2017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

2017年12月

目 录

一、引 言.....3

二、DDoS 攻击资源分析.....4

（一）控制端资源分析.....4

（二）肉鸡资源分析.....7

（三）反射攻击资源分析.....10

1. 反射服务器资源.....10
2. 反射攻击流量来源路由器.....13

（四）发起伪造流量的路由器分析.....14

1. 跨域伪造流量来源路由器.....14
2. 本地伪造流量来源路由器.....17

一、引 言

近期，CNCERT 深度分析了我国大陆地区发生的数千起 DDoS（分布式拒绝服务）攻击事件。本报告围绕互联网环境威胁治理问题，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、 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。

二、DDoS 攻击资源分析

（一）控制端资源分析

根据 CNCERT 监测数据，今年以来，利用肉鸡发起 DDoS 攻击的控制端总量为 25,532 个。发起的攻击次数呈现幂律分布，如图 1 所示。平均每个控制端发起过 7.7 次攻击。

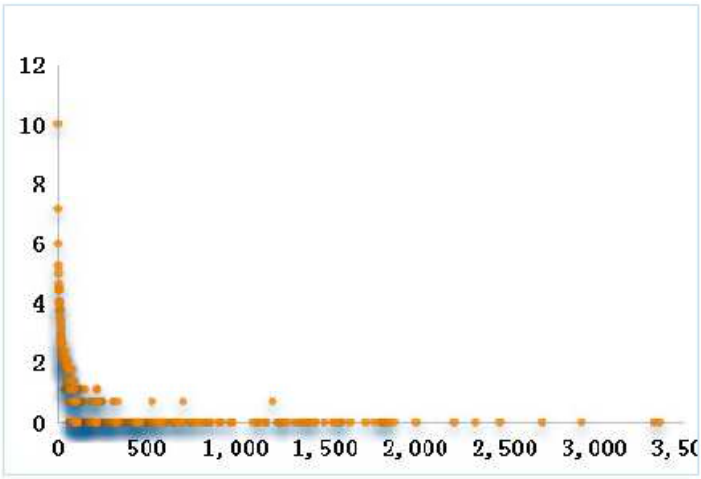

图 1 控制端利用肉鸡发起 DDoS 攻击的事件次数呈幂律分布

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 10.1%；其次是韩国和中国台湾，如图 2 所示。

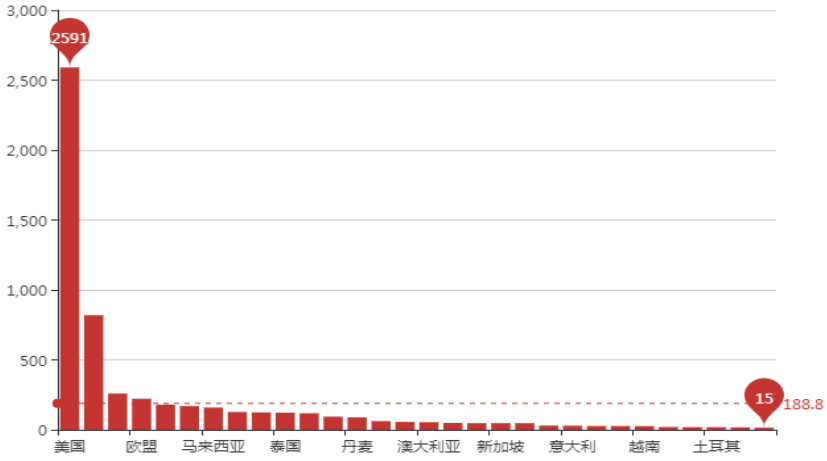

图 2 发起 DDoS 攻击的境外控制端数量按国家或地区 TOP30

位于境内的控制端按省份统计，广东省占的比例最大，占 12.2%；其次是江苏省、四川省和浙江省，如图 3 所示。

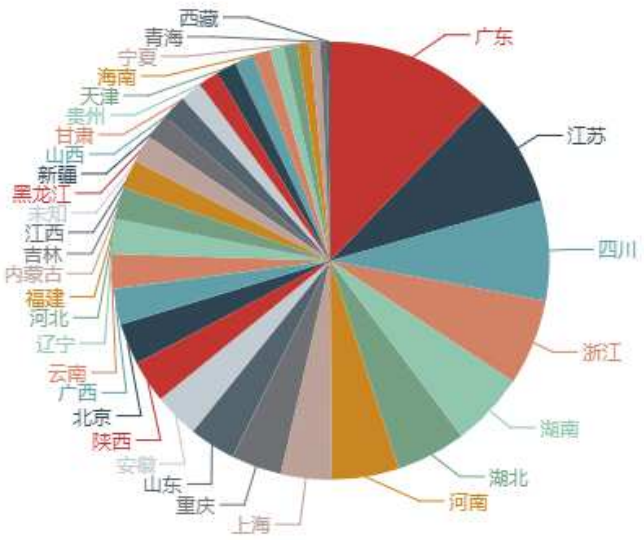

图 3 发起 DDoS 攻击的境内控制端数量按省份分布

控制端发起攻击的天次总体呈现幂律分布，如图 4 所示。平均每个控制端在 1.51 天被尝试发起了 DDoS 攻击，最多的控制端在 119 天范围内发起了攻击，占总监测天数的五分之二。

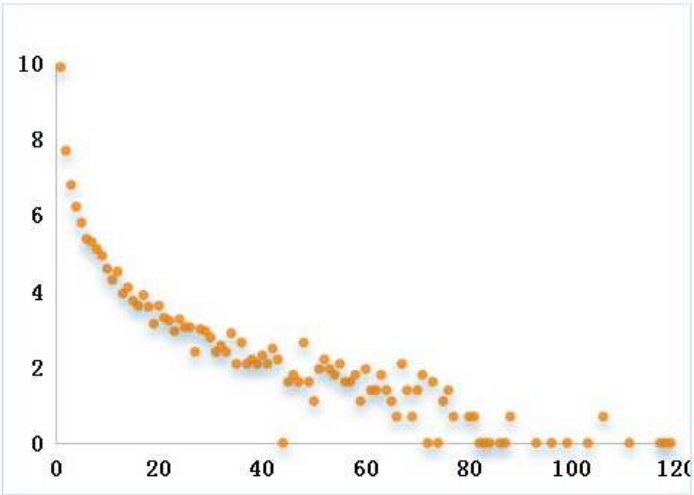

图 4 控制端尝试发起攻击天次呈现幂律分布

控制端尝试发起攻击的月次情况如表 1 所示。平均每个控制端在今年的 1.19 个月发起了 DDoS 攻击，有 3 个控制端地址在至少连续 7 个月次持续发起攻击。

表 1 控制端发起攻击月次情况

月次	控制端数量
7	3
6	18
5	169
4	333
3	539
2	2013
1	22456

（二）肉鸡资源分析

根据 CNCERT 监测数据，利用真实肉鸡地址直接攻击（包含直接攻击与其它攻击的混合攻击）的 DDoS 攻击事件占事件总量的 80%。其中，共有 751,341 个真实肉鸡地址参与攻击，涉及 193,723 个 IP 地址 C 段。肉鸡地址参与攻击的次数总体呈现幂律分布，如图 5 所示，平均每个肉鸡地址参与 2.13 次攻击。

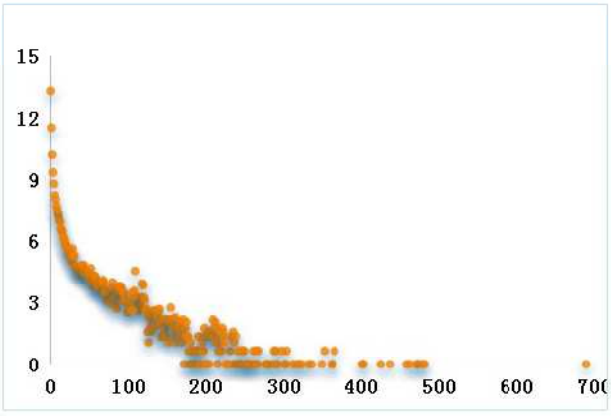

图 5 肉鸡地址参与攻击次数呈现幂律分布

参与攻击最多的肉鸡地址为归属于山西省运城市闻喜县

联通的某地址，共参与了 690 次攻击。其次是归属于安徽省铜陵市铜官区联通的某地址，共参与了 482 次攻击；以及归属于贵州省贵阳市云岩区联通的某地址，共参与了 479 次攻击。

这些肉鸡按境内省份统计，北京占的比例最大，占 9%；其次是山西省、重庆市和浙江省，如图 6 所示。按运营商统计，电信占的比例最大，占 49.3%，移动占 23.4%，联通占 21.8%，如图 7 所示。

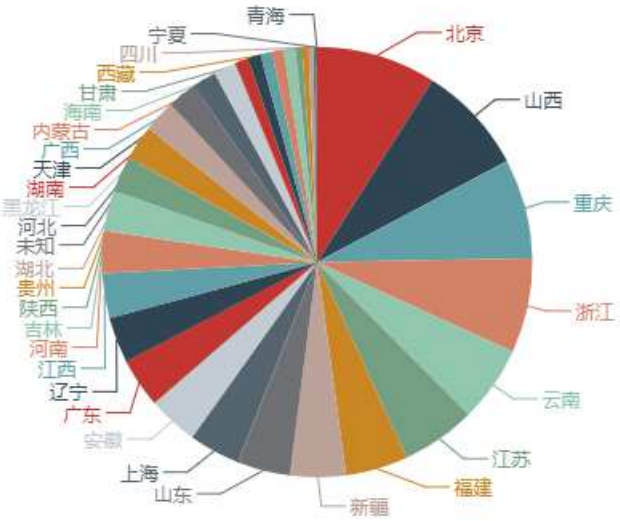

图 6 肉鸡地址数量按省份分布

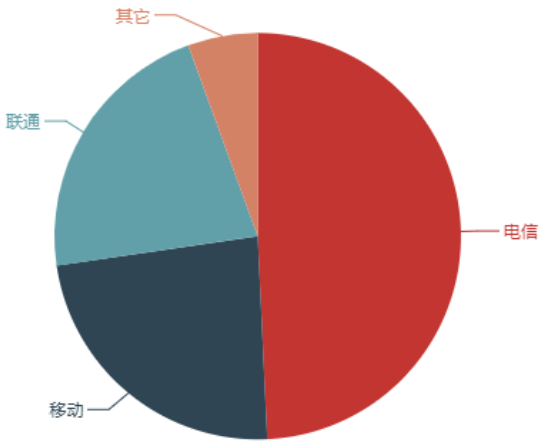

图 7 肉鸡地址数量按运营商分布

肉鸡资源参与攻击的天次总体呈现幂律分布，如图 8 所示。平均每个肉鸡资源在 1.51 天被利用发起了 DDoS 攻击，最多的肉鸡资源在 145 天范围内被利用发起攻击，占总监测天数的五分之三。

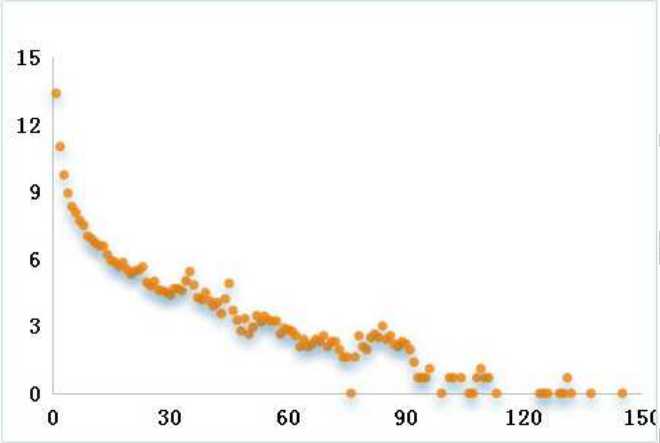

图 8 肉鸡参与攻击天次呈现幂律分布

肉鸡资源参与攻击的月次总体情况如表 2 所示。平均每个肉鸡资源在今年的 1.11 个月被利用发起了 DDoS 攻击，有 271 个肉鸡地址在连续 8 个月次被利用发起攻击，也就是说，这些肉鸡资源在监测月份中每个月都被利用以发起 DDoS 攻击，没有得到有效的清理处置。

表 2 肉鸡参与攻击月次情况

参与攻击月次	肉鸡数量
8	271
7	295
6	759
5	1488
4	2916
3	9434
2	44530
1	691648

（三）反射攻击资源分析

1. 反射服务器资源

根据 CNCERT 监测数据，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 25%，其中，共涉及 251,828 台反射服务器，反射服务器被利用以攻击的次数呈现幂律分布，如图 9 所示，平均每台反射服务器参与 1.76 次攻击。

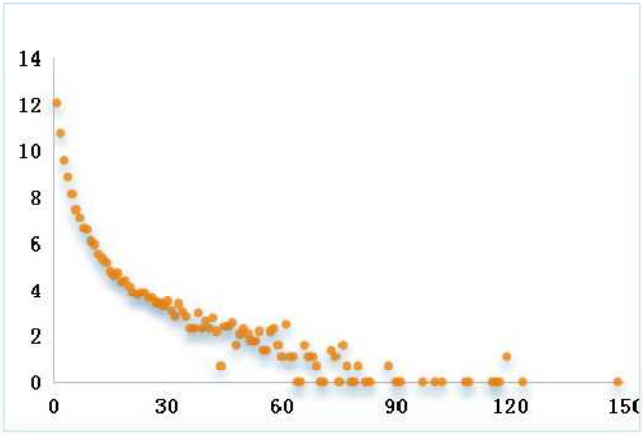

图 9 反射服务器被利用攻击次数呈现幂律分布

被利用最多发起反射放大攻击的服务器归属于新疆伊犁哈萨克自治州伊宁市移动，共参与了 148 次攻击。其次，是归属于新疆昌吉回族自治州阜康市移动的某地址，共参与了 123 次攻击；以及归属于新疆阿勒泰地区阿勒泰市联通的某地址，共参与了 119 次攻击。

反射服务器被利用发起攻击的天次总体呈现幂律分布，如图 10 所示。平均每个反射服务器在 1.38 天被利用发起了 DDoS 攻击，最多的反射服务器在 65 天范围内被利用发起攻击，近占监测总天数的三分之一。

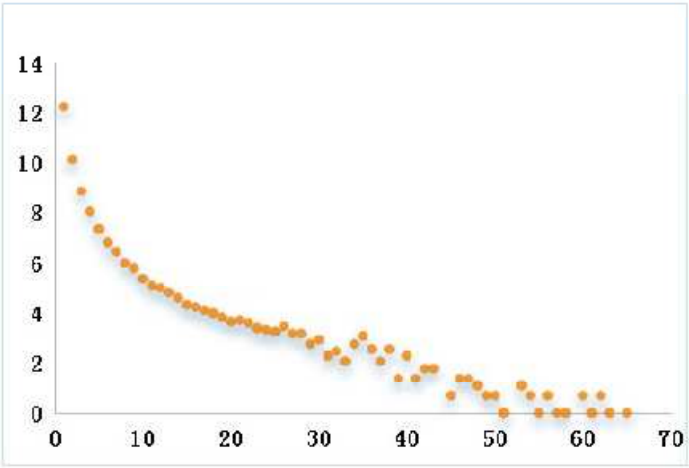

图 10 反射服务器参与攻击天次呈现幂律分布

反射服务器被利用发起攻击的月次情况如表 3 所示。平均每个反射服务器在今年的 1.1 个月被利用发起了 DDoS 攻击，有 101 个反射服务器在 8 个月次连续被利用发起攻击，也就是说，这些反射器在监测月份中每个月都被利用以发起 DDoS 攻击.

表 3 反射服务器参与攻击月次情况

参与攻击月次	反射服务器数量
8	101
7	196
6	345
5	586
4	1169
3	2454
2	11462
1	235515

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。被利用发起攻击的反射服务器中，93.8%曾通过 1900 号端口发起反射放大攻击，占反射攻击事件总量的 75.6%。如图 11

所示。

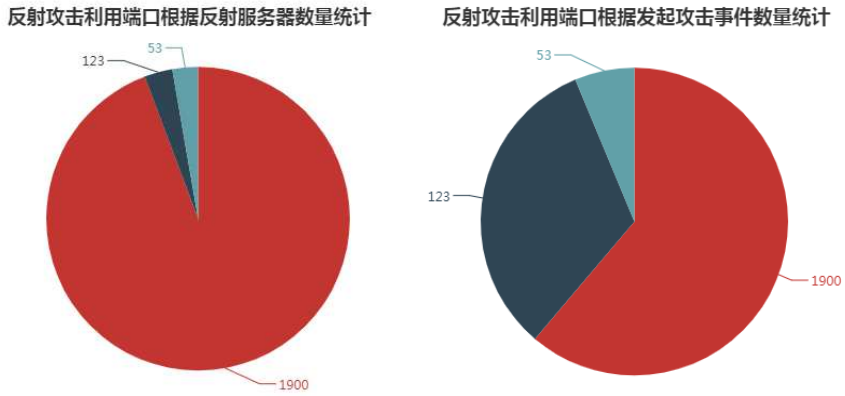

图 11 反射攻击利用端口根据服务器数量及事件数量统计

根据反射服务器数量按省份统计，新疆占的比例最大，占 18.7%；其次是山东省、辽宁省和内蒙古，如图 12 所示。按运营商统计，联通占的比例最大，占 47%，电信占比 27%，移动占比 23.2%，如图 13 所示。

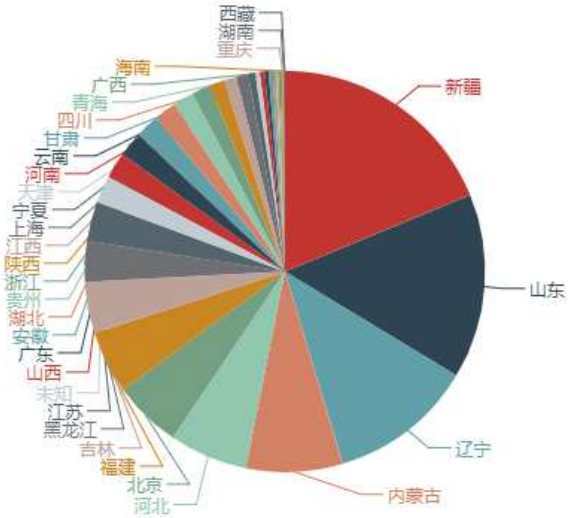

图 12 反射服务器数量按省份分布

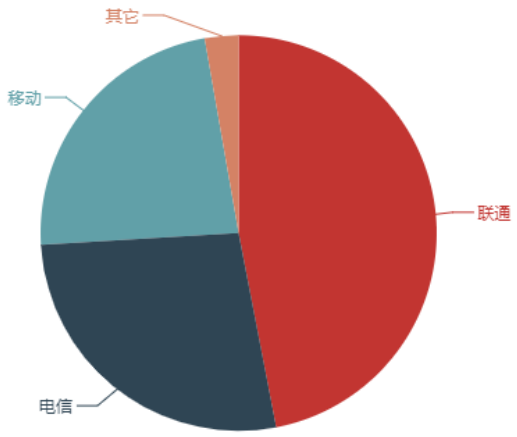

图 13 反射服务器数量按运营商分布

2. 反射攻击流量来源路由器

境内反射攻击流量主要来源于 412 个路由器，根据参与攻击事件的数量统计，归属于国际口的某路由器发起的攻击事件最多，为 227 件，其次是归属于河北省、北京市、以及天津的路由器，如图 14 所示。

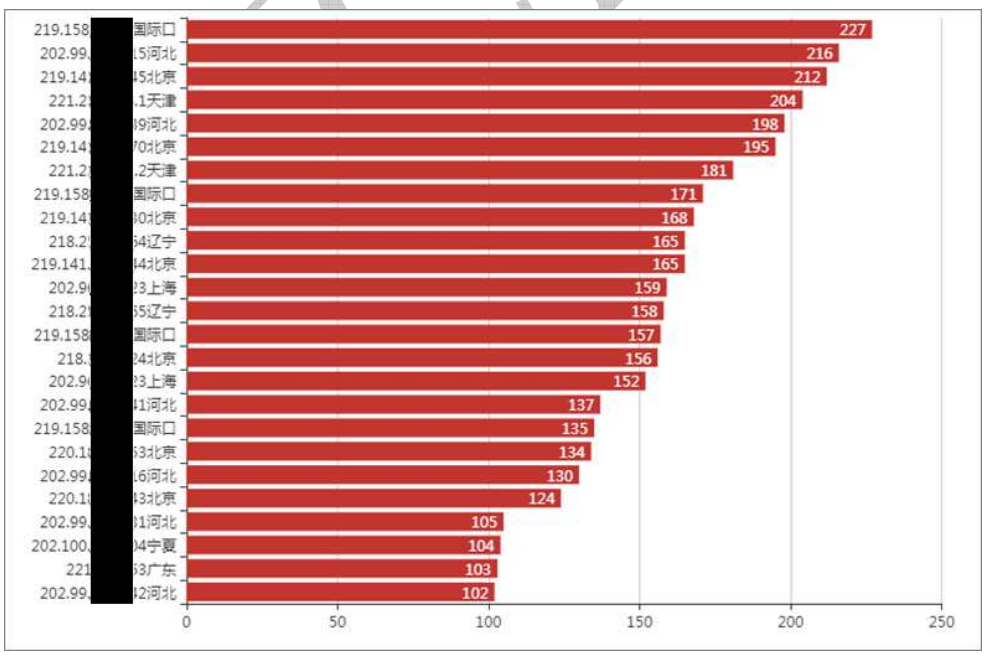

图 14 发起反射放大攻击事件的流量来源路由器按事件 TOP25

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%；其次是山东省、广东省和辽宁省，如图 15 所示。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 45.1%，电信占比 36.4%，移动占比 18.5%，如图 16 所示。

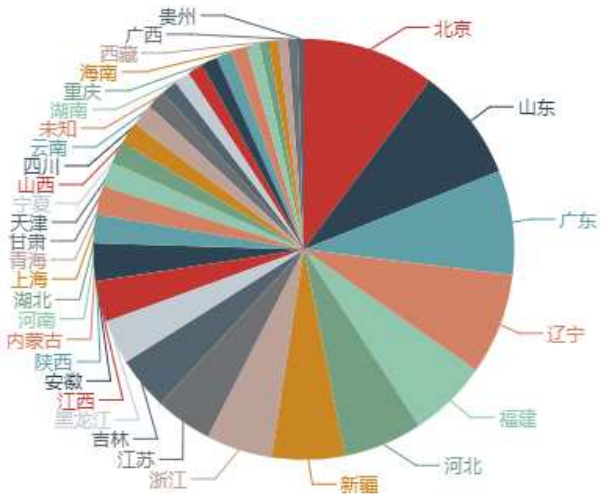

图 15 反射攻击流量来源路由器数量按省分布

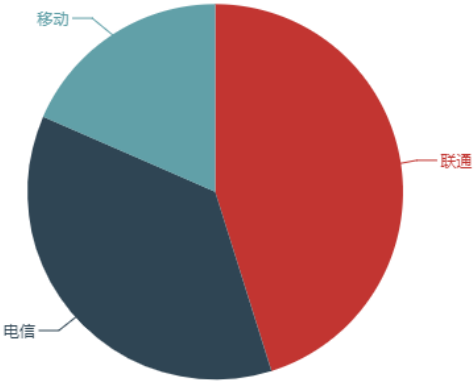

图 16 反射攻击流量来源路由器数量按运营商分布

（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 监测数据，包含跨域伪造流量的 DDoS 攻击

事件占事件总量的 49.8%，通过跨域伪造流量发起攻击的流量来源于 379 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参与的攻击事件数量最多，均参与了 326 件，其次是归属于安徽省电信的路由器，如图 17 所示。

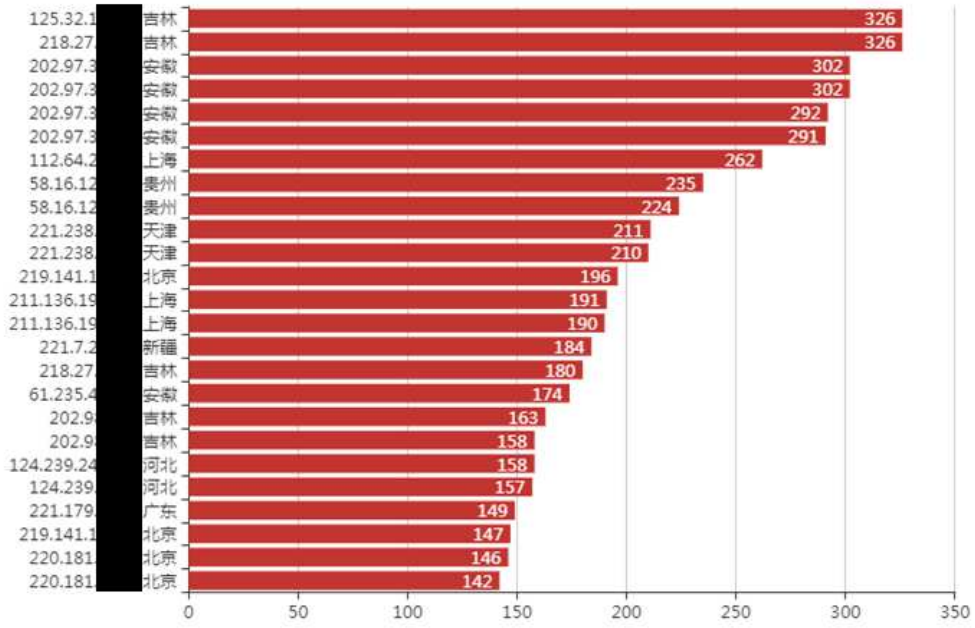

图 17 跨域伪造流量来源路由器按参与事件数量 TOP25

发起跨域伪造流量的路由器参与发起攻击的天次总体呈现幂律分布，如图 18 所示。平均每个路由器在 15.5 天被发现发起跨域伪造地址流量攻击，最多的路由器在 105 天范围内被发现发起跨域攻击流量，近占监测总天数的二分之一。

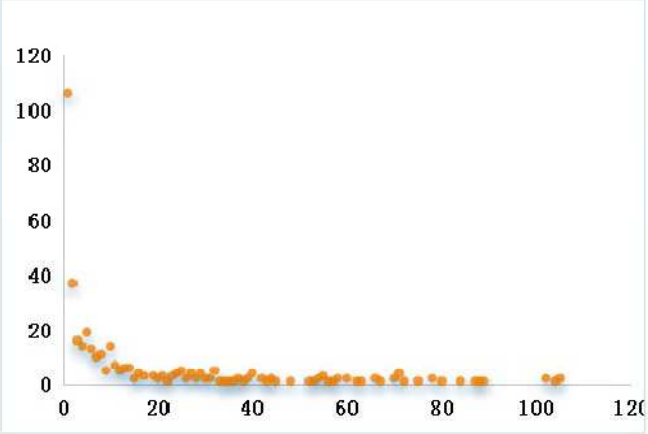

图 18 跨域伪造流量来源路由器参与攻击天次呈现幂律分布

发起跨域伪造流量的路由器参与发起攻击的月次情况如表 4 所示。平均每个路由器在 2.7 个月次被发现发起跨域伪造地址流量攻击，14 个路由器在连续 8 个月内被发现发起跨域攻击流量，也就是说，这些路由器长期多次地被利用发起跨域伪造流量攻击。

表 4 跨域伪造流量来源路由器参与攻击月次情况

参与攻击月次	跨域伪造流量来源路由器数量
8	14
7	16
6	18
5	24
4	37
3	42
2	71
1	156

跨区域伪造流量涉及路由器按省份分布统计如图 19 所示，其中，北京市占的比例最大，占 13.2%；其次是江苏省、山东省、及广东省。按路由器所属运营商统计，联通占的比例最大，占 46.7%，电信占比 30.6%，移动占比 22.7%，如图 20 所示。

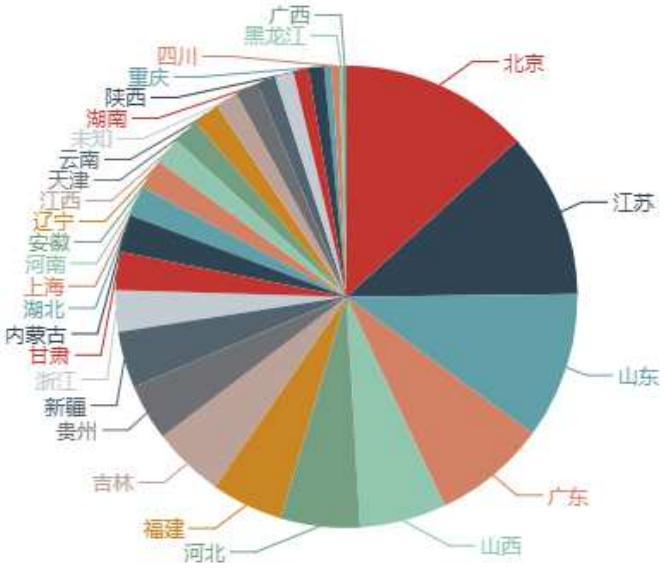

图 19 跨域伪造流量来源路由器数量按省分布

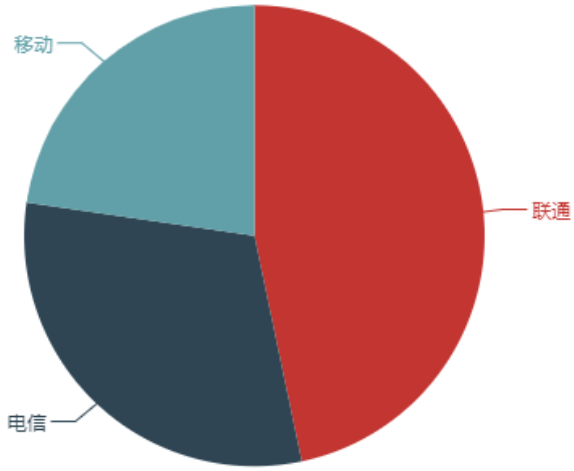

图 20 跨域伪造流量来源路由器数量按运营商分布

2. 本地伪造流量来源路由器

根据 CNCERT 监测数据，包含本地伪造流量的 DDoS 攻击事件占事件总量的 51.3%，通过本地伪造流量发起攻击的流量来源于 725 个路由器。根据参与攻击事件的数量统计，归属于安徽省电信的路由器参与的攻击事件数量最多，最多参与了 424 件，其次是归属于陕西省电信的路由器，如图 21 所示。

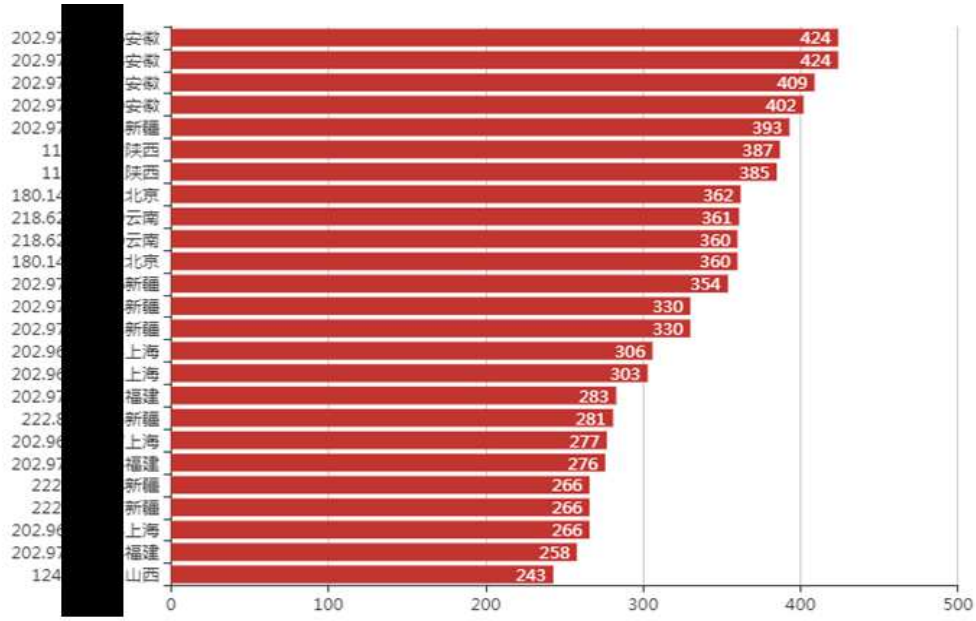

图 21 本地伪造流量来源路由器按参与事件数量 TOP25

发起本地伪造流量的路由器参与发起攻击的天次总体呈现幂律分布，如图 22 所示。平均每个路由器在 18.3 天被发现发起跨域伪造地址流量攻击，最多的路由器在 123 天范围内被发现发起跨域攻击流量，占监测总天数的二分之一。

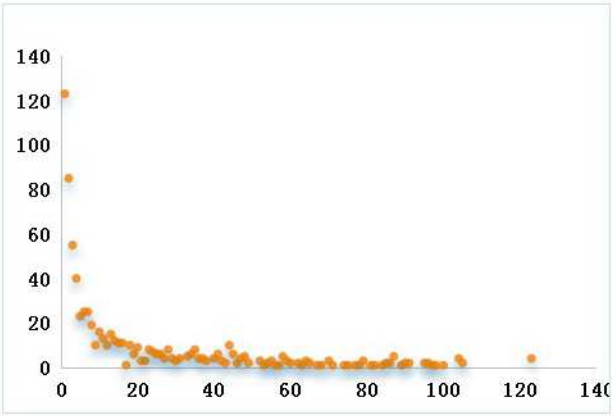

图 22 本地伪造流量来源路由器参与攻击天次呈现幂律分布

发起本地伪造流量的路由器参与发起攻击的月次总体情况如表 5 所示。平均每个路由器在 3.1 个月次被发现发起本地伪造地址流量攻击，26 个路由器在连续 8 个月内被发现发起

本地攻击流量，也就是说，这些路由器长期多次地被利用发起本地伪造流量攻击，主要集中在湖北省及江西省。

表 5 本地伪造流量来源路由器参与攻击月次情况

参与攻击月次	本地伪造流量来源路由器数量
8	26
7	41
6	58
5	49
4	89
3	107
2	127
1	228

本地伪造流量涉及路由器按省份分布统计如图 23 所示。其中，江苏省占的比例最大，占 8.7%；其次是北京市、河南省、及广东省。按路由器所属运营商统计，电信占的比例最大，占 54.2%，如图 24 所示。

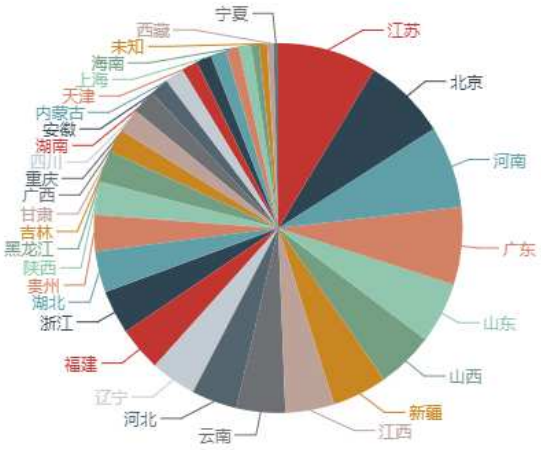

图 23 本地伪造流量来源路由器数量按省分布

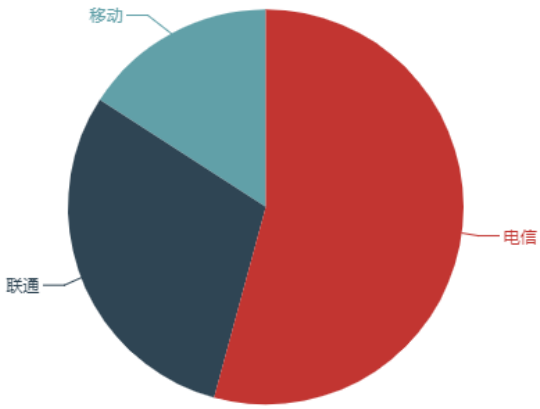

图 24 本地伪造流量来源路由器数量按运营商分布