2018 年我国 DDoS 攻击资源分析报告

国家计算机网络应急技术处理协调中心

2019 年 3 月

目 录

一、引言

（一）攻击资源定义

本报告为 2018 年的 DDoS 攻击资源年度分析报告。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

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

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）2018 年重点关注情况

1、2018 年利用肉鸡发起 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，其次是浙江省、贵州省和广东省，按归属运营商统计，中国电信占的比例最大。

2、2018 年参与攻击较多的境内肉鸡地址主要位于江苏省、浙江省和山东省，其中大量肉鸡地址归属于中国电信。当前仍旧存活且持续活跃超过六个月的境内肉鸡资源中，位于广东省、浙江省、山东省的地址占的比例最大。

3、2018 年被利用发起 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是广东省、山东省和河南省；按归属运营商统计，数量最多的是中国电信。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、河南省和河北省；按归属运营商统计，数量最多的是中国联通。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、山东省和浙江省；按归属运营商统计，数量最多的是中国联通。

4、2018 年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路由器参与的攻击事件数量最多；跨域伪造流量来源路由器数量按省份统计，最多位于北京市、江苏省和广东省。持续被利用超过三个月的跨域伪造流量来源路由器中，归属于江苏省、北京市和山东省路由器数量最多。

5、2018 年转发伪造本地攻击流量的路由器中，归属于北京市电信的路由器参与的攻击事件数量最多；本地伪造流量来源路由器数量按省份统计，最多位于江苏省、山东省和河南省。持续被利用超过三个月的本地伪造流量来源路由器中，归属于浙江省、广东省、河南省的路由器数量最多。

6、经过一年来针对我国境内的攻击资源的专项治理工作，**根据 CNCERT 自主监测数据**，与 2017 年相比，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每月的新增率不变、消亡率呈现一定程度的上升，意味着资源消亡速度加快，可利用的资源数量逐步减少；境内反射服务器资源每月的消亡率不变、新增率呈现一定程度的下降，意味着可新增的资源数量逐步减少。**根据外部相关分析报告**，我国境内的僵尸网络控制端数量持续减少；我国境内全年 DDoS 攻击次数明显下降，特别是反射攻击较去年减少了 80%。

二、全年 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 年以来利用肉鸡发起 DDoS 攻击的控制端有 2108 个，其中，334 个控制端位于我国境内，1774 个控制端位于境外。

位于境外的控制端按国家或地区分布，美国占比最大，占 36.3%，其次是中国香港和加拿大，如图 1 所示。

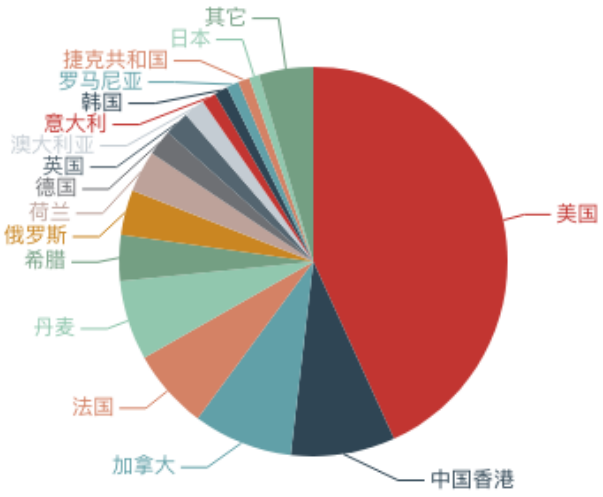

图 1 2018 年以来发起 DDoS 攻击的境外控制端数量按国家或地区分布

位于境内的控制端按省份统计，江苏省占比最大，占 27.5%，其次是浙江省、贵州省和广东省；按运营商统计，中国电信占比最大，占 76.9%，中国联通占 9.9%，中国移动占 0.9%，如图 2 所示。

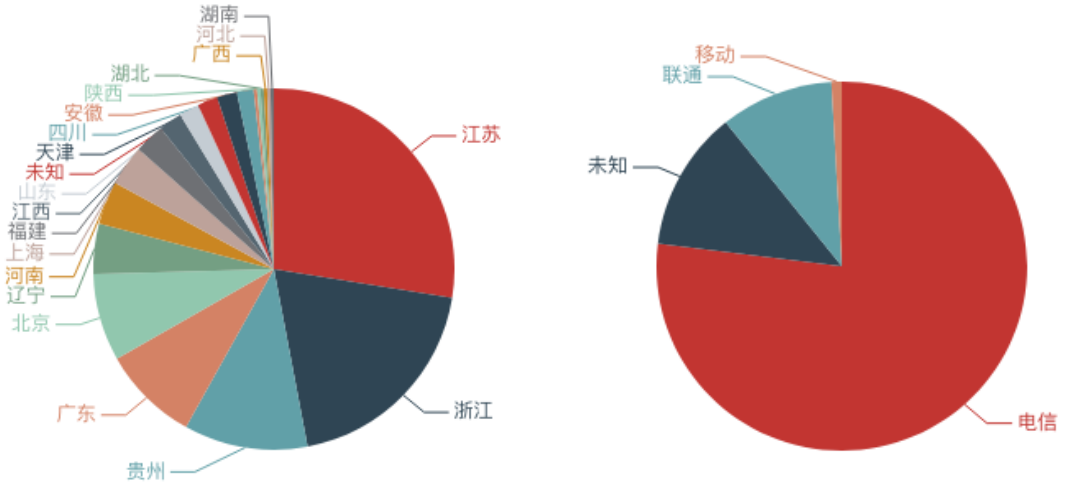

图 2 2018 年以来发起 DDoS 攻击的境内控制端数量按省份和运营商分布

2018 年以来发起攻击最多的境内控制端前二十名及归属如表 1 所示。

表 1 2018 年以来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.167	山东省	中国联通
183.X.X.78	浙江省	中国电信
222.X.X.122	江苏省	中国电信
118.X.X.216	江西省	中国联通
123.X.X.146	贵州省	中国电信
27.X.X.234	福建省	中国电信
116.X.X.2	广东省	中国电信
222.X.X.232	江苏省	中国电信
219.X.X.226	河南省	中国电信
117.X.X.110	陕西省	中国电信
123.X.X.147	贵州省	中国电信
183.X.X.243	浙江省	中国电信
183.X.X.90	浙江省	中国电信
125.X.X.100	福建省	中国电信
183.X.X.57	广东省	中国电信
58.X.X.158	江苏省	中国电信
61.X.X.154	江苏省	中国电信
119.X.X.162	广东省	中国电信
222.X.X.7	江苏省	中国电信
220.X.X.54	湖南省	中国电信

（二）肉鸡资源分析

根据 CNCERT 抽样监测数据，2018 年以来共有 1,444,633 个肉鸡地址参与真实地址攻击(包含真实地址攻击与反射攻击等其它攻击的混合攻击)。

这些肉鸡资源按省份统计，江苏省占比最大，为 14.6%，其次是浙江省、山东省和广东省；按运营商统计，中国电信占比最大，为 61.6%，中国联通占 27.3%，中国移动占 9.4%，如图 3 所示。

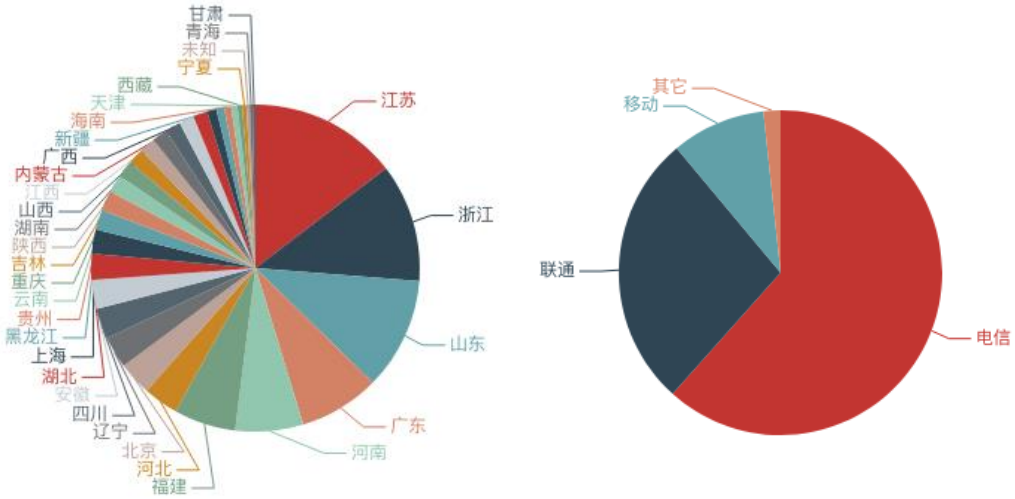

图 3 2018 年以来肉鸡地址数量按省份和运营商分布

2018 年以来参与攻击最多的肉鸡地址前三十名及归属如表 2 所示。

表 2 2018 年以来参与攻击最多的肉鸡地址 TOP30

肉鸡地址	归属省份	归属运营商或云服务商
60.X.X.174	新疆维吾尔自治区	中国联通
61.X.X.28	甘肃省	中国电信
61.X.X.66	青海省	中国电信
220.X.X..58	广西壮族自治区	中国电信
118.X.X.186	甘肃省	中国电信
221.X.X.129	内蒙古自治区	中国联通
61.X.X.114	河南省	中国联通

61.X.X.243	内蒙古自治区	中国联通
222.X.X.186	广西壮族自治区	中国电信
111.X.X.53	吉林省	中国移动
139.X.X.208	北京市	待确认
202.X.X.202	北京市	中国联通
221.X.X.144	贵州省	中国联通
202.X.X.138	新疆维吾尔自治区	中国电信
42.X.X.155	上海市	中国电信
175.X.X.131	湖南省	中国电信
222.X.X.242	贵州省	中国电信
60.X.X.211	山西省	中国联通
58.X.X.114	湖南省	中国联通
183.X.X.79	浙江省	中国电信
112.X.X.146	安徽省	中国联通
211.X.X.78	上海市	中国联通
27.X.X.250	上海市	中国联通
112.X.X.234	江苏省	中国联通
219.X.X.97	黑龙江省	中国电信
114.X.X.253	北京市	待确认
60.X.X.30	安徽省	中国电信
42.X.X.56	上海市	中国电信
218.X.X.182	河南省	中国联通
111.X.X.69	河南省	中国移动

（三）反射攻击资源分析

根据 CNCERT 抽样监测数据，2018 年以来利用反射服务器发起的三类重点反射攻击共涉及 19,708,130 台反射服务器，其中境内反射服务器 16,549,970 台，境外反射服务器 3,158,160 台。被利用发起 Memcached 反射攻击的反射服务器有 232,282 台，占比 1.2%，其中境内 187,247 台，境外 45,035 台；被利用发起 NTP 反射攻击的反射服务器有 3,200,200 台，占比 16.2%，其中境内 2,040,066 台，境外 1,160,134 台；被利用发起 SSDP 反射攻击的反射服务器有 16,275,648 台，占比 82.6%，其中境内 14,322,657 台，境外 1,952,991 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 服务器的默认 11211 端口发送伪造受害者 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 年以来利用 Memcached 服务器实施反射攻击的事件共涉及境内 187,247 台反射服务器，境外 45,035 台反射服务器。

2018 年以来境内反射服务器数量按省份统计，广东省占比最大，占 14.1%，其次是山东省、河南省和江苏省；按归属运营商或云服务商统计，中国电信占比最大，占 53.5%，中国移动占 23.8%，中国联通占 13.4%，阿里云占 4.5%，如图 4 所示。

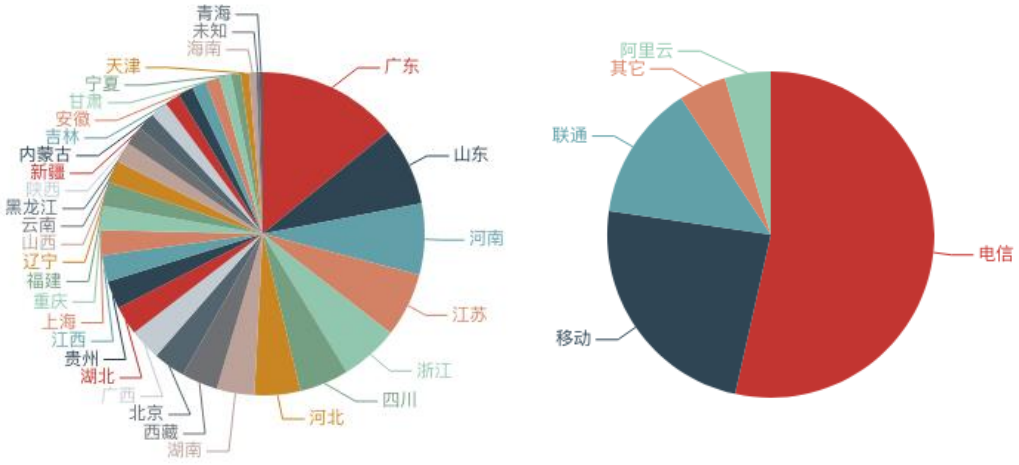

图 4 2018 年以来境内 Memcached 反射服务器数量按省份、运营商或云服务商分布

2018 年以来被利用发起攻击的境外 Memcached 反射服务器数量按国家或地区统计，美国占比最大，占 25.2%，其次是中国香港、法国和日本，如图 5 所示。

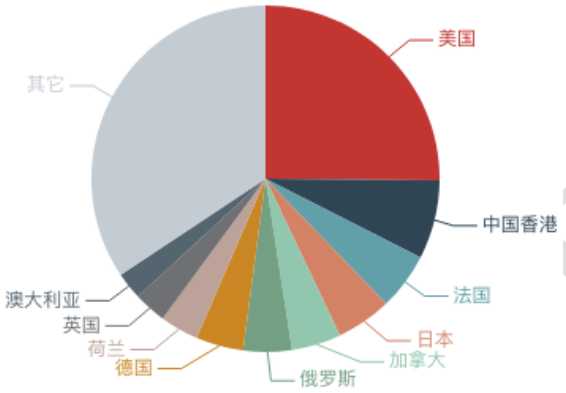

图 5 2018 年以来境外 Memcached 反射服务器数量按国家或地区分布

2018 年被利用发起 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 3 所示，位于北京市的地址最多。

表 3 2018 年以来境内被利用发起 Memcached 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	归属运营商或云服务商
106.X.X.51	北京市	中国电信
202.X.X.240	新疆维吾尔自治区	中国电信
123.X.X.195	北京市	阿里云
119.X.X.93	北京市	中国电信
123.X.X.233	北京市	阿里云
123.X.X.30	北京市	阿里云
101.X.X.97	北京市	阿里云
123.X.X.237	北京市	阿里云
101.X.X.178	北京市	阿里云
112.X.X.84	北京市	阿里云
121.X.X.197	北京市	中国联通
116.X.X.10	云南省	中国电信
101.X.X.74	北京市	阿里云
123.X.X.118	北京市	阿里云
182.X.X.228	北京市	阿里云

223.X.X.13	四川省	中国移动
202.X.X.100	山西省	中国联通
123.X.X.128	北京市	阿里云
119.X.X.156	北京市	中国电信
182.X.X.75	北京市	阿里云
123.X.X.216	北京市	阿里云
101.X.X.68	北京市	阿里云
113.X.X.112	广东省	中国电信
182.X.X.145	北京市	阿里云
182.X.X.145	北京市	阿里云
101.X.X.71	北京市	阿里云
58.X.X.166	山东省	中国电信
123.X.X.197	北京市	阿里云
101.X.X.55	北京市	阿里云
123.X.X.76	北京市	阿里云

（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 服务器的默认 123 端口发送伪造受害者 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 年以来 NTP 反射攻击事件共涉及我国境内 2,040,066 台反射服务器，境外 1,160,134 台反射服务器。

2018 年以来被利用发起 NTP 反射攻击的境内反射服务器数量按省份统计，山东省占比最大，占 20.3%，其次是河南省、河北省和湖北省；按归属运营商统计，中国联通占比最大，占 37.1%，中国移动占 32.0%，中国电信占 28.8%，如图 6 所示。

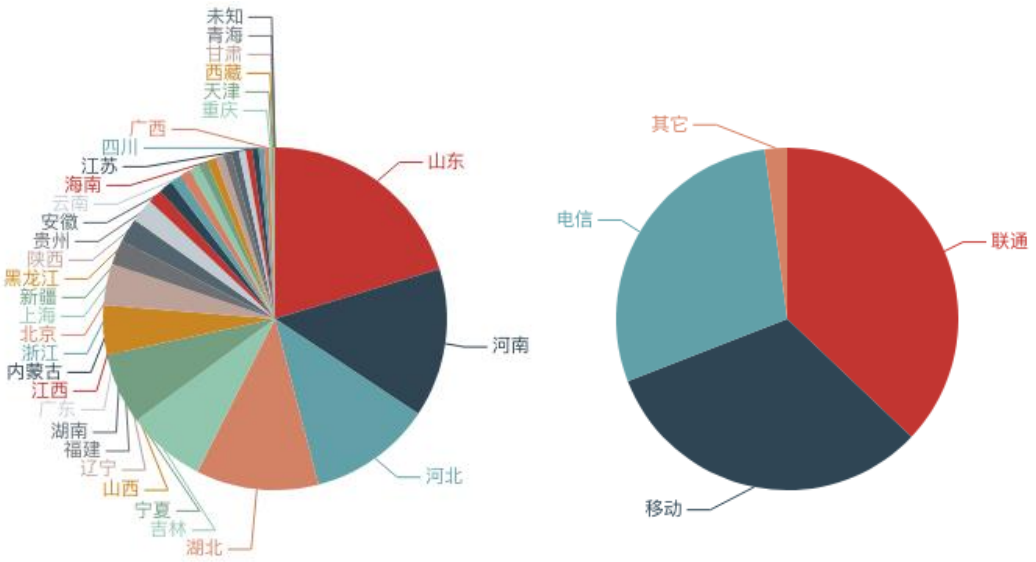

图 6 2018 年以来被利用发起 NTP 反射攻击的境内反射服务器数量按省份和运营商分布

2018 年以来被利用发起 NTP 反射攻击的境外反射服务器数量按国家或地区统计，越南占比最大，占 51.9%，其次是澳大利亚、美国和巴西，如图 7 所示。

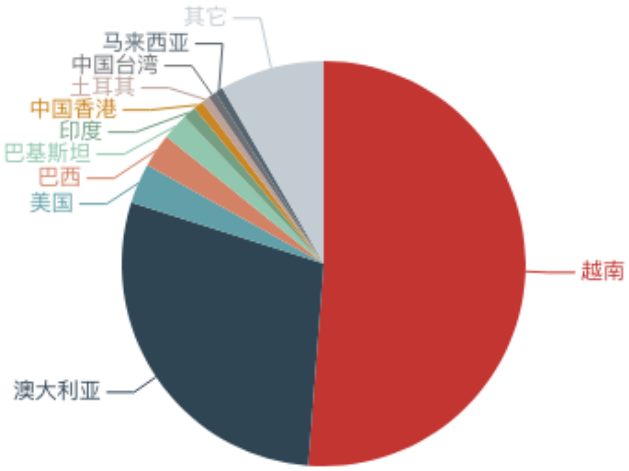

图 7 2018 年以来被利用发起 NTP 反射攻击的境外反射服务器数量按国家或地区分布

2018 年以来被利用发起 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 4 所示，位于新疆维吾尔自治区的地址最多。

表 4 2018 年以来境内被利用发起 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	归属运营商或云服务商
221.X.X.37	河南省	中国移动
119.X.X.37	四川省	中国联通
220.X.X.54	安徽省	中国联通
111.X.X.30	贵州省	中国联通
202.X.X.70	新疆维吾尔自治区	中国电信
60.X.X.118	新疆维吾尔自治区	中国联通
218.X.X.126	广西壮族自治区	中国电信
61.X.X.24	北京市	中国联通
125.X.X.194	吉林省	中国联通
119.X.X.198	吉林省	中国联通
203.X.X.100	湖南省	中国联通
60.X.X.126	新疆维吾尔自治区	中国联通
123.X.X.82	北京市	中国联通
123.X.X.134	河南省	中国电信
60.X.X.134	河北省	中国联通
117.X.X.61	天津市	中国联通
124.X.X.22	北京市	中国联通
202.X.X.14	吉林省	中国联通
124.X.X.166	北京市	中国联通
122.X.X.170	江苏省	中国联通
60.X.X.158	新疆维吾尔自治区	中国联通
119.X.X.3	四川省	中国联通
61.X.X.174	山东省	中国联通
60.X.X.102	山东省	中国联通
183.X.X.166	浙江省	中国电信
61.X.X.59	河南省	中国联通
60.X.X.12	新疆维吾尔自治区	中国联通
124.X.X.90	北京市	中国联通
221.X.X.174	新疆维吾尔自治区	中国联通
221.X.X.10	黑龙江省	中国联通
123.X.X.76	北京市	阿里云

（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 服务器的默认 1900 端口发送伪造受害者 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 年以来 SSDP 反射攻击事件共涉及境内 14,322,657 台反射服务器，境外 1,952,991 台反射服务器。

2018 年以来被利用发起 SSDP 反射攻击的境内反射服务器数量按省份统计，辽宁省占比最大，占 14.8%，其次是山东省、浙江省和江苏省；按归属运营商统计，中国联通占比最大，占 57.8%，中国电信占 39.5%，中国移动占 2.3%，如图 8 所示。

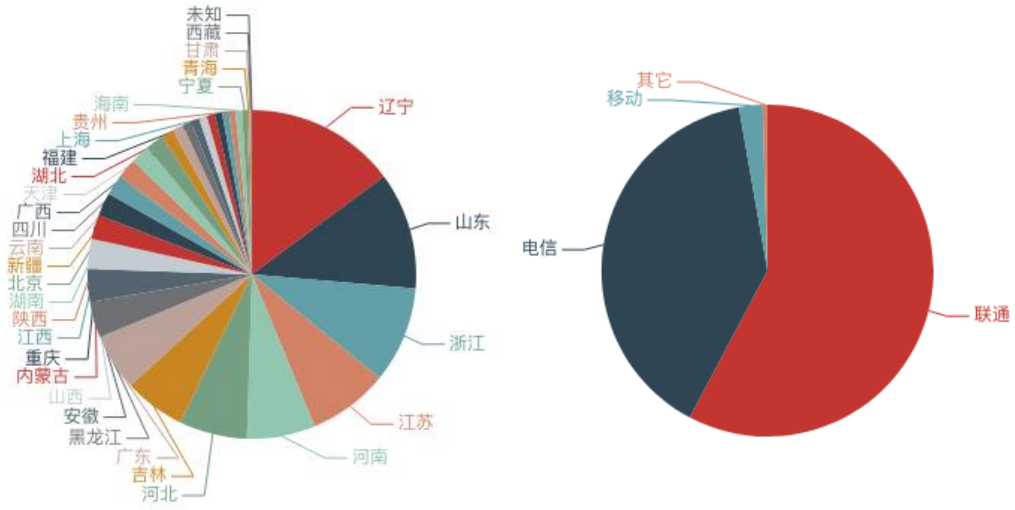

图 8 2018 年以来被利用发起 SSDP 反射攻击的境内反射服务器数量按省份和运营商分布

2018 年以来被利用发起 SSDP 反射攻击的境外反射服务器数量按国家或地区统计，俄罗斯占比最大，占 19.7%，其次是中国台湾、美国和意大利，如图 9 所示。

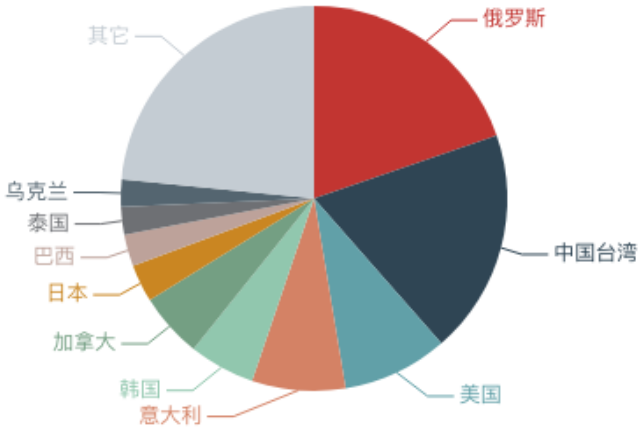

图 9 2018 年以来被利用发起 SSDP 反射攻击的境外反射服务器数量按国家或地区分布

2018 年以来被利用发起 SSDP 反射攻击的境内反射服务器按攻击事件数量排名 TOP30 的反射服务器及归属如表 5 所示，位于云南省的地址最多。

表 5 2018 年以来境内被利用发起 SSDP 反射攻击的反射服务器按涉事数量 TOP30

反射服务器地址	归属省份	归属运营商
116.X.X.15	云南省	中国电信
123.X.X.202	内蒙古自治区	中国电信
120.X.X.234	新疆维吾尔自治区	中国电信
111.X.X.5	湖北省	中国移动
112.X.X.50	云南省	中国电信
113.X.X.14	广西壮族自治区	中国电信
101.X.X.206	上海市	中国电信
111.X.X.69	宁夏回族自治区	中国移动
218.X.X.90	宁夏回族自治区	中国电信
116.X.X.98	上海市	中国电信
111.X.X.182	湖南省	中国移动
118.X.X.118	甘肃省	中国电信
124.X.X.54	上海市	中国电信
116.X.X.163	广西壮族自治区	中国电信
117.X.X.196	新疆维吾尔自治区	中国移动
116.X.X.191	云南省	中国电信
120.X.X.102	新疆维吾尔自治区	中国电信
120.X.X.138	新疆维吾尔自治区	中国电信
117.X.X.46	上海市	中国联通
1.X.X.10	内蒙古自治区	中国电信

119.X.X.138	广东省	中国电信
116.X.X.10	云南省	中国电信
182.X.X.97	云南省	中国电信
218.X.X.163	湖南省	中国电信
117.X.X.182	新疆维吾尔自治区	中国移动
125.X.X.192	广西壮族自治区	中国电信
222.X.X.209	云南省	中国电信
111.X.X.6	黑龙江省	中国移动
101.X.X.34	上海市	中国电信
113.X.X.94	陕西省	中国电信

（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 年以来通过跨域伪造流量发起攻击的流量来源于 426 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.9、221.X.X.5）参与的攻击事件数量最多，其次是归属于北京市电信（219.X.X.70）的路由器，如表 6 所示。

表 6 2018 年以来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.9	新疆维吾尔自治区	中国移动
221.X.X.5	新疆维吾尔自治区	中国移动
219.X.X.70	北京市	中国电信
113.X.X.253	湖北省	中国联通
113.X.X.252	湖北省	中国联通
221.X.X.6	新疆维吾尔自治区	中国移动
61.X.X.25	浙江省	中国电信
218.X.X.101	内蒙古自治区	中国联通
120.X.X.9	广东省	中国联通
120.X.X.8	广东省	中国联通
222.X.X.200	山东省	中国电信
150.X.X.2	山东省	中国电信
222.X.X.1	广西省	中国电信
211.X.X.19	贵州省	中国移动
150.X.X.1	山东省	中国电信

222.X.X.2	广西省	中国电信
221.X.X.253	广东省	中国联通
221.X.X.254	广东省	中国联通
222.X.X.201	山东省	中国电信
220.X.X.253	北京市	中国电信
218.X.X.177	贵州省	中国移动
218.X.X.176	贵州省	中国移动
220.X.X.243	北京市	中国电信
211.X.X.20	贵州省	中国移动
202.X.X.137	浙江省	中国电信

2018 年以来跨域伪造流量涉及路由器按省份分布统计，北京市占比最大，占 16.2%，其次是江苏省和广东省；按路由器所属运营商统计，中国联通占比最大，占 34.4%，中国移动占 28.8%，中国电信占 22.8%，如图 10 所示。

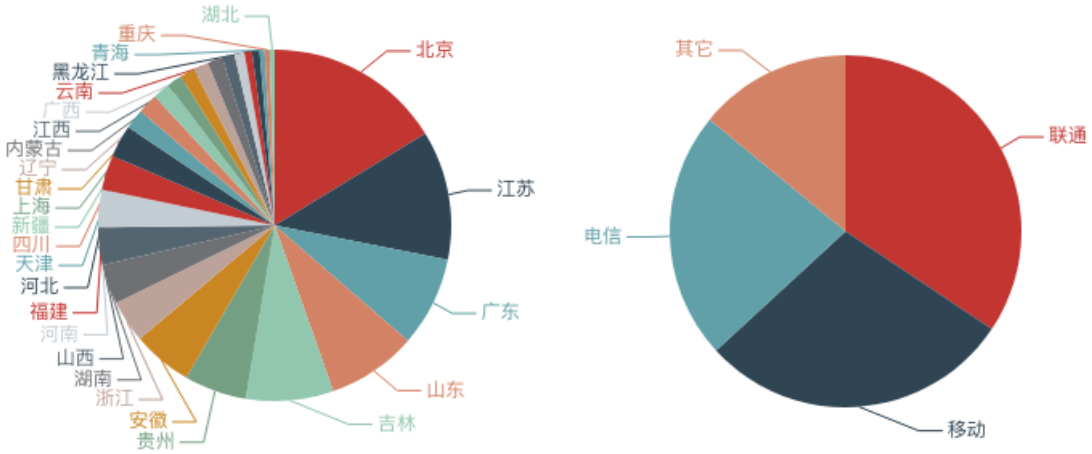

图 10 2018 年以来跨域伪造流量来源路由器数量按省份和运营商分布

2.本地伪造流量来源路由器

根据 CNCERT 抽样监测数据，2018 年以来通过本地伪造流量发起攻击的流量来源于 1019 个路由器。根据参与攻击事件的数量统计，归属于北京市电信的路由器（220.X.X.243、220.X.X.253）参与的攻击事件数量最多，其次是归属于浙江省电信的路由器（220.X.X.127、220.X.X.126），如表 7 所示。

表 7 2018 年以来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.X.X.243	北京市	中国电信
220.X.X.253	北京市	中国电信
220.X.X.127	浙江省	中国电信
220.X.X.126	浙江省	中国电信
219.X.X.2	山西省	中国电信
61.X.X.4	浙江省	中国电信
118.X.X.169	四川省	中国电信
219.X.X.10	山西省	中国电信
211.X.X.19	贵州省	中国移动
61.X.X.8	浙江省	中国电信
211.X.X.254	河南省	中国移动
211.X.X.253	河南省	中国移动
221.X.X.1	河南省	中国移动
221.X.X.2	河南省	中国移动
222.X.X.16	新疆维吾尔自治区	中国电信
222.X.X.15	新疆维吾尔自治区	中国电信
211.X.X.20	贵州省	中国移动
222.X.X.2	吉林省	中国联通
150.X.X.1	山东省	中国电信
150.X.X.2	山东省	中国电信
118.X.X.168	四川省	中国电信
218.X.X.177	贵州省	中国移动
218.X.X.176	贵州省	中国移动
222.X.X.4	吉林省	中国联通
218.X.X.130	四川省	中国电信

2018 年以来本地伪造流量涉及路由器按省份分布，江苏省占比最大，占 10.4%，其次是山东省、河南省和北京市；按路由器所属运营商统计，中国电信占比最大，占 37.9%，中国移动占 32.5%，中国联通占 20.6%，如图 11 所示。

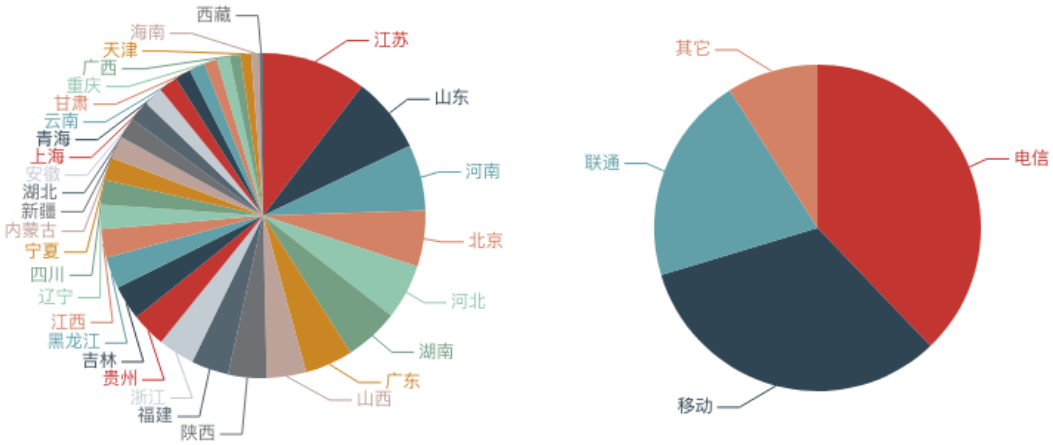

图 11 2018 年以来本地伪造流量来源路由器数量按省份和运营商分布

三、我国境内攻击资源年度活跃及治理情况分析

2018 年以来，在主管部门指导下，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 DDoS 网络攻击资源进行了专项治理，取得了较好的效果:

根据 CNCERT 自主监测数据，综合境内各类 DDoS 网络攻击资源的变化趋势，（1）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；（2）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每月的新增率不变、消亡率相比 2017 年月度平均数值呈现一定程度的上升，意味着资源消亡速度加快，可利用的资源数量逐步减少；（3）反射服务器资源每月的消亡率不变、新增率相比 2017 年月度平均数值呈现一定程度的下降，意味着可新增的资源数量逐步减少。

根据外部分析报告，（1）国际安全厂商卡巴斯基“全球

DDoS 攻击每季度分析系列报告”[1]显示，位于我国境内的僵尸网络控制端数量在全球的占比呈现逐年下降趋势，控制端数量在全球的排名呈现上升趋势，说明位于我国境内的僵尸网络控制端数量持续减少；（2）中国电信云堤与安全企业绿盟共同发布的《2018 年 DDoS 攻击态势报告》[2]指出，得益于对反射攻击的有效治理，全年 DDoS 攻击次数较 2017 年下降 28.4%，特别是反射攻击较去年减少了 80%，活跃反射源下降了 60%，特别是 SSDP 反射源有显著的减少。

具体情况如下:

（一）我国境内攻击资源年度活跃趋势

1、控制端资源

2018 年，利用肉鸡发起 DDoS 攻击的境内控制端平均每月数量为 38.5 个，较 2017 年平均每月数量相比下降 46%。境内控制端资源每月的新增率为 75%，消亡率为 77%，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。其中，位于上海市的境内控制端（182.X.X.227）、位于浙江省的境内控制端（120.X.X.114）、位于北京市的境内控制端（117.X.X.204）、在近三个月甚至半年内持续活跃。

2、肉鸡资源

2018 年以来，被利用发起 DDoS 攻击的境内肉鸡平均每月

[1] https://securelist.com
[2] http://www.nsfocus.com.cn/content/details_62_2915.html

数量为 130,292 个，与 2017 年平均每月数量相比下降 37%。境内肉鸡资源每月的新增率为 78%，消亡率为 76%，与 2017 年平均每月 87%的新增率和 88%的消亡率相比均有所下降。

截止 2018 年 12 月仍被利用的境内肉鸡资源中，监测发现有 2,658 个肉鸡本年度持续活跃超过六个月，这些肉鸡资源根据涉及事件数量排序 TOP20 如表 8 所示。

表 8 2018 年持续活跃超过六个月的境内肉鸡根据发起 DDoS 攻击事件数量 TOP20

肉鸡地址	归属省份	归属运营商或云服务商
222.X.X.63	贵州省	中国电信
122.X.X.166	浙江省	中国电信
122.X.X.199	河南省	中国联通
60.X.X.211	山西省	中国联通
121.X.X.3	浙江省	阿里云
121.X.X.2	浙江省	阿里云
121.X.X.1	浙江省	阿里云
202.X.X.138	新疆维吾尔自治区	中国电信
220.X.X.58	广西壮族自治区	中国电信
183.X.X.101	江苏省	中国移动
42.X.X.7	北京市	中国电信
58.X.X.243	江苏省	中国联通
183.X.X.79	浙江省	中国电信
117.X.X.248	江西省	中国电信
218.X.X.249	广西壮族自治区	中国电信
202.X.X.202	北京市	中国联通
119.X.X.27	广东省	中国电信
183.X.X.182	浙江省	中国移动
121.X.X.89	浙江省	阿里云
112.X.X.234	江苏省	中国联通

上述持续活跃超过六个月的境内肉鸡资源按省份统计，广东省占的比例最大，占 14.6%，其次是浙江省、山东省和江苏省；按运营商统计，中国电信占的比例最大，占 57.2%，中国联通占 24.9%，中国移动占 14.3%，如图 12 所示。

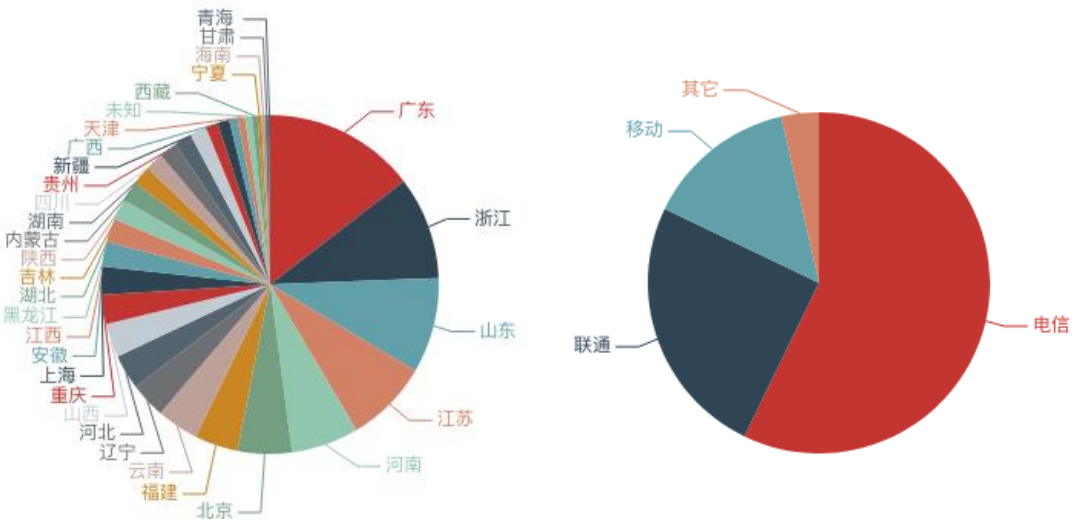

图 12 2018 年持续活跃超过 6 个月的肉鸡数量按省份和运营商分布

3、反射服务器资源

2018 年，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 2,258,099 个。境内反射服务器资源每月的新增率为 65%，消亡率为 71%，与 2017 年平均每月的 85%新增率和的 71%消亡率相比，新增率呈现减缓趋势。

截止 2018 年 12 月仍被利用的境内 Memcached 反射服务器中，监测发现有 1,348 个在本年度持续活跃超过六个月，这些 Memcached 反射服务器根据涉及事件数量排序 TOP20 如表 9 所示。

表 9 2018 年被利用发起攻击超过六个月的境内 Memcached 反射服务器根据攻击事件数量 TOP20

反射服务器地址	归属省份	归属运营商或云服务商
115.X.X.100	山东省	阿里云
123.X.X.128	北京市	阿里云
121.X.X.127	浙江省	阿里云
223.X.X.13	四川省	中国移动
123.X.X.237	北京市	阿里云
182.X.X.143	北京市	阿里云
115.X.X.4	山东省	阿里云
106.X.X.51	北京市	中国电信

117.X.X.92	陕西省	中国电信
101.X.X.178	北京市	阿里云
120.X.X.127	广东省	阿里云
139.X.X.137	上海市	阿里云
60.X.X.105	天津市	中国联通
119.X.X.156	北京市	中国电信
182.X.X.145	北京市	阿里云
101.X.X.253	北京市	阿里云
115.X.X.53	浙江省	阿里云
115.X.X.236	山东省	阿里云
121.X.X.156	浙江省	中国电信
211.X.X.112	湖南省	中国移动

上述持续活跃超过六个月的境内 Memcached 反射服务器按省份统计，山东省占的比例最大，占 10.6%，其次是辽宁省、广东省、浙江省和河南省；按运营商或云服务统计，中国联通占的比例最大，占 45.6%，中国电信占 33.0%，中国移动占 12.0%，阿里云占 6.2%，如图 13 所示。

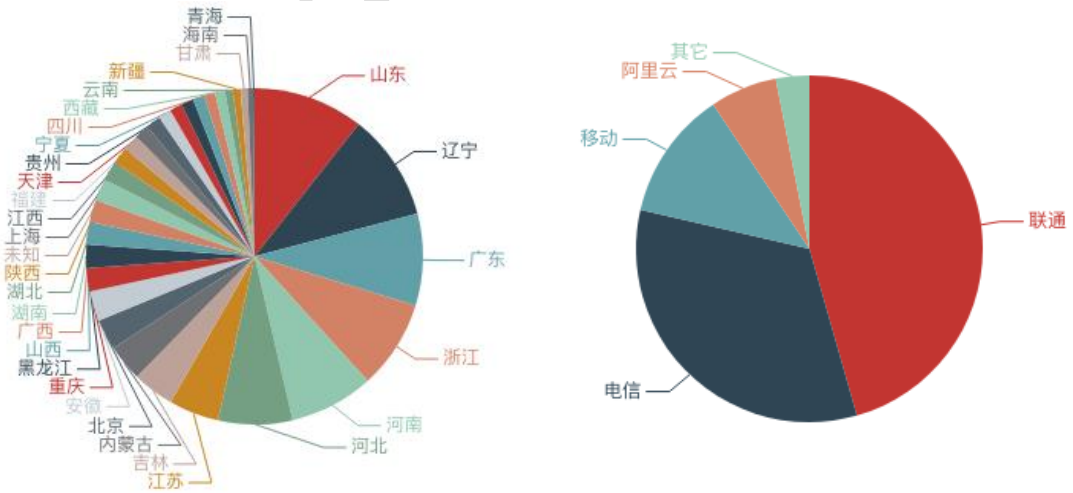

图 13 2018 年活跃超过 6 个月的 Memcached 反射服务器数量按省份运营商或云服务商分布

截止 2018 年 12 月仍被利用的境内 NTP 反射服务器中，监测发现有 89,303 个在本年度持续活跃超过六个月，这些 NTP 反射服务器根据涉及事件数量排序 TOP20 如表 10 所示。

表 10 2018 年被利用发起攻击超过六个月的境内 NTP 反射服务器根据攻击事件数量 TOP20

反射服务器地址	归属省份	归属运营商或云服务商
124.X.X.22	北京市	中国联通
223.X.X.33	四川省	中国移动
59.X.X.62	海南省	中国电信
120.X.X.12	河北省	中国联通
111.X.X.105	河北省	中国移动
101.X.X.56	浙江省	中国联通
125.X.X.2	浙江省	中国电信
61.X.X.130	湖北省	中国联通
221.X.X.37	河南省	中国移动
60.X.X.196	河北省	中国联通
111.X.X.130	西藏自治区	中国移动
61.X.X.38	北京市	中国联通
221.X.X.40	广西壮族自治区	中国联通
183.X.X.179	河北省	中国移动
113.X.X.28	湖北省	中国联通
125.X.X.157	河南省	中国联通
218.X.X.131	安徽省	中国电信
175.X.X.38	吉林省	中国联通
220.X.X.13	湖南省	中国电信
221.X.X.28	浙江省	中国联通

上述持续活跃超过六个月的境内 NTP 反射服务器按省份统计，河北省占的比例最大，占 15.3%，其次山东省、辽宁省、河南省和湖北省；按运营商或云服务统计，中国联通占的比例最大，占 50.8%，中国电信占 31.5%，中国移动占 16.9%，如图 14 所示。

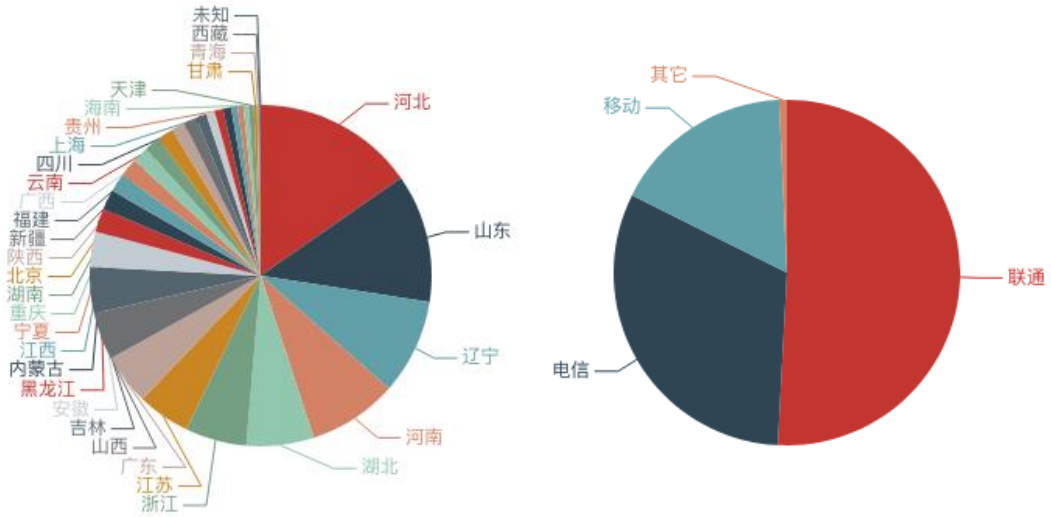

图 14 2018 年以来持续活跃超过 6 个月的 NTP 反射服务器数量按省份运营商或云服务商分布

截止 2018 年 12 月仍被利用的境内 SSDP 反射服务器中，监测发现有 84,867 个在本年度持续活跃超过六个月，这些 SSDP 反射服务器根据涉及事件数量排序 TOP20 如表 11 所示。

表 11 2018 年被利用发起攻击超过六个月的境内 SSDP 反射服务器根据攻击事件数量 TOP20

反射服务器地址	归属省份	归属运营商或云服务商
1.X.X.122	内蒙古自治区	中国联通
124.X.X.122	北京市	鹏博士
119.X.X.114	广东省	中国电信
119.X.X.178	宁夏回族自治区	中国电信
111.X.X.31	安徽省	中国移动
111.X.X.5	湖北省	中国移动
116.X.X.3	上海市	中国电信
1.X.X.38	内蒙古自治区	中国电信
111.X.X.94	湖南省	中国移动
113.X.X.62	广西壮族自治区	中国电信
1.X.X.246	内蒙古自治区	中国电信
183.X.X.202	重庆市	中国电信
120.X.X.150	新疆维吾尔自治区	中国移动
111.X.X.27	山西省	中国移动
111.X.X.191	湖北省	中国移动
220.X.X.120	湖南省	中国电信
182.X.X.22	云南省	中国电信
111.X.X.20	广西壮族自治区	中国移动
222.X.X.230	云南省	中国电信

218.X.X.45	湖北省	中国移动

上述持续活跃超过六个月的境内 SSDP 反射服务器按省份统计，辽宁省占的比例最大，占 14.4%，其次是山东省、浙江省、河北省和河南省；按运营商或云服务统计，中国联通占的比例最大，占 53.0%，中国电信占 38.2%，中国移动占 7.9%，如图 15 所示。

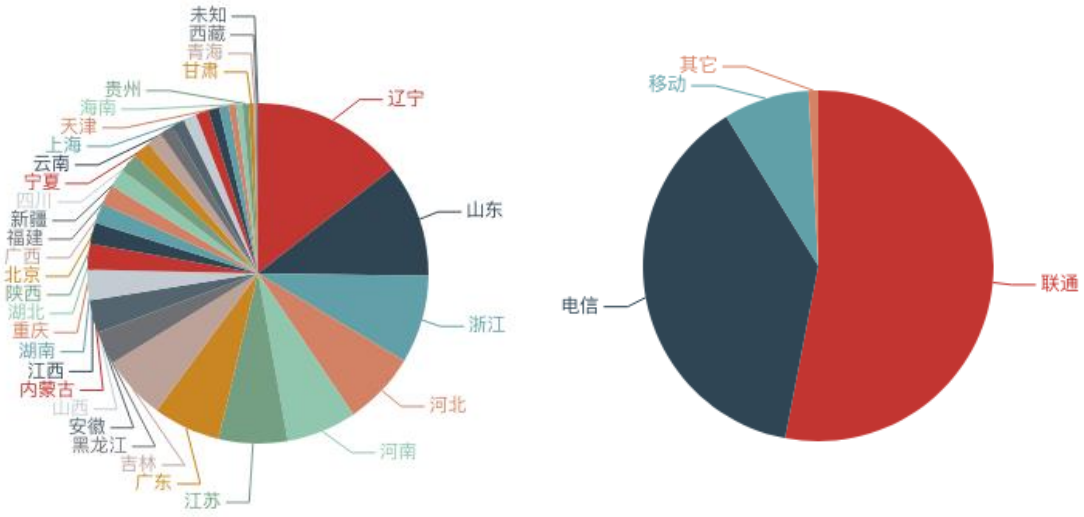

图 15 2018 年以来持续活跃超过 6 个月的 SSDP 反射服务器数量按省份运营商或云服务商分布

4、跨域伪造流量来源路由器资源

2018 年，被利用转发跨域伪造攻击流量的境内运营商路由器平均每月数量为 110 个；境内跨域伪造流量来源路由器资源每月的新增率为 22%，消亡率为 34%，与 2017 年平均每月 22%的新增率和 20%的消亡率相比，资源消亡率加快。

截止 2018 年 12 月，被持续利用转发 DDoS 攻击的境内跨域伪造流量来源路由器中，监测发现有 31 个在近三个月持续活跃，这些路由器根据涉及事件数量排序如表 12 所示。

表 12 近 3 个月持续活跃的境内跨域伪造流量来源路由器地址

跨域伪造流量来源路由器	归属省份	归属运营商
219.X.X.70	北京	中国电信
221.X.X.1	天津	中国电信
220.X.X.243	北京	中国电信
202.X.X.116	天津	中国电信
222.X.X.200	北京	中国电信
222.X.X.201	北京	中国电信
202.X.X.118	天津	中国电信
202.X.X.194	江苏	中国电信集团
202.X.X.195	江苏	中国电信集团
202.X.X.191	江苏	中国电信集团
218.X.X.6	北京	中国电信
222.X.X.201	北京	中国电信
221.X.X.2	天津	中国电信
202.X.X.193	江苏	中国电信集团
202.X.X.192	江苏	中国电信集团
221.X.X.2	江苏	中国移动
221.X.X.3	江苏	中国移动
220.X.X.253	北京	中国电信
202.X.X.232	甘肃	中国电信
202.X.X.210	河南	中国电信
202.X.X.213	河南	中国电信
202.X.X.234	甘肃	中国电信
218.X.X.2	山西	中国联通
112.X.X.38	上海	中国联通
180.X.X.2	北京	中国电信
221.X.X.12	江苏	中国移动
120.X.X.4	山东	中国移动
120.X.X.1	山东	中国移动
218.X.X.1	山西	中国联通
61.X.X.14	北京	中国联通
61.X.X.12	北京	中国联通

5、本地伪造流量来源路由器资源

2018 年，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每月数量为 337 个;境内本地伪造流量来源路由器资源每月的新增率为 12%，消亡率为 26%，与 2017 年平均每月 14%的新增率和 13%的消亡率相比，资源消亡率加快。

截止 2018 年 12 月，被持续利用转发本地伪造流量 DDoS 攻击的境内运营商路由器中，监测发现有 80 个在近三个月持续活跃，这些路由器根据涉及事件数量排序 TOP20 如表 13 所示。

表 13 近 3 个月持续活跃的境内 TOP20 本地伪造流量来源路由器地址

本地伪造流量来源路由器	归属省份	归属运营商
221.X.X.189	广东	中国移动
218.X.X.254	山东	中国联通
61.X.X.1	浙江	中国电信
61.X.X.8	浙江	中国电信
221.X.X.18	河南	中国移动
202.X.X..50	福建	中国电信
61.X.X.4	浙江	中国电信
119.X.X.9	广东	中国电信
221.X.X.229	广东	中国移动
202.X.X.136	浙江	中国电信
59.X.X.1	广东	中国电信
202.X.X.193	江苏	中国电信集团
220.X.X.243	北京	中国电信
180.X.X.2	北京	中国电信
202.X.X.192	江苏	中国电信集团
202.X.X.236	贵州	中国电信
218.X.X.254	山东	中国联通
211.X.X.254	河南	中国移动
211.X.X.253	河南	中国移动
61.X.X.13	江苏	中国电信

按省份统计，浙江省占的比例最大，占 15.0%，其次是广东省、河南省和山东省；按路由器所属运营商统计，中国电信占的比例最大，占 53.8%，中国移动占比 27.5%，中国联通占比 12.5%，如图 16 所示。

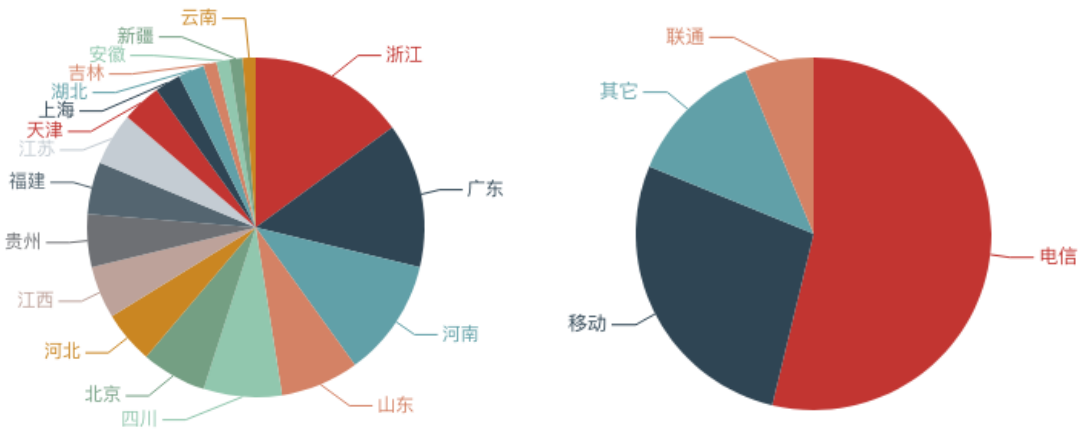

图 16 2018 年被持续利用且本月仍活跃的本地伪造流量来源路由器数量按省份运营商分布

（二）DDoS 攻击资源治理情况及典型案例

1、控制端资源

从 2012 年起，在主管部门指导下，CNCERT 定期组织分中心协调基础电信企业、云服务商持续对恶意程序控制端进行打击，国际安全厂商卡巴斯基 2015 年以来的 DDoS 攻击季度分析报告显示，位于我国境内的僵尸网络控制端数量在全球的占比呈现逐年下降趋势，控制端数量在全球的排名呈现上升趋势，如图 17 和图 18 所示，说明位于我国境内的僵尸网络控制端数量持续减少，治理取得较好成效。

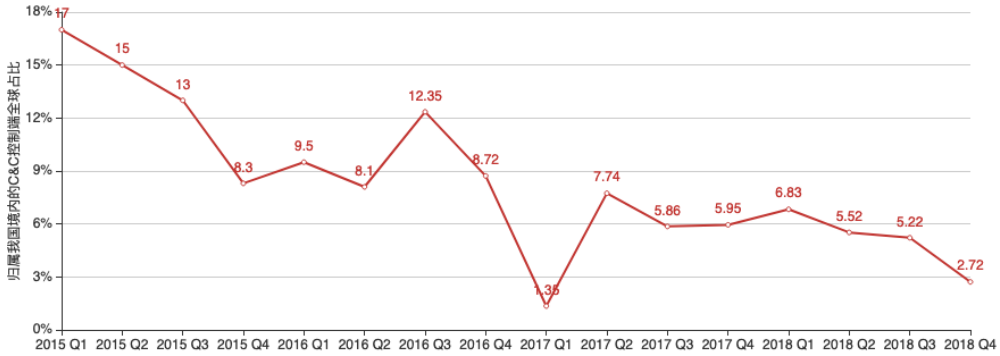

图 17 2015 年至 2018 年我国境内控制端全球占比趋势图

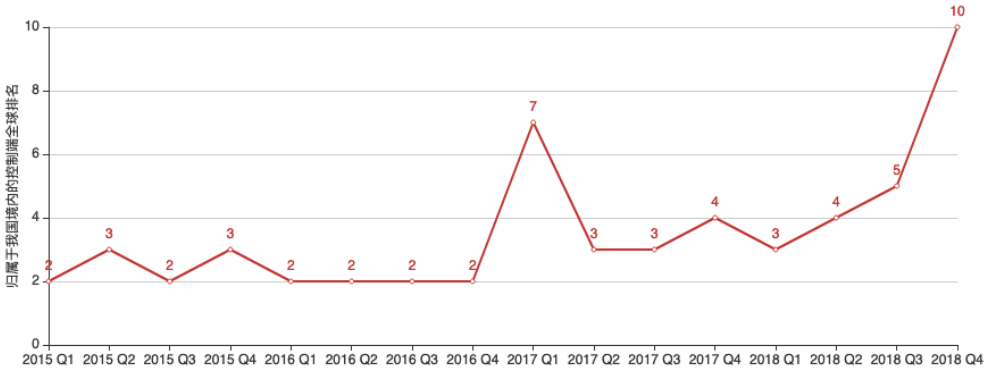

图 18 2015 年至 2018 年我国境内控制端数量全球排名趋势图

2、反射服务器资源

2017 年 12 月开始，在主管部门指导下，CNCERT 组织分中心每月协调基础电信企业、云服务商对我国境内被利用发起反射攻击的反射服务器资源进行通报治理，每月上百万的反射服务器资源的治理难度非常大，经过一年的治理，部分省份取得了较好的治理效果，典型案例如下：

（1）2018 年 4 月，宁夏回族自治区被利用发起 NTP 反射放大攻击的反射服务器 IP 地址数量突增，当月参与攻击的 NTP 反射服务器数量超过 5 万个，在全国排名第一。CNCERT 宁夏分中心协同宁夏电信研判发现，主要原因为宁夏电信近百万台家庭光猫产品均开启了 NTP 服务，黑客可利用 NTP 协议的漏洞向这些光猫发起伪造请求，从而导致大规模 DDoS 攻击。宁夏分中心一方面协调宁夏电信在出口路由器设置了访问控制策略，限制了这些 IP 地址出入口的 NTP 请求；另一方面督促宁夏电信协调中兴、华为、TP-LNK 等光猫厂商对光猫产品升级固件，调整家庭宽带网络架构，从根本上杜绝 NTP 反射

放大攻击行为。此后数月，发起于宁夏回族自治区的 NTP 反射放大攻击大幅度下降。

（2）2018 年 6 月前，山东省每月被利用发起 SSDP 反射放大攻击的反射服务器 IP 地址数量在我国境内范围内一直排名前两位。针对此情况，CNCERT 山东分中心协同山东省运营商研判，山东联通结合自身情况，在网络出口对 1900 端口、11211 端口等采取治理措施，从月均数十万的反射攻击资源规模下降至万量级，大幅降低了省内发起 SSDP、Memcache 等反射放大攻击风险。

3、伪造流量来源路由器资源

2012 年开始，为防范伪造流量攻击，各基础运营商开展了虚假源地址整治工作，通过部署 URPF 或 ACL 等策略实现对虚假源地址的过滤。2018 年度，CNCERT 组织分中心加大力度，协助各地基础运营商，为其提供虚假源地址验证策略效果不明显、仍存在虚假流量的相关区域的攻击事件详情，帮助进一步减少运营商网内发起的包含反射攻击在内的伪造流量攻击。经过一年的治理，部分省份取得了较好的治理效果，典型案例如下:

（1）在跨域伪造流量来源路由器治理方面，存在多地基础运营商的接入层路由器部署的 URPF 或 ACL 等策略与某些业务冲突或未生效的情况，通过以 CNCERT 发现的攻击事件触发排查，江西、福建、吉林、河北、甘肃等省市等多个省市运营

商都对相应的路由器进行了查漏补缺，CNCERT 监测已基本没有发起于该省运营商网内的伪造流量攻击事件;

（2）在本地伪造流量来源路由器治理方面，安徽分中心积极研究虚假源地址防御策略，建立了 URPF 和 ACL 白名单精确过滤法的伪造流量处置方法,实现了只允许本路由器分配给用户的 IP 地址段(白名单)出去，非用户 IP 地址段(虚假 IP)直接丢弃，并纳入了运营商省内交换机、路由器配置规范，确保了以后新增的交换机均按照配置规范进行配置,在本地伪造流量来源路由器治理方面取得了较好的效果。

四、下一步 DDoS 攻击资源治理建议

综上,经过针对我国境内的互联网 DDoS 攻击资源的专项治理工作,各类攻击资源的被利用情况从不同方面呈现了好转趋势,各省针对当地重点资源的集中治理也不同程度地取得了积极效果。我们主要采取了以下措施:

1.针对伪造流量来源路由器，请各基础电信企业根据 CNCERT 监测的攻击事件记录，核查相关路由器的策略配置问题，发现存在配置遗漏的路由器。

2.针对多次参与攻击的控制端和肉鸡由各运营企业对用户进行及时通报并督促其整改并加固设备。

3.针对多次被利用发起反射放大攻击的服务器,由各运营企业及时通知所属用户，NTP 服务器建议升级版本进行 NTP monlist 漏洞修复，关闭 NTP 服务的 monlist 功能；SSDP 服务

器建议所属客户进行 ACL 访问权限控制；Memcached 服务器建议所属用户升级到最新软件版本，以及配置启用 SASL 认证等权限控制策略等措施。

但是，目前的治理工作还存在虚假源地址验证策略部分区域效果不明显、仍存在虚假流量；动态地址定位难、用户不重视；反射服务器资源数量庞大治理难等问题，下一步的治理工作建议如下：

1、 继续做好虚假源地址过滤工作，请**基础电信企业将虚假源地址的安全配置策略下沉到其运营网内的接入层路由器，并做好定期核查**，加大运营企业对其网络下可被利用发起 DDoS 攻击的资源设备的处置力度。

2、 根据各地基础电信企业核查，目前大量被利用的互联网设备为路由器、光纤猫等设备对互联网开放了不必要的端口，**建议推动落实国内各类网络设备厂商网络安全责任，对产品开展出厂检测，严格落实控制默认端口开放和默认口令管理，减轻威胁隐患，联网设备厂商支持在网设备的远程升级，封堵相关漏洞及端口。**

3、加大宣传力度，加强个人用户的安全意识，对网络主机及网络设备需要随时更新漏洞、关闭不需要的服务，安装必要的防毒和防火墙软件，随时注意系统安全。收到基础运营商等运营企业的安全隐患通知后应加以重视。

4、制定工作机制，在各主管部门指导下，由 CNCERT、

基础电信运营企业、互联网企业、安全企业、云服务商等组织联合，共同开展 DDoS 黑产治理工作，充分将企业与中心的数据和监测分析能力相结合，从攻击检测、溯源、处置等不同角度实现优势互补，**发现新型及大规模 DDoS 攻击、从源头上处置大的黑产组织，形成威慑作用。**