我国 DDoS 攻击资源分析报告
(2020 年第 3 季度)

国家计算机网络应急技术处理协调中心

2020 年 11 月

目 录

一、引言.....3

（一）攻击资源定义.....3

（二）本季度重点关注情况.....4

二、DDoS 攻击资源分析.....5

（一）控制端资源分析.....5

（二）肉鸡资源分析.....7

（三）反射攻击资源分析.....10

（1）Memcached 反射服务器资源.....10

（2）NTP 反射服务器资源.....12

（3）SSDP 反射服务器资源.....14

（四）转发伪造流量的路由器分析.....17

（1）跨域伪造流量来源路由器.....17

（2）本地伪造流量来源路由器.....19

一、引言

（一）攻击资源定义

本报告为 2020 年第 3 季度的 DDoS 攻击资源分析报告。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，它们提供的某些网络服务（如 DNS 服务器，NTP 服务器等），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，从而成为被利用发起 DDoS 反射攻击的网络资源。

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）本季度重点关注情况

1、本季度利用肉鸡发起攻击的活跃控制端中，境外控制端按国家和地区统计，最多位于美国、德国和荷兰；境内控制端按省份统计，最多位于上海市、江苏省和北京市，按归属运营商统计，使用 BGP 多线的控制端数量最多。

2、本季度参与攻击的活跃境内肉鸡中，按省份统计最多位于江苏省、安徽省和广东省；按归属运营商统计，电信占比最大。

3、本季度被利用参与 Memcached 反射攻击的活跃境内反射服务器中，按省份统计排名前三名的省份是广东省、河北省、和四川省；数量最多的归属运营商是电信。被利用参与 NTP 反射攻击的活跃境内反射服务器中，按省份统计排名前三名的

省份是河北省、河南省和山东省；数量最多的归属运营商是联通。被利用参与 SSDP 反射攻击的活跃境内反射服务器中，按省份统计排名前三名的省份是浙江省、辽宁省和广东省；数量最多的归属运营商是联通。

4、本季度转发伪造跨域攻击流量的路由器中，位于浙江省、上海市和江苏省的路由器数量最多。本季度转发伪造本地攻击流量的路由器中，位于江苏省、湖南省和江西省的路由器数量最多。

二、DDoS 攻击资源分析

（一）控制端资源分析

2020 年第 3 季度 CNCERT/CC 监测发现，利用肉鸡发起 DDoS 攻击的活跃控制端有 1194 个，其中境外控制端占比 96.3%、云平台控制端占比 75.5%，如图 1 所示，与 2020 年第 2 季度相比境外控制端占比略有下降。

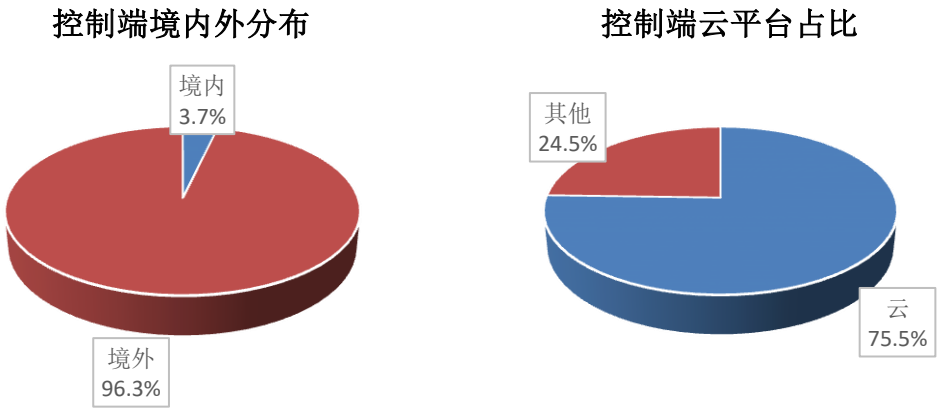


图 1 2020 年第 3 季度发起 DDoS 攻击的控制端数量境内外分布和云平台占比

位于境外的控制端按国家或地区统计，排名前三位的分别为美国（35.3%）、德国（15.7%）和荷兰（14.3%），其中如图 2 所示。

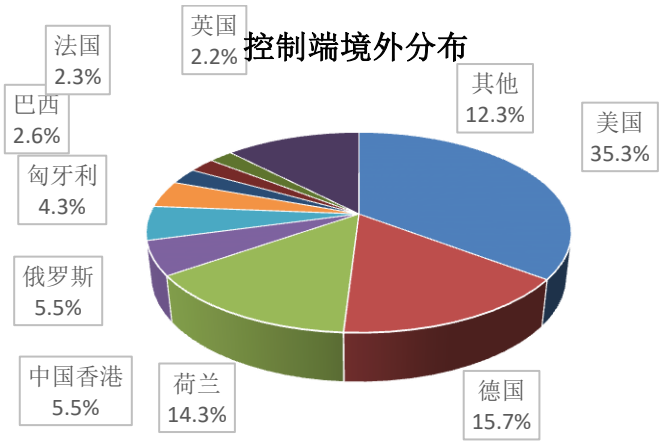


图 2 2020 年第 3 季度发起 DDoS 攻击的境外控制端数量按国家或地区分布

位于境内的控制端按省份统计，排名前三位的分别为上海市（20.5%）、江苏省（13.6%）和北京市（11.4%）；按运营商统计，BGP 多线占 61.4%，电信占 25.0%，联通占 11.4%，移动占 2.3%，如图 3 所示。

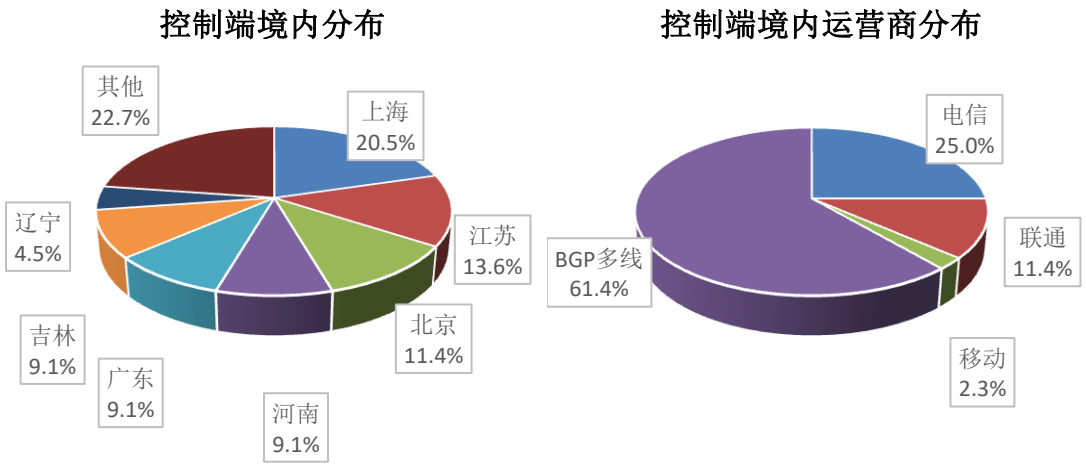


图 3 2020 年第 3 季度发起 DDoS 攻击的境内控制端数量按省份和运营商分布

发起攻击最多的境内控制端地址前二十名及归属如表 1

所示，位于上海市的地址最多。

表 1 2020 年第 3 季度发起攻击的境内控制端 TOP20

控制端地址	归属省份	归属运营商或云服务商
116.X.X.29	湖北	电信
47.X.X.231	广东	阿里云
39.X.X.232	北京	阿里云
61.X.X.190	江苏	电信
116.X.X.215	河南	BGP 多线
119.X.X.154	上海	BGP 多线
122.X.X.98	上海	BGP 多线
119.X.X.92	上海	BGP 多线
122.X.X.232	上海	BGP 多线
47.X.X.240	山东	阿里云
122.X.X.123	河南	BGP 多线
122.X.X.62	上海	BGP 多线
113.X.X.44	吉林	联通
49.X.X.243	上海	BGP 多线
221.X.X.134	吉林	联通
39.X.X.117	广东	阿里云
47.X.X.145	浙江	阿里云
113.X.X.132	吉林	联通
61.X.X.59	江苏	电信
39.X.X.19	北京	阿里云

（二）肉鸡资源分析

2020 年第 3 季度 CNCERT/CC 监测发现，参与真实地址攻击（包含真实地址攻击与反射攻击等其他攻击的混合攻击）的肉鸡 799824 个，其中境内肉鸡占比 92.3%、云平台肉鸡占比 2.9%，如图 4 所示。

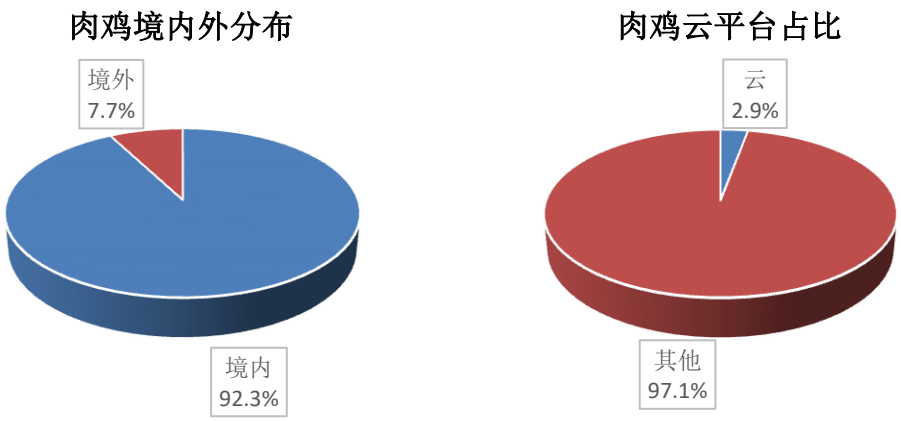


图 4 2020 年第 3 季度参与 DDoS 攻击的肉鸡数量境内外分布和云平台占比

位于境外的肉鸡按国家或地区统计，排名前三位的分别为越南（18.6%）、美国（10.0%）和印度（7.6%），其中如图 5 所示。

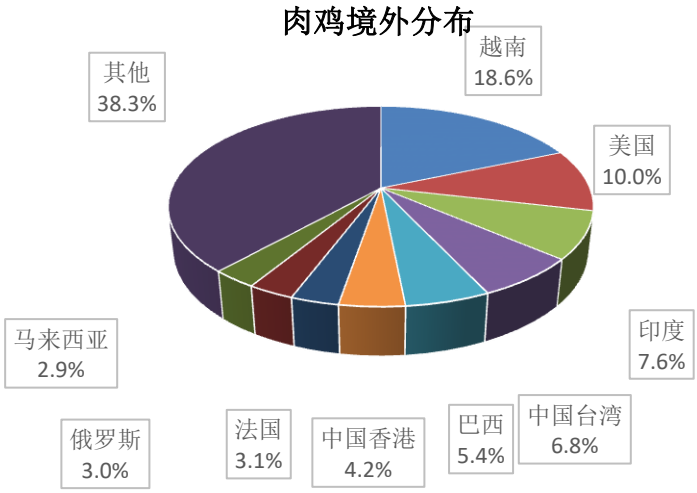


图 5 2020 年第 3 季度参与 DDoS 攻击的境外肉鸡数量按国家或地区分布

位于境内的肉鸡按省份统计，排名前三位的分别为江苏省（10.8%）、安徽省（9.4%）和广东省（8.7%）；按运营商统计，电信占 60.6%，联通占 27.0%，移动占 11.3%，如图 6 所示。

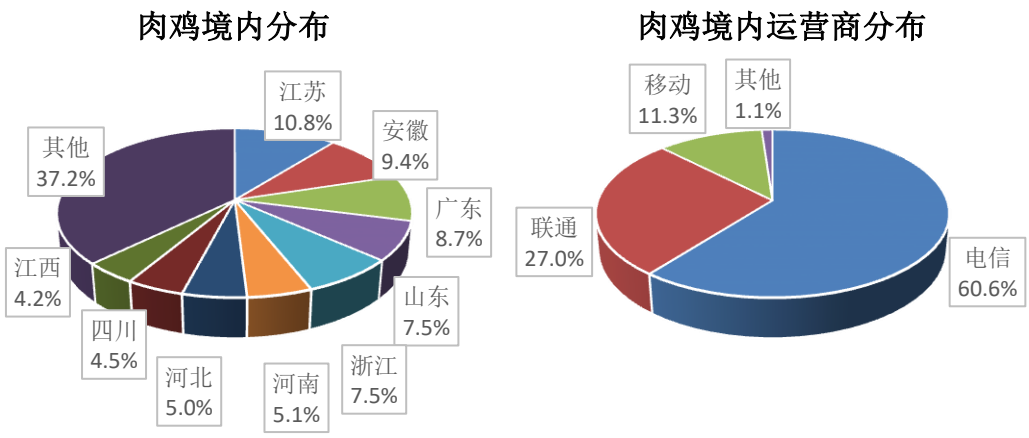


图 6 2020 年第 3 季度参与 DDoS 攻击的境内肉鸡数量按省份和运营商分布

参与攻击最多的境内肉鸡地址前二十名及归属如表 2 所示，位于北京市的地址最多。

表 2 2020 年第 3 季度参与攻击最多的境内肉鸡地址 TOP20

肉鸡地址	归属省份	归属运营商或云服务商
123.X.X.121	北京	BGP 多线
111.X.X.145	北京	联通
124.X.X.117	北京	BGP 多线
111.X.X.201	北京	联通
111.X.X.233	北京	联通
111.X.X.227	北京	联通
39.X.X.75	广东	阿里云
111.X.X.195	北京	联通
36.X.X.5	北京	电信
39.X.X.100	北京	阿里云
139.X.X.173	四川	BGP 多线
36.X.X.66	北京	电信
36.X.X.69	北京	电信
119.X.X.153	上海	BGP 多线
60.X.X.86	黑龙江	联通
61.X.X.245	河北	联通
210.X.X.11	北京	联通
36.X.X.3	北京	电信
101.X.X.238	河北	联通
182.X.X.213	广东	电信

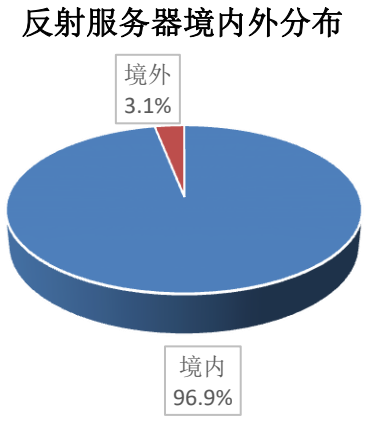
（三）反射攻击资源分析

2020 年第 3 季度 CNCERT/CC 监测发现，参与反射攻击的三类重点反射服务器 6059573 台，其中境内反射服务器占比 57.6%，Memcached 反射服务器占比 1.5%，NTP 反射服务器占比 63.9%，SSDP 反射服务器占比 34.7%。

（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。

2020 年第 3 季度 CNCERT/CC 监测发现，参与反射攻击的 Memcached 反射服务器 88517 个，其中境内反射服务器占比 96.9%、云平台反射服务器占比 2.7%，如图 7 所示。



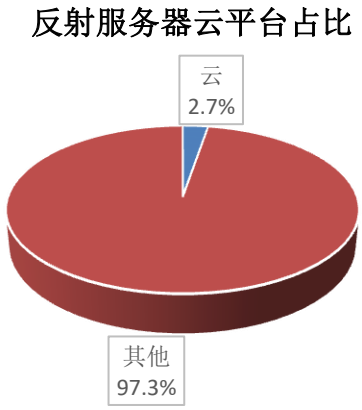


图 7 2020 年第 3 季度 Memcached 反射服务器数量境内外分布和云平台占比

位于境外的反射服务器按国家或地区统计，排名前三位的分别为美国（25.2%）、德国（8.2%）和越南（6.6%），其中如图 8 所示。

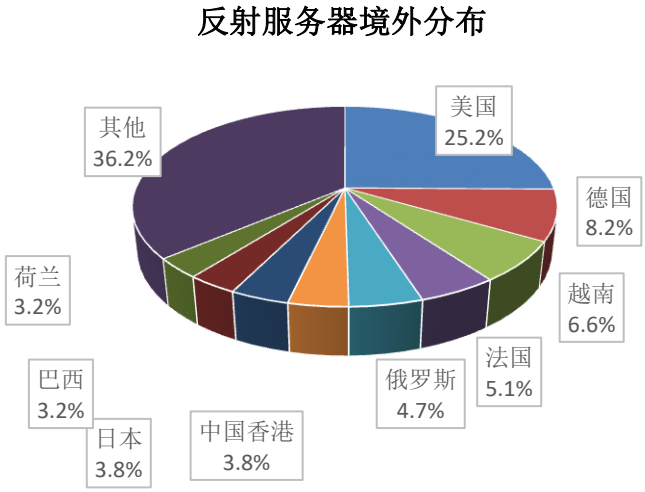


图 8 2020 年第 3 季度境外 Memcached 反射服务器数量按国家或地区分布

位于境内的反射服务器按省份统计，排名前三位的分别为广东省（18.5%）、河北省（6.1%）和四川省（5.3%）；按运营商统计，电信占 81.1%，移动占 9.6%，联通占 8.3%，如图 9 所示。

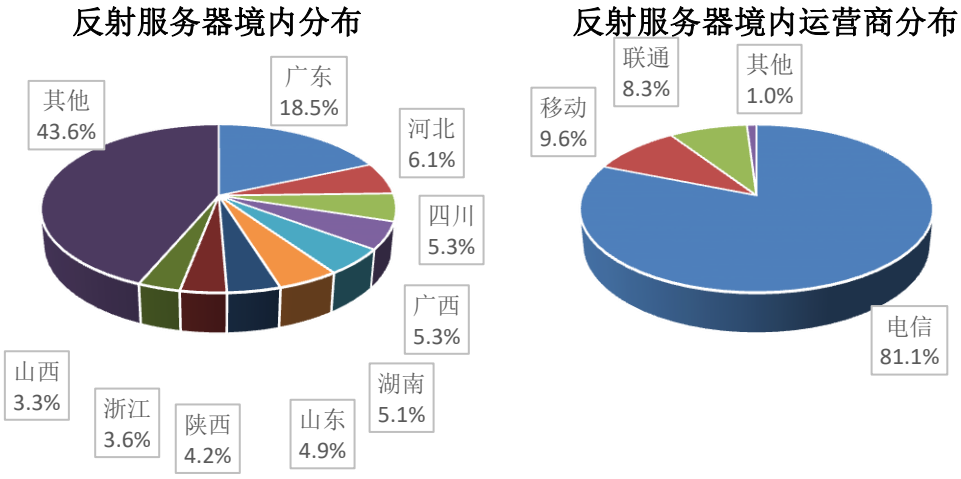


图 9 2020 年第 3 季度境内 Memcached 反射服务器数量按省份和运营商分布

被利用参与 Memcached 反射攻击最多的境内反射服务器地址前二十名及归属如表 3 所示，位于北京市的地址最多。

表 3 2020 年第 3 季度被利用参与 Memcached 反射攻击最多的反射服务器地址 Top20

反射服务器地址	归属省份	归属运营商或云服务商
113.X.X.29	黑龙江	联通
114.X.X.107	上海	京东云
61.X.X.62	北京	联通
121.X.X.221	广东	BGP 多线
117.X.X.56	甘肃	移动
117.X.X.4	广东	BGP 多线
106.X.X.142	北京	电信
183.X.X.143	山西	移动
58.X.X.30	广东	联通
180.X.X.253	北京	电信
116.X.X.169	浙江	阿里云
139.X.X.209	上海	阿里云
112.X.X.182	浙江	阿里云
124.X.X.76	海南	电信
113.X.X.112	广东	电信
39.X.X.227	北京	阿里云
115.X.X.89	江西	电信
117.X.X.220	北京	BGP 多线
121.X.X.171	浙江	阿里云
106.X.X.98	北京	电信

（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。

2020 年第 3 季度 CNCERT/CC 监测发现，参与反射攻击的 NTP 反射服务器 3869980 个，其中境内反射服务器占比 40.

8%、云平台反射服务器占比 1.1%，如图 10 所示。

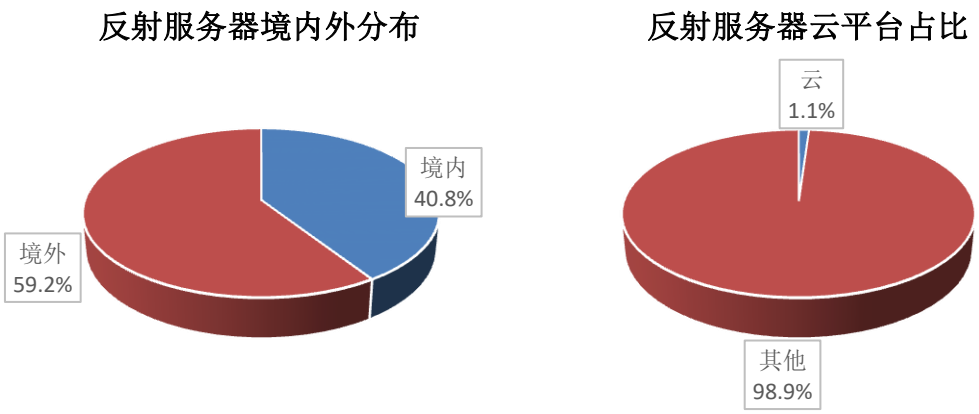


图 10 2020 年第 3 季度 NTP 反射服务器数量境内外分布和云平台占比

位于境外的反射服务器按国家或地区统计，排名前三位的分别为越南（39.1%）、印度（10.9%）和巴西（10.4%），其中如图 11 所示。

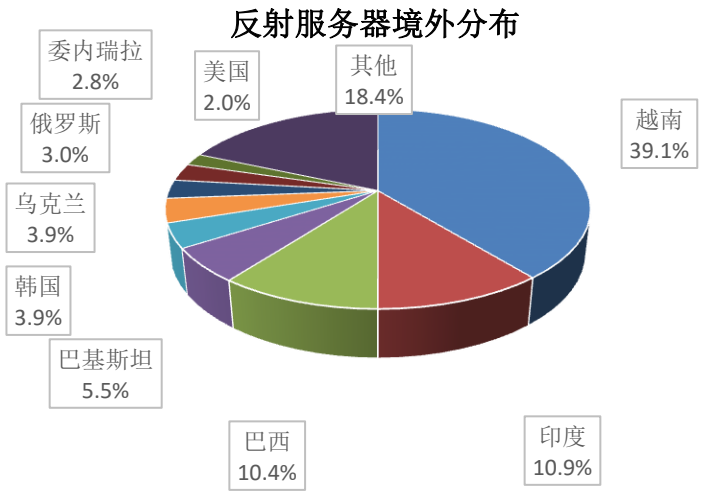


图 11 2020 年第 3 季度境外 NTP 反射服务器数量按国家或地区分布

位于境内的反射服务器按省份统计，排名前三位的分别为河北省（14.4%）、河南省（13.5%）和山东省（12.7%）；按运营商统计，联通占 76.9%，电信占 20.7%，移动占 1.7%，如图 12 所示。

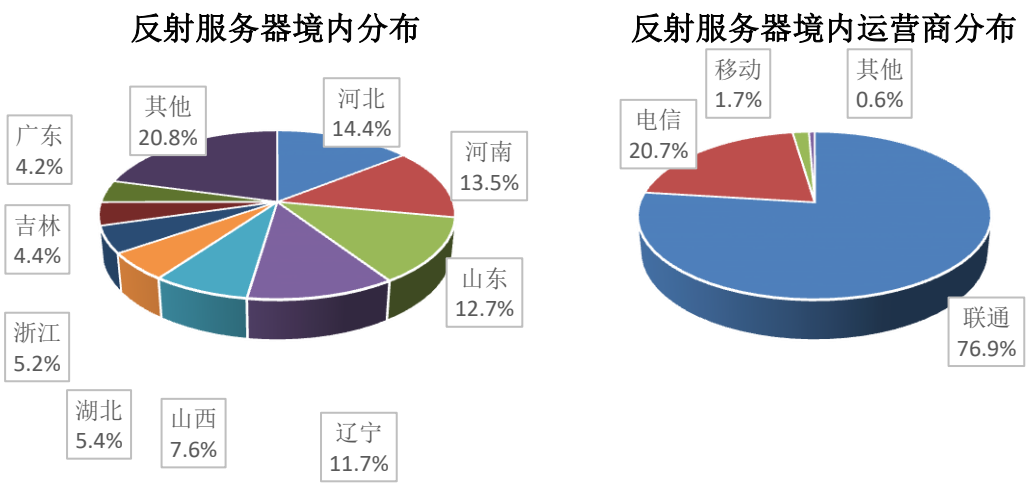


图 12 2020 年第 3 季度境内 NTP 反射服务器数量按省份和运营商分布

被利用参与 NTP 反射攻击最多的境内反射服务器地址前二十名及归属如表 4 所示，位于山西省的地址最多。

表 4 2020 年第 3 季度被利用参与 NTP 反射攻击最多的反射服务器地址 Top20

反射服务器地址	归属省份	归属运营商
119.X.X.50	宁夏	电信
221.X.X.201	山西	联通
221.X.X.196	山西	联通
221.X.X.70	山西	联通
221.X.X.52	山西	联通
221.X.X.209	山西	联通
221.X.X.227	山西	联通
221.X.X.207	山西	联通
221.X.X.197	山西	联通
221.X.X.52	山西	联通
221.X.X.61	山西	联通
221.X.X.96	山西	联通
221.X.X.56	山西	联通
221.X.X.93	山西	联通
221.X.X.61	山西	联通
221.X.X.83	山西	联通
221.X.X.76	山西	联通
221.X.X.73	山西	联通
221.X.X.58	山西	联通
221.X.X.57	山西	联通

（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。

2020 年第 3 季度 CNCERT/CC 监测发现，参与反射攻击的 SSDP 反射服务器 2101076 个，其中境内反射服务器占比 86.9%、云平台反射服务器占比 0.1%，如图 13 所示。

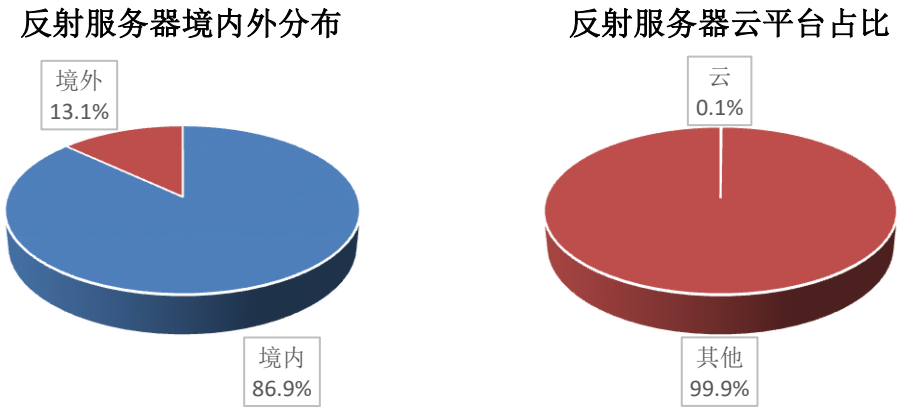


图 13 2020 年第 3 季度 SSDP 反射服务器数量境内外分布和云平台占比

位于境外的反射服务器按国家或地区统计，排名前三位的分别为俄罗斯（13.3%）、韩国（9.6%）和日本（7.9%），其中如图 14 所示。

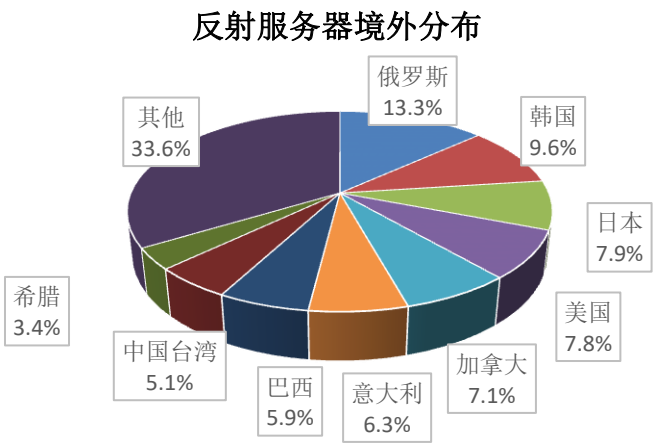


图 14 2020 年第 3 季度境外 SSDP 反射服务器数量按国家或地区分布

位于境内的反射服务器按省份统计，排名前三位的分别为浙江省（17.1%）、辽宁省（16.6%）和广东省（11.8%）；按运营商统计，联通占 51.0%，电信占 47.9%，移动占 0.4%，如图 15 所示。

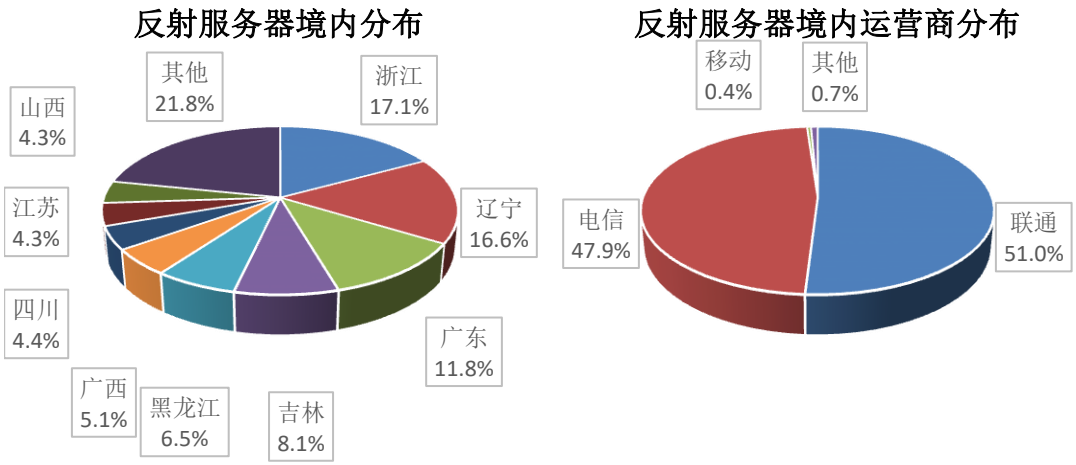


图 15 2020 年第 3 季度境内 SSDP 反射服务器数量按省份和运营商分布

被利用参与 SSDP 反射攻击最多的境内反射服务器地址前二十名及归属如表 5 所示，位于陕西省的地址最多。

表 5 2020 年第 3 季度被利用参与 SSDP 反射攻击最多的反射服务器地址 Top20

反射服务器地址	归属省份	归属运营商

59.X.X.242	山西	电信
60.X.X.203	山西	联通
219.X.X.146	山西	电信
60.X.X.115	山西	联通
118.X.X.118	甘肃	电信
203.X.X.62	辽宁	电信
110.X.X.18	青海	电信
61.X.X.38	陕西	电信
122.X.X.10	浙江	电信
58.X.X.110	上海	联通
27.X.X.62	上海	联通
223.X.X.133	山西	电信
222.X.X.254	内蒙古	电信
61.X.X.14	陕西	电信
219.X.X.42	陕西	电信
222.X.X.245	上海	电信
1.X.X.130	内蒙古	电信
60.X.X.181	山西	联通
219.X.X.60	陕西	电信
61.X.X.175	陕西	电信

（四）转发伪造流量的路由器分析

（1）跨域伪造流量来源路由器

2020 年第 3 季度 CNCERT/CC 监测发现，转发跨域伪造流量的路由器 57 个；按省份统计，排名前三位的分别为浙江省（19.6%）、上海市（19.6%）和江苏省（15.7%）；按运营商统计，电信占 84.2%，移动占 8.8%，联通占 7.0%，如图 16 所示。

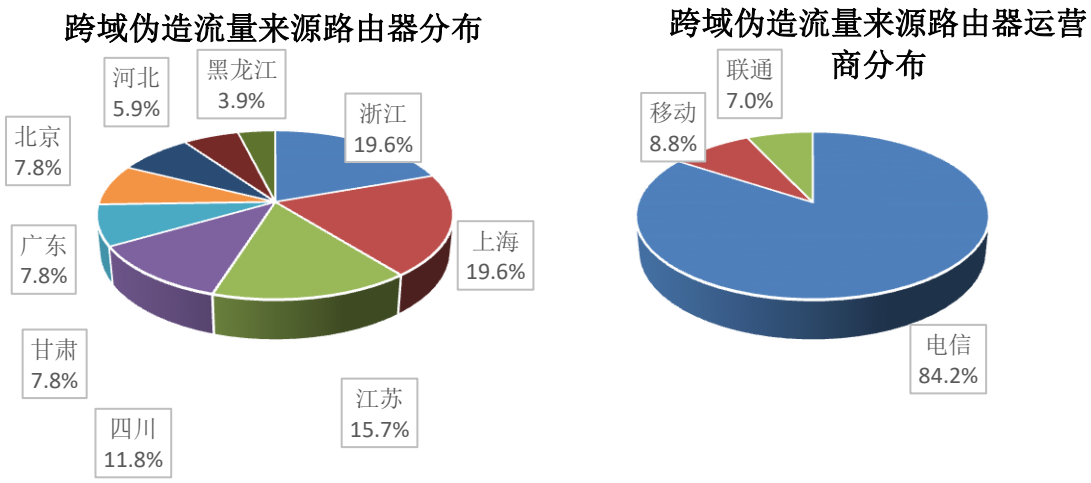


图 16 跨域伪造流量来源路由器数量按省份和运营商分布

根据参与攻击事件的数量统计，参与攻击事件最多的跨域伪造流量来源路由器地址前二十名及归属如表 6 所示，位于浙江省的地址最多。

表 6 2020 年第 3 季度参与攻击最多的跨域伪造流量来源路由器 TOP20

跨域伪造流量来源路由器	归属省份	归属运营商
202.X.X.60	北京	电信
202.X.X.61	北京	电信
61.X.X.1	浙江	电信
61.X.X.1	浙江	电信
61.X.X.8	浙江	电信
61.X.X.4	浙江	电信
202.X.X.160	浙江	电信
211.X.X.156	上海	移动
202.X.X.161	浙江	电信
218.X.X.249	内蒙古	联通
211.X.X.155	上海	移动
202.X.X.222	四川	电信
202.X.X.223	四川	电信
202.X.X.16	上海	电信
219.X.X.70	北京	电信
202.X.X.136	浙江	电信
202.X.X.137	浙江	电信
218.X.X.242	黑龙江	联通
202.X.X.17	上海	电信
202.X.X.118	天津	电信

（2）本地伪造流量来源路由器

2020 年第 3 季度 CNCERT/CC 监测发现，转发本地伪造流量的路由器 505 个；按省份统计，排名前三位的分别为江苏省（16.2%）、湖南省（6.7%）和江西省（6.3%）；按运营商统计，电信占 53.7%，移动占 30.7%，联通占 15.6%，如图 17 所示。

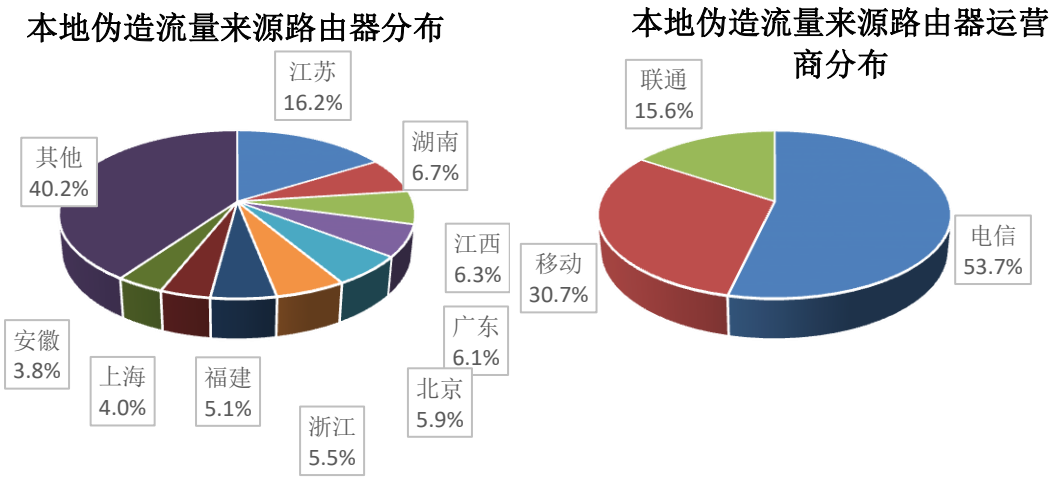


图 17 2020 年第 3 季度本地伪造流量来源路由器数量按省份和运营商分布

根据参与攻击事件的数量统计，参与攻击事件最多的本地伪造流量来源路由器地址前二十名及归属如表 7 所示，位于江苏省的地址最多。

表 7 2020 年第 3 季度参与攻击最多的本地伪造流量来源路由器 TOP20

本地伪造流量来源路由器	归属省份	归属运营商
222.X.X.127	江苏	电信
222.X.X.128	江苏	电信
61.X.X.1	江苏	电信
61.X.X.2	江苏	电信
61.X.X.252	江苏	电信
61.X.X.255	江苏	电信
202.X.X.21	上海	电信
202.X.X.191	江苏	电信

202.X.X.17	上海	电信
219.X.X.70	北京	电信
220.X.X.127	浙江	电信
220.X.X.126	浙江	电信
123.X.X.1	内蒙古	电信
61.X.X.71	江苏	电信
61.X.X.70	江苏	电信
202.X.X.23	上海	电信
202.X.X.241	江苏	电信
61.X.X.254	江苏	电信
222.X.X.1	江苏	电信
220.X.X.253	北京	电信