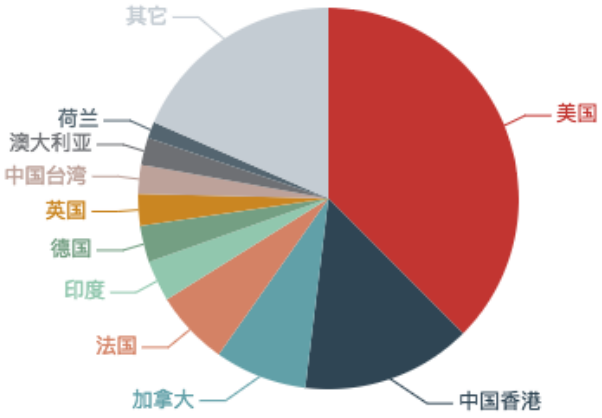

图 7 本月境外反射服务器数量按国家或地区分布

本月境内发起反射攻击事件数量 TOP100 中目前仍存活的 Memcached 服务器及归属如表 5 所示，位于北京市和河南省的地址最多。

表 5 本月境内发起反射攻击事件数量 TOP100 中仍存活的 Memcached 服务器 TOP30

反射服务器地址	归属省份	归属运营商或云服务商
106.X.X.51	北京市	电信
122.X.X.232	河南省	联通
122.X.X.38	河南省	联通
58.X.X.166	山东省	电信
116.X.X.114	河南省	联通
123.X.X.118	北京市	阿里云
116.X.X.206	河南省	联通
116.X.X.102	河南省	联通
116.X.X.195	河南省	联通
101.X.X.82	北京市	阿里云
101.X.X.42	北京市	阿里云
182.X.X.107	北京市	阿里云

116.X.X.252	河南省	联通
123.X.X.151	北京市	阿里云
123.X.X.195	北京市	阿里云
119.X.X.93	北京市	电信
116.X.X.34	河南省	联通
123.X.X.233	北京市	阿里云
202.X.X.240	新疆维吾尔族自治区	电信
122.X.X.188	山东省	电信
117.X.X.92	陕西省	电信
101.X.X.97	北京市	阿里云
119.X.X.156	北京市	电信
119.X.X.137	北京市	电信
117.X.X.58	河南省	移动
120.X.X.23	安徽省	移动
122.X.X.100	河南省	联通
123.X.X.237	北京市	阿里云
116.X.X.233	云南省	电信

近两月至今被利用发起攻击的 Memcached 反射服务器中，共计 4,215 个在本月仍处于活跃状态，其中 2,718 个位于境内，1,497 个位于境外。近两月至今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 18.7%，其次是北京市、浙江省、和山东省；按运营商或云服务商统计，电信占的比例最大，占 30.5%，阿里云占 28.0%，联通占 14.3%，移动占 11.1%，如图 8 所示。

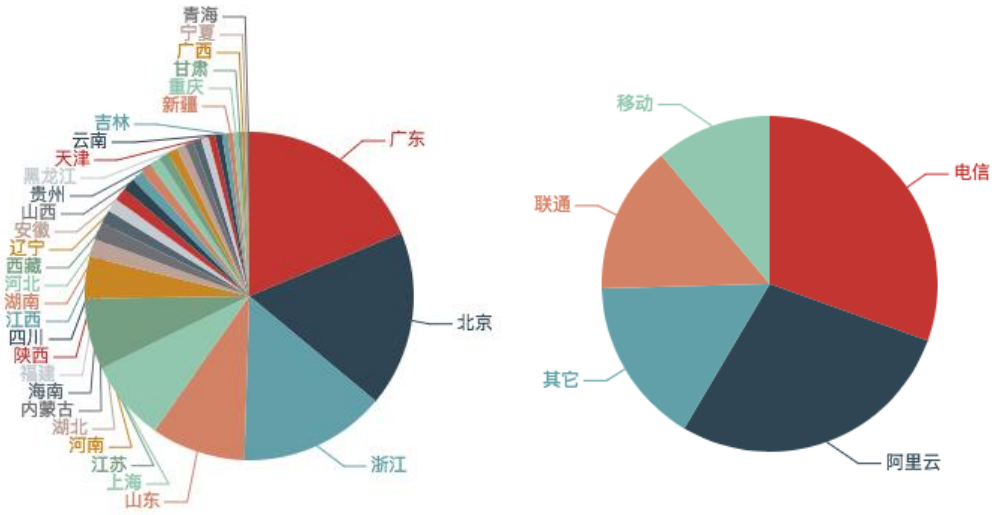

图 8 近两月被持续利用发起攻击的 Memcached 反射服务器数量按省份运营商或云服务商分布

（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 6 月，NTP 反射攻击事件共涉及我国境内 754,496 台反射服务器，境外 18,339 台反射服务器。被利用发起攻击的 NTP 反射服务器总量较上月有一定数量的回落。

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，广东省占的比例最大，占 15.6%，其次是山东省、甘肃省和江苏省；按归属运营商统计，移动占的比例最大，占

39.9%，电信占比 39.4%，联通占比 19.1%，如图 9 所示。

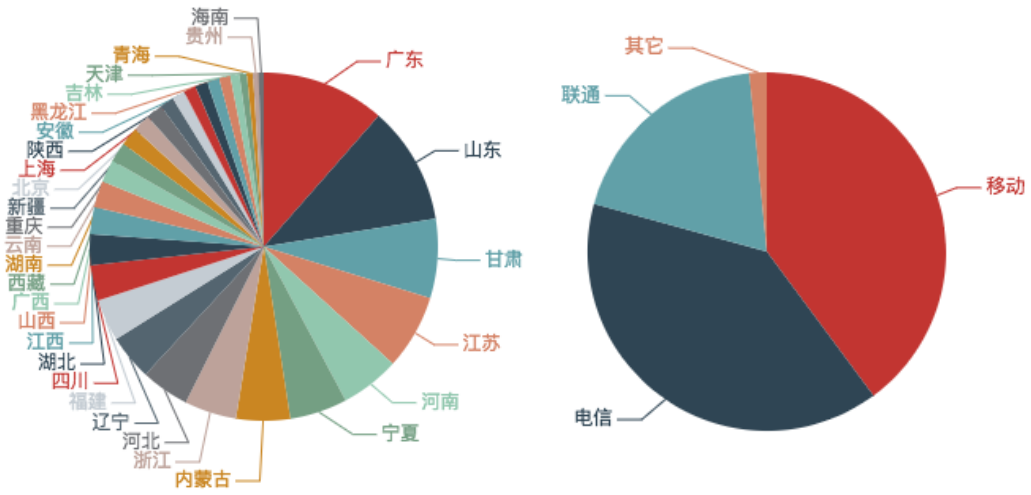

图 9 本月被利用发起 NTP 反射攻击的境内反射服务器数量按省份和运营商分布

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 76.1%，其次是美国、巴基斯坦和印度，如图 10 所示。

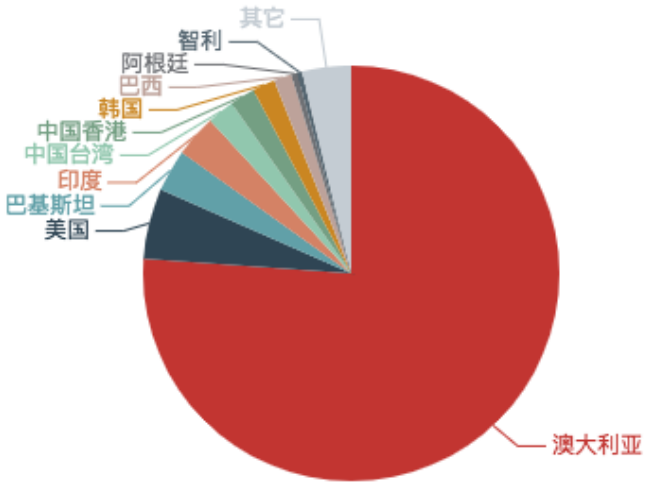

图 10 本月被利用发起 NTP 反射攻击的境外反射服务器数量按国家或地区分布

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 TOP25 及归属如表 6 所示，位于山东省和宁夏回族自治区的地址最多。

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 TOP25

反射服务器地址	归属省份	归属运营商
58.X.X.44	贵州省	联通
111.X.X.208	山西省	移动
222.X.X.199	宁夏回族自治区	电信
111.X.X.203	湖南省	移动
112.X.X.253	山东省	移动
112.X.X.251	山东省	移动
119.X.X.174	宁夏回族自治区	电信
218.X.X.38	宁夏回族自治区	电信
111.X.X.116	山东省	移动
61.X.X.190	宁夏回族自治区	电信
111.X.X.168	山东省	移动
112.X.X.202	山东省	移动
218.X.X.130	宁夏回族自治区	电信
14.X.X.143	宁夏回族自治区	电信
120.X.X.162	山东省	移动
112.X.X.75	山东省	移动
111.X.X.204	湖南省	移动
123.X.X.126	内蒙古自治区	电信
111.X.X.234	山西省	移动
218.X.X.10	宁夏回族自治区	电信
223.X.X.173	山东省	移动
211.X.X.188	山西省	移动
222.X.X.131	河南省	电信
111.X.X.88	山东省	移动
223.X.X.82	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 27,539 个在本月仍处于活跃状态，其中 26,063 个位于境内，1,476 个位于境外。近两月持续活跃的 NTP 反射服务器按省份统计，河南省占的比例最大，占 36.1%，其次是宁夏回族自治区、湖北省和湖南省；按运营商统计，电信占的比例最大，占 44.3%，移动占 24.3%，联通占 19.9%，如图 11 所示。

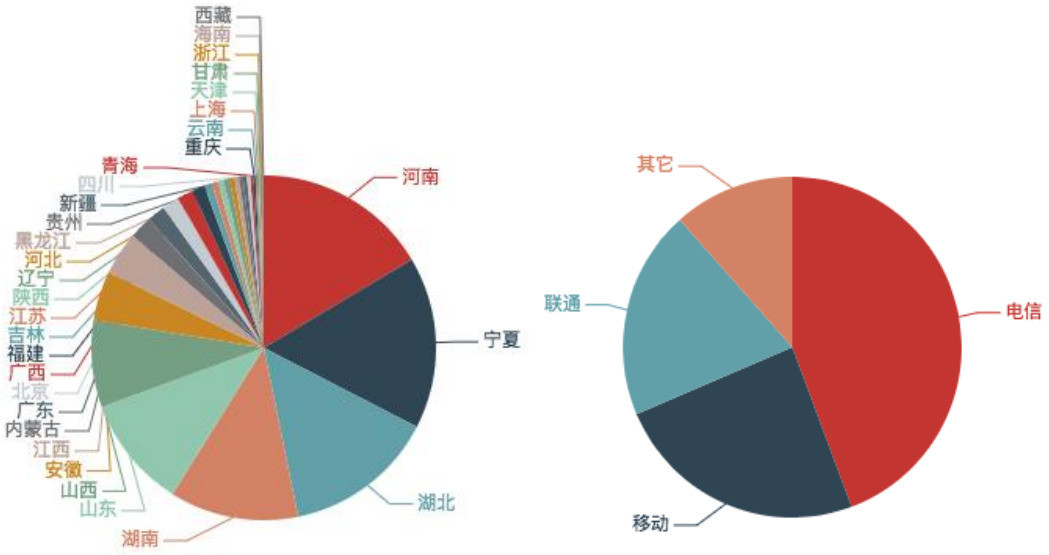

图 11 近两月被持续利用发起攻击的 NTP 反射服务器数量按省份运营商分布

（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 6 月，SSDP 反射攻击事件共涉及境内 2,684,026 台反射服务器，境外 216,281 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 17.3%，其次是江苏省、河南省和浙江省；按归属运营商统计，联通占的比例最大，占 54.9%，电信占比 41.4%，移动占比 3.3%，如图 12 所示。

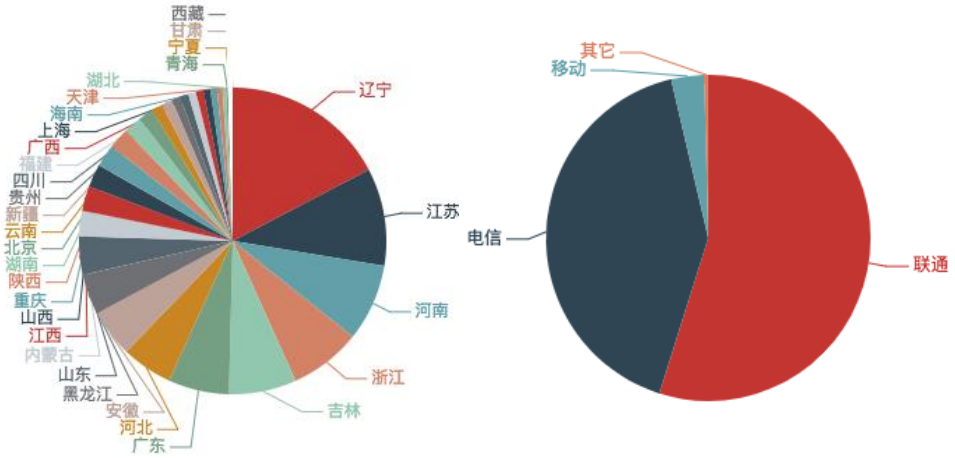

图 12 本月被利用发起 SSDP 反射攻击的境内反射服务器数量按省份和运营商分布

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 30.9%，其次是中国台湾、加拿大和韩国，如图 13 所示。

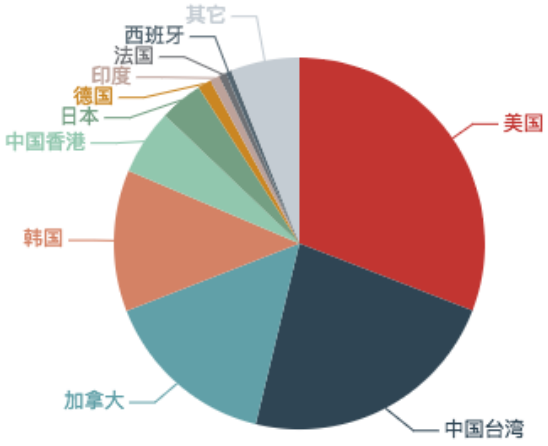

图 13 本月被利用发起 SSDP 反射攻击的境外反射服务器数量按国家或地区或地区分布

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 TOP20 的反射服务器及归属如表 7 所示，位于云南省和山东省的地址最多。

表 7 本月境内被利用发起 SSDP 反射攻击事件数量中排名 TOP20 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.185	云南省	电信
111.X.X.12	黑龙江省	移动
113.X.X.14	广西壮族自治区	电信
202.X.X.51	贵州省	电信
222.X.X.6	山东省	电信
218.X.X.186	云南省	电信
222.X.X.6	山东省	电信
183.X.X.56	湖南省	移动
61.X.X.6	宁夏回族自治区	电信
221.X.X.8	四川省	电信
106.X.X.14	内蒙古自治区	电信
116.X.X.15	云南省	电信
58.X.X.142	山东省	电信
218.X.X.18	云南省	电信
218.X.X.62	宁夏回族自治区	电信
222.X.X.54	山东省	电信
222.X.X.10	重庆市	电信
220.X.X.102	湖南省	电信
222.X.X.22	宁夏回族自治区	电信
111.X.X.11	黑龙江省	移动

近两月被持续利用发起攻击的 SSDP 反射服务器中，共计 423,548 个在本月仍处于活跃状态,其中 297,805 个位于境内，125,743 个位于境外。近两月持续活跃的 SSDP 反射服务器按省份统计，辽宁省占的比例最大，占 36.1%，其次是吉林省、广东省和河北省;按运营商统计,联通占的比例最大,占 65.7%，电信占 29.3%，移动占 4.4%，如图 14 所示。

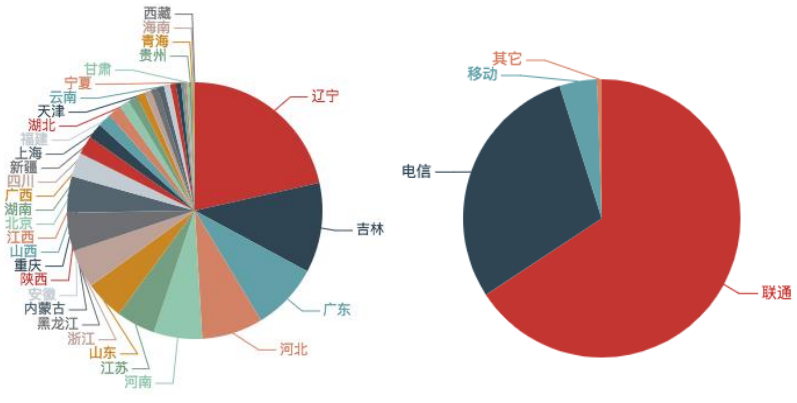

图 14 近两月被持续利用发起攻击的 SSDP 反射服务器数量按省份运营商分布

（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 6 月，通过跨域伪造流量发起攻击的流量来源于 193 个路由器。根据参与攻击事件的数量统计，归属于新疆维吾尔自治区移动的路由器（221.X.X.5、221.X.X.9)和北京电信的路由器(219.X.X.70）参与的攻击事件数量最多，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
221.X.X.5	新疆维吾尔族自治区	移动
221.X.X.9	新疆维吾尔族自治区	移动
219.X.X.70	北京市	电信
221.X.X.6	新疆维吾尔族自治区	移动
118.X.X.169	四川省	电信
113.X.X.253	湖北省	联通
113.X.X.252	湖北省	联通
61.X.X.25	浙江省	电信
219.X.X.30	北京市	电信
211.X.X.48	云南省	移动
211.X.X.43	贵州省	移动
222.X.X.200	山东省	电信
218.X.X.101	内蒙古自治区	联通
118.X.X.168	四川省	电信
222.X.X.201	山东省	电信
220.X.X.235	浙江省	电信
221.X.X.254	江苏省	联通
221.X.X.246	江苏省	联通
220.X.X.236	浙江省	电信
124.X.X.250	上海市	电信
202.X.X.223	河北省	联通
202.X.X.224	河北省	联通
61.X.X.184	吉林省	联通
61.X.X.185	吉林省	联通
219.X.X.144	北京市	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 12.4%，其次是江苏省和山东省；按路由器所属运营商统计，联通占的比例最大，占 37.3%，电信占比 31.6%，移动占比 31.1%，如图 15 所示。

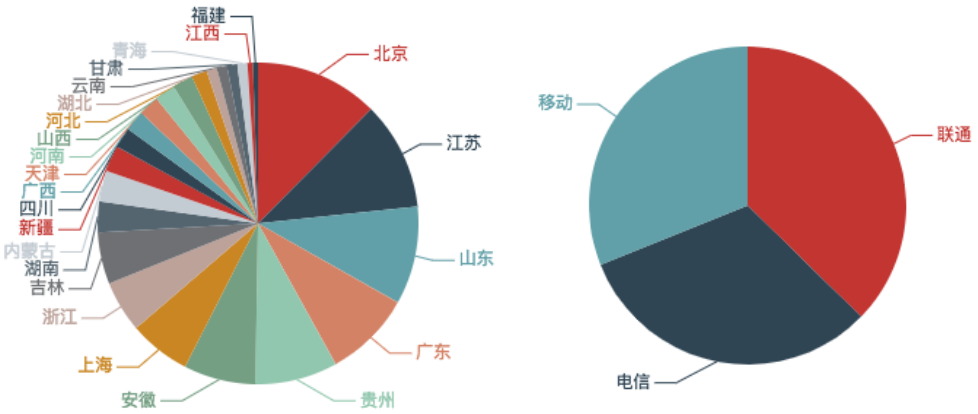

图 15 跨域伪造流量来源路由器数量按省份和运营商分布

2、本地伪造流量来源路由器

根据 CNCERT 抽样监测数据，2018 年 6 月，通过本地伪造流量发起攻击的流量来源于 395 个路由器。根据参与攻击事件的数量统计，归属于山西省电信的路由器（219.X.X.2、219.X.X.10）参与的攻击事件数量最多，其次是归属于山东省电信的路由器（150.X.X.1、150.X.X.2），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
219.X.X.2	山西省	电信
219.X.X.10	山西省	电信
150.X.X.1	山东省	电信
150.X.X.2	山东省	电信
118.X.X.169	四川省	电信
218.X.X.177	贵州省	移动
218.X.X.176	贵州省	移动
202.X.X.141	山西省	电信

220.X.X.253	北京市	电信
220.X.X.243	北京市	电信
202.X.X.143	山西省	电信
220.X.X.127	浙江省	电信
211.X.X.20	贵州省	移动
211.X.X.19	贵州省	移动
222.X.X.122	福建省	电信
222.X.X.121	福建省	电信
220.X.X.126	浙江省	电信
123.X.X.2	内蒙古自治区	电信
218.X.X.130	四川省	电信
202.X.X.167	山东省	电信
218.X.X.162	四川省	电信
221.X.X.233	宁夏回族自治区	联通
112.X.X.2	云南省	电信
61.X.X.1	四川省	电信
211.X.X.10	贵州省	移动

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 11.1%，其次是山西省、陕西省和广东省；按路由器所属运营商统计，电信占的比例最大，占 45.3%，移动占比 30.9%，联通占比 23.0%，如图 16 所示。

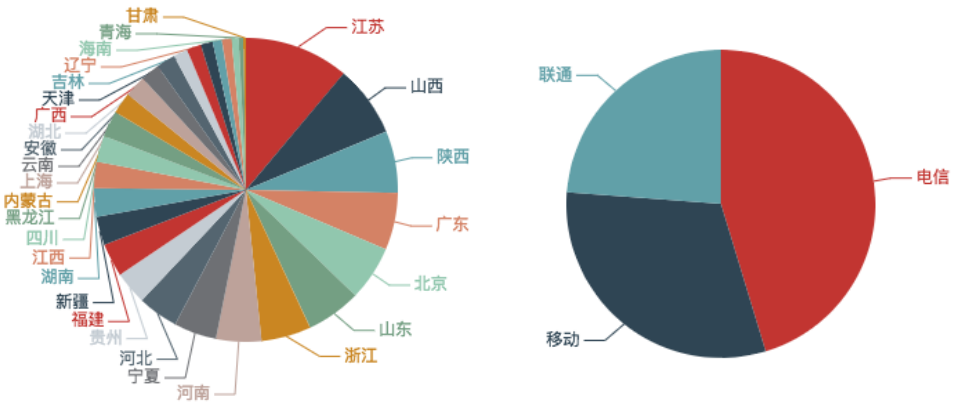

图 16 本地伪造流量来源路由器数量按省份和运营商分布

三、近半年我国境内攻击资源活跃及治理情况分析

2018 年以来，CNCERT 组织各省分中心，联合各地运营商、云服务商等对我国境内的攻击资源进行了专项治理。经过半年

以来的资源治理工作，综合境内各类攻击资源的变化趋势，我们分析发现控制端、肉鸡等资源的月活跃数量较 2017 年有了较明显的下降趋势；控制端、跨域伪造流量来源路由器、本地伪造流量来源路由器等资源近三个月每月的新增率、消亡率相比 2017 年月度平均数值有一定程度的上升，意味着资源变化速度加快，可被利用的资源稳定性降低；反射服务器资源近三个月每月的新增率、消亡率相比 2017 年月度平均数值，新增率不变、消亡率呈现一定程度的下降，意味着可利用的资源数量逐步减少。资源的具体变化趋势如下:

（一）我国境内攻击资源活跃情况分析

1、控制端资源

近三个月以来，利用肉鸡发起 DDoS 攻击的境内控制端平均每月数量为 40 个,较 2017 年平均每月数量相比下降 44%。境内控制端资源每月的新增率为 81%，消亡率为 83%，与 2017 年平均每月 70%的新增率和 71%的消亡率相比，资源变化速度加快，可被利用的稳定性降低。其中，只有 1 个位于上海的境内控制端（182.X.X.227）在近三个月甚至半年内持续活跃。

2、肉鸡资源

近三个月以来，被利用发起 DDoS 攻击的境内肉鸡平均每月数量为 103,970 个,与 2017 年平均每月数量相比下降近 50%。境内肉鸡资源每月的新增率为 87%，消亡率为 88%，与 2017 年平均每月的新增率和的消亡率相比无明显变化；存在 3,209

个肉鸡在近三个月内持续活跃，其所属省份和运营商分布如图 17 所示，主要位于浙江省、广东省和山西省，电信占的比例最大。其中，存在 78 个境内肉鸡历史活跃月度超过 12 个月。

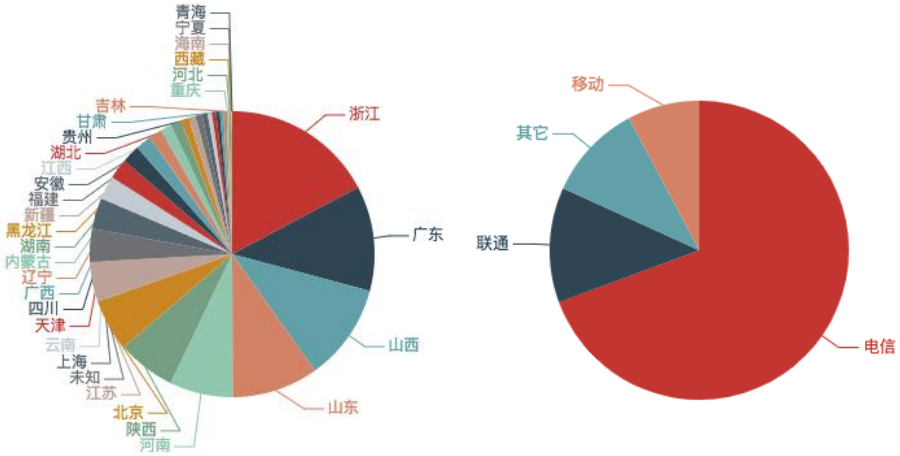

图 17 近三个月内持续活跃的境内肉鸡数量按省份和运营商分布

3、反射服务器资源

近三个月以来，利用境内服务器、主机等设施发起 DDoS 反射攻击的反射服务器平均数量为 2,812,943 个。境内反射服务器资源每月的新增率为 81%，消亡率为 84%，与 2017 年平均每月的 85%新增率和的 71%消亡率相比，消亡率呈现增快趋势；存在 75,777 个反射服务器在近三个月内持续活跃，其所属省份和运营商分布如图 18 所示，主要位于辽宁省、广东省和吉林省，联通占的比例最大。其中，存在 85 个境内反射服务器历史活跃月度超过 12 个月。

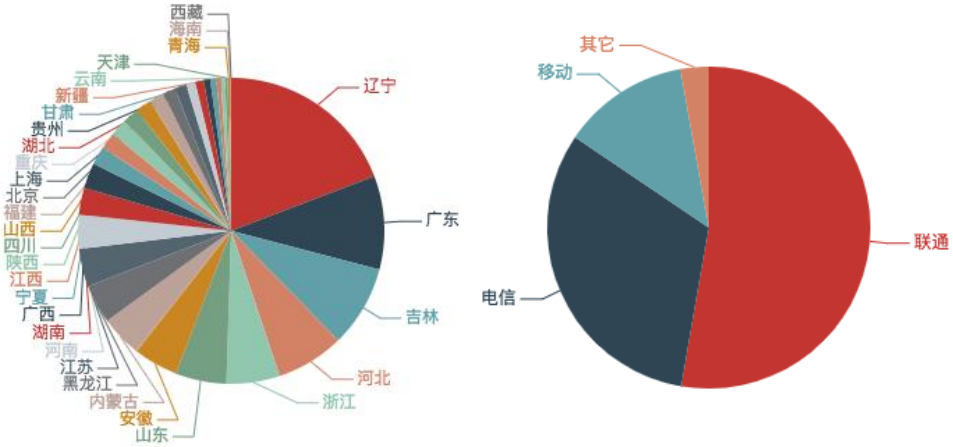

图 18 近三个月内持续活跃的反射服务器数量按省份和运营商分布

4、跨域伪造流量来源路由器资源

近三个月以来，被利用转发跨域伪造攻击流量的境内运营商路由器平均数量为 177 个；境内跨域伪造流量来源路由器资源每月的新增率为 33%，消亡率为 29%，与 2017 年平均每月 22%的新增率和 20%的消亡率相比，资源变化速度加快，可被利用的稳定性降低；存在 72 个跨域伪造流量来源路由器在近三个月内持续活跃，其所属省份和运营商分布如图 19 所示，主要位于广东省、上海市和四川省，电信所占的比例最大。其中，存在 9 个历史活跃月度超过 12 个月，详细信息如表 10 所示。

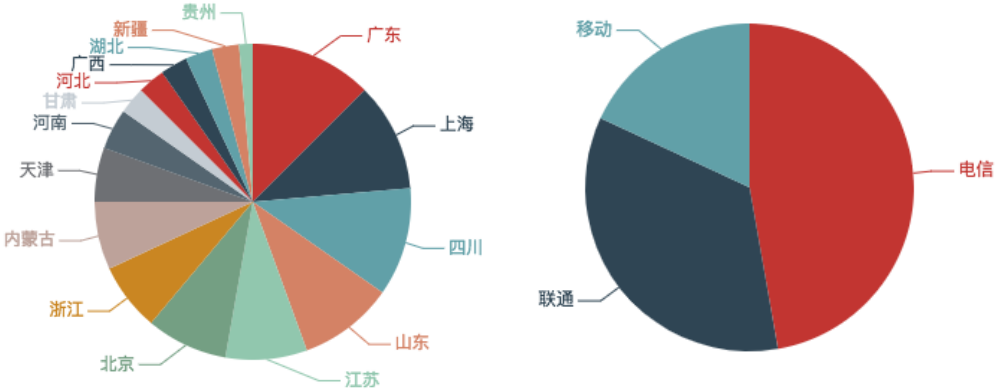

图 19 近三个月内持续活跃的跨域伪造流量来源路由器数量按省份和运营商分布

表 10 近两年历史活跃月度超过 12 个月的跨域流量来源路由器信息

跨域伪造来源路由器	历史活跃月份	所属省份	所属运营商
61.X.X.25	13	浙江	电信
219.X.X.30	14	北京	电信
218.X.X.254	13	山东	联通
180.X.X.2	13	北京	电信
218.X.X.254	13	山东	联通
221.X.X.2	14	天津	电信
221.X.X.1	14	天津	电信
221.X.X.254	14	广东	联通
219.X.X.70	14	北京	电信

5、本地伪造流量来源路由器资源

近三个月以来，被利用转发伪造本区域攻击流量的境内运营商路由器平均数量为 440 个；境内本地伪造流量来源路由器资源每月的新增率为 23%，消亡率为 29%，与 2017 年平均每月 14%的新增率和 13%的消亡率相比，资源变化速度有较明显的加快，可被利用的稳定性降低；存在 174 个本地伪造流量来源路由器在近三个月内持续活跃，其所属省份和运营商分布如图 20 所示，主要位于江苏省、浙江省和广东省，电信占的比例最大。其中，有 20 个路由器历史活跃月度超过 12 个月，如表 11 所示。

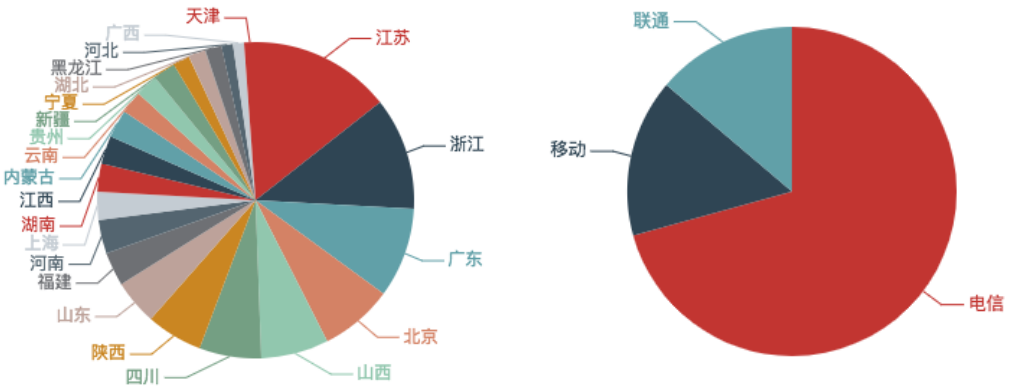

图 20 近三个月内持续活跃的本地伪造流量来源路由器数量按省份和运营商分布

表 11 近两年历史活跃月度超过 12 个月的跨域流量来源路由器信息

本地伪造来源路由器	历史活跃月度	所属省份	所属运营商
124.X.X.1	14	山西	联通
124.X.X.2	14	山西	联通
218.X.X.101	13	河北	移动
220.X.X.243	13	北京	电信
202.X.X.159	13	江西	电信
202.X.X.155	13	福建	电信
202.X.X.156	13	江西	电信
202.X.X.157	13	江西	电信
202.X.X.158	13	江西	电信
202.X.X.151	13	福建	电信
202.X.X.154	13	福建	电信
202.X.X.150	13	福建	电信
220.X.X.253	13	北京	电信
222.X.X.122	13	福建	电信
222.X.X.121	13	福建	电信
61.X.X.26	13	浙江	电信
219.X.X.1	13	山西	电信
61.X.X.8	13	浙江	电信
61.X.X.4	13	浙江	电信
220.X.X.59	13	江西	电信

（二）近半年各省治理情况分析

近半年来，各省份资源数量排名变化情况如图 21 至图 25 所示，图中纵轴为省份，横轴为排名。红色的点表示各省攻击

数量在某月的排名情况，月份越临近，点越大；月份越久远，点越小。例如，最小的点代表的是 2017 年全年各省资源数量排名；最大的点代表的是 2018 年 6 月的资源数量排名。

图中体现的排名变化存在以下情况:（1）红点如从左至右由小变大，则表明资源排名相较好转，治理效果较明显；（2）红点从左至右由大变小,表明资源排名相较无好转或恶化;（3）红点持续位于左侧，表明资源数量排名一直位于前列;（4）红点持续位于右侧，表明资源数量排在后部;（5）图中未出现的省份，表明 2017 年以来未在该省发现过此类活跃攻击资源。

1、控制端资源

2017 年以来，共监测发现我国境内 535 个曾经发起较大规模 DDoS 攻击的控制端资源，主要位于我国境内 20 个省市，未发现位于甘肃、河北、吉林、内蒙古、宁夏、青海、山东、山西、西藏、新疆等省市的控制端。

各省市控制端资源数量的月度排名变化情况如图 21 所示。从图中可以看出，陕西、天津、湖北、黑龙江、广西、重庆、湖南等省市的控制端资源排名普遍排在后部,或是近期无存活;福建、广东、江苏、上海等省市的控制端资源排名相较有一定的好转；北京、浙江、贵州等省市的控制端资源排名情况相较无好转、或存在一定恶化。

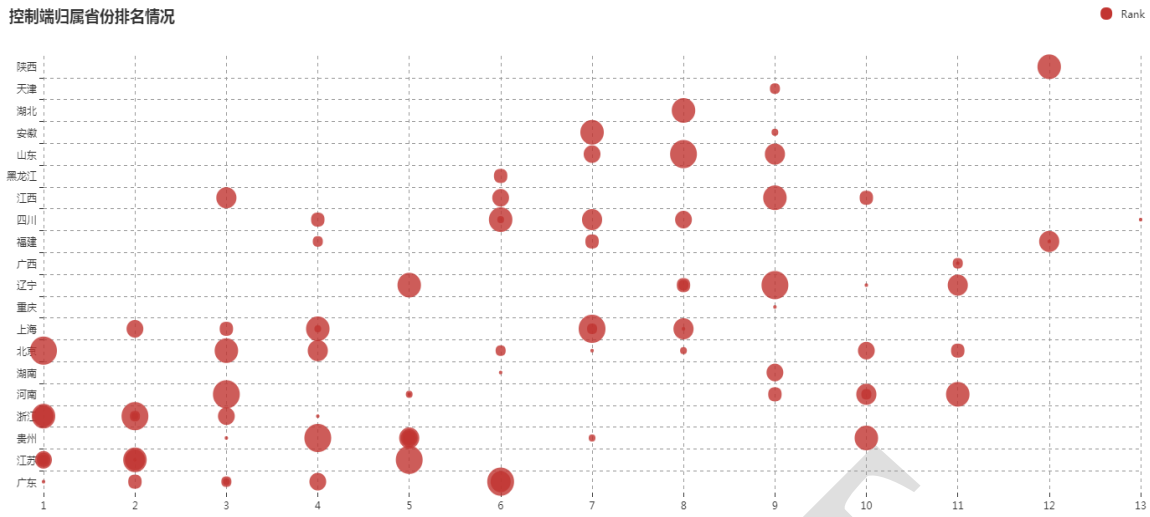

图 21 近半年境内控制端所属省份排名情况变化趋势

2、肉鸡资源

2017 年以来，共监测发现我国境内 1,700,146 个曾经被利用发起较大规模 DDoS 攻击的肉鸡资源。

各省市肉鸡资源数量的月度排名变化情况如图 22 所示。从图中可以看出，青海、宁夏、西藏、甘肃、海南、内蒙古、广西、天津等省市的肉鸡资源排名普遍排在后部，或是近期无存活；湖南、湖北、江西、新疆、重庆等省市的肉鸡资源排名相较有一定的好转；广东、上海、山东、江苏、浙江、山西等省市的被利用资源数量排名近几月相较有一定的好转，但仍普遍排在前列；北京、四川、黑龙江、河北、贵州、河南等省市的肉鸡资源排名情况相较无好转、或存在一定恶化。

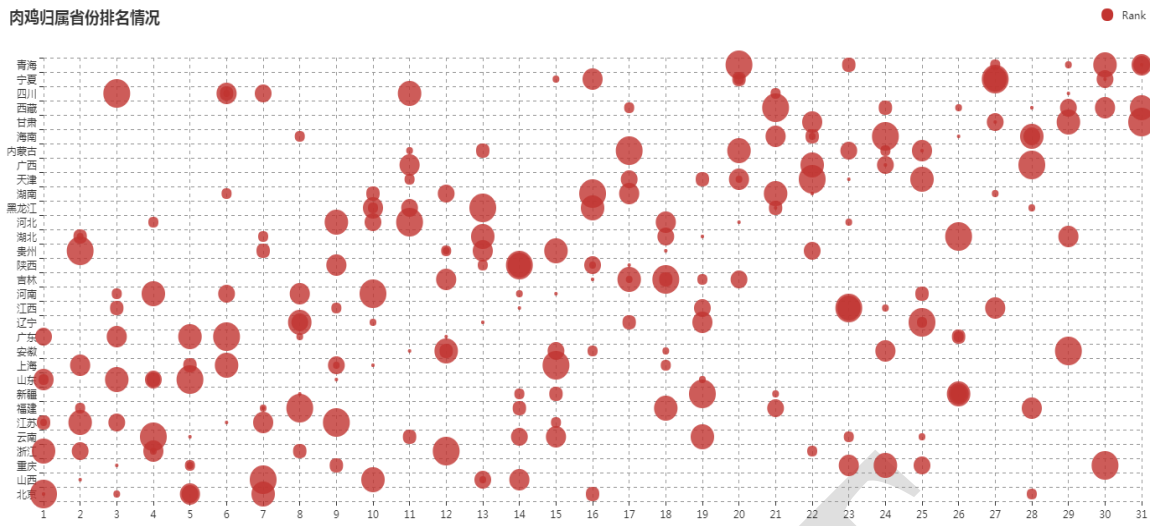

图 22 近半年境内肉鸡所属省份排名情况变化趋势

3、反射服务器资源

2017 年以来，共监测发现我国境内 11,199,098 个曾经被利用发起 DDoS 反射攻击的反射服务器资源。

各省市反射服务器资源数量的月度排名变化情况如图 23 所示。从图中可以看出，西藏、海南、广西、青海、甘肃、云南、上海等省市的反射服务器资源排名普遍排在后部，或是近期无存活；四川、天津、宁夏、贵州、湖北、福建、北京、新疆等省市的反射服务器资源排名相较有一定的好转；山西、黑龙江、吉林、河北、山东等省市的被利用资源数量排名近几月相较有一定的好转，但仍普遍排在前列；辽宁、广东、江苏、内蒙古、河南、浙江、重庆、安徽、湖南等省市的反射服务器资源排名情况相较无好转、或存在一定恶化。

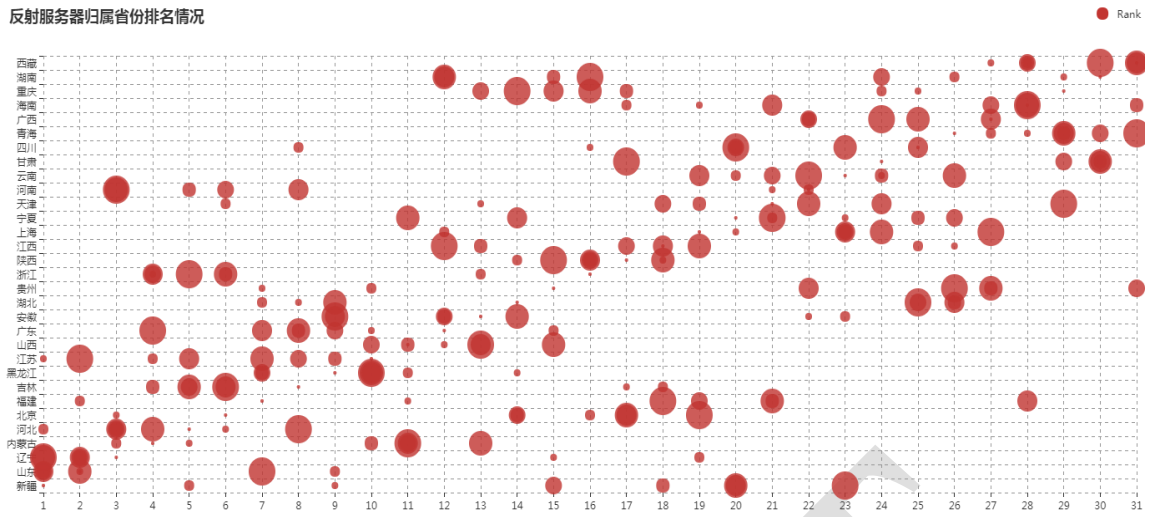

图 23 近半年境内反射服务器所属省份排名情况变化趋势

4、跨域伪造流量来源路由器资源

2017 年以来，共监测发现我国境内 580 个曾经被利用转发跨域伪造攻击流量的运营商路由器。主要位于 28 个省市，未发现位于宁夏、西藏等省市的转发跨域伪造攻击流量的运营商路由器。

各省市跨域伪造流量来源路由器资源数量的月度排名变化情况如图 24 所示。从图中可以看出，青海、黑龙江、重庆、陕西、山西等省市的被利用资源数量排名普遍排在后部，或是近期无存活；江西、福建、辽宁、河南、河北、甘肃等省市的被利用资源数量排名相较有一定的好转；广东、浙江、上海等省市的被利用资源数量排名近几月相较有一定的好转，但仍普遍排在前列；北京、江苏、山东、贵州、安徽、内蒙古、湖南、新疆等省市的被利用资源数量排名情况相较无好转、或存在一定恶化。

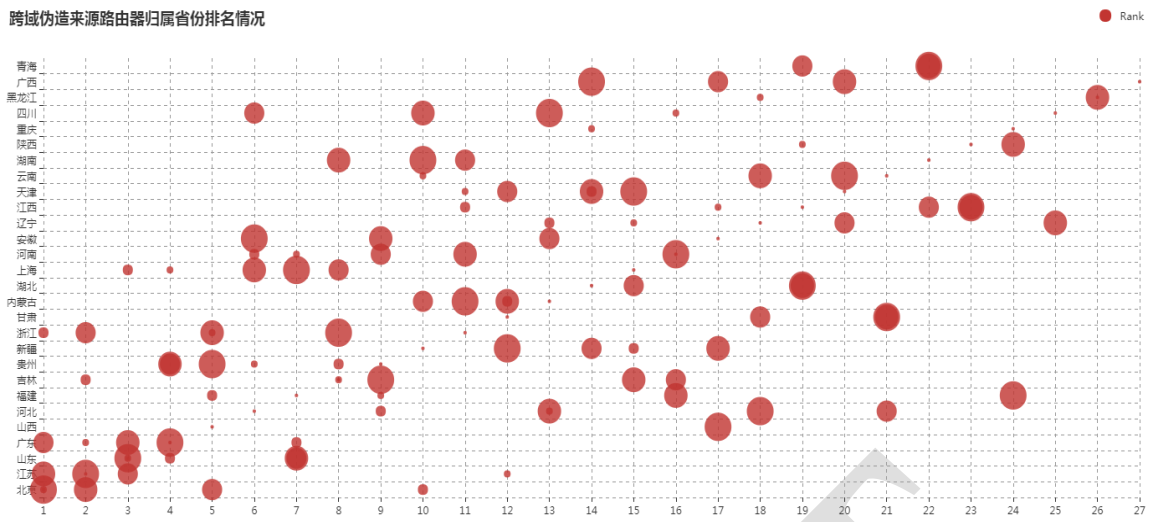

图 24 近半年境内跨域伪造流量来源路由器归属省份排名情况变化趋势

5、本地伪造来源路由器资源

2017 年以来，共监测发现我国境内 1,081 个曾经被利用转发本区域伪造攻击流量的运营商路由器。

各省市本地伪造流量来源路由器资源数量的月度排名变化情况如图 25 所示。从图中可以看出，青海、西藏、海南、天津、内蒙古、重庆、广西、甘肃、吉林、黑龙江等省市的被利用资源数量排名普遍排在后部，或是近期无存活；安徽、上海、四川、湖北、辽宁、云南、江西、新疆等省市的被利用资源数量排名相较有一定的好转；贵州、浙江等省市的被利用资源数量排名近几月相较有一定的好转，但仍普遍排在前列；江苏、北京、广东、陕西、湖南、山西、山东、河北、河南等省市的被利用资源数量排名情况相较无好转、或存在一定恶化。

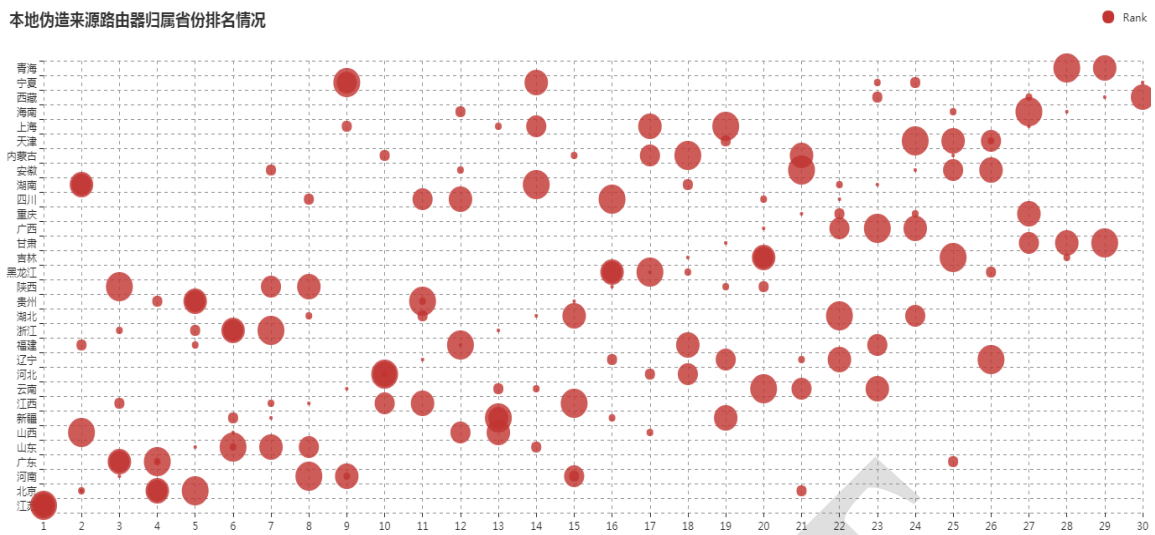

图 25 近半年境内本地伪造流量来源路由器归属省份排名情况变化趋势