我国 DDoS 攻击资源月度分析报告

(2018 年 5 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 5 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，境外控制端超过一半位于美国；境内控制端最多位于浙江省，其次是江苏省、北京市和上海市，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、山东省和河南省，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广东省、浙江省和江苏省；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湖北省、

宁夏回族自治区和河南省；数量最多的归属运营商是电信。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、山东省和河南省；数量最多的归属运营商是联通。

4、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，2018 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、广东省和贵州省路由器数量最多。

5、转发伪造本地攻击流量的路由器中，归属于新疆维吾尔自治区电信的路由器参与的攻击事件数量最多，2018 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、江西省、贵州省和浙江省路由器数量最多。

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，2018 年 5 月，利用肉鸡发起 DDoS 攻击的控制端有 259 个，其中，43 个控制端位于我国境内，216 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 50.5%，其次是中国香港和法国，如图 1 所示。

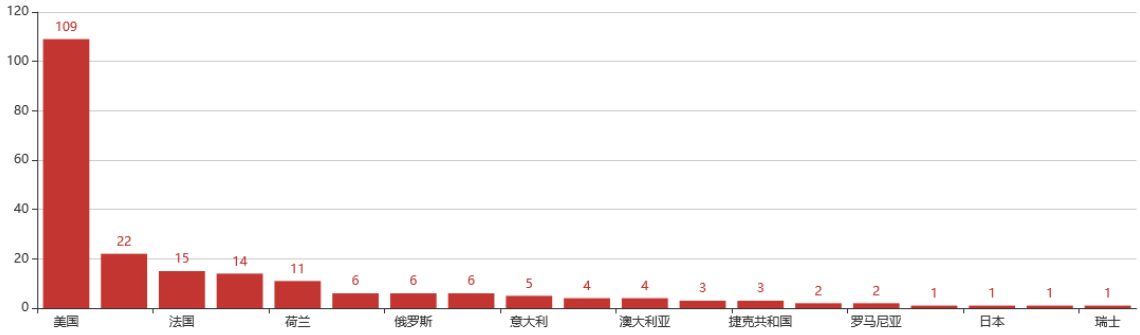

图 1 本月发起 DDoS 攻击的境外控制端数量按国家或地区分布

位于境内的控制端按省份统计，浙江省占的比例最大，占 34.9%，其次是江苏省、北京市和上海市；按运营商统计，电信占的比例最大，占 76.7%，联通占 7.0%，移动占 2.3%，如图 2 所示。

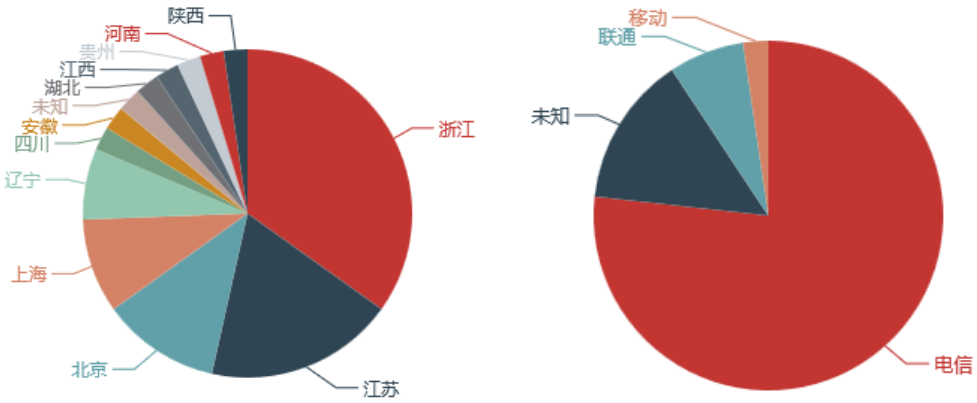

图 2 本月发起 DDoS 攻击的境内控制端数量按省份和运营商分布

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
118.X.X.11	上海市	腾讯云
61.X.X.112	江苏省	电信
122.X.X.165	浙江省	电信
115.X.X.60	浙江省	电信

115.X.X.235	浙江省	电信
58.X.X.57	江苏省	电信
42.X.X.249	河南省	联通
118.X.X.239	辽宁省	联通
222.X.X.200	江苏省	电信
120.X.X.68	安徽省	移动
115.X.X.239	上海市	电信
123.X.X.60	贵州省	电信
101.X.X.158	北京市	电信
111.X.X.180	上海市	腾讯云
115.X.X.6	浙江省	电信
115.X.X.133	浙江省	电信
115.X.X.128	浙江省	电信
115.X.X.184	浙江省	电信
183.X.X.6	浙江省	电信
115.X.X.72	浙江省	电信

2018 年 1 月至今监测到的控制端中，13.1%的控制端在本月仍处于活跃状态，共计 34 个，其中位于我国境内的控制端数量为 9 个，位于境外的控制端数量为 25 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
42.X.X.249	河南省	联通
118.X.X.11	上海市	腾讯云
182.X.X.227	上海市	腾讯云
222.X.X.36	江苏省	电信
115.X.X.72	浙江省	电信
115.X.X.184	浙江省	电信
115.X.X.120	浙江省	电信
111.X.X.196	江西省	电信
122.X.X.165	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 37.5%；按运营商统计，电信占的比例最大，为 66.7%，联通占 11.1%，如图 3 所示。

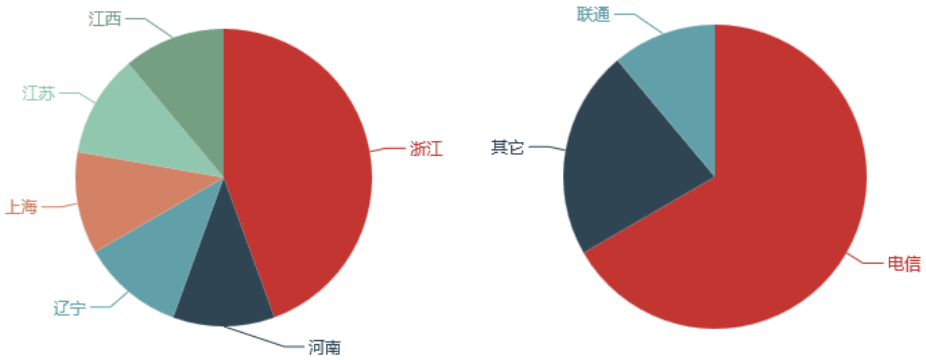

图 3 2018 年以来持续活跃发起 DDoS 攻击的境内控制端数量按省份和运营商分布

（二）肉鸡资源分析

根据 CNCERT 抽样监测数据，2018 年 5 月，共有 295,101 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 15.3%，其次是江苏省、山东省和河南省；按运营商统计，电信占的比例最大，为 61.8%，联通占 28.8%，移动占 7.1%，如图 4 所示。

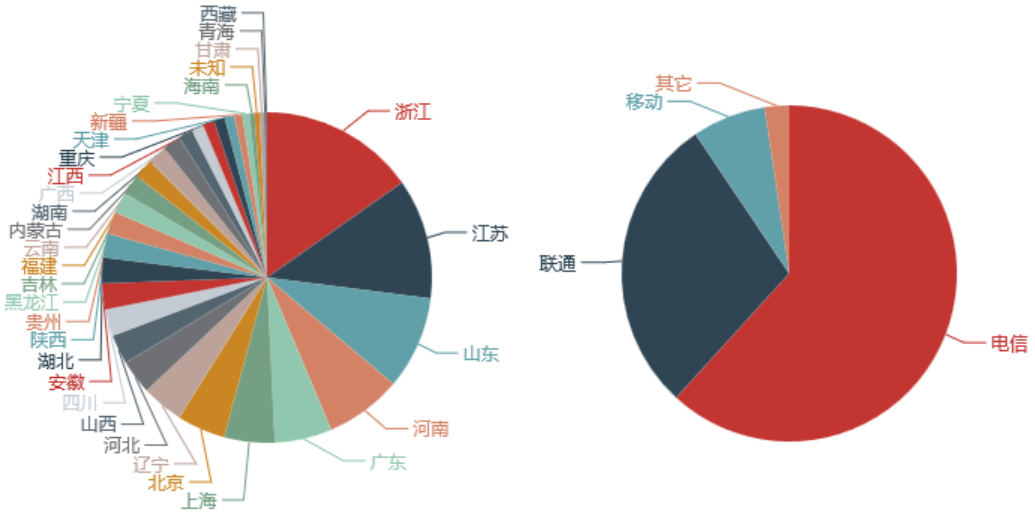

图 4 本月肉鸡地址数量按省份和运营商分布

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，位于河南省和北京市的地址最多。

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
219.X.X.182	广西壮族自治区	电信
111.X.X.34	北京市	联通
61.X.X.28	甘肃省	电信
61.X.X.66	青海省	电信
175.X.X.131	湖南省	电信
122.X.X.16	上海市	待确认
220.X.X.58	广西壮族自治区	电信
118.X.X.186	甘肃省	电信
58.X.X.114	湖南省	联通
139.X.X.54	上海市	电信
61.X.X.12	河南省	联通
1.X.X.170	北京市	电信
60.X.X.228	新疆维吾尔自治区	联通
123.X.X.201	广东省	电信
61.X.X.4	河南省	联通
61.X.X.138	北京市	联通
60.X.X.174	新疆维吾尔自治区	联通
61.X.X.114	河南省	联通
202.X.X.138	新疆维吾尔自治区	电信
52.X.X.39	北京市	待确认

2018 年 1 月至今监测到的肉鸡资源中，共计 63,111 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 34,842 个，位于境外的肉鸡数量为 28,269 个。2018 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 2018 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
219.X.X.182	广西壮族自治区	电信
111.X.X.34	北京市	联通
61.X.X.28	甘肃省	电信
61.X.X.66	青海省	电信
175.X.X.131	湖南省	电信
122.X.X.16	上海市	待确认

220.X.X.58	广西壮族自治区	电信
118.X.X.186	甘肃省	电信
58.X.X.114	湖南省	联通
139.X.X.54	上海市	电信
61.X.X.12	河南省	联通
1.X.X.170	北京市	电信
60.X.X.228	新疆维吾尔自治区	联通
123.X.X.201	广东省	电信
61.X.X.4	河南省	联通
61.X.X.138	北京市	联通
60.X.X.174	新疆维吾尔自治区	联通
61.X.X.114	河南省	联通
202.X.X.138	新疆维吾尔自治区	电信
52.X.X.39	北京市	待确认

2018 年 1 月至今持续活跃的境内肉鸡资源按省份统计，山东省占的比例最大，占 26.9%，其次是上海市、广东省和四川省；按运营商统计，电信占的比例最大，占 74.6%，联通占 15.2%，移动占 5.7%，如图 5 所示。

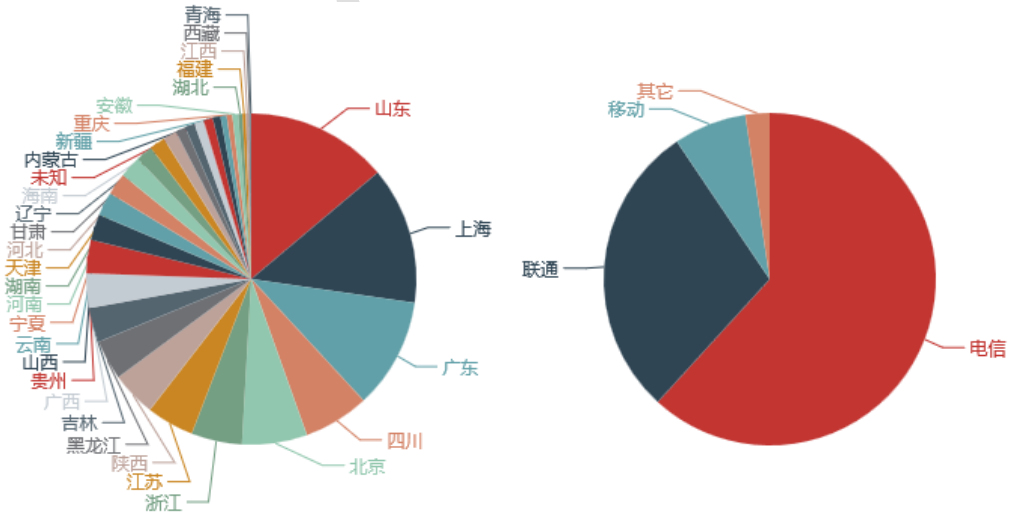

图 5 2018 年以来持续活跃的肉鸡数量按省份和运营商分布

（三）反射攻击资源分析

根据 CNCERT 抽样监测数据，2018 年 5 月，利用反射服

务器发起的三类重点反射攻击共涉及 3,114,385 台反射服务器，其中境内反射服务器 3,396,315 台，境外反射服务器 173,014 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 18,721 台，占比 0.6%，其中境内反射服务器 14,903 台，境外反射服务器 3,818 台；利用 NTP 反射发起反射攻击的反射服务器有 227,065 台，占比 7.3%，其中境内反射服务器 217,575 台，境外反射服务器 9,490 台；利用 SSDP 反射发起反射攻击的反射服务器有 2,868,599 台，占比 92.1%，其中境内反射服务器 2,603,187 台，境外反射服务器 265,412 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 5 月，利用 memcached 服务器实施反射攻击的事件共涉及境内 14,903 台反射服务器，境外 3,818 台反射服务器。

本月境内反射服务器数量按省份统计，广东省占的比例最

大，占 15.5%，其次是浙江省、江苏省和北京市；按归属运营商或云服务商统计，电信占的比例最大，占 31.9%，移动占比 28.2%，联通占比 15.5%，阿里云占比 12.0%，如图 6 所示。

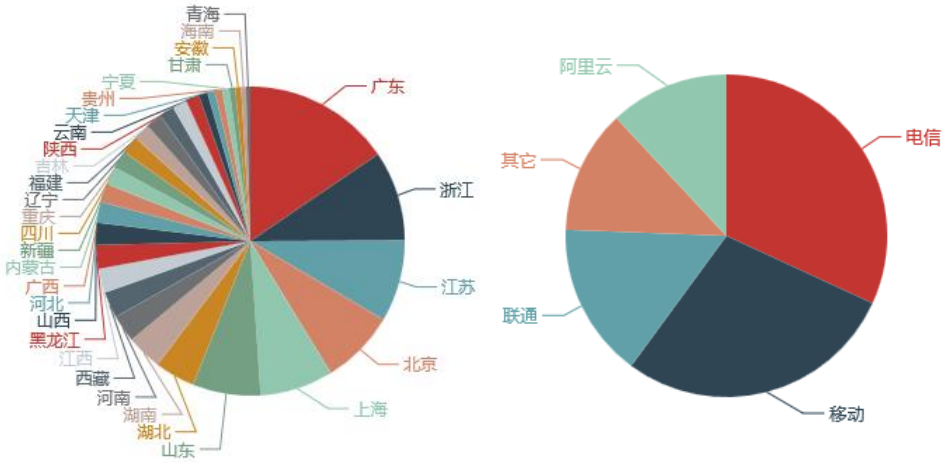

图 6 本月境内 memcached 反射服务器数量按省份、运营商或云服务商分布

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 36.2%，其次是中国香港、加拿大和法国，如图 7 所示。

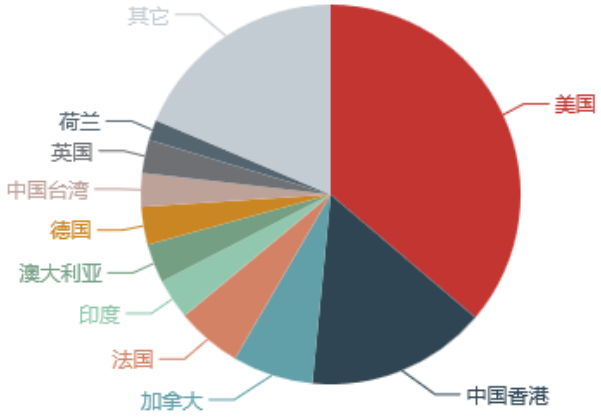

图 7 本月境外反射服务器数量按国家或地区分布

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
59.X.X.158	辽宁省	电信
106.X.X.51	北京市	电信
120.X.X.112	上海市	移动
61.X.X.98	北京市	联通
139.X.X.188	上海市	阿里云
101.X.X.113	北京市	阿里云
113.X.X.190	广东省	电信
218.X.X.215	上海市	电信
182.X.X.107	北京市	阿里云
123.X.X.195	北京市	阿里云
101.X.X.228	北京市	阿里云
123.X.X.151	北京市	阿里云
123.X.X.13	北京市	阿里云
139.X.X.134	上海市	阿里云
123.X.X.130	北京市	阿里云
123.X.X.192	北京市	阿里云
139.X.X.9	上海市	阿里云
123.X.X.49	北京市	阿里云
221.X.X.226	江苏省	联通
123.X.X.118	北京市	阿里云
123.X.X.86	北京市	阿里云
182.X.X.39	北京市	阿里云
139.X.X.145	上海市	阿里云
123.X.X.233	北京市	阿里云
123.X.X.4	北京市	阿里云
112.X.X.190	北京市	阿里云
218.X.X.157	新疆维吾尔自治区	电信
202.X.X.240	新疆维吾尔自治区	电信
113.X.X.230	广东省	电信

近两月被利用发起攻击的 memcached 反射服务器中，共计 5,746 个在本月仍处于活跃状态，其中 3,597 个位于境内，2,149 个位于境外。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 20.5%，其

次是浙江省、北京市和山东省；按运营商或云服务统计，阿里云占的比例最大，占 37.3%，电信占 28.5%，联通占 13.7%，移动占 6.5%，如图 8 所示。

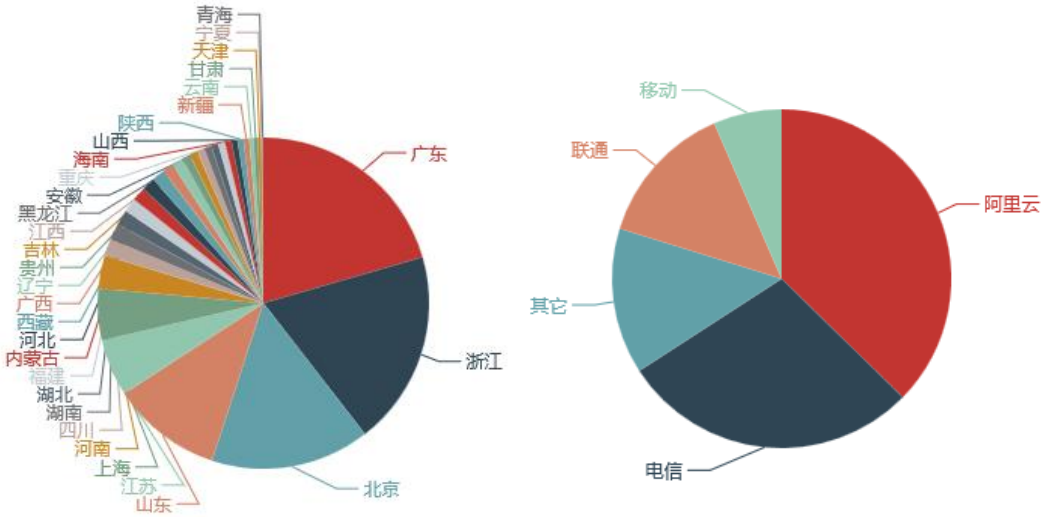

图 8 近两月被持续利用发起攻击的 memcached 反射服务器数量按省份运营商或云服务商分布

（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 5 月，NTP 反射攻击事件共涉及我国境内 217,575 台反射服务器，境外 9,490 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，湖北省占的比例最大，占 15.6%，其次是宁夏回族自治区、河南省和湖南省；按归属运营商统计，电信占的比例最大，占 42.3%，联通占比 35.3%，移动占比 12.9%，如图 9 所示。

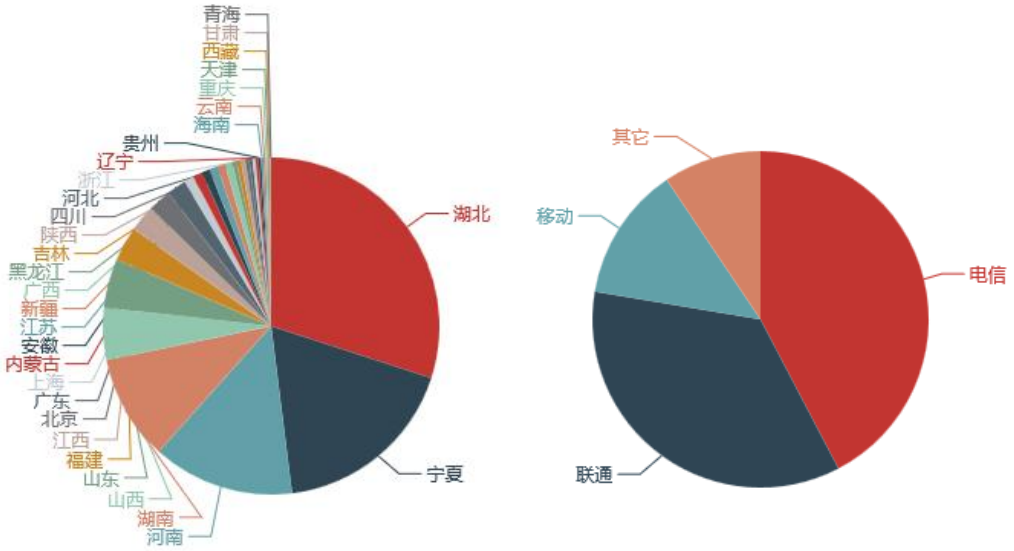

图 9 本月被利用发起 NTP 反射攻击的境内反射服务器数量按省份和运营商分布

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，美国占的比例最大，占 30.6%，其次是中国台湾、中国香港和韩国，如图 10 所示。

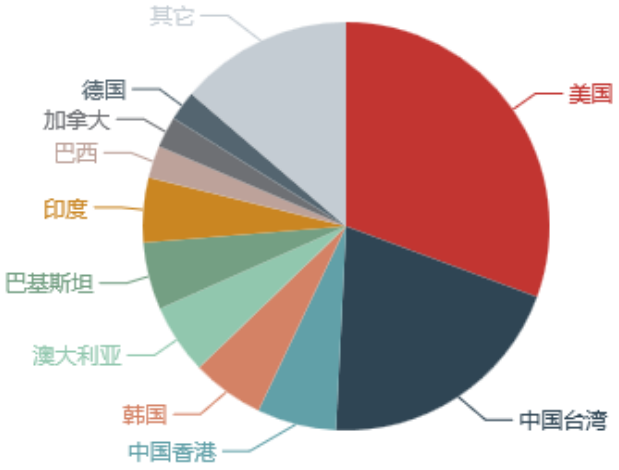

图 10 本月被利用发起 NTP 反射攻击的境外反射服务器数量按国家或地区分布

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 TOP30 及归属如表 6 所示，位于北京市和上海市的地址最多。

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	归属运营商或云服务商
59.X.X.158	辽宁省	电信
106.X.X.51	北京市	电信
120.X.X.112	上海市	移动
61.X.X.98	北京市	联通
139.X.X.188	上海市	阿里云
101.X.X.113	北京市	阿里云
47.X.X.143	北京市	阿里云
101.X.X.234	北京市	阿里云
113.X.X.190	广东省	电信
218.X.X.215	上海市	电信
47.X.X.89	北京市	阿里云
182.X.X.107	北京市	阿里云
123.X.X.195	北京市	阿里云
101.X.X.228	北京市	阿里云
123.X.X.151	北京市	阿里云
123.X.X.13	北京市	阿里云
47.X.X.11	北京市	阿里云
112.X.X.219	北京市	阿里云

139.X.X.134	上海市	阿里云
123.X.X.130	北京市	阿里云
123.X.X.192	北京市	阿里云
139.X.X.9	上海市	阿里云
123.X.X.49	北京市	阿里云
139.X.X.74	上海市	阿里云
123.X.X.156	北京市	阿里云
221.X.X.226	江苏省	联通
123.X.X.118	北京市	阿里云
123.X.X.209	北京市	阿里云
123.X.X.86	北京市	阿里云
139.X.X.150	上海市	阿里云

近两月被持续利用发起攻击的 NTP 反射服务器中，共计 63,309 个在本月仍处于活跃状态，其中 61,318 个位于境内，1,991 个位于境外。持续活跃的 NTP 反射服务器按省份统计，宁夏回族自治区占的比例最大，占 36.1%，其次是湖南省、湖北省和山西省；按运营商统计，电信占的比例最大，占 49.0%，联通占 13.9%，移动占 12.1%，如图 11 所示。

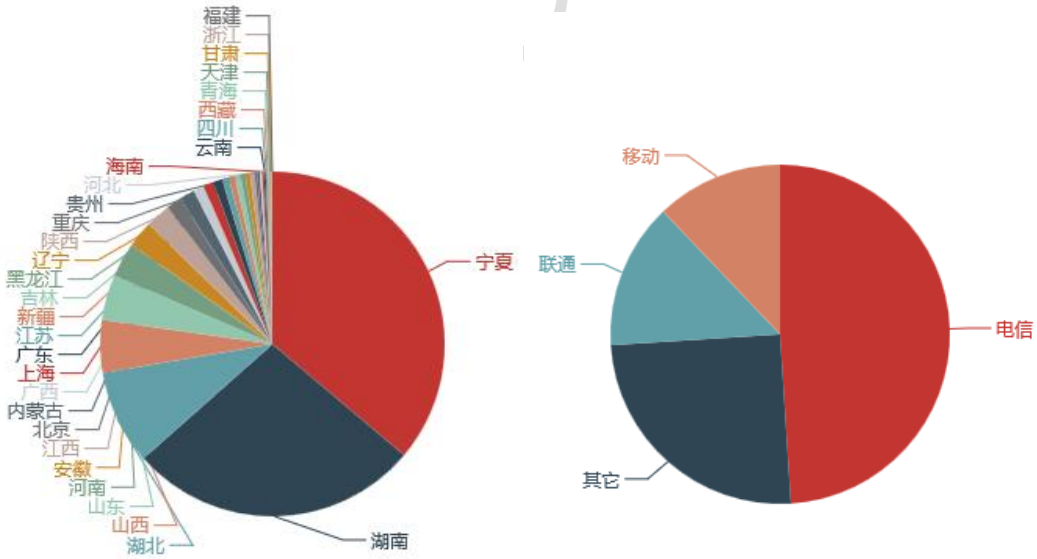

图 11 近两月被持续利用发起攻击的 NTP 反射服务器数量按省份运营商分布

（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 5 月，SSDP 反射攻击事件共涉及境内 2,603,187 台反射服务器，境外 265,412 台反射服务器。被利用发起攻击的 SSDP 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 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 14.1%，其次是山东省、河南省和河北省；按归属运营商统计，联通占的比例最大，占 61.2%，电信占比 35.2%，移动占比 2.5%，如图 12 所示。

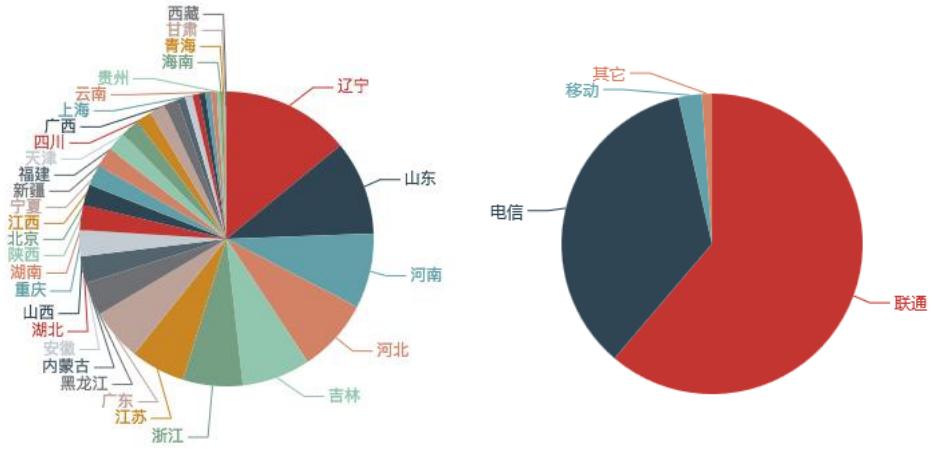

图 12 本月被利用发起 SSDP 反射攻击的境内反射服务器数量按省份和运营商分布

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 27.3%，其次是中国台湾、韩国和加拿大，如图 13 所示。

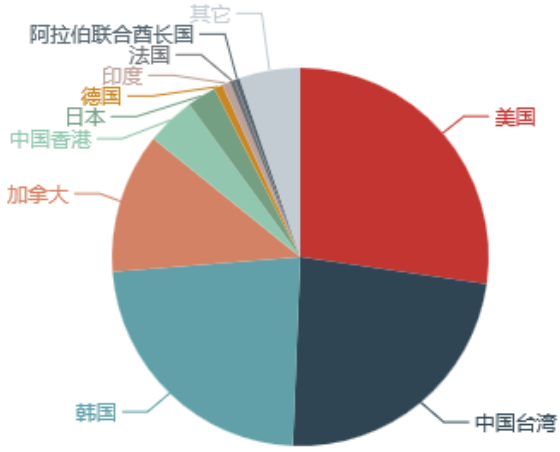

图 13 本月被利用发起 SSDP 反射攻击的境外反射服务器数量按国家或地区或地区分布

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，位于黑龙江省的地址最多。

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.53	贵州省	移动
111.X.X.57	黑龙江省	移动
111.X.X.58	黑龙江省	移动
112.X.X.26	黑龙江省	电信
111.X.X.102	黑龙江省	移动
222.X.X.26	黑龙江省	电信
111.X.X.66	黑龙江省	移动
111.X.X.8	黑龙江省	移动
111.X.X.17	黑龙江省	移动
120.X.X.188	新疆维吾尔自治区	电信
111.X.X.12	黑龙江省	移动
218.X.X.30	新疆维吾尔自治区	移动
60.X.X.190	天津市	联通

111.X.X.6	黑龙江省	移动
222.X.X.89	黑龙江省	电信
111.X.X.94	黑龙江省	移动
219.X.X.94	黑龙江省	电信
111.X.X.125	黑龙江省	移动
112.X.X.65	黑龙江省	电信
117.X.X.107	广东省	移动

此外，上月被利用发起 DDoS 攻击次数 TOP100 的 SSDP 反射服务器中，监测发现全部在本月仍活跃，存活率为 100%。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，黑龙江省占的比例最大，占 36.1%，其次是内蒙古自治区、广西壮族自治区和宁夏回族自治区；按运营商统计，电信占的比例最大，占 54.0%，移动占 46.0%，如图 14 所示。

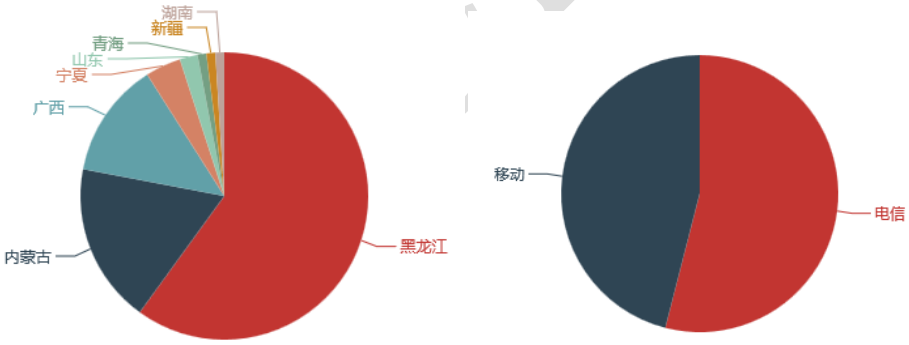

图 14 近两月被持续利用发起攻击的 SSDP 反射服务器数量按省份运营商分布

（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 5 月，通过跨域伪造流量发起攻击的流量来源于 208 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）参与的攻击事件数量最多，其次是归属于广东省联通（120.X.X.8、120.X.X.9）的路由器，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	新疆维吾尔自治区	移动(铁通)
221.X.X.9	新疆维吾尔自治区	移动(铁通)
120.X.X.8	广东省	联通
120.X.X.9	广东省	联通
221.X.X.254	广东省	联通
113.X.X.253	湖北省	联通
221.X.X.253	广东省	联通
218.X.X.254	内蒙古自治区	联通
219.X.X.70	北京市	电信
218.X.X.177	贵州省	移动
218.X.X.176	贵州省	移动
211.X.X.19	贵州省	移动
219.X.X.30	北京市	电信
211.X.X.20	贵州省	移动
61.X.X.25	浙江省	电信
218.X.X.241	内蒙古自治区	联通
113.X.X.252	湖北省	联通
113.X.X.253	广东省	电信
113.X.X.254	广东省	电信
222.X.X.200	山东省	电信
222.X.X.201	山东省	电信
222.X.X.200	山东省	电信
222.X.X.1	广西壮族自治区	电信
219.X.X.144	北京市	电信
222.X.X.2	广西壮族自治区	电信

跨域伪造流量涉及路由器按省份分布统计，江苏省占的比例最大，占 13.9%，其次是北京市和广东省；按路由器所属运营商统计，电信占的比例最大，占 36.1%，联通占比 33.2%，移动占比 30.7%，如图 15 所示。

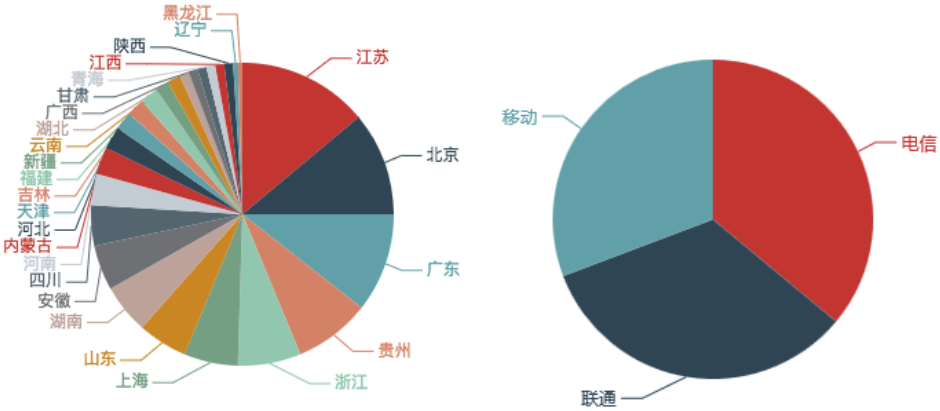

图 15 跨域伪造流量来源路由器数量按省份和运营商分布

2018 年度被持续利用转发 DDoS 攻击的跨域伪造流量来源路由器中，监测发现有 169 个在本月仍活跃，存活率为 81.3%。按省份分布统计，江苏省占的比例最大，占 14.8%，其次是广东省和贵州省；按路由器所属运营商统计，电信占的比例最大，占 40.8%，移动占比 30.2%，联通占比 29.0%，如图 16 所示。

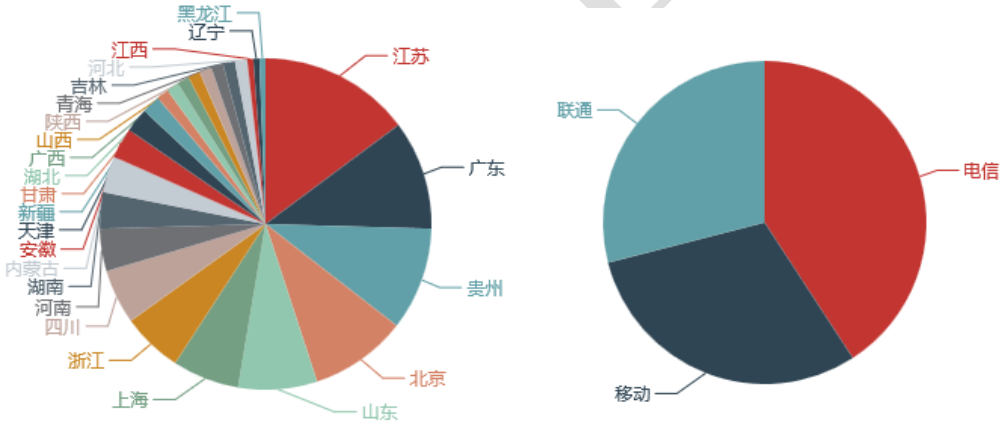

图 16 2018 年被持续利用转发跨域伪造攻击流量本月仍活跃路由器数量按省份和运营商分布

2. 本地伪造流量来源路由器

根据 CNCERT 抽样监测数据，2018 年 5 月，通过本地伪造流量发起攻击的流量来源于 543 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电信的路由器（222.X.X.16、222.X.X.15）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.253、220.X.X.243），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
222.X.X.16	新疆维吾尔自治区	电信
222.X.X.15	新疆维吾尔自治区	电信
220.X.X.253	北京市	电信
220.X.X.243	北京市	电信
218.X.X.176	贵州省	移动
218.X.X.177	贵州省	移动
219.X.X.2	山西省	电信
202.X.X.24	上海市	电信
211.X.X.19	贵州省	移动
211.X.X.254	河南省	移动
211.X.X.253	河南省	移动
117.X.X.254	天津市	联通
117.X.X.253	天津市	联通
219.X.X.10	山西省	电信
221.X.X.2	河南省	移动(铁通)
221.X.X.1	河南省	移动(铁通)
221.X.X.186	江苏省	电信
117.X.X.2	陕西省	电信
117.X.X.1	陕西省	电信
218.X.X.138	湖北省	联通
211.X.X.20	贵州省	移动
61.X.X.4	浙江省	电信
61.X.X.8	浙江省	电信
219.X.X.144	北京市	电信
124.X.X.2	山西省	联通

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 11.4%，其次是湖南省、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 50.3%，移动占比 27.4%，联通占比 22.3%，如图 17 所示。

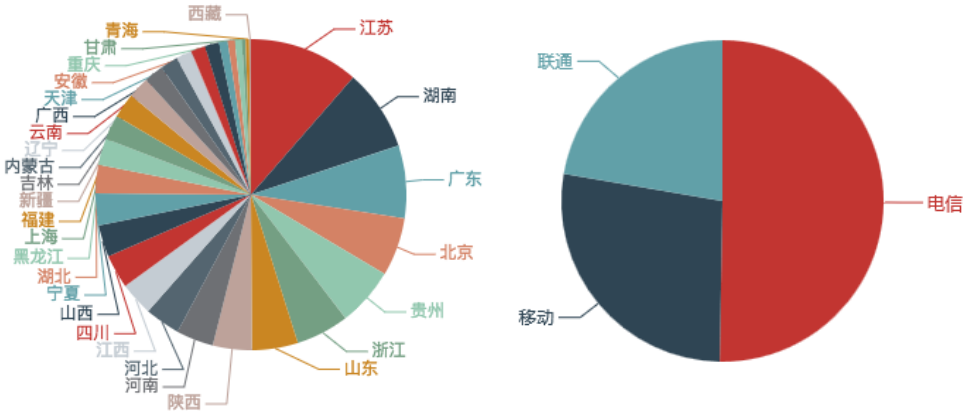

图 17 本地伪造流量来源路由器数量按省份和运营商分布

2018 年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 109 个在本月仍活跃，存活率为 20.1%。按省份统计，江苏省占的比例最大，占 24.8%，其次是江西省、贵州省和浙江省；按路由器所属运营商统计，电信占的比例最大，占 60.6%，移动占比 28.4%，联通占比 11.0%，如图 18 所示。

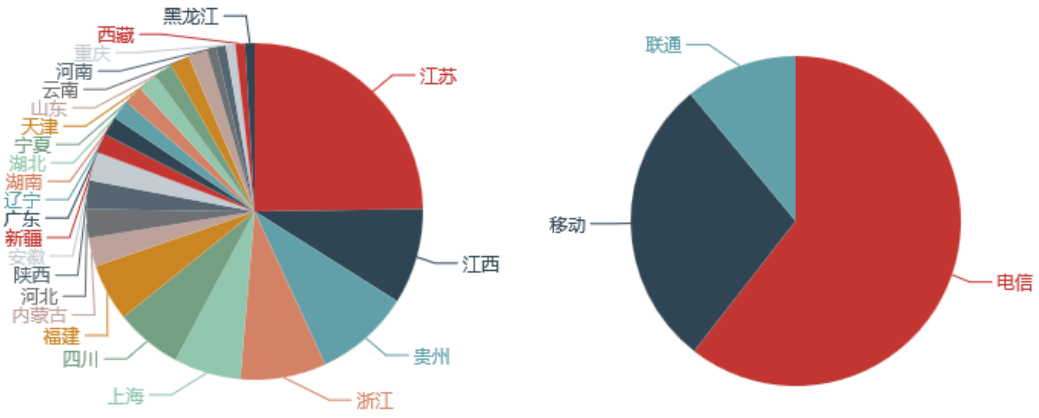

图 18 2018 年被持续利用且本月仍活跃的本地伪造流量来源路由器数量按省份运营商分布