我国 DDoS 攻击资源月度分析报告

（2018 年 1 月）

国家计算机网络应急技术处理协调中心

2018 年 1 月

目 录

一、引言

（一）攻击资源定义

本报告为 2018 年 1 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 攻击的受控主机节点。

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、 反射攻击流量来源路由器是指转发了大量反射攻击发起流量的运营商路由器。由于反射攻击发起流量需要伪造 IP 地址，因此反射攻击流量来源路由器本质上也是跨域伪造流量来源路由器或本地伪造流量来源路由器。由于反射攻击形式特殊，本报告将反射攻击流量来源路由器单独统计。

5、 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。

6、 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。

为保护网络资源信息不被恶意利用，报告中提及的具体 IP 地址都进行了脱敏处理。

（二）本月重点关注情况

1、本月参与攻击较多的肉鸡地址大量归属于江苏省。其中，涉及江苏省移动多个地址段的肉鸡被反复多次利用，需要重点关注，详见 2.2 节。

2、本月包含跨域伪造流量的 DDoS 攻击事件占事件总量的比例较上月有较大程度的下降。归属于浙江省和上海市的近两年持续活跃的跨域伪造流量来源路由器数量最多，详见 2.4

节。

3、近期持续活跃的本地伪造流量来源路由器数量占比最大的省份为江苏省、江西省、和福建省，详见 2.4 节。

4、通过对近两月的 DDoS 攻击情况进行对比，境内真实地址攻击事件量、伪造流量攻击事件量在绝大部分省份均有不同程度的减少，治理效果较明显。特别地，北京市、山西省上月的威胁治理工作效果显著，攻击资源和事件数量均有较大程度的下降。

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，2018 年 1 月，利用肉鸡发起 DDoS 攻击的控制端总量为 1,617 个，其中，1,010 个控制端位于境内，607 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 44.0%，其次是加拿大和中国香港，如图 1 所示。

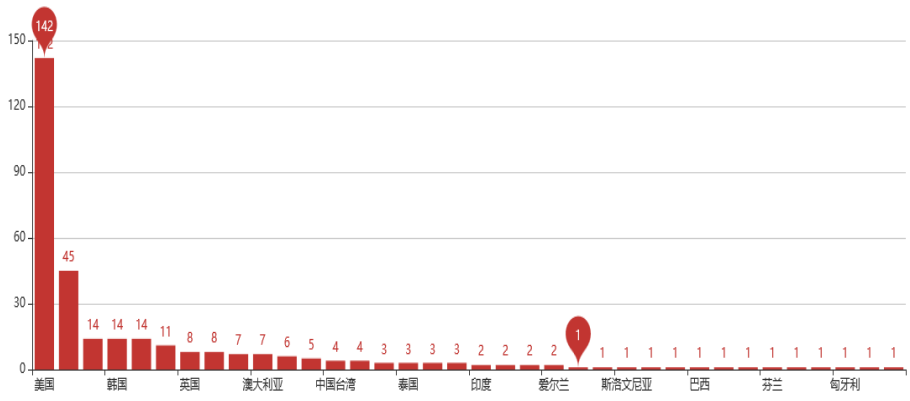

图 1 本月发起 DDoS 攻击的境外控制端数量按国家或地区 TOP30

位于境内的控制端按省份统计，广东省占的比例最大，占 15.9%，其次是北京市、上海市和浙江省；按运营商统计，电信占的比例最大，占 46.8%，联通占 29.3%，移动占 15.6%，如图 2 所示。

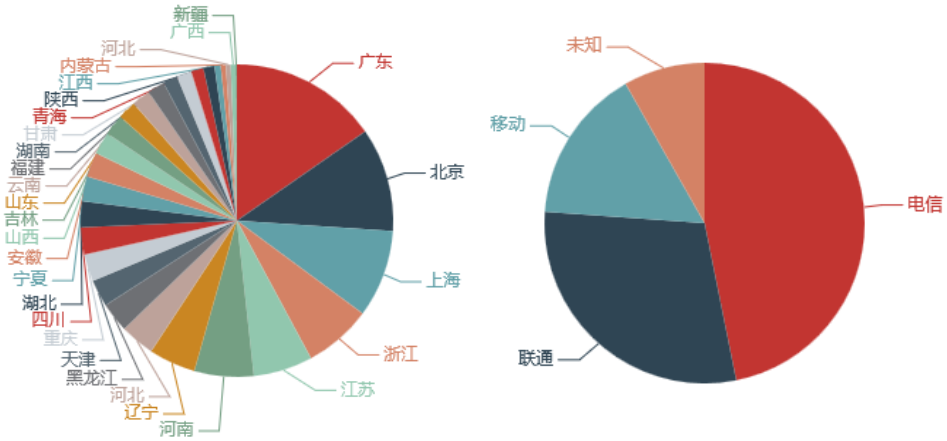

图 2 本月发起 DDoS 攻击的境内控制端数量按省份和运营商分布

发起攻击最多的境内控制端前二十名及归属如表 1 所示，主要位于广东省、江苏省、浙江省和北京市。

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
119.X.X.94	广东省	电信
123.X.X.230	广东省	电信
61.X.X.52	江苏省	电信
222.X.X.120	江苏省	电信
14.X.X.42	广东省	电信
119.X.X.195	广东省	电信
47.X.X.74	广东省	待确认
183.X.X.78	浙江省	电信
58.X.X.97	江苏省	电信
223.X.X.9	辽宁省	移动
183.X.X.19	浙江省	电信
52.X.X.23	北京市	待确认
52.X.X.87	北京市	待确认
52.X.X.180	北京市	待确认

180.X.X.82	江苏省	电信
54.X.X.116	北京市	电信
104.X.X.93	上海市	待确认
183.X.X.227	浙江省	电信
103.X.X.175	广东省	待确认
183.X.X.43	浙江省	电信

本月平均每个控制端在 3.69 天尝试发起了 DDoS 攻击，攻击天次最多的控制端地址位于美国（155.X.X.207），在 28 天范围内发起了攻击，超过总监测天数的十分之九。

2017 年度攻击月次超过 6 月次的 21 个控制端中，有两个控制端在本月仍活跃，分别是归属浙江省的电信地址（121.X.X.62）及归属上海市的电信地址（180.X.X.134）。此外，2017 年度发起 DDoS 攻击次数在 TOP100 的控制端中，仅发现位于美国的两个 IP 地址（23.X.X.170、23.X.X.131）在本月仍活跃外，其它控制端均未监测到其进一步发起 DDoS 攻击事件。

2017 年 12 月监测到的控制端中，41.1%的控制端在本月仍处于活跃状态，共计 627 个，其中位于我国境内的控制端数量为 557 个，位于境外的控制端数量为 70 个。近两月持续活跃的境内控制端按省份统计，广东省占的比例最大，为 13.1%，其次是北京市、浙江省和上海市；按运营商统计，电信占的比例最大，为 42.2%，联通占 30.2%，移动占 18.5%，如图 3 所示。

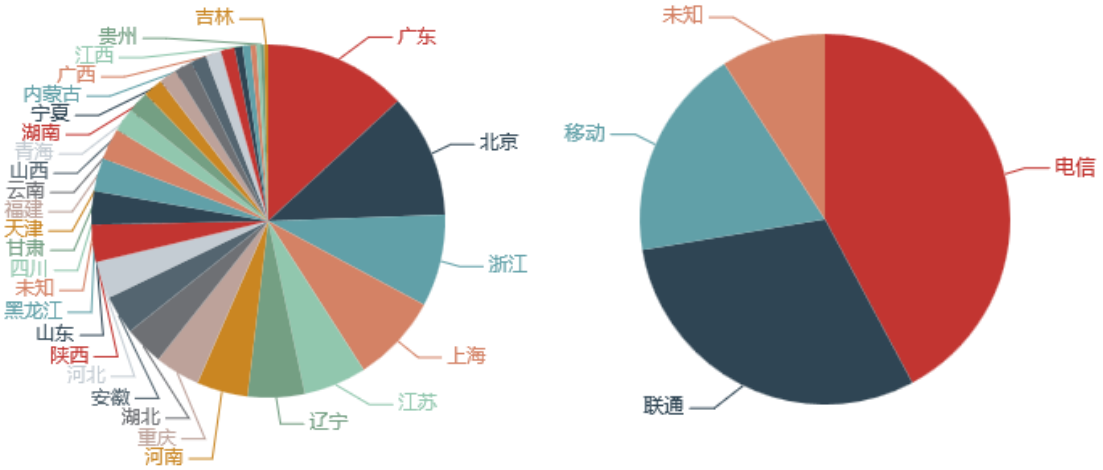

图 3 近两月活跃的发起 DDoS 攻击的境内控制端数量按省份和运营商分布

（二）肉鸡资源分析

根据 CNCERT 抽样监测数据，2018 年 1 月，利用真实地址攻击（包含真实地址攻击与其它攻击的混合攻击）的 DDoS 攻击事件占事件总量的 70.3%。其中，共有 104,597 个肉鸡地址参与攻击，涉及 38,482 个 IP 地址 C 段。

这些肉鸡资源按省份统计，江苏省占的比例最大，为 28.8%，其次是重庆市、湖北省和福建省；按运营商统计，电信占的比例最大，为 46.3%，移动占 41.8%，联通占 9.5%，如图 4 所示。

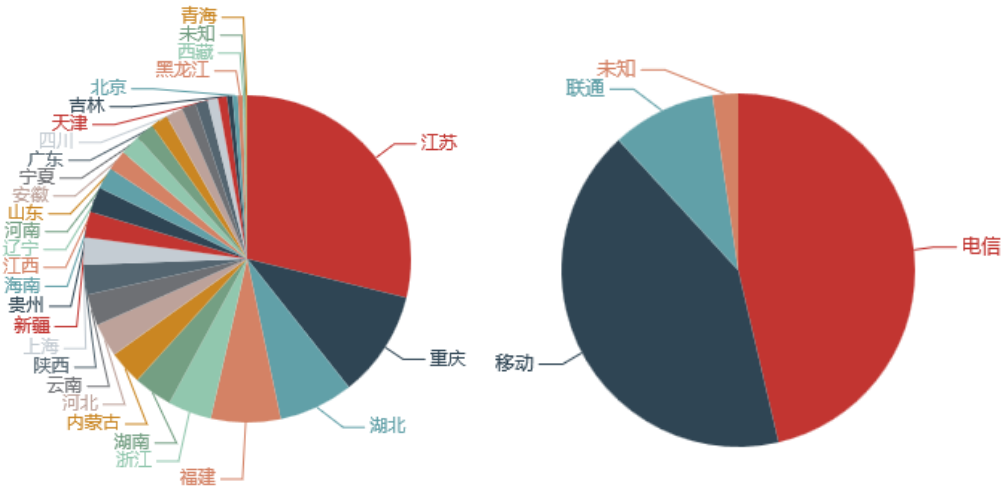

图 4 本月肉鸡地址数量按省份和运营商分布

本月参与攻击最多的肉鸡地址前二十名及归属如表 2 所示，位于江苏省的地址最多。其中，涉及江苏省移动多个地址段的肉鸡被反复多次利用，需要重点关注。

表 2 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
112.X.X.229	江苏省	移动
112.X.X.230	江苏省	移动
112.X.X.31	江苏省	移动
112.X.X.49	江苏省	移动
112.X.X.48	江苏省	移动
112.X.X.33	江苏省	移动
112.X.X.32	江苏省	移动
112.X.X.154	安徽省	移动
112.X.X.180	安徽省	移动
120.X.X.150	安徽省	移动
183.X.X.87	江苏省	移动
223.X.X.175	江苏省	移动
223.X.X.40	江苏省	移动
223.X.X.103	江苏省	移动
223.X.X.121	江苏省	移动
223.X.X.178	江苏省	移动
223.X.X.49	江苏省	移动
223.X.X.35	江苏省	移动
223.X.X.251	江苏省	移动
223.X.X.142	新疆维吾尔自治区	移动

肉鸡资源在本月被利用参与发起 DDoS 攻击的平均天次达 1.98 次。其中参与攻击天次最多的肉鸡地址为归属于江苏省移动（112.X.X.16、112.X.X.210、112.X.X.10）的地址，分别参与了 18 天次的攻击，接近监测天数的五分之三。

2017 年度攻击月次超过 6 月次的肉鸡中(共计 2094 个)，监测发现有 380 个在本月仍活跃，存活率为 18.1%。这些活跃肉鸡地址按省份统计，辽宁省的数量最多，为 68 个，其次是江苏省、河南省和上海市;按运营商统计，电信占的比例最大，占 43.3%，联通占 39.3%，移动占 13.2%，如图 5 所示。

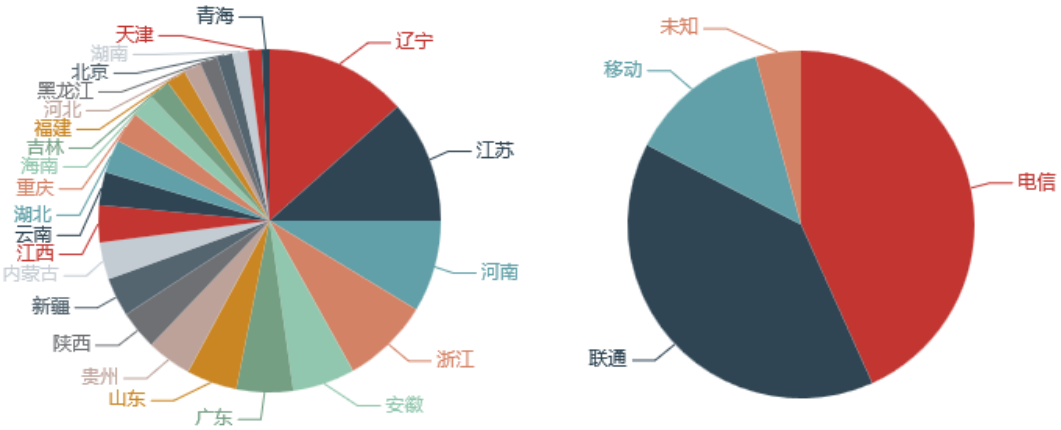

图 52017 年度攻击月次超过 6 月次且本月仍活跃的肉鸡数量按省份和运营商分布

此外，2017 年度被利用发起 DDoS 攻击次数 TOP100 的肉鸡中，监测发现有 29 个在本月仍活跃，存活率为 29%。持续活跃的 29 个肉鸡地址如表 3 所示，其中归属于河南省联通的地址数量最多。

表 3 2017 年度攻击次数 TOP100 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.211	贵州省	联通
58.X.X.211	安徽省	联通
60.X.X.95	安徽省	电信
61.X.X.230	上海市	电信
103.X.X.2	浙江省	待确认
111.X.X.35	黑龙江省	移动
115.X.X.60	浙江省	电信
115.X.X.85	浙江省	电信
116.X.X.84	河南省	联通
116.X.X.128	河南省	联通
122.X.X.166	浙江省	电信
124.X.X.212	安徽省	电信
180.X.X.74	上海市	电信
202.X.X.133	浙江省	电信
202.X.X.138	新疆维吾尔自治区	电信
202.X.X.14	河南省	联通
202.X.X.15	河南省	联通
202.X.X.13	河南省	联通
202.X.X.20	河南省	联通
202.X.X.21	河南省	联通
202.X.X.18	河南省	联通
202.X.X.19	河南省	联通
202.X.X.16	河南省	联通
202.X.X.17	河南省	联通
218.X.X.232	上海市	电信
218.X.X.238	云南省	电信
218.X.X.127	上海市	电信
218.X.X.254	新疆维吾尔自治区	电信
222.X.X.133	新疆维吾尔自治区	电信
58.X.X.211	贵州省	联通
58.X.X.211	安徽省	联通
60.X.X.95	安徽省	电信
61.X.X.230	上海市	电信
103.X.X.2	浙江省	待确认
111.X.X.35	黑龙江省	移动
115.X.X.60	浙江省	电信
115.X.X.85	浙江省	电信
116.X.X.84	河南省	联通
116.X.X.128	河南省	联通
122.X.X.166	浙江省	电信
124.X.X.212	安徽省	电信
180.X.X.74	上海市	电信
202.X.X.133	浙江省	电信

202.X.X.138	新疆维吾尔自治区	电信
202.X.X.14	河南省	联通
202.X.X.15	河南省	联通
202.X.X.13	河南省	联通
202.X.X.20	河南省	联通
202.X.X.21	河南省	联通
202.X.X.18	河南省	联通
202.X.X.19	河南省	联通
202.X.X.16	河南省	联通
202.X.X.17	河南省	联通

2017 年 12 月监测到的肉鸡资源中，5.9%的肉鸡在本月仍处于活跃状态，共计 8161 个。近两月持续活跃的肉鸡资源按省份统计，江苏省占的比例最大，占 31.4%，其次是福建省、重庆市和内蒙古自治区；按运营商统计，移动占的比例最大，占 53.0%，电信占 40.0%，联通占 6.2%，如图 6 所示。

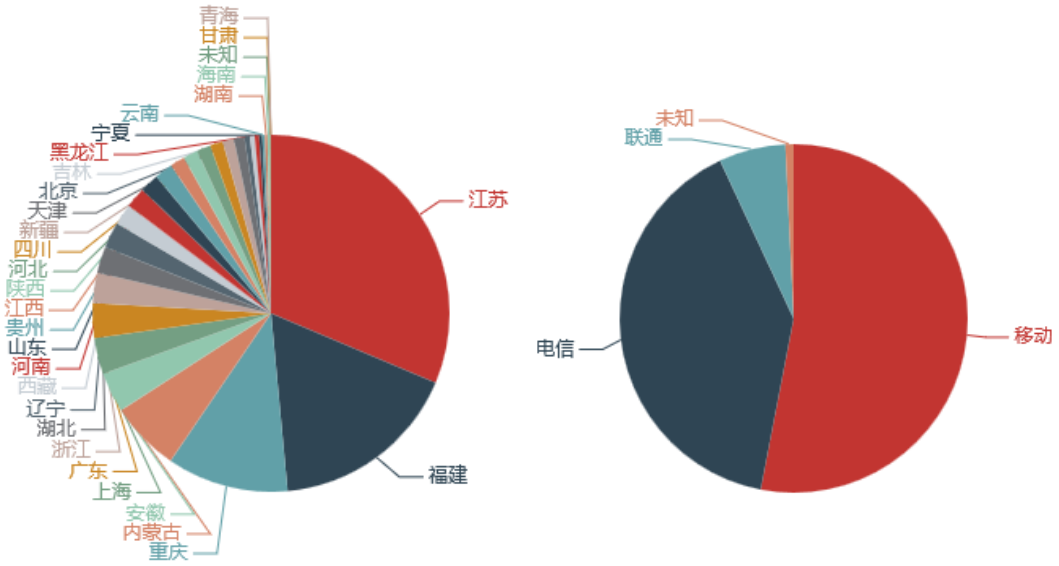

图 6 近两月持续活跃的肉鸡数量按省份和运营商分布

（三）反射攻击资源分析

1. 反射服务器资源

根据 CNCERT 抽样监测数据，2018 年 1 月，利用反射服务器发起的反射攻击的 DDoS 攻击事件占事件总量的 21.7%，共涉及 33,731 台反射服务器。

反射攻击所利用的服务端口根据反射服务器数量统计、以及按发起反射攻击事件数量统计，被利用最多的均为 1900 端口。如图 7 所示。

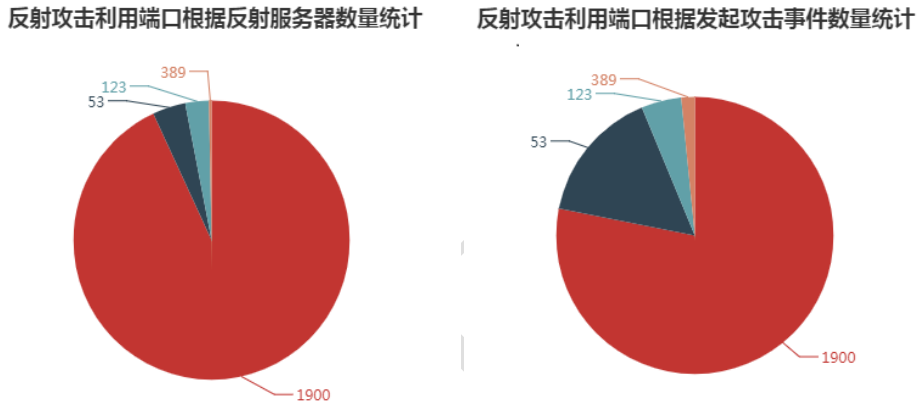

图 7 本月反射攻击利用端口根据服务器数量及事件数量统计

根据反射服务器数量按省份统计，河北省占的比例最大，占 19.1%，其次是福建省、内蒙古自治区和江苏省；按运营商统计，联通占的比例最大，占 49.6%，电信占比 41.5%，移动占比 8.4%，如图 8 所示。

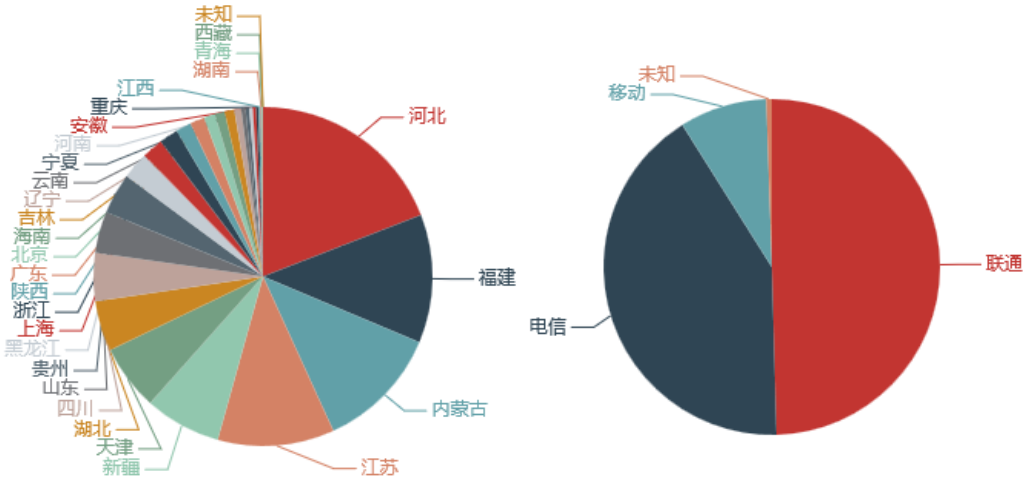

图 8 本月反射服务器数量按省份和运营商分布

参与攻击最多的反射服务器前二十名及归属如表 4 所示，位于重庆市移动的地址最多。

表 4 本月参与攻击最多的反射服务器 TOP20

反射服务器地址	归属省份	归属运营商
111.X.X.30	青海省	移动
111.X.X.38	青海省	移动
111.X.X.30	青海省	移动
111.X.X.89	内蒙古自治区	移动
111.X.X.252	内蒙古自治区	移动
120.X.X.23	内蒙古自治区	移动
183.X.X.167	重庆市	移动
183.X.X.36	重庆市	移动
183.X.X.197	重庆市	移动
183.X.X.133	重庆市	移动
183.X.X.200	重庆市	移动
183.X.X.118	重庆市	移动
183.X.X.221	重庆市	移动
183.X.X.217	重庆市	移动
218.X.X.201	重庆市	移动
218.X.X.244	重庆市	移动
218.X.X.168	贵州省	移动
218.X.X.183	贵州省	移动
221.X.X.59	西藏自治区	联通
221.X.X.21	西藏自治区	联通

反射服务器在本月被利用参与发起 DDoS 攻击的平均天次为 1.23 次。其中参与攻击最多的反射服务器地址为归属于重庆市移动的地址（183.X.X.36），共参与了 15 天攻击，约占监测天数的二分之一。

2017 年度被利用发起攻击超过 6 月次的反射服务器中（共计 1151 个），监测发现有 481 个在本月仍活跃，存活率为 41.8%。这些持续被利用的反射服务器按省份统计，贵州省的数量最多，为 84 个，其次是湖北省、辽宁省和新疆维吾尔自治区；按运营商统计，电信占的比例最大，占 42.8%，移动占 30.5%，联通占 26.3%，如图 9 所示。

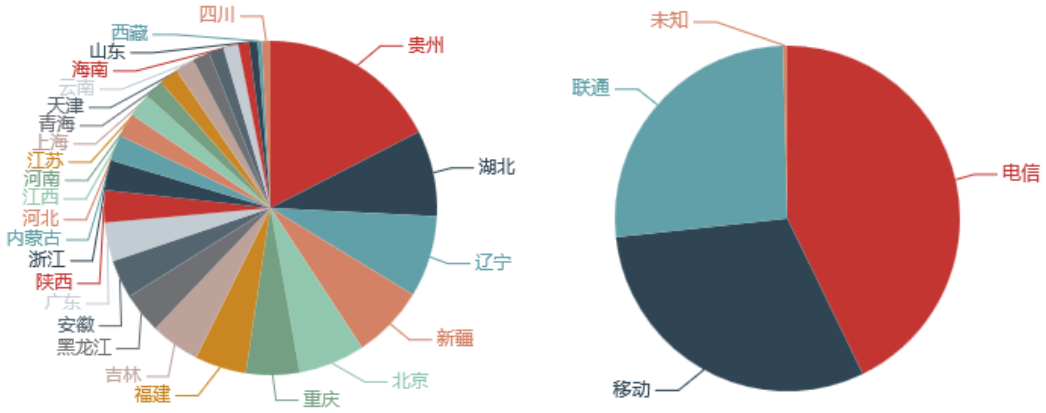

图 92017 年被利用发起攻击超过 6 月次且本月仍活跃的反射服务器数量按省份运营商分布

此外，2017 年度被利用发起 DDoS 攻击次数 TOP100 的反射服务器中，监测发现有 48 个在本月仍活跃，存活率为 48%。其中，位于新疆维吾尔自治区和辽宁省的地址数量最多。

表 5 2017 年度被利用发起攻击次数 TOP100 且在本月持续活跃的反射服务器地址

反射服务器地址	归属省份	归属运营商
43. X. X. 110	北京市	联通

59.X.X.139	辽宁省	电信
59.X.X.164	辽宁省	电信
59.X.X.101	辽宁省	电信
59.X.X.39	辽宁省	电信
59.X.X.58	辽宁省	电信
59.X.X.242	辽宁省	电信
59.X.X.62	辽宁省	电信
59.X.X.74	辽宁省	电信
59.X.X.142	辽宁省	电信
59.X.X.22	辽宁省	电信
60.X.X.83	新疆维吾尔自治区	联通
60.X.X.251	新疆维吾尔自治区	联通
111.X.X.87	安徽省	移动
112.X.X.42	黑龙江省	电信
117.X.X.196	新疆维吾尔自治区	移动
117.X.X.182	新疆维吾尔自治区	移动
117.X.X.154	新疆维吾尔自治区	移动
117.X.X.177	新疆维吾尔自治区	移动
117.X.X.184	新疆维吾尔自治区	移动
117.X.X.125	新疆维吾尔自治区	移动
117.X.X.234	新疆维吾尔自治区	移动
117.X.X.98	新疆维吾尔自治区	移动
117.X.X.249	新疆维吾尔自治区	移动
117.X.X.6	广东省	移动
120.X.X.232	新疆维吾尔自治区	移动
120.X.X.150	新疆维吾尔自治区	移动
123.X.X.118	黑龙江省	电信
124.X.X.22	北京市	联通
124.X.X.90	北京市	联通
124.X.X.248	新疆维吾尔自治区	联通
124.X.X.218	北京市	鹏博士
125.X.X.194	吉林省	联通
175.X.X.2	吉林省	联通
180.X.X.16	北京市	电信
183.X.X.36	重庆市	移动
183.X.X.36	重庆市	移动
183.X.X.42	重庆市	移动
218.X.X.166	新疆维吾尔自治区	电信
218.X.X.221	重庆市	移动
218.X.X.136	北京市	移动
218.X.X.203	重庆市	移动
219.X.X.34	北京市	电信
220.X.X.70	新疆维吾尔自治区	电信

221.X.X.37	河南省	移动(铁通)
222.X.X.146	黑龙江省	电信
222.X.X.90	黑龙江省	电信
222.X.X.134	黑龙江省	电信

2017 年 12 月监测到的反射服务器资源中，7.0%的反射服务器在本月仍处于活跃状态，共计 2231 个。这些近两月持续活跃的反射服务器资源按省份统计，福建省占的比例最大，为 15.7%，其次是江苏省、贵州省和四川省；按运营商统计，电信占的比例最大，为 53.4%，联通占 29.7%，移动占 16.0%，如图 10 所示。

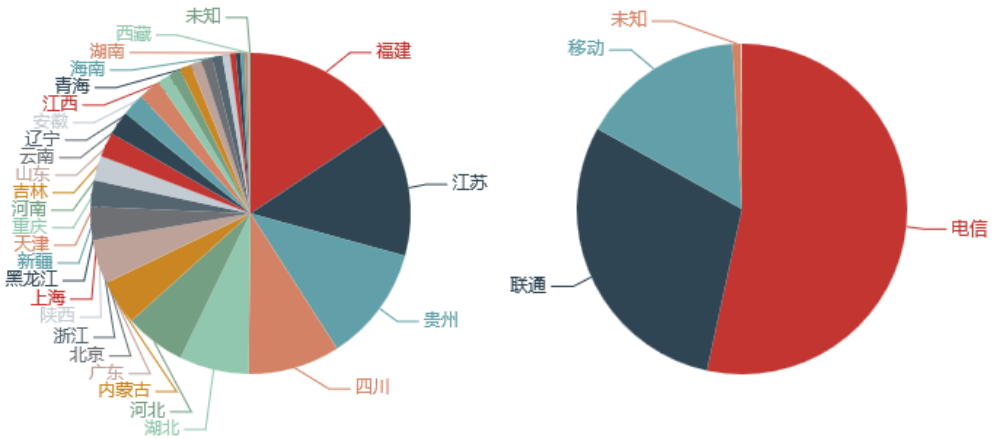

图 10 近两月持续活跃的反射服务器数量按省份和运营商分布

2. 反射攻击流量来源路由器

2018 年 1 月，境内反射攻击流量主要来源于 193 个路由器，根据参与攻击事件的数量统计，归属于天津市电信的路由器（221.X.X.2）涉及的攻击事件最多，其次是归属于天津市电信（221.X.X.1）、浙江省联通（221.X.X.23、221.X.X.22）的路由器，如表 5 所示。在图中用黄色标注的 6 个反射攻击流量来源路由器，为 2017 年被利用发起 DDoS 攻击次数的排名位列

TOP25，且监测发现在本月仍排在前列的路由器地址。

表 6 本月发起反射放大攻击事件的流量来源路由器按事件 TOP25

反射攻击流量来源路由器	所属省份	所属运营商
221.X.X.2	天津	电信
221.X.X.1	天津	电信
221.X.X.23	浙江	联通
221.X.X.22	浙江	联通
221.X.X.12	海南	联通
112.X.X.39	上海	联通
61.X.X.8	浙江	电信
61.X.X.4	浙江	电信
58.X.X.201	安徽	联通
219.X.X.70	北京	电信
58.X.X.201	安徽	联通
218.X.X.254	陕西	电信
58.X.X.201	安徽	联通
218.X.X.251	陕西	电信
58.X.X.201	安徽	联通
221.X.X.224	辽宁	联通
221.X.X.247	辽宁	联通
202.X.X.17	上海	电信
221.X.X.253	广东	联通
202.X.X.21	上海	电信
61.X.X.14	北京	联通
61.X.X.12	北京	联通
61.X.X.40	北京	联通
58.X.X.202	安徽	联通
202.X.X.23	上海	电信

根据发起反射攻击事件的来源路由器数量按省份统计，北京市占的比例最大，占 10.2%，其次是浙江省、广东省和安徽省；按发起反射攻击事件的来源运营商统计，联通占的比例最大，占 51.2%，电信占比 48.8%，如图 11 所示。

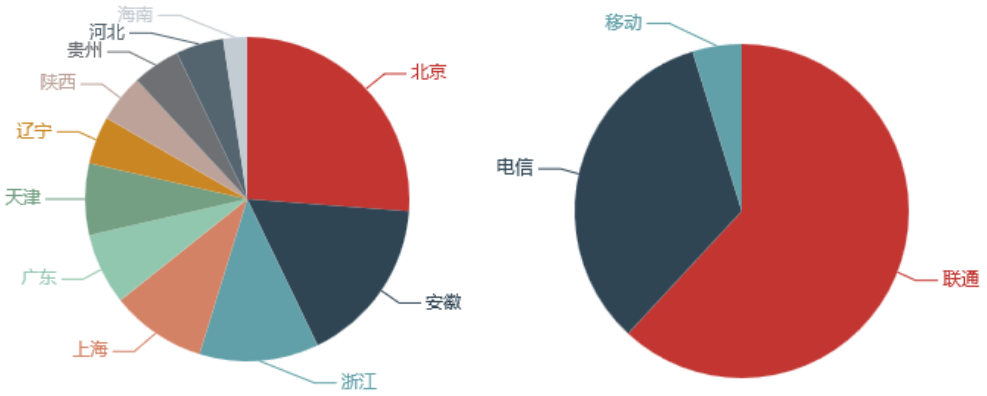

图 11 本月反射攻击流量来源路由器数量按省份和运营商分布

（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 1 月，包含跨域伪造流量的 DDoS 攻击事件占事件总量的 11.8%，较上月的比例（53.4%）有较大程度的下降。通过跨域伪造流量发起攻击的流量来源于 52 个路由器。根据参与攻击事件的数量统计，归属于吉林省联通的路由器（125.X.X.57、218.X.X.9）参与的攻击事件数量最多，其次是归属于辽宁省移动（211.X.X.44、211.X.X.45）的路由器，如表 6 所示。在图中用黄色标注的 5 个跨域攻击流量来源路由器，为 2017 年被利用发起 DDoS 攻击次数的排名位列 TOP25，且监测发现在本月仍排在前列的路由器地址。

表 7 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
125.X.X.57	吉林	联通
218.X.X.9	吉林	联通
211.X.X.44	辽宁	移动
211.X.X.45	辽宁	移动

218. X. X. 204	福建	移动
202. X. X. 1	河北	联通
125. X. X. 202	吉林	联通
221. X. X. 9	河南	移动
221. X. X. 10	河南	移动
218. X. X. 205	福建	移动
218. X. X. 218	福建	移动
211. X. X. 205	上海	移动
218. X. X. 219	福建	移动
221. X. X. 2	河南	移动
58. X. X. 253	贵州	联通
120. X. X. 1	山东	移动
211. X. X. 203	上海	移动
202. X. X. 224	河北	联通
61. X. X. 25	浙江	电信
221. X. X. 2	天津	电信
58. X. X. 254	贵州	联通
211. X. X. 3	浙江	移动
211. X. X. 9	浙江	移动
120. X. X. 2	山东	移动
211. X. X. 8	浙江	移动

跨域伪造流量涉及路由器按省份分布统计，浙江省占的比例最大，占 13.5%，其次是吉林省和上海市；按路由器所属运营商统计，移动占的比例最大，占 53.8%，联通占比 25.0%，电信占比 21.2%，如图 12 所示。

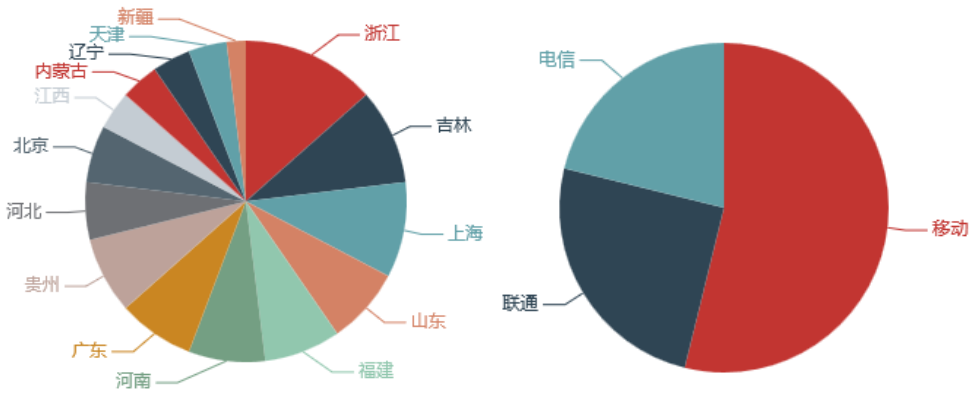

图 12 跨域伪造流量来源路由器数量按省份和运营商分布

本月转发跨域伪造攻击流量的路由器中，平均每个路由器

在 1.9 天被发现发起跨域伪造地址流量攻击，归属于于吉林省联通的路由器（218.X.X.9、125.X.X.57）参与攻击天次最多，分别在 6 天范围内被发现发起跨域攻击流量，约占监测总天数的五分之一。

2017 年度被利用转发跨域伪造攻击流量的路由器超过 6 月次的跨域伪造流量来源路由器中（共计 66 个），监测发现有 22 个在本月仍活跃，存活率为 33.3%。这些活跃的转发跨域伪造攻击流量的路由器按省份统计，归属浙江省和上海市的路由器数量最多，如表 9 所示。

表 92017 年长期被利用转发跨域伪造攻击流量且本月仍活跃路由器地址

跨域伪造流量来源路由器	归属省份	归属运营商
61.X.X.25	浙江省	电信
111.X.X.1	北京市	移动
112.X.X.38	上海市	联通
118.X.X.1	江西省	联通
125.X.X.202	吉林省	联通
125.X.X.57	吉林省	联通
202.X.X.21	上海市	电信
202.X.X.23	上海市	电信
211.X.X.203	上海市	移动
211.X.X.205	上海市	移动
211.X.X.8	浙江省	移动
211.X.X.9	浙江省	移动
211.X.X.2	浙江省	移动
211.X.X.3	浙江省	移动
218.X.X.9	吉林省	联通
218.X.X.254	山东省	联通
220.X.X.127	浙江省	电信
220.X.X.126	浙江省	电信
221.X.X.238	广东省	移动(铁通)
221.X.X.237	广东省	移动(铁通)
221.X.X.2	天津市	电信
221.X.X.1	天津市	电信

此外，2017 年度被利用转发 DDoS 攻击事件次数 TOP100

的跨域伪造流量来源路由器中，监测发现有 24 个在本月仍活跃，存活率为 24%。按省份统计，浙江省和上海市路由器数量最多，如表 10 所示。

表 10 2017 年被利用转发跨域伪造流量攻击次数 TOP100 且本月仍活跃路由器地址

跨域伪造流量来源路由器	归属省份	归属运营商
61.X.X.25	浙江省	电信
112.X.X.38	上海市	联通
118.X.X.1	江西省	联通
125.X.X.202	吉林省	联通
125.X.X.57	吉林省	联通
202.X.X.21	上海市	电信
202.X.X.23	上海市	电信
202.X.X.243	新疆维吾尔自治区	电信
202.X.X.224	河北省	联通
202.X.X.223	河北省	联通
211.X.X.203	上海市	移动
211.X.X.205	上海市	移动
211.X.X.8	浙江省	移动
211.X.X.9	浙江省	移动
211.X.X.2	浙江省	移动
211.X.X.3	浙江省	移动
218.X.X.9	吉林省	联通
218.X.X.254	山东省	联通
220.X.X.127	浙江省	电信
220.X.X.126	浙江省	电信
221.X.X.238	广东省	移动(铁通)
221.X.X.237	广东省	移动(铁通)
221.X.X.2	天津市	电信
221.X.X.1	天津市	电信

2017 年 12 月监测到的跨域攻击流量来源路由器资源中，36.6%的路由器在本月仍处于活跃状态，共计 37 个。近两月持续活跃的跨域攻击流量来源路由器资源按省份统计，浙江省和上海市的路由器数量最多，如表 11 所示。

表 11 近两月持续活跃的跨域攻击流量来源路由器

跨域伪造流量来源路由器	归属省份	归属运营商
58.X.X.253	贵州省	联通

58.X.X.254	贵州省	联通
61.X.X.25	浙江省	电信
112.X.X.38	上海市	联通
118.X.X.1	江西省	联通
125.X.X.202	吉林省	联通
125.X.X.57	吉林省	联通
202.X.X.21	上海市	电信
202.X.X.23	上海市	电信
202.X.X.224	河北省	联通
202.X.X.223	河北省	联通
211.X.X.203	上海市	移动
211.X.X.205	上海市	移动
211.X.X.45	辽宁省	移动
211.X.X.44	辽宁省	移动
211.X.X.8	浙江省	移动
211.X.X.9	浙江省	移动
211.X.X.2	浙江省	移动
211.X.X.3	浙江省	移动
218.X.X.9	吉林省	联通
218.X.X.254	山东省	联通
218.X.X.204	福建省	移动
218.X.X.205	福建省	移动
218.X.X.219	福建省	移动
218.X.X.218	福建省	移动
220.X.X.127	浙江省	电信
220.X.X.126	浙江省	电信
221.X.X.13	山东省	联通
221.X.X.1	河南省	移动(铁通)
221.X.X.2	河南省	移动(铁通)
221.X.X.9	河南省	移动(铁通)
221.X.X.10	河南省	移动(铁通)
221.X.X.238	广东省	移动(铁通)
221.X.X.237	广东省	移动(铁通)
221.X.X.2	天津市	电信
221.X.X.1	天津市	电信

2.本地伪造流量来源路由器

根据 CNCERT 抽样监测数据，2018 年 1 月，包含本地伪造流量的 DDoS 攻击事件占事件总量的 18.5%，通过本地伪造流量发起攻击的流量来源于 562 个路由器。根据参与攻击事件的

数量统计，11 个归属于江苏省移动的路由器（221.X.X.4、221.X.X.3、221.X.X.1、221.X.X.2、202.X.X.241、221.X.X.160、221.X.X.159、221.X.X.5、221.X.X.6、221.X.X.8、221.X.X.9）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（61.X.X.4），如表 12 所示。在图中用黄色标注的 8 个本地攻击流量来源路由器，为 2017 年被利用发起 DDoS 攻击次数的排名位列 TOP25，且监测发现在本月仍排在前列的路由器地址。

表 12 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
221.X.X.4	江苏	移动
221.X.X.3	江苏	移动
221.X.X.1	江苏	移动
221.X.X.2	江苏	移动
202.X.X.241	江苏	电信
221.X.X.160	江苏	移动
221.X.X.159	江苏	移动
221.X.X.5	江苏	移动
221.X.X.6	江苏	移动
221.X.X.8	江苏	移动
221.X.X.9	江苏	移动
61.X.X.4	浙江	电信
221.X.X.21	江苏	移动
61.X.X.1	四川	电信
202.X.X.155	福建	电信
221.X.X.10	江苏	移动
221.X.X.17	江苏	移动
61.X.X.2	四川	电信
218.X.X.129	四川	电信
202.X.X.154	福建	电信
221.X.X.22	江苏	移动
218.X.X.130	四川	电信
61.X.X.71	江苏	电信
221.X.X.7	江苏	移动
61.X.X.8	浙江	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 26.3%，其次是福建省、江西省、及贵州省；按路由器所属运营商统计，电信占的比例最大，占 52.2%，移动占比 35.5%，联通占比 12.4%，如图 13 所示。

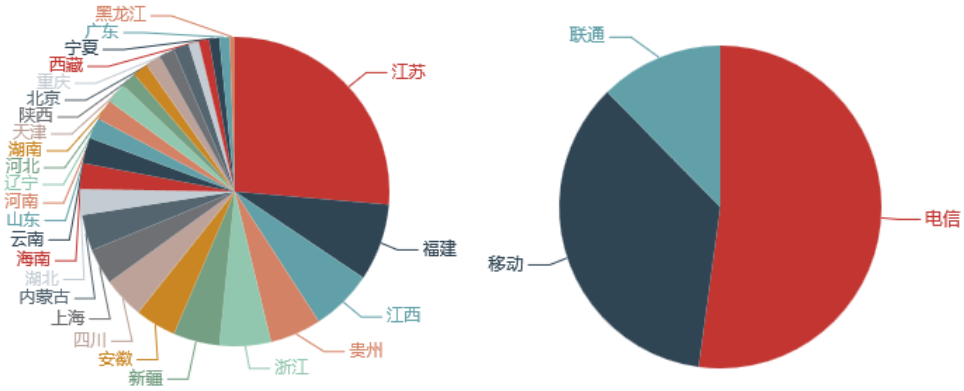

图 13 本地伪造流量来源路由器数量按省份和运营商分布

本月转发本地伪造攻击流量的路由器中，平均每个路由器在 2.49 天被发现发起跨域伪造地址流量攻击，最多的归属于江苏省移动的路由器（221.X.X.3、221.X.X.3）均在 9 天范围内被发现发起跨域攻击流量，约占监测总天数的三分之一。

2017 年度被利用转发本地伪造攻击流量的路由器超过 6 月次的本地伪造流量来源路由器中（共计 169 个），监测发现有 69 个在 1 月份仍活跃，存活率为 40.8%。这些活跃的转发本地伪造攻击流量的路由器按省份统计，浙江省和江西省数量最多，其次是江苏省、上海市、和福建省；按运营商统计，电信占的比例最大，占 79.4%，联通占 11.8%，移动占 8.8%，如图 14 所示。

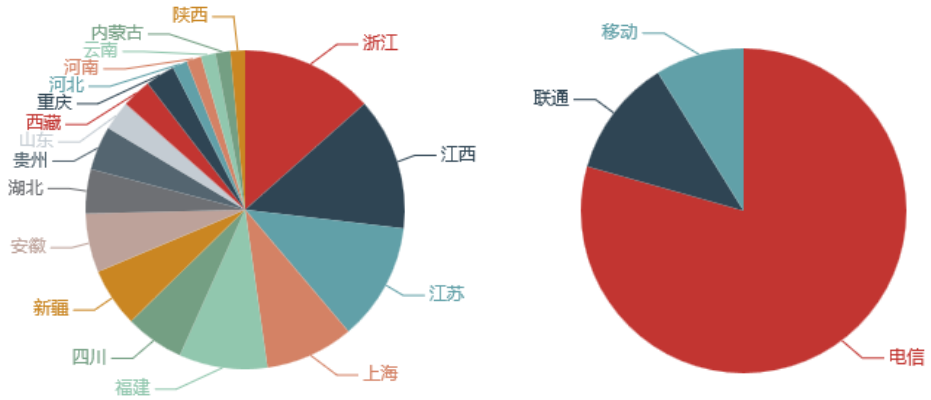

图 14 2017 年活跃超 6 月次且本月仍活跃的本地伪造流量来源路由器数量按省份运营商分布

此外，2017 年被利用转发本地伪造流量 DDoS 攻击事件次数 TOP100 的路由器中，监测发现有 50 个在本月仍活跃，存活率为 50%。按省份统计，福建省、江西省和江苏省的数量最多；按运营商统计，电信占的比例最大，占 89.8%。

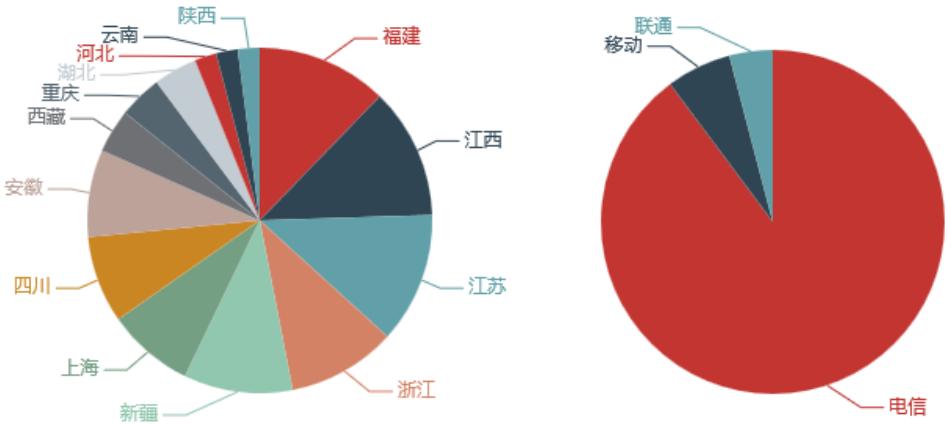

图 15 2017 年被利用 TOP100 且本月仍活跃的本地伪造流量来源路由器数量按省份运营商分布

2017 年 12 月监测到的本地攻击流量来源路由器资源中，40.2%的路由器在本月仍处于活跃状态，共计 80 个。近两月持续活跃的本地攻击流量来源路由器资源按省份统计，江苏省占的比例最大，占 32.9%；按运营商统计，电信和联通占的比例最大，占 40.5%，如图 16 所示。

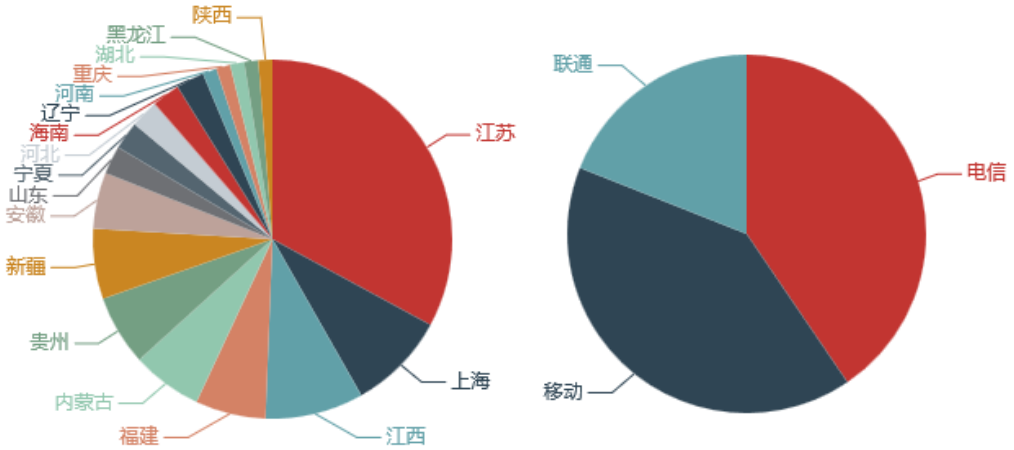

图 16 近两月活跃的本地伪造流量来源路由器数量按省份和运营商分布

三、本月攻击资源治理效果分析

（一）攻击资源维度

1. 控制端资源

根据 CNCERT 抽样监测数据，与 2017 年 12 月相比，本月利用肉鸡发起 DDoS 攻击的控制端总量较之增加 93 个，其中境内控制端数量比 12 月减少 246 个，境外控制端数量比 12 月增加 339 个。其中境内控制端中，浙江省减少数量最多，达 44 个，其次是河南省、陕西省和北京市；而宁夏回族自治区相比于上月境内控制端数量提高最多，达 13 个，如图 17 所示。

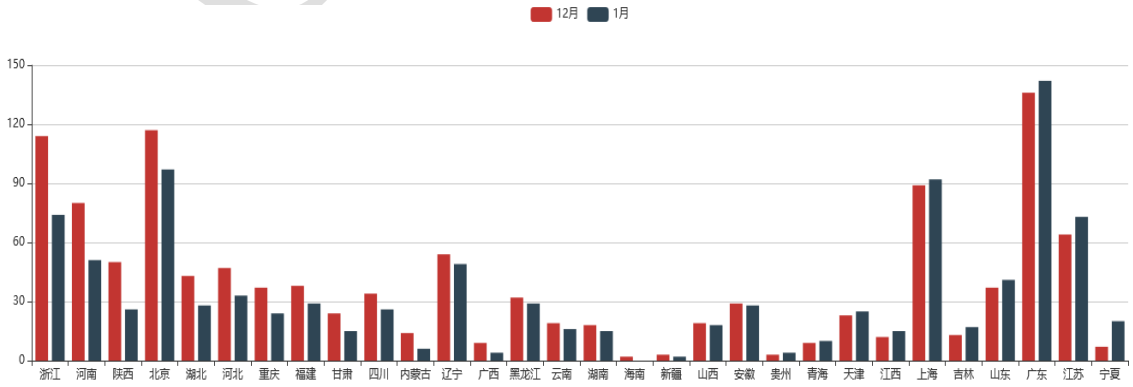

图 17 近两月各省份控制端数量变化情况

2. 肉鸡资源

根据 CNCERT 抽样监测数据，本月利用肉鸡资源发起 DDoS 攻击的境内肉鸡数量按省份统计，江苏省最多，占 28.8%，其次是重庆市、湖北省和福建省。相较于 2017 年 12 月的肉鸡资源数量，北京市本月减少的肉鸡数量最多，达 15,930 个，其次是湖北省、浙江省和四川省，山西省本月未监测发现被利用发起攻击的肉鸡地址；而江苏省相比于 12 月肉鸡 IP 数增加最多，达 7,757 个，如图 18 所示。

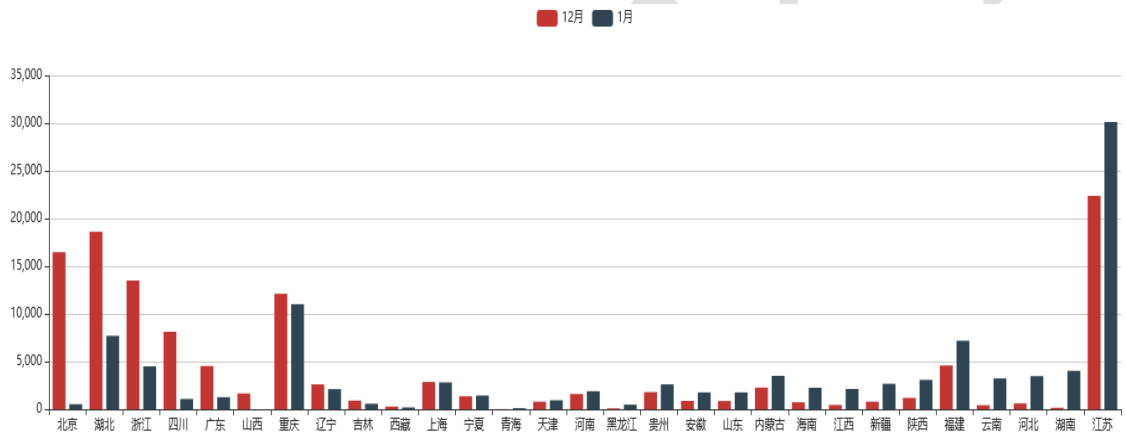

图 18 近两月各省份肉鸡数量变化情况

3. 反射服务器资源

根据 CNCERT 抽样监测数据，本月利用境内反射服务器发起反射攻击的服务器数量按省份统计，河北省最多，占 19.1%，其次是福建省、内蒙古自治区和江苏省。相较于 2017 年 12 月份利用反射服务器发起反射攻击的服务器数量，山东省减少的数量最多，达 2,832 个，其次是北京市和浙江省；而河北省相比于 12 月反射服务器数量增加最多，达 2,131 个，如图 19

所示。

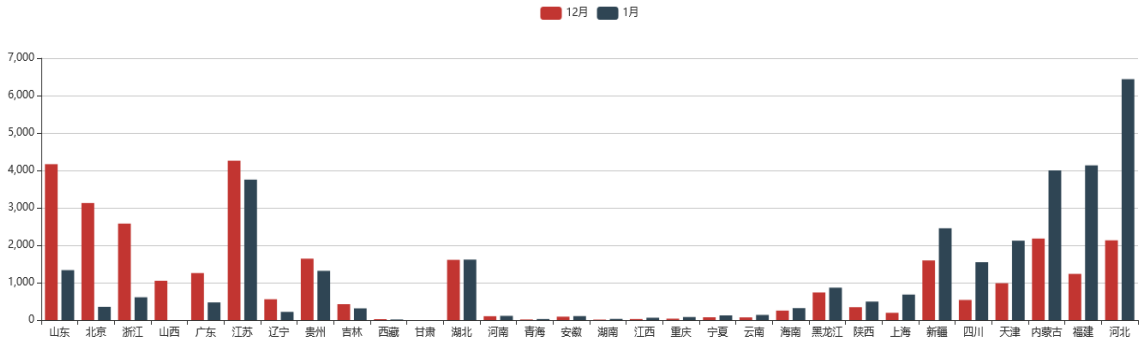

图 19 近两月各省份反射服务器数量变化情况

4. 反射来源服务器资源

根据 CNCERT 抽样监测数据，境内转发反射攻击流量主要来源于 42 个运营商路由器，根据涉及的路由器数量按照省份统计，归属于北京市的路由器最多，其次是安徽省、浙江省以及上海市。相较于 2017 年 12 月份，北京市本月减少的反射攻击流量来源路由器数量最多，达 8 个，其次是江苏省、广东省和江西省，如图 20 所示，图中未出现的省份表示两月均未发现来源于该省的转发反射攻击流量的路由器。

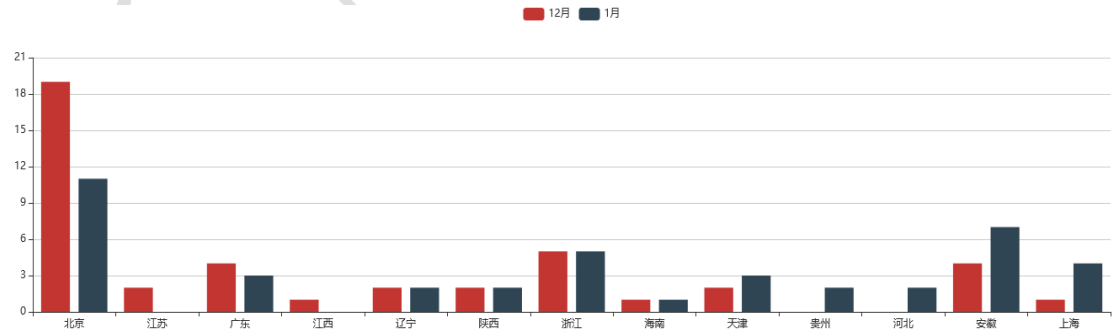

图 20 近两月各省份反射攻击来源路由器数量变化情况

5. 跨域伪造流量来源路由器资源

根据 CNCERT 抽样监测数据，本月转发跨域伪造流量的运

营商路由器按省份统计，浙江省所占比例最大，为 13.0%，其次是吉林省和上海市。相较于 2017 年 12 月的跨域伪造流量来源服务器资源，北京市本月份减少的路由器数量最多，达 17 个，其次是广东省、山东省和云南省；而内蒙古自治区、河北省、新疆、江西省和吉林省的路由器数量有所增加，如图 21 所示，其中未出现的省份表示两月均未发现来源于该省的转发跨域伪造攻击流量的路由器。

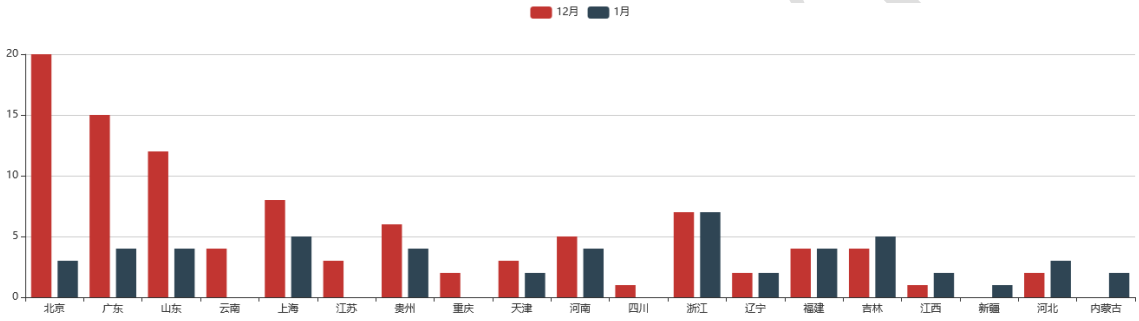

图 21 近两月各省份跨域伪造流量来源路由器数量变化情况

6. 本地伪造流量来源路由器资源

根据 CNCERT 抽样监测数据，本月转发本地伪造流量的运营商路由器按省份统计，江苏省所占比例最大，为 26.3%，其次是福建省、江西省和浙江省。相较于 2017 年 12 月份的本地伪造流量来源服务器资源，北京市和广东省本月减少的路由器数量最多，达 14 个。而四川省的路由器数量增加最多，达 4 个，如图 22 所示。

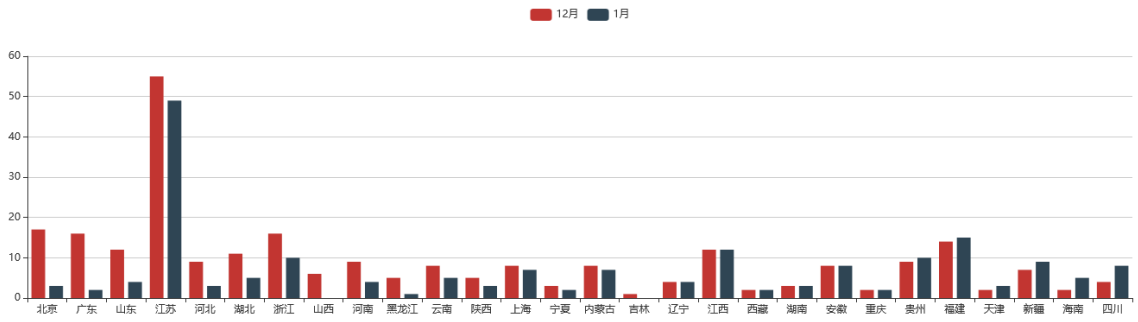

图 22 近两月各省份本地伪造流量来源路由器数量变化情况

（二）攻击事件维度

1. 真实地址攻击事件

根据 CNCERT 抽样监测数据，本月利用真实地址发起 DDoS 攻击的事件按省份统计，江苏省事件数量最多，其次是重庆市、湖北省和浙江省。对比 2017 年 12 月各省份的此类攻击事件，北京市本月的事件数减少的最多，其次是广东省、浙江省和湖北省，如图 23 所示。

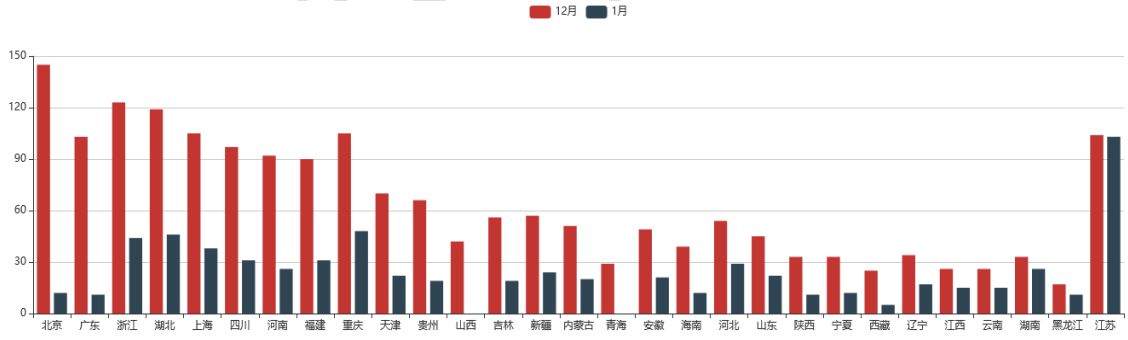

图 23 近两月各省份真实地址攻击事件数量变化情况

2. 反射攻击事件

根据 CNCERT 抽样监测数据，本月利用反射服务器发起的 DDoS 反射攻击事件按省份统计，浙江省的事件数量最多，其次是天津市、重庆市和河北省。对比 2017 年 12 月各省份利用

反射服务器发起的攻击事件，北京市本月减少的事件数量最多，其次是山西省、陕西省和江苏省。大部分省份的反射攻击事件数量均有所增加，最多的是重庆市、四川省、河北省，如图 24 所示。

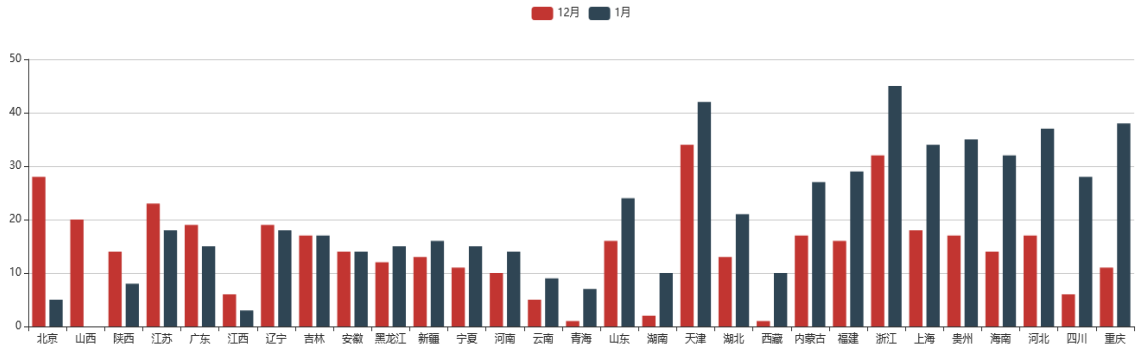

图 24 近两月各省份反射攻击事件数量对比

3. 跨域伪造流量攻击

根据 CNCERT 抽样监测数据，本月包含跨域伪造流量的 DDoS 攻击事件按省份统计，吉林省的事件数量最多，其次是黑龙江省、辽宁省和河北省。对比 2017 年 12 月各省份跨域伪造流量攻击事件，北京市本月事件数量减少的最多，其次是贵州省、广东省和浙江省，如图 28 所示。从图中可以看出本月治理效果较为明显，大部分省份发出的跨域伪造流量事件数量均有较大程度的减少，如图 25 所示。

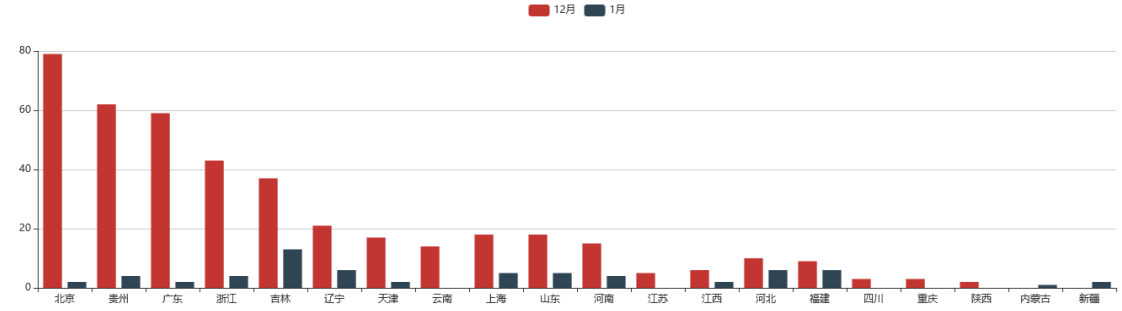

图 25 近两月各省份跨域伪造流量攻击事件数量变化情况

4. 本地伪造流量攻击

根据 CNCERT 抽样监测数据，本月包含本地伪造流量的 DDoS 攻击事件按省份统计，江苏省事件数量最多，其次是浙江省、上海市和福建省。对比 2017 年 12 月各省份本地伪造流量攻击事件，浙江省本月事件数量减少的最多，其次是四川省、湖北省和江苏省，如图 26 所示。从图中可以看出本月治理效果较为明显，除上海市外，其它省份发出的本地伪造流量事件数量均有不同程度的减少。

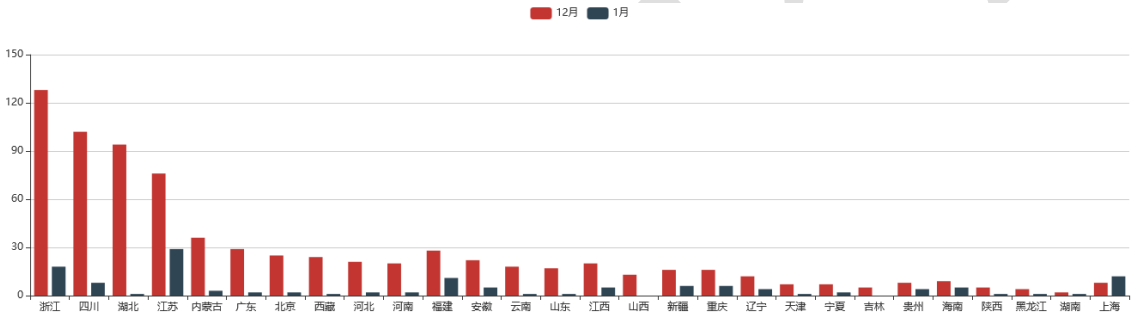

图 26 近两月各省份本地伪造流量攻击事件数量比较情况