我国 DDoS 攻击资源月度分析报告

——重点反射攻击专题分析

（2018 年 2 月）

国家计算机网络应急技术处理协调中心

2018 年 2 月

目 录

一、引言.....3

（一）攻击资源定义.....3

（二）本月重点关注情况.....4

二、反射攻击资源总情况分析.....5

（一）反射服务器资源分析.....5

（二）memchache 反射服务器反射攻击资源分析.....6

1. 反射服务器资源.....6

2. 反射攻击发起流量来源路由器.....8

（三）NTP 反射攻击资源分析.....10

1. 反射服务器资源.....10

2. 反射攻击发起流量来源路由器.....12

（四）SSDP 反射攻击资源分析.....14

1. 反射服务器资源.....14

2. 反射攻击发起流量来源路由器.....16

（五）反射攻击受害目标统计及治理建议.....18

一、引言

（一）攻击资源定义

近日，利用 memcached 服务器实施反射 DDoS 攻击的事件大幅上升。CNCERT 对三类重点反射攻击事件进行了集中监测和分析，本报告为 2018 年 2 月份的反射攻击资源专项分析报告。围绕互联网环境威胁治理问题，重点对“被利用发起 DDoS 反射攻击的重要网络资源有哪些”这个问题进行分析。反射攻击的网络资源包括：

1、 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。

2、 反射攻击发起流量来源路由器，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，因此反射攻击发起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，本报告将反射攻击发起流量来源路由器单独统计。

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 memcached 服务器实施反射攻击的事件大幅上升，自 2 月 21 日开始在我国境内尤为活跃。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、和北京市；数量最多的归属云服务商是阿里云。反射攻击发起流量来源路由器根据转发攻击事件的数量统计，最多的路由器归属于安徽省移动、上海市移动、和北京市电信。

2、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排名前三名的省份是河南省、北京市、和河北省；数量最多的归属运营商是联通。反射攻击发起流量来源路由器根据转发攻击事件的数量统计，最多的路由器归属于辽宁省电信、浙江省电信和浙江省联通。

3、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排名前三名的省份是山东省、辽宁省、和河北省；数量最多的归属运营商是联通。而反射攻击发起流量来源路由器根据转发攻击事件的数量统计，最多的路由器归属于北京市电信、天津市电信、和辽宁省移动。

二、反射攻击资源总情况分析

（一）反射服务器资源分析

根据 CNCERT 抽样监测数据，2018 年 2 月，利用反射服务器发起的三类重点反射攻击共涉及 2,252,085 台反射服务器，其中境内反射服务器 1,804,807 台，境外反射服务器 447,278 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 45,412 台，占比 2.0%，其中境内反射服务器 16,594 台，境外反射服务器 28,818 台；利用 NTP 反射发起反射攻击的反射服务器有 32,693 台，占比 1.5%，其中境内反射服务器 3,806 台，境外反射服务器 28,887 台；利用 SSDP 反射发起反射攻击的反射服务器有 2,173,980 台，占比 96.5%，其中境内反射服务器 1,784,407 台，境外反射服务器 389,573 台。

三种重点反射攻击类型根据所利用的反射服务器数量统计，占比最多的是 SSDP 反射攻击，占 96.5%；根据攻击事件数量统计，占比最多的也是 SSDP 反射攻击，占 51.9%。如图 1 所示。

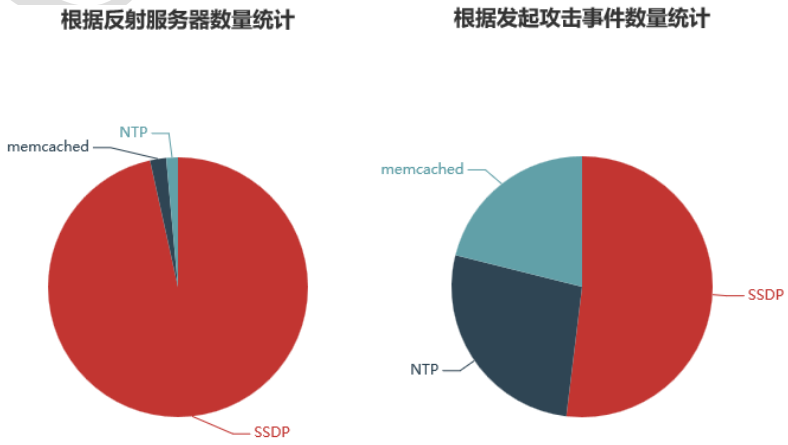

图 1 本月反射攻击利用端口根据服务器数量及事件数量统计

（二）memchache 反射服务器反射攻击资源分析

1．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 2 月，利用 memcached 服务器实施反射攻击的事件共涉及境内 16,594 台反射服务器，境外 28,818 台反射服务器。本月此类事件涉及的反射服务器数量趋势图，如图 2 所示，监测发现自 2 月 21 日开始被利用发起攻击的反射服务器数量上升明显。

图 2 本月 memcached 反射服务器数量按天分布图

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 24.1%，其次是浙江省、北京市和山东省；按归属运营商或云服务商统计，阿里云占的比例最大，占 35.9%，电信占比 31.3%，联通占比 11.7%，移动占比 8.2%，如图 3 所示。

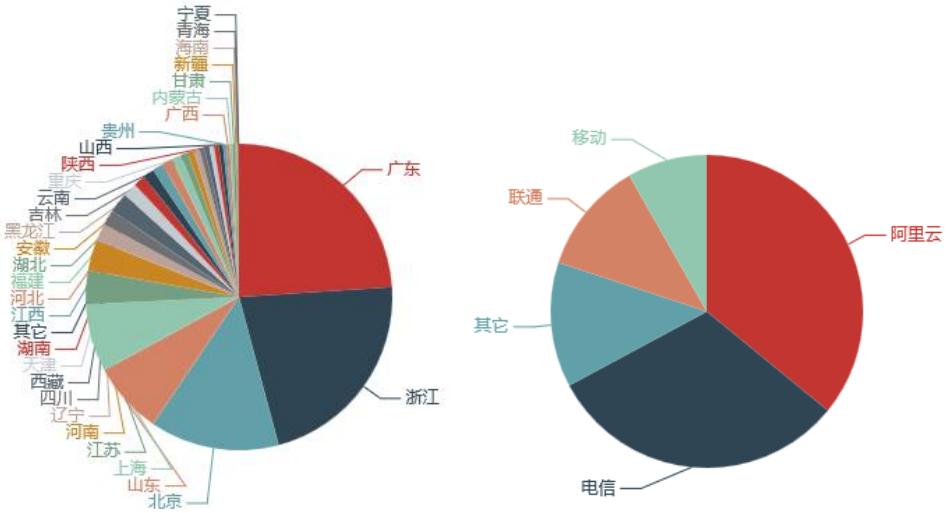

图 3 本月境内 memcached 反射服务器数量按省份、运营商或云服务商分布

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 29.8%，其次是日本、法国和俄罗斯，如图 4 所示。

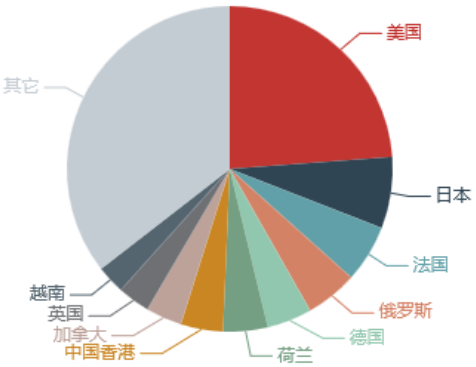

图 4 本月境外反射服务器数量按国家或地区分布

为防止 memchached 反射攻击事件蔓延，CNCERT 从事件爆发开始，密切关注事件的演变情况，并在工业和信息化部网络安全管理局的指导下，组织各省分中心集中开展应急响应工作，截止 3 月初通报处置了 1.4 万个已被利用发起攻击或探测

扫描的 memcached 服务器。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 1 所示，位于上海市和浙江省的地址最多。

表 1 本月境内发起反射攻击事件数量 TOP100 中仍存活的 memcached 服务器

反射服务器地址	归属省份	归属运营商或云服务商
42.X.X.187	辽宁省	电信
42.X.X.244	辽宁省	电信
58.X.X.124	湖南省	联通
101.X.X.242	上海市	电信
101.X.X.187	上海市	电信
101.X.X.215	上海市	电信
101.X.X.84	上海市	电信
101.X.X.152	上海市	电信
111.X.X.170	江西省	电信
111.X.X.245	江西省	电信
111.X.X.6	江西省	电信
112.X.X.225	辽宁省	移动
114.X.X.55	浙江省	阿里云
120.X.X.17	浙江省	阿里云
120.X.X.127	浙江省	阿里云
120.X.X.177	浙江省	阿里云
120.X.X.186	浙江省	阿里云
120.X.X.160	浙江省	阿里云
121.X.X.109	浙江省	电信
123.X.X.208	北京市	待确认
139.X.X.192	广东省	电信
211.X.X.13	浙江省	电信

2．反射攻击发起流量来源路由器

2018 年 2 月，境内利用 memcached 服务器实施反射攻击的发起流量主要来源于 626 个路由器，根据参与攻击事件的数量统计，归属于安徽省移动的路由器（120.X.X.2、120.X.X.1）涉及的攻击事件最多，其次是归属于上海市移动（211.X.X.203）、和北京市电信（202.X.X.17）的路由器，如表 2 所示。

表 2 本月转发反射放大攻击事件流量的来源路由器按事件数量 TOP25

反射攻击发起流量来源路由器	所属省份	所属运营商
120.X.X.2	安徽省	移动
120.X.X.1	安徽省	移动
211.X.X.203	上海市	移动
202.X.X.17	北京市	电信
112.X.X.39	上海市	联通
220.X.X.126	浙江省	电信
220.X.X.127	浙江省	电信
202.X.X.16	北京市	电信
211.X.X.205	上海市	移动
202.X.X.137	山西省	电信
202.X.X.136	山西省	电信
221.X.X.1	河南省	移动
202.X.X.21	上海市	电信
112.X.X.38	上海市	联通
211.X.X.44	辽宁省	移动
211.X.X.4	湖南省	移动
220.X.X.243	北京市	电信
124.X.X.2	浙江省	联通
211.X.X.3	湖南省	移动
211.X.X.45	辽宁省	移动
120.X.X.247	安徽省	移动
220.X.X.253	北京市	电信
211.X.X.3	浙江省	移动
219.X.X.70	北京市	电信
211.X.X.8	浙江省	移动

根据反射发起攻击流量的来源路由器数量按省份统计，北京市占的比例最大，占 18.4%，其次是广东省、江苏省和四川省；按反射发起攻击流量的来源路由器数量按归属运营商统计，联通占的比例最大，占 30.9%，移动占比 29.8%，电信占比 24.3%，如图 5 所示。

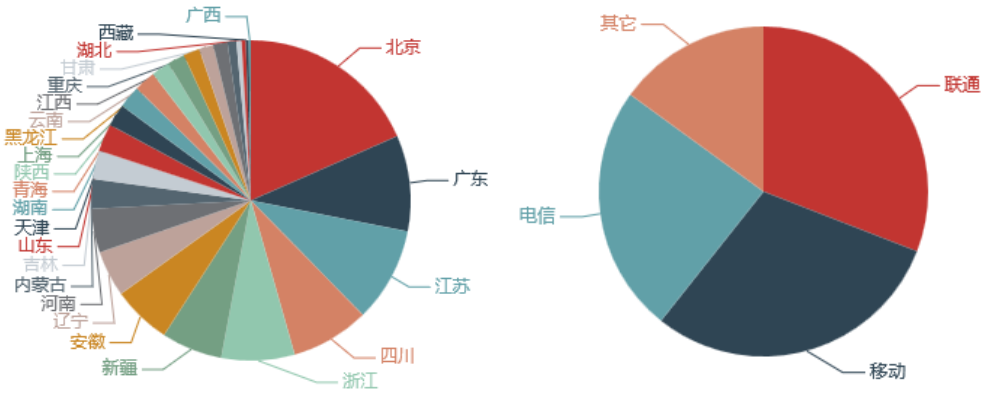

图 5 本月 memcached 反射攻击发起流量来源路由器数量按省份和运营商分布

（三）NTP 反射攻击资源分析

1．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 2 月，NTP 反射攻击事件共涉及我国境内 3,806 台反射服务器，境外 28,887 台反射服务器。

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，河南省占的比例最大，占 17.7%，其次是北京市、河北省和广东省；按归属运营商统计，联通占的比例最大，占 54.4%，电信占比 28.7%，移动占比 12.7%，如图 6 所示。

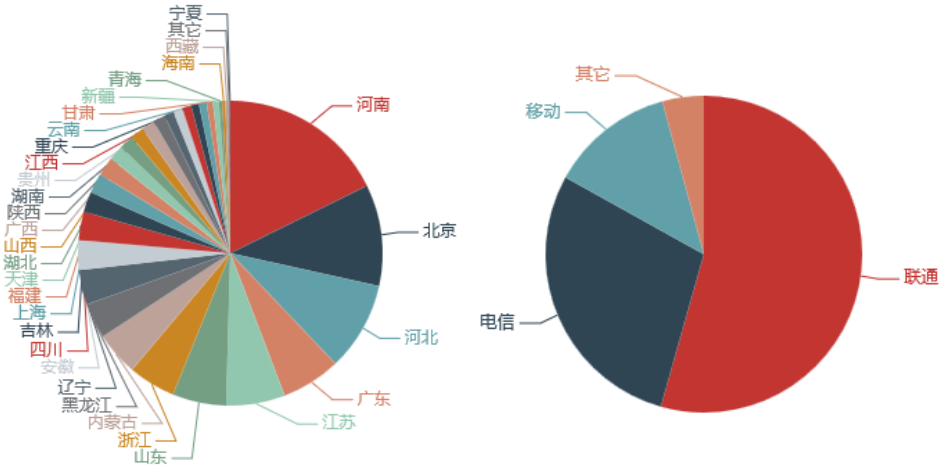

图 6 本月被利用发起 NTP 反射攻击的境内反射服务器数量按省份和运营商分布

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，越南占的比例最大，占 11.7%，其次是美国、中国台湾和土耳其，如图 7 所示。

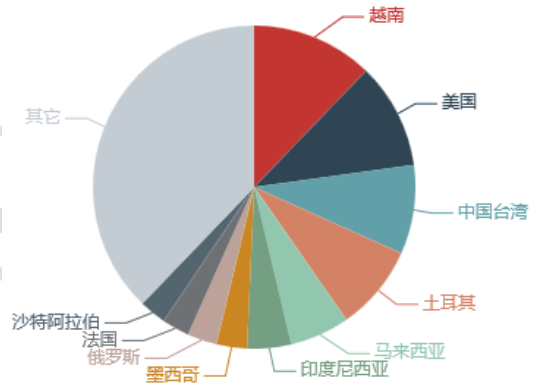

图 7 本月被利用发起 NTP 反射攻击的境外反射服务器数量按国家或地区分布

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 3 所示，位于吉林省和北京市的地址最多。

表 3 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
221.X.X.37	河南省	移动

120.X.X.12	河北省	联通
61.X.X.59	河南省	联通
113.X.X.56	西藏自治区	电信
122.X.X.170	江苏省	联通
119.X.X.93	湖南省	联通
119.X.X.12	山东省	联通
119.X.X.147	吉林省	联通
119.X.X.43	四川省	联通
113.X.X.27	湖北省	联通
61.X.X.174	山东省	联通
125.X.X.42	河南省	联通
218.X.X.23	河南省	联通
124.X.X.110	河北省	电信
218.X.X.14	山东省	联通
60.X.X.131	黑龙江省	联通
221.X.X.28	浙江省	联通
113.X.X.8	黑龙江省	联通
218.X.X.80	黑龙江省	联通
218.X.X.2	黑龙江省	联通
60.X.X.12	新疆维吾尔自治区	联通
60.X.X.126	新疆维吾尔自治区	联通
124.X.X.166	北京市	联通
220.X.X.54	安徽省	联通
114.X.X.108	北京市	联通
211.X.X.26	山东省	联通
119.X.X.114	吉林省	联通
119.X.X.138	吉林省	联通
221.X.X.132	山东省	联通
111.X.X.10	浙江省	移动

2．反射攻击发起流量来源路由器

2018 年 2 月，境内 NTP 反射攻击事件的发起流量主要来源于 111 个路由器，根据参与攻击事件的数量统计，归属于辽宁省电信的路由器（219.X.X.11）涉及的攻击事件最多，其次是归属于浙江省电信（220.X.X.127）、和浙江省联通（124.X.X.21）的路由器，如表 4 所示。

表 4 本月 NTP 反射攻击事件的流量来源路由器按事件数量 TOP25

反射攻击发起流量来源路由器	所属省份	所属运营商
219.X.X.11	辽宁省	电信
220.X.X.127	浙江省	电信
124.X.X.21	浙江省	联通
124.X.X.22	浙江省	联通
220.X.X.126	浙江省	电信
219.X.X.12	辽宁省	电信
222.X.X.121	吉林省	电信
211.X.X.45	辽宁省	移动
211.X.X.44	辽宁省	移动
202.X.X.136	山西省	电信
211.X.X.54	辽宁省	移动
221.X.X.1	天津市	电信
211.X.X.17	辽宁省	移动
202.X.X.137	山西省	电信
221.X.X.2	天津市	电信
221.X.X.192	广东省	移动
61.X.X.14	北京市	联通
61.X.X.152	北京市	联通
61.X.X.12	北京市	联通
61.X.X.40	北京市	联通
61.X.X.4	北京市	联通
61.X.X.153	北京市	联通
111.X.X.1	青海省	移动
221.X.X.191	广东省	移动
220.X.X.253	北京市	电信

根据发起 NTP 反射攻击流量的来源路由器数量按省份统计，广东省占的比例最大，占 23.4%，其次是北京市、内蒙古和浙江省；按发起 NTP 反射攻击流量的来源路由器数量按归属运营商统计，移动占的比例最大，占 39.6%，电信占比 30.6%，联通占比 29.7%，如图 8 所示。

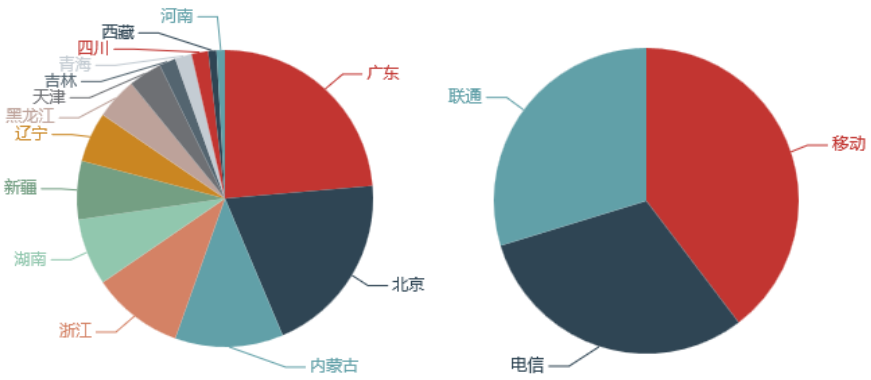

图 8 本月发起 NTP 反射攻击流量的来源路由器数量按省份和运营商分布

（四）SSDP 反射攻击资源分析

1. 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 ICMP 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 2 月，SSDP 反射攻击事件共涉及境内 1,784,407 台反射服务器，境外 389,573 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，山东省占的比例最大，占 25.1%，其次是辽宁省、河北省和吉林省；按归属运营商统计，联通占的比例最大，占 74.4%，电信占比 23.3%，移动占比 2.0%，如图 9 所示。

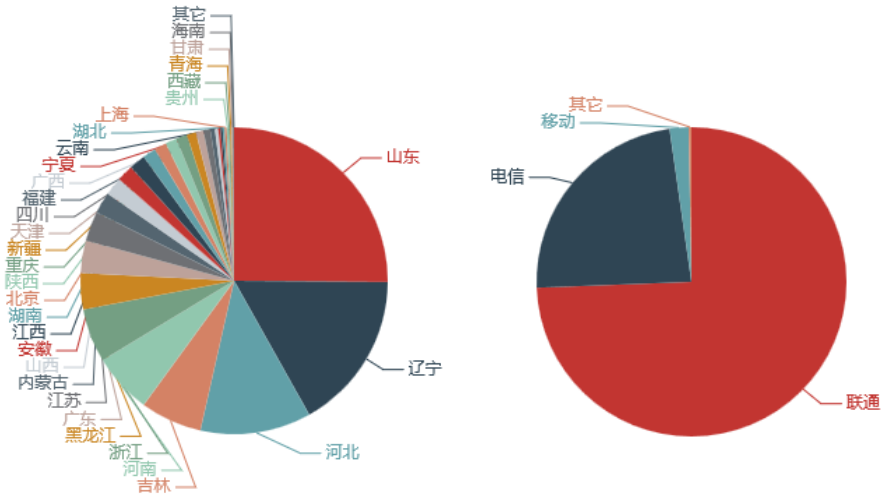

图 9 本月被利用发起 SSDP 反射攻击的境内反射服务器数量按省份和运营商分布

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，俄罗斯占的比例最大，占 29.7%，其次是美国、加拿大和土耳其，如图 10 所示。

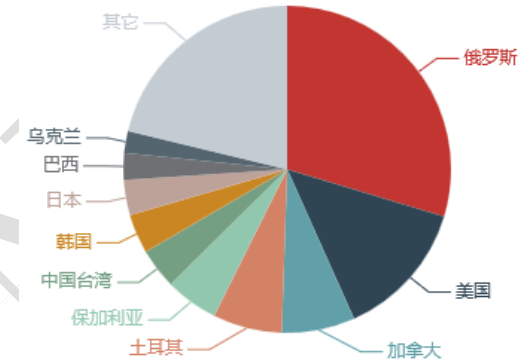

图 10 本月被利用发起 SSDP 反射攻击的境外反射服务器数量按国家或地区或地区分布

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 TOP30 的反射服务器及归属如表 5 所示，地址大量位于黑龙江省。

表 5 本月境内被利用发起 SSDP 反射攻击事件数量中排名 TOP30 的反射服务器

反射服务器地址	归属省份	归属运营商或云服务商
111.X.X.27	黑龙江省	移动
111.X.X.40	黑龙江省	移动

111.X.X.203	黑龙江省	移动
111.X.X.94	黑龙江省	移动
112.X.X.26	黑龙江省	电信
112.X.X.163	黑龙江省	电信
112.X.X.18	黑龙江省	电信
112.X.X.55	黑龙江省	电信
112.X.X.4	黑龙江省	电信
123.X.X.81	黑龙江省	电信
219.X.X.198	黑龙江省	电信
222.X.X.22	黑龙江省	电信
222.X.X.130	黑龙江省	电信
222.X.X.178	黑龙江省	电信
222.X.X.81	黑龙江省	电信
222.X.X.107	黑龙江省	电信
222.X.X.124	黑龙江省	电信
222.X.X.90	黑龙江省	电信
222.X.X.26	黑龙江省	电信
222.X.X.106	黑龙江省	电信
222.X.X.34	黑龙江省	电信
222.X.X.105	黑龙江省	电信
222.X.X.29	黑龙江省	电信
39.X.X.4	辽宁省	移动
59.X.X.98	辽宁省	电信
59.X.X.101	辽宁省	电信
39.X.X.53	辽宁省	移动
219.X.X.150	辽宁省	电信
59.X.X.100	辽宁省	电信
220.X.X.145	西藏自治区	电信

2. 反射攻击发起流量来源路由器

2018 年 2 月，境内 SSDP 反射攻击事件的发起流量主要来源于 705 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（219.X.X.70）涉及的攻击事件最多，其次是归属于北京市电信（219.X.X.45、219.X.X.30、219.X.X.144）和天津市电信（221.X.X.1、221.X.X.2）的路由器，如表 6 所示。

表 6 本月 SSDP 反射攻击事件的发起流量来源路由器按事件数量 TOP25

反射攻击发起流量来源路由器	所属省份	所属运营商
219.X.X.70	北京市	电信
219.X.X.45	北京市	电信
219.X.X.30	北京市	电信
219.X.X.144	北京市	电信
221.X.X.1	天津市	电信
221.X.X.2	天津市	电信
211.X.X.44	辽宁省	移动
220.X.X.243	北京市	电信
220.X.X.253	北京市	电信
211.X.X.54	辽宁省	移动
211.X.X.17	辽宁省	移动
61.X.X.104	北京市	联通
61.X.X.238	北京市	联通
180.X.X.1	北京市	电信
218.X.X.6	北京市	电信
218.X.X.24	北京市	电信
61.X.X.245	北京市	联通
180.X.X.2	北京市	电信
221.X.X.253	广东省	联通
117.X.X.1	辽宁省	移动
221.X.X.1	安徽省	移动
117.X.X.2	北京市	电信
124.X.X.21	浙江省	移动
61.X.X.12	北京市	电信
124.X.X.22	浙江省	移动

根据发起 SSDP 反射攻击流量的来源路由器数量按省份统计，北京市占的比例最大，占 12.5%，其次是广东省、湖南省和新疆维吾尔族自治区；发起 SSDP 反射攻击流量的来源路由器数量按归属运营商统计，移动占的比例最大，占 38.9%，电信占比 33.3%，联通占比 27.8%，如图 11 所示。

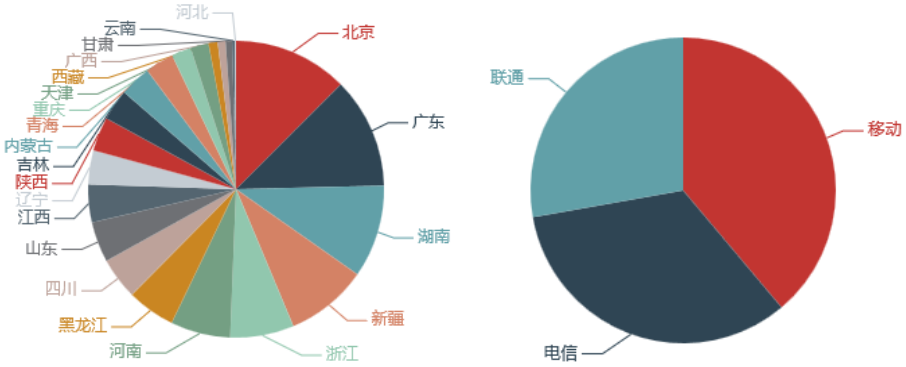

图 11 本月发起 SSDP 反射攻击流量的来源路由器数量按省份和运营商分布

（五）反射攻击受害目标统计及治理建议

CNCERT 根据抽样监测分析发现，2018 年 2 月我国境内超过 1500 个攻击目标遭受到 DDoS 反射攻击，其中，遭受 memcached 反射攻击的受害目标占比 14.3%；遭受 NTP 反射攻击的受害目标占比 34.7%；遭受 SSDP 反射攻击的受害目标占比 51.0%。这些攻击目标按省份分布如图 12 所示，其中浙江省占比最大，占 21.3%；其次是江苏省、广东省和福建省。

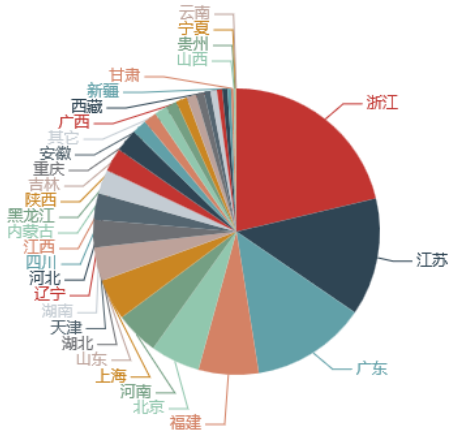

图 12 本月遭受反射攻击的攻击目标数量按省份分布

目前，在工业和信息化部网络安全管理局的指导下，CNCERT 组织各省分中心、运营商、安全企业、云服务商等持续开展 DDoS 攻击资源治理工作，要求各单位对发现被用于反

射攻击的服务器、电脑主机和智能设备及时进行通知处理，要求运营商加强对虚假源地址流量的精细化整治工作。此外，建议用户及相关使用单位提高网络安全意识和安全防护能力，及时更新升级固件或服务程序、修复漏洞，规范安全配置。针对无需提供公开互联网服务的服务器、电脑主机和智能设备，建议直接关闭 DNS、SSDP、NTP、SNMP、Chargen、Memcached 等服务，或在防火墙或网络出入口上封禁外部 IP 访问这些服务端口。针对需要对指定 IP 提供服务的，可通过配置防火墙等访问控制策略允许授权 IP 的访问并禁止其他 IP 的访问，另外 Memcached 等部分服务也可通过更改默认服务端口或更改传输协议类型为 TCP 等方式来预防反射攻击。针对需要提供公开互联网服务的，可根据反射攻击的特点，对特定反射攻击指令的报文流量进行监测识别和过滤、对反射攻击的伪造源 IP 地址进行监测识别和限速、限流、拦截。