


2017全球僵尸网络DDoS攻击威胁态势报告

 antiylab

2018-01-12

共21418人围观，发现1个不明物体

安全报告

1 概述

本报告由安天捕风小组与电信云堤联合发布，本年度报告主要以安天捕风蜜网和电信云堤流量监测数据为基础，对2017年发生的僵尸网络DDoS（分布式拒绝服务）攻击事件进行汇总分析。报告给出了2017年全球范围内僵尸网络DDoS攻击的事件分布、地区分布情况以及攻击情报数据，并对黑客的攻击方法、攻击资源、僵尸网络家族进行了分析。

从整体的攻击情报数据来看，全球DDoS僵尸网络全年攻击态势呈“山”形，其主要爆发在第二季度的4、5、6三个月。在比特币交易价格暴涨期间，大部分DDoS僵尸网络被更换为挖矿僵尸网络，所以第四季度则处于相对低迷的阶段。

根据全球数据统计，2017年，美国境内发起的DDoS攻击数量是最多的，占全球DDoS攻击总事件的37.06%；而中国成为了遭受DDoS攻击的重灾区，承受了全球DDoS攻击数量的84.79%（占整个亚洲DDoS攻击量的98.63%）。DDoS攻击我国的事件，37.47%来源于美国，27.77%来源于我国国内，23.28%来源于法国，10.17%来源于韩国。

黑客发起DDoS攻击事件采用的主流僵尸网络家族为Xor（Xor_Ex和Xor_D）家族，黑客通过控制Xor家族僵尸网络发起的DDoS攻击占全球DDoS攻击的51.04%。SYN flood为目前黑客使用的主流DDoS攻击方式，Xor、BillGate、Mayday等大型的僵尸网络家族的攻击方式均以SYN flood为主。物联网僵尸网络爆发式增长是2017年的一个趋势，由于Mirai[2]开源导致众多IoT变种出现，同时传统的Windows、Linux僵尸网络家族也向IoT平台进行拓展。

2017年僵尸网络活动的主要表现为：

以Linux僵尸网络为主流

由于Linux服务器所在环境带宽大、长时间在线、安全措施落后，该类僵尸网络具有稳定性且易形成规模化。

IoT僵尸网络大发展

开源Mirai导致物联网僵尸网络变种快速增加，同时传统的Windows平台家族僵尸网络发觉IoT的规模和攻击威力后，快速向IoT平台演进。Jenki、台风等僵尸家族就是典型代表。

具有明显的趋利性

今年以来比特币等电子加密货币快速发展，僵尸网络作为网络犯罪组织的重要工具从DDoS攻击转到挖矿，Linux、僵尸网络成为DDoS攻击、挖矿的主流。



DDoS攻击的受害者主要分布在中国和美国。近年来中国互联网事业飞速发展，数据中心和云服务发展迅速，网络需求与日俱增，导致勒索和因同行竞争导致的恶意攻击频繁。

2 DDoS僵尸网络攻击情报

通过对2017年捕获的DDoS攻击情报进行统计分析，可得到全球及国内DDoS攻击情报在这2017年度的分布情况，如下图所示。



图1 2017年全球DDoS僵尸网络发起DDoS攻击态势



图2 2017年国内DDoS僵尸网络DDoS攻击态势

2.1 DDoS僵尸网络DDoS攻击情报全球分布情况

跟据监测情报数据统计分析，2017年全球各国发起的DDoS攻击分布如下图。其中，C2位于美国境内对各国发起DDoS攻击数为5800多万，占全球各国发起DDoS攻击总数的37.06%；C2位于中国境内对各国发起的DDoS攻击占19.10%；C2位于法国境内对各国发起的DDoS攻击占比19.10%。



图3 DDoS僵尸网络发起攻击的全球分布比例

2.2 DDoS僵尸网络发起DDoS攻击全国分布情报

对国内各地区发起的DDoS攻击情报进行分析，可得如下图所示的各省份DDoS（间歇性）攻击量分布情况。其中，西省内发起的DDoS攻击量为1600多万，在全国占比最高，为30.40%；香港特别行政区内发起的DDoS攻击量为130万，在全国占比中位列第二，为26.07%；广东省内发起的DDoS攻击量为1200多万，在全国占比中中位列第三，23.12%。



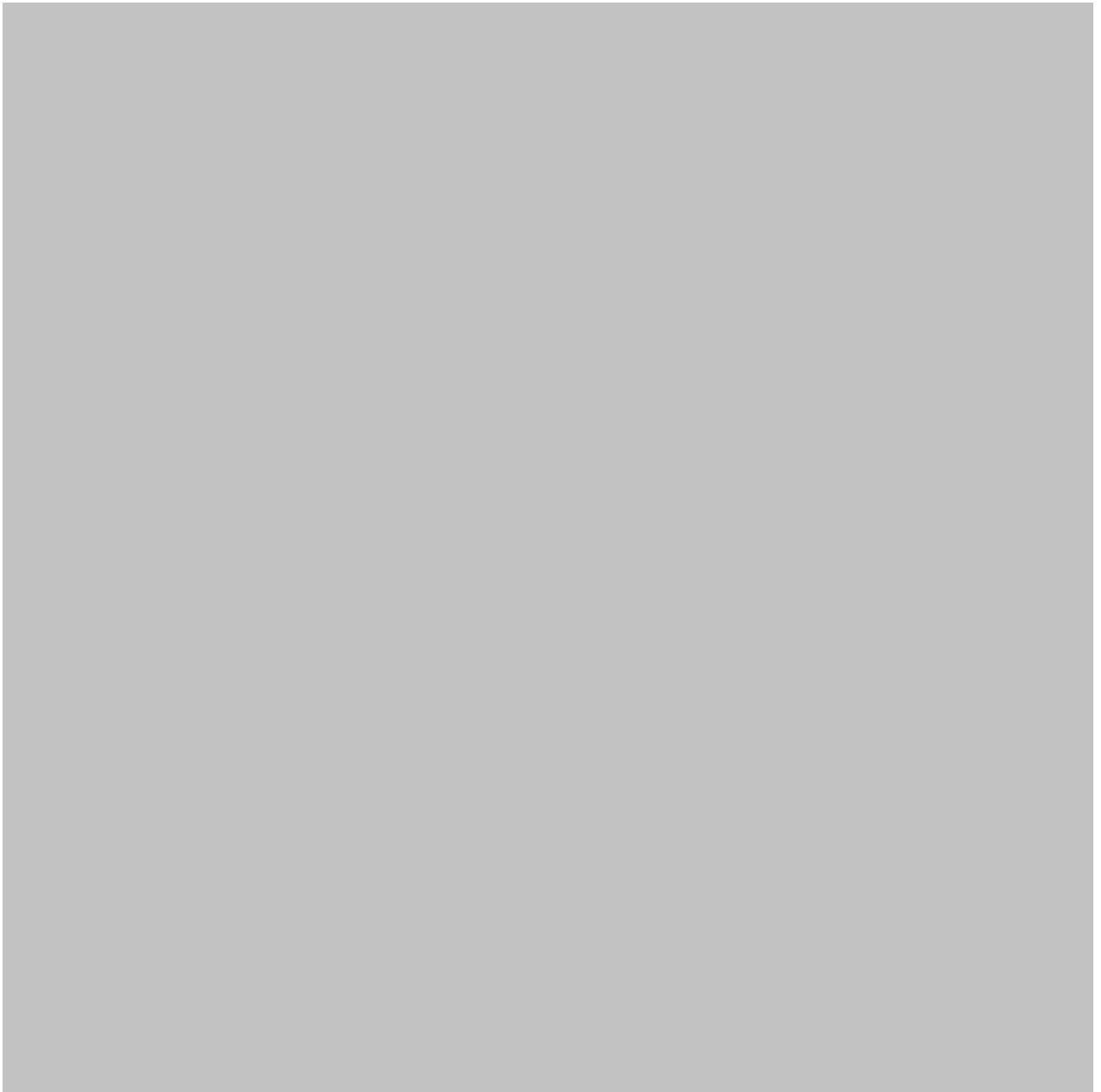


图4 DDoS僵尸网络发起攻击的国内分布统计

3 DDoS攻击带宽流量情报信息

对2017年1月到12月份国际、互联互通、电信来自三方的攻击总带宽流量进行统计分析可得，国际和互联互通发起的TB带宽流量均稳定在10000左右；而通过电信发起的TB带宽流量在前半年一直处于上升趋势，5月份时出现了峰值达到56397.336TB，而后半年的带宽流量开始下降并趋于平稳。攻击带宽流量数据与攻击情报数据的“山”形趋势吻合。



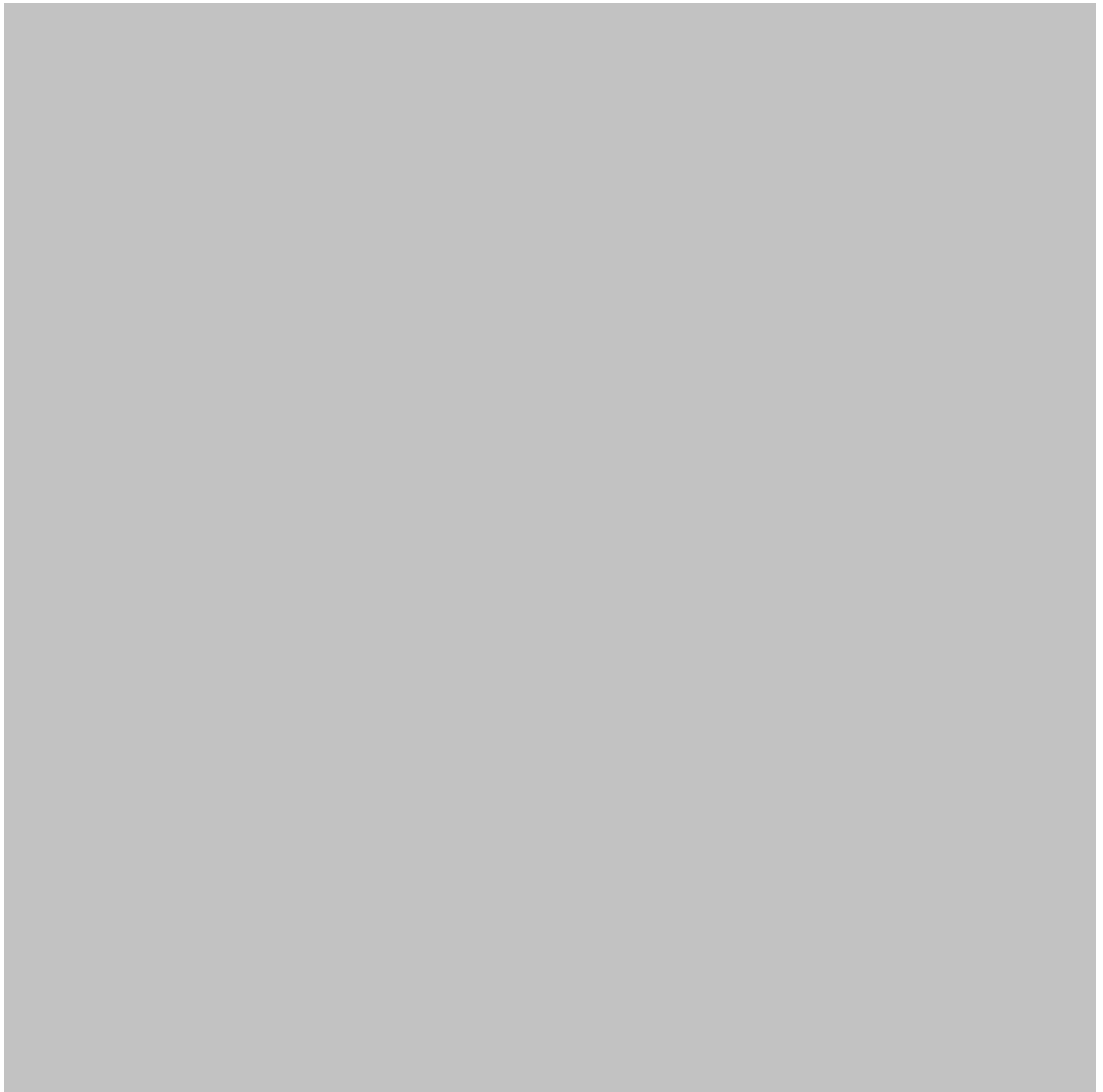


图5 DDoS攻击带宽总流量统计

据数据统计分析，2017年DDoS攻击持续时间多数少于30分钟，占每个月攻击的70%左右。





图6 DDoS攻击带宽流量持续时间分布统计

12个月中，当月单个攻击目标被DDoS攻击的流量峰值排名前三的分别是在5月份、3月份和4月份。5月份的攻击目标单次攻击峰值最大为1393.66 Gbps，3月份的攻击目标单次攻击峰值最大为953.78 Gbps，4月份的攻击目标单次攻击峰值最大为798.00 Gbps。分段攻击峰值在每个月中占比情况如下图，其中攻击峰值普遍集中于50G以内。



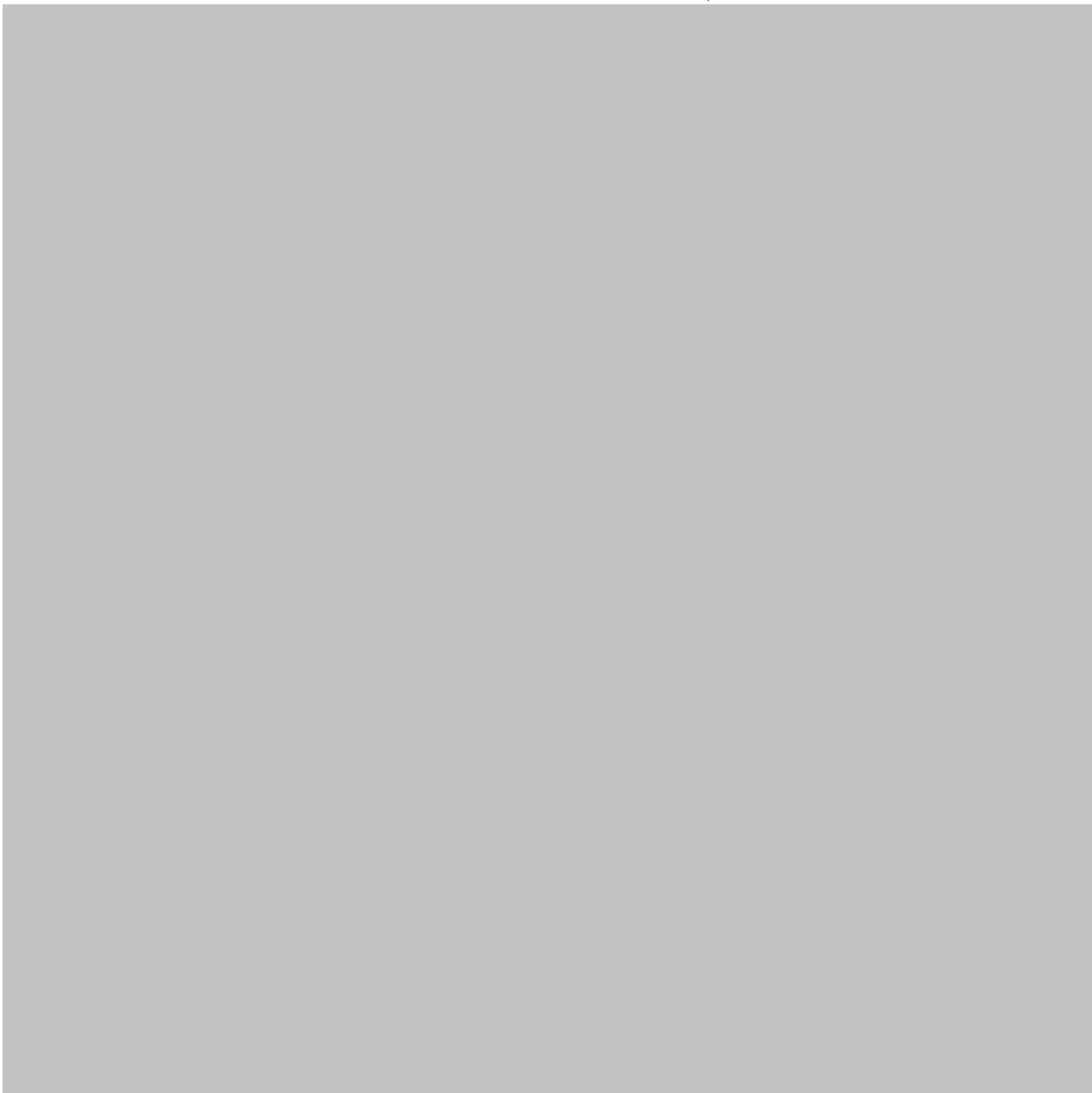


图7 DDoS攻击峰值段在每月的分布统计

攻击带宽流量Top 10的省份在每月攻击总带宽流量中的占比情况如下图。数据显示，在12个月中，浙江的攻击带宽流量在每个月的攻击带宽流量中都占据了较大的比例，福建和湖北在后半年的攻击带宽流量中有大幅度提升。



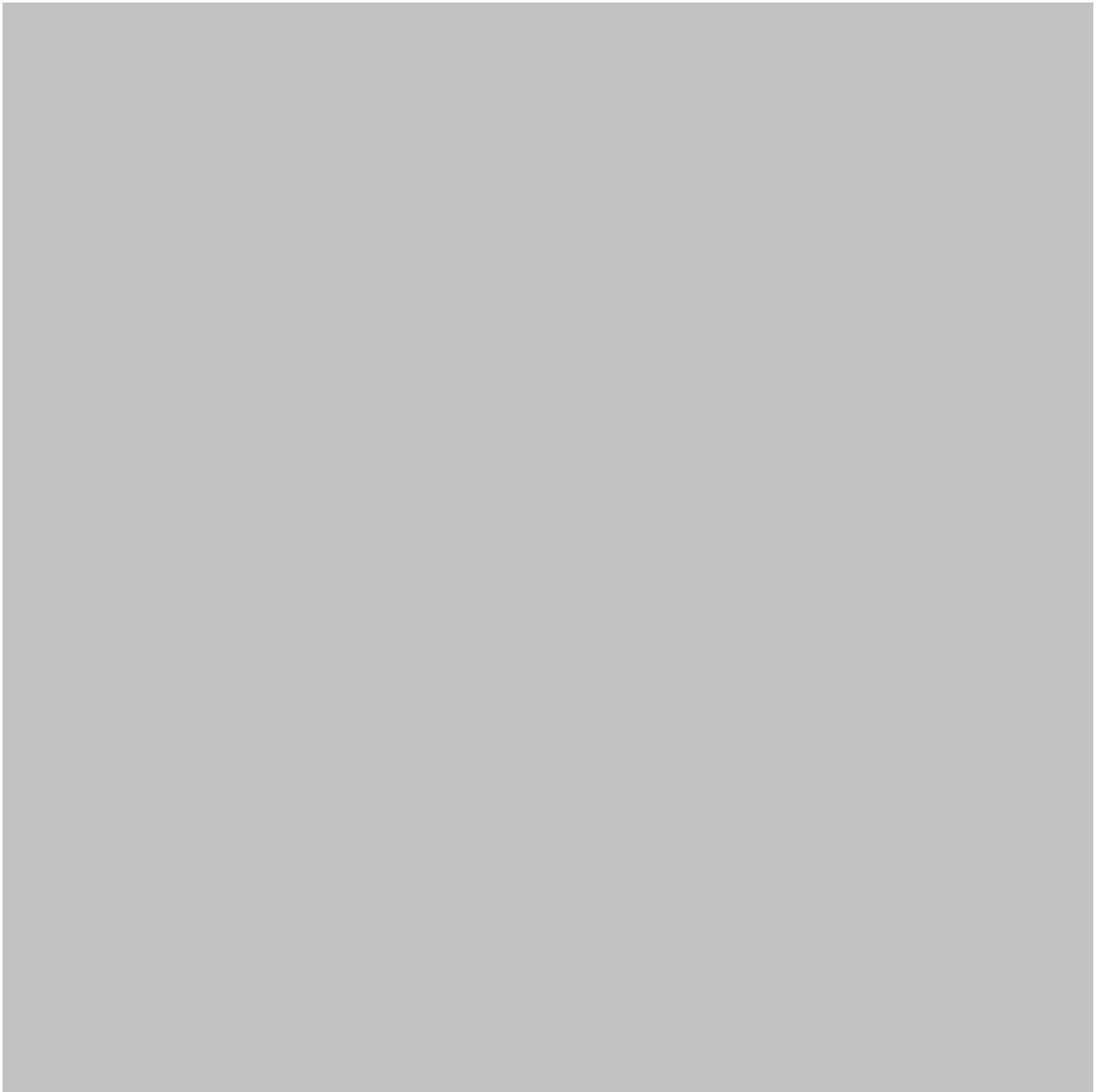


图8 DDoS攻击Top 10地区每月攻击带宽流量分布统计

4 DDoS僵尸网络C2情报信息

4.1 DDoS僵尸网络C2攻击情报

4.1.1 DDoS僵尸网络C2分布

对2017年所捕获的DDoS攻击C2信息进行追溯并分析，发起DDoS攻击的C2在全球范围内的分布情况如下。其中位于中国的C2最多，为14744个，占比全球C2分布的58.36%；其次是美国，占比全球C2分布的24.98%；排在第三位的国家，位于韩国的C2有1039个，占比全球C2分布的4.11%。



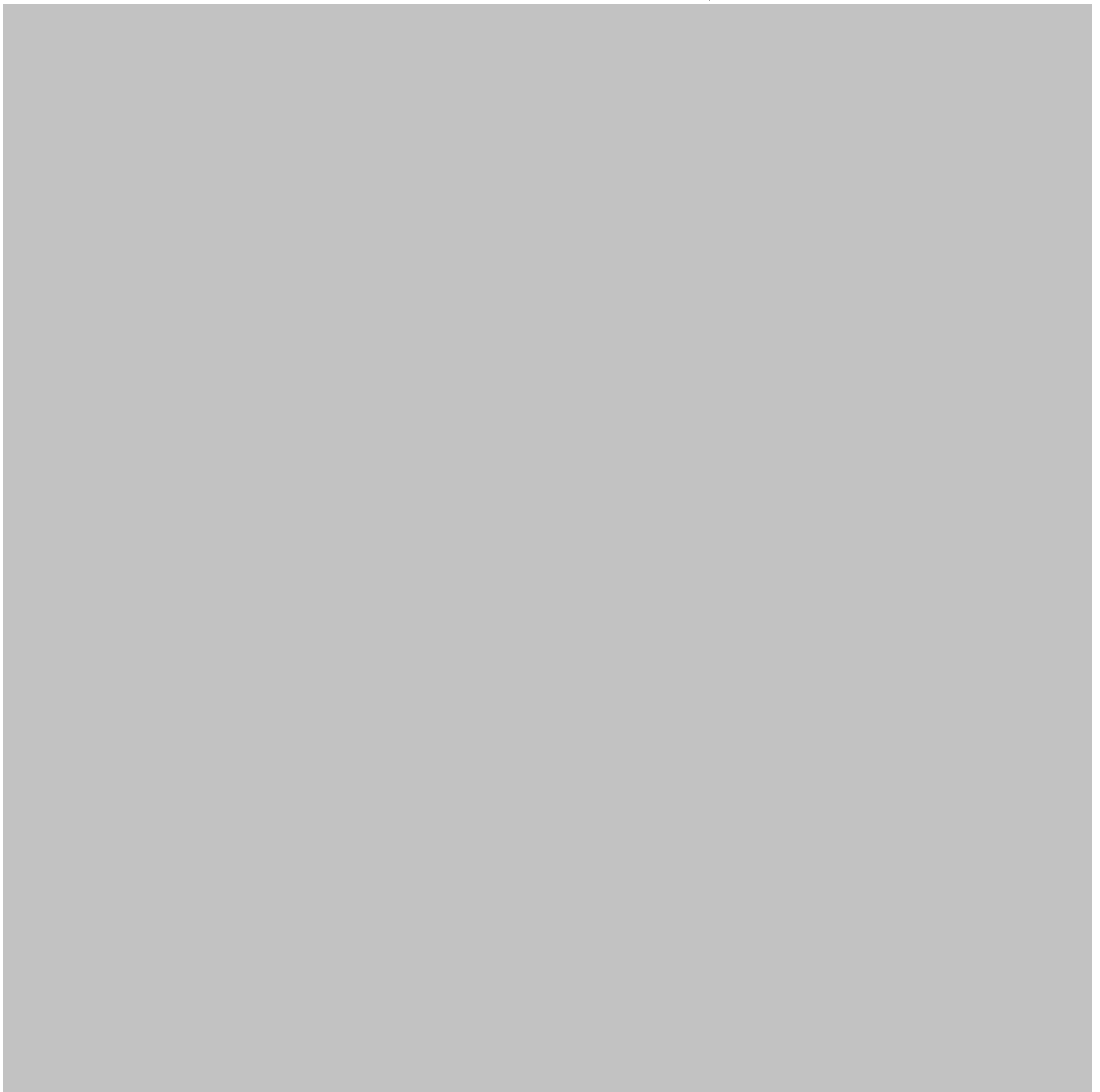


图9 DDoS僵尸网络C2全球的分布情报统计

对每一个C2进行攻击目标的溯源统计，并按照C2所在国家进行划分，得出以下统计数据如下图所示。可以看到，C2产生的攻击事件数由高到低、排名前三的分别是法国（729343个）、美国（231916个）和中国（65840个）。

对攻击事件数TOP100的C2进行国家划分，71个C2位于法国，27个C2位于美国，其余2个C2分别位于韩国和瑞士，产生的攻击事件最多的一个C2来自法国，该C2存活时间为7494.9个小时，攻击事件数量达到19172个。





图10 全球DDoS僵尸网络C2攻击目标统计

对国内C2进行统计，得出以下C2在各省份的分布统计图。其中位于江苏省的C2最多，为3420个，占比国内C2总数的23.20%；其次是位于香港的C2，有2632个，占比国内C2总数的17.85%。





图11 全国DDoS僵尸网络C2各省份的分布统计

对国内的C2进行溯源分析，并按省份划分得出以下各省份C2的攻击事件量统计数据，产生攻击事件个数排前三省份，由高到低依次为香港（19687个）、广东（18065个）和江西（10750个）

对国内攻击情报TOP100的C2按照省份划分，其中31个C2位于香港，19个C2位于广东，14个C2位于江苏，7个C2位于浙江，6个C2位于福建，6个C2位于江西。产生攻击事件数最多的一个C2位于香港，其产生的攻击事件数为6162个，C2的存活时间为508.05个小时。





图12 全国DDoS僵尸网络C2攻击事件统计

4.1.2 DDoS僵尸网络C2存活时间

国内C2的存活时间在1000小时以内的占比40%，超过6000小时的接近20%；国外C2的存活时间在1000小时以内的，80%，超过1000小时的仅占比20%。可见，国内C2的存活时间超过1000小时的数量是国外的3倍之多。



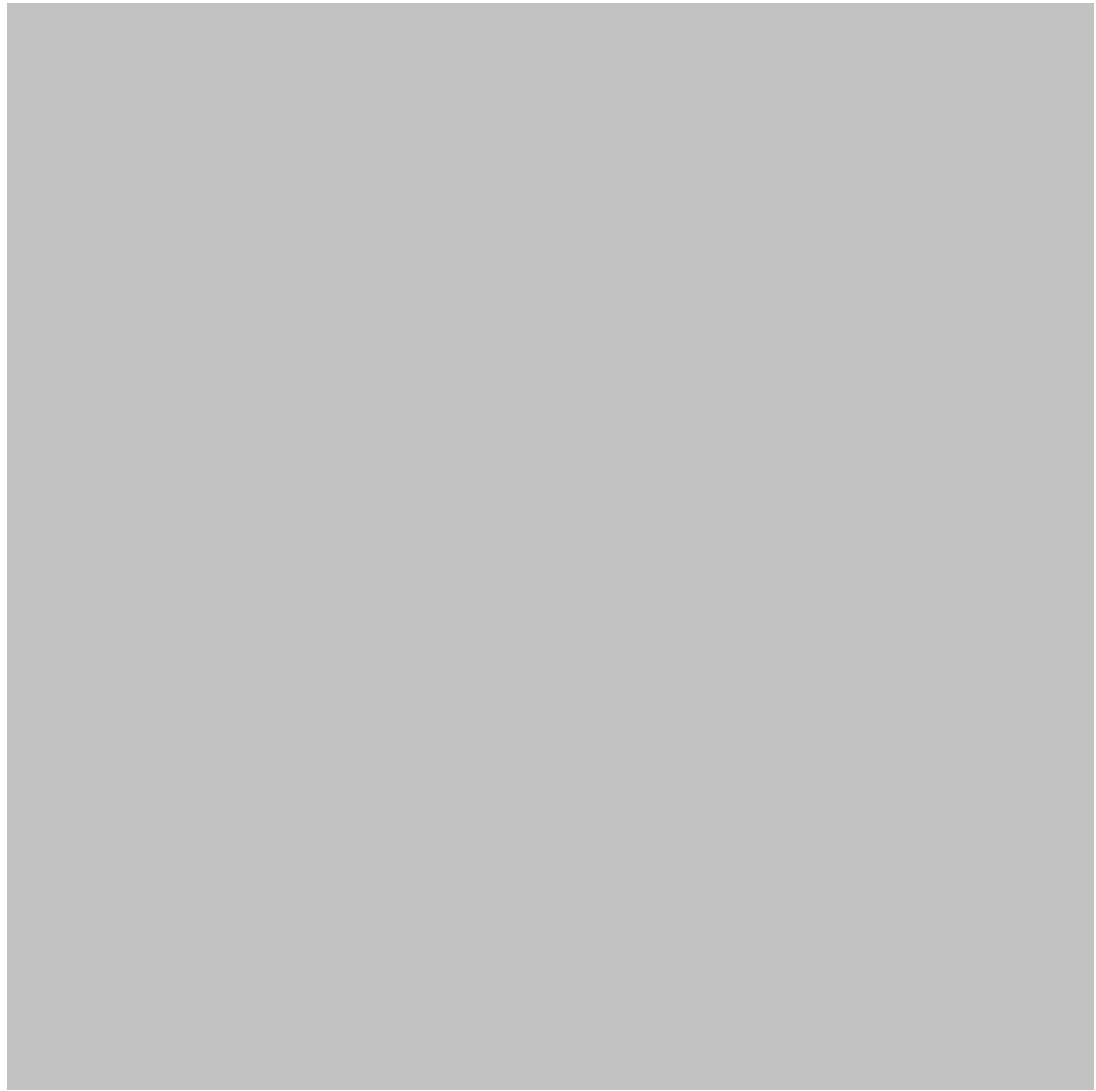


图13 国内DDoS僵尸网络C2存活时间





图14 国外DDoS僵尸网络C2存活时间

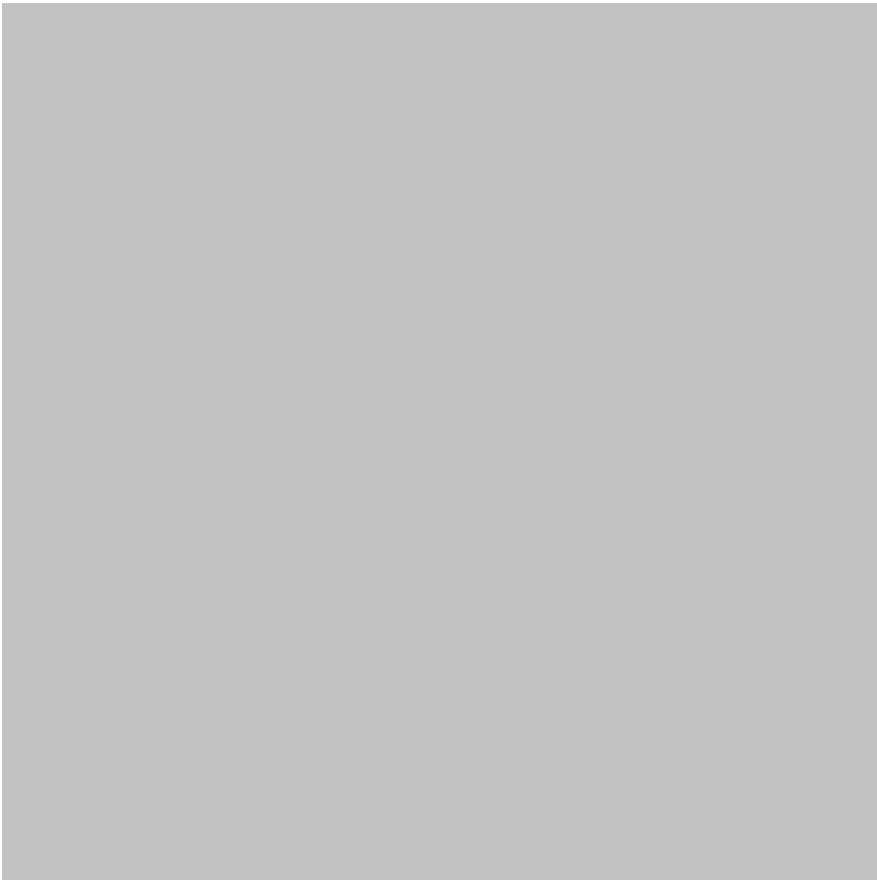
4.2 黑客攻击工具

4.2.1 DDoS僵尸网络木马传播布

无论是何种类型的僵尸网络，“肉鸡”都是执行各种攻击的基础，所以拓展“肉鸡”便是黑客要进行的第一步，而“肉鸡”拓展方法主要有以下几种：

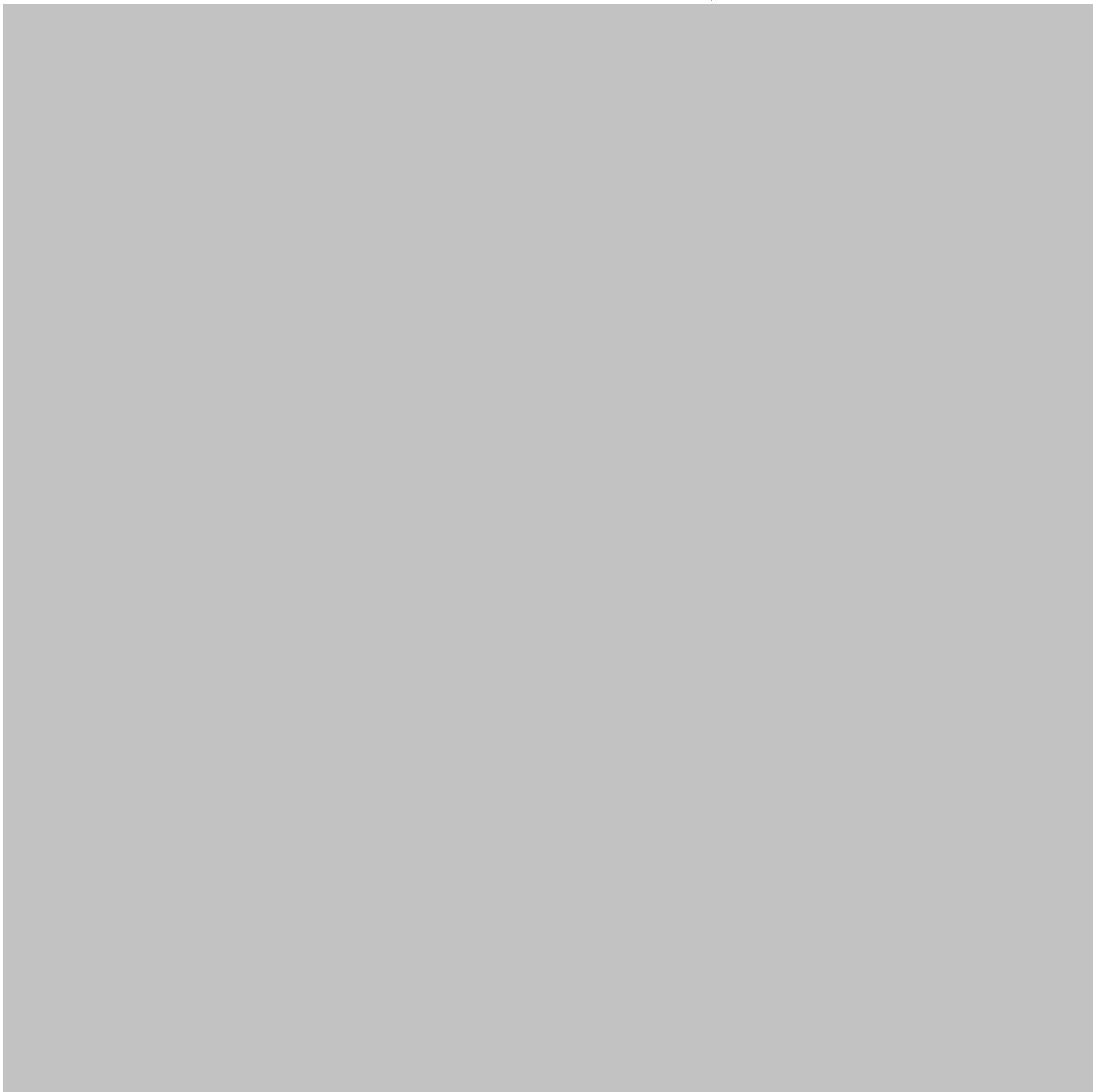
1. 弱口令爆破。通过常见远程服务端口（例如22、2222、23、2323、1433、3306、3389端口）的自动化弱口令爆破执行远程命令植入木马。通过安天捕风蜜网捕获的爆破数据统计，上述端口每天的爆破量在300万到500万之间，上次新一波物联网僵尸网络爆发时，爆破数据都会呈几何式上升，特别是在国外相关的物联网类型僵尸网络上比之尤甚。





表格 1 扫描端口可疑IP

2. 漏洞扫描。通过自动化漏洞利用，执行远程命令拓展“肉鸡”已经是新趋势，这一点在Mirai家族的僵尸网络上已表现得淋漓尽致。下表为Mirai变种利用的部分漏洞信息及受影响设备情况。



表格 2 Mirai利用的部分漏洞列表

对于导致德国断网的SOAP漏洞，黑客尝试通过对网络时间协议、NTP服务器名称字段执行注入式攻击，在易受攻击设备中远程执行恶意命令。最终，NTP服务器名称会解析为引发RCE漏洞的命令。恶意代码可以通过TR-069协议找到NTP服务器名称字段。互联网服务提供商（ISP）可以利用此协议远程管理网络中的设备。遭受攻击的设备可以来自互联网的TR-064命令，进而改变NTP设置。TR-064基于HTTP和SOAP，其默认端口为TCP 7547。

Embedthis公司的Web服务器 GoAhead爆出远程代码执行漏洞CVE-2017-8225[3]。当与glibc动态链接器结合使用时，可以利用特殊参数名称，如LD_PRELOAD，就可以实施远程代码执行。攻击者可以在请求的正文中POST其共享对有效Payload, 并使用/proc/self/fd/0引用它。GoAhead是一个开源（商业许可）、简单、轻巧、功能强大、可以在多台运行的嵌入式Web Server。GoAhead Web Server是为嵌入式实时操作系统（RTOS）量身定制的Web服务器，支持多种操作系统，包括eCos、Linux、LynxOS、QNX、VxWorks、WinCE、pSOS等。



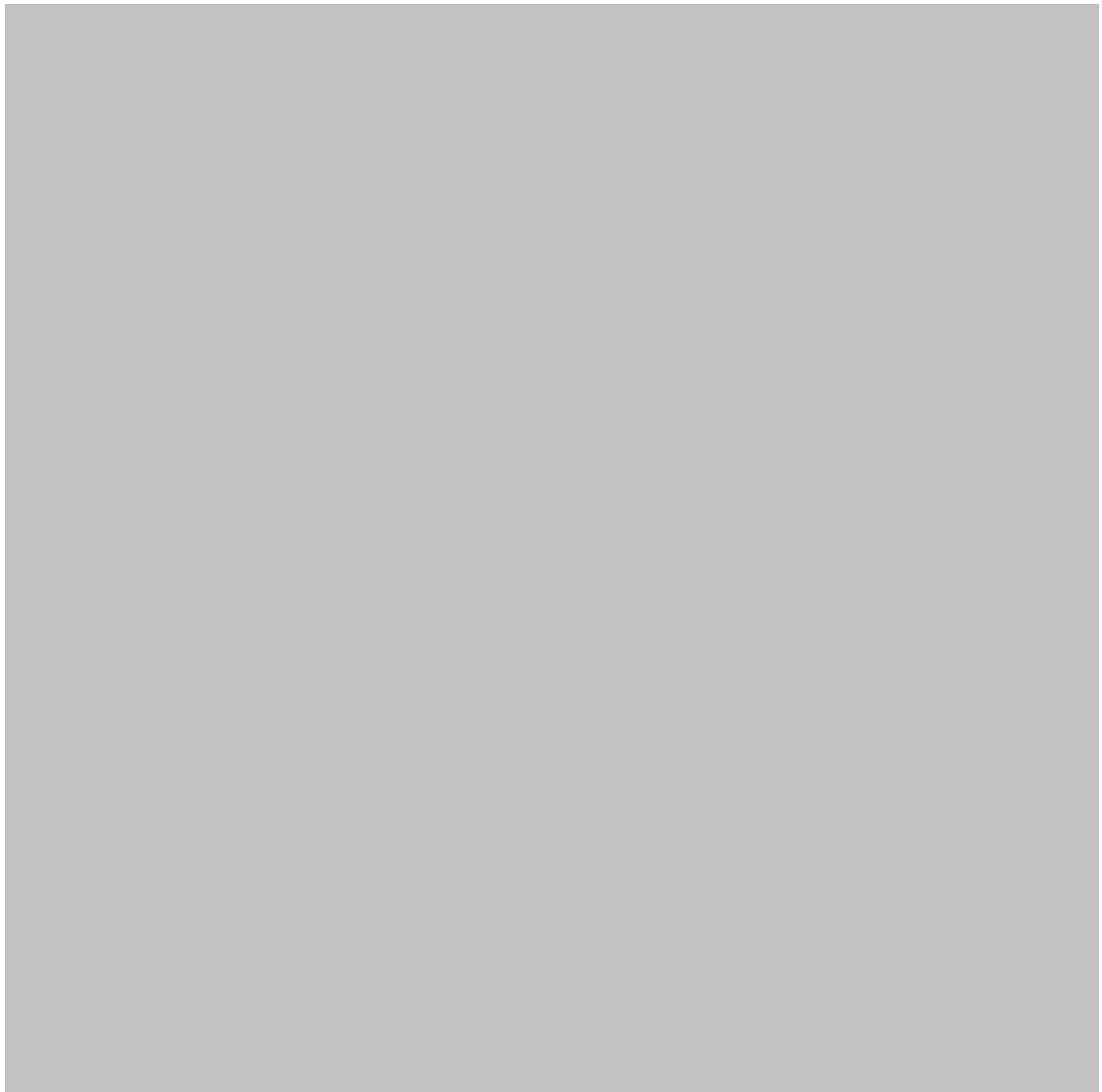
据CheckPoint披露，IoTroop恶意利用多种漏洞进行入侵，包括Zyxel（路由器）、Dlink（路由器）、Netgear（路由器）、Linksys（路由器）、Goahead（摄像头）、JAWS（摄像头）、AVTECH（摄像头）、Vacron（NVR）设备漏洞。

3. 捆绑下载暗藏后门。可通过激活工具捆绑木马，魔釉DDoS木马[1]就是利用小马激活工具捆绑来进行大规模传播。在很多非正规的应用网站中，很多“绿色”小应用程序中被黑客绑定了木马，木马会随着小应用程序的扩散使用而感染设备拓展“肉鸡”。捆绑传播方式，因为“绿马甲”的身份可以有效地避免杀毒软件的查杀，所以通过这种传播形成的僵尸网络，经过时间的积累往往会形成一个庞大的“肉鸡”群。

4. 交叉感染。通过已有的僵尸网络传播新木马，实现不同僵尸网络的交叉传播。由于这种方式可以实现快速部署的僵尸网络，所以在常见的DDoS僵尸网络中出现得特别频繁。

4.2.2 全球各DDoS家族僵尸网络威胁情报

对2017年捕获的样本进行统计分析得出，捕获到的Gafgyt僵尸网络家族的样本最多，为26083个；其次是Nitol，样本为10667个。如下图所示：



对全球的DDoS攻击以及黑客控制的僵尸网络家族进行统计分析可知，黑客最为惯用的僵尸网络家族为Xor_Ex家族，其利用Xor_Ex家族发起的DDoS攻击达6500多万次，占使用的所有家族的34.92%；其次是BillGates家族，黑客利用该家族发起的DDoS攻击达3400多万次，占使用的所有家族的21.87%；排名第三的家族是Mayday家族，占使用的所有家族的19.44%。



图16 全球DDoS僵尸网络各家族攻击量的情报统计

对全国DDoS攻击占比排名前6位的僵尸网络家族的攻击行为进行统计分析，可得出以下僵尸网络家族在使用的攻击方式分布情况。

1、Xor家族

Xor家族是全国甚至全球近两年来攻击态势最为活跃的DDoS僵尸网络家族。根据目前掌握的情报显示，操作Xor僵尸网络的黑客为了隐藏身份，从2016年下半年开始将大部分僵尸网络C2逐渐向国外转移，而且C2对应的设备基

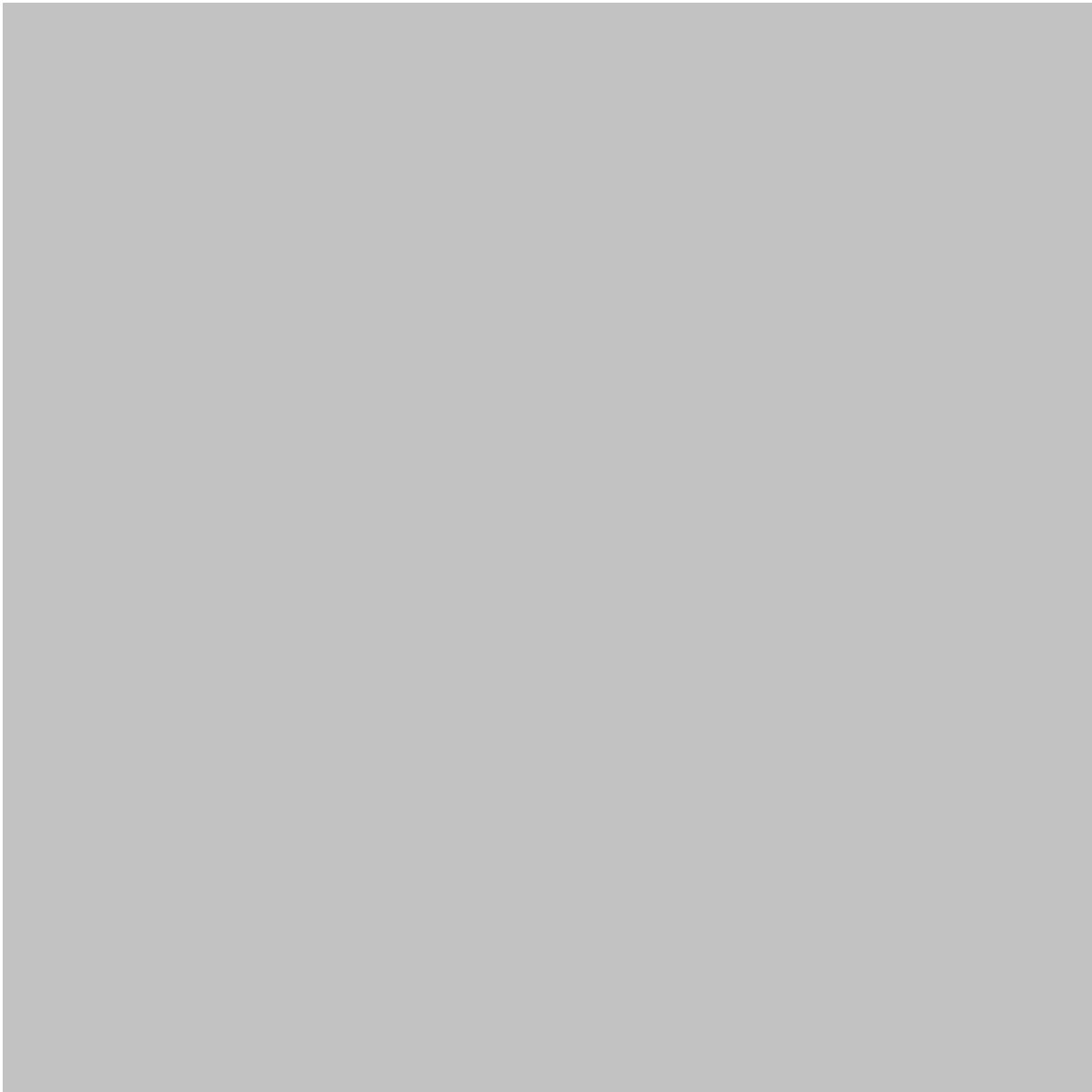


图17 Xor_Ex家族攻击方式分布统计

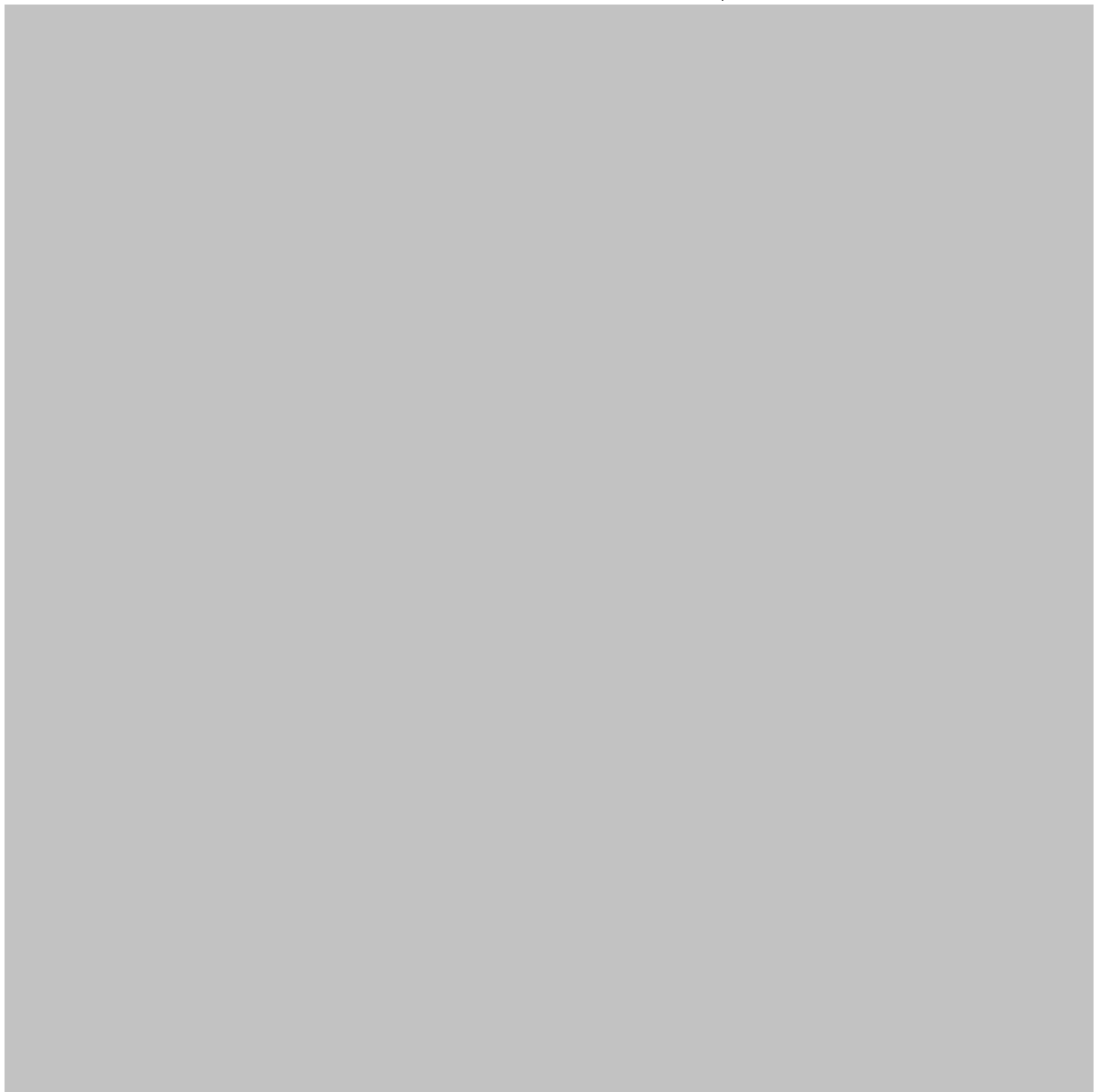


图18 Xor_D家族攻击方式分布统计

2、BillGates家族

BillGates又名Setag/Ganiw，其活跃度仅次于Xor家族。情报数据显示，BillGates家族的活跃事件主要集中在上半年，攻击类型主要是SYN flood；7月中旬后，随着虚拟货币交易价格大幅攀升，大部分BillGates家族的僵尸网络开始转为挖矿僵尸网络从事挖矿。



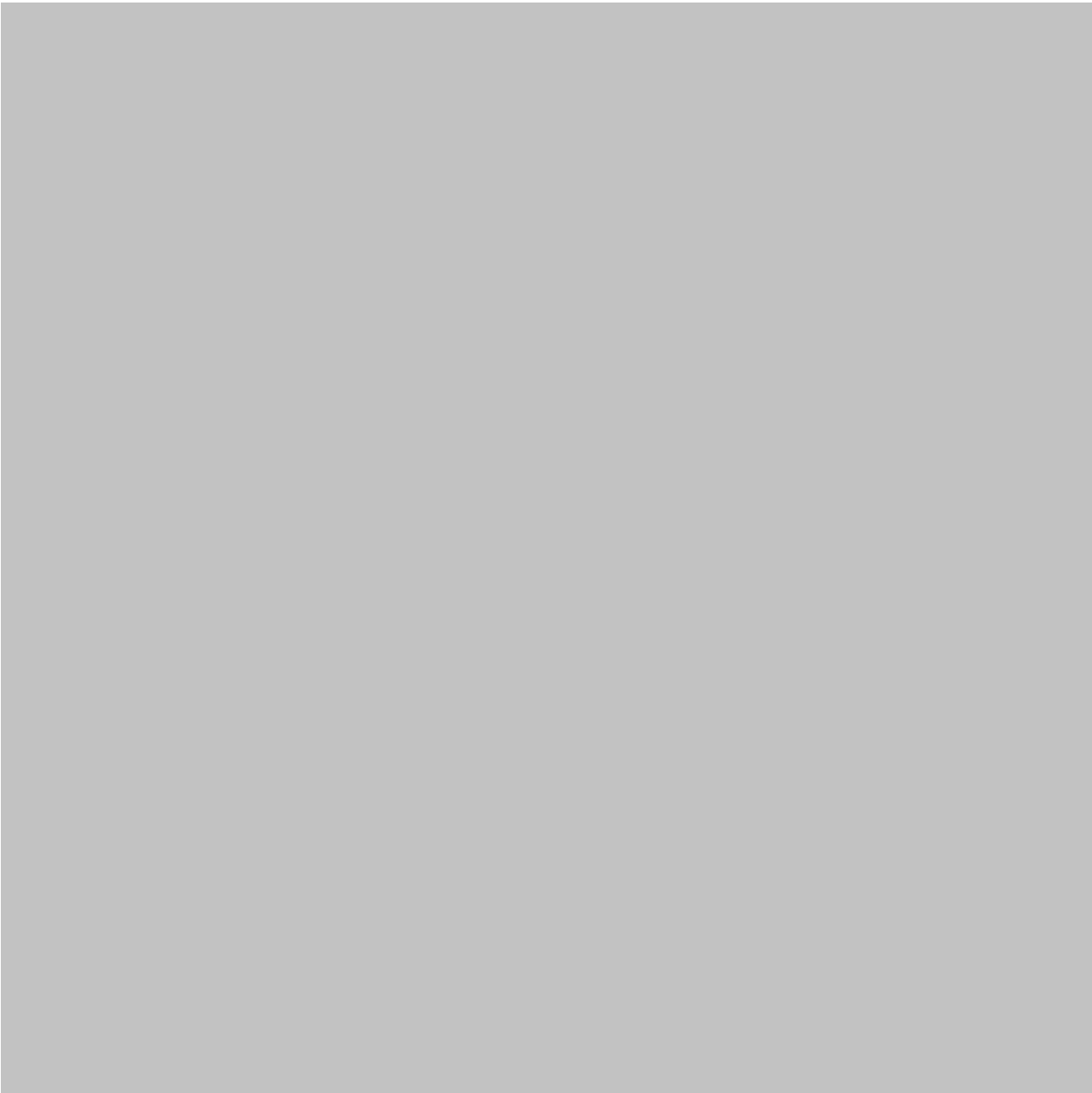


图19 BillGates年度攻击情报时间分布

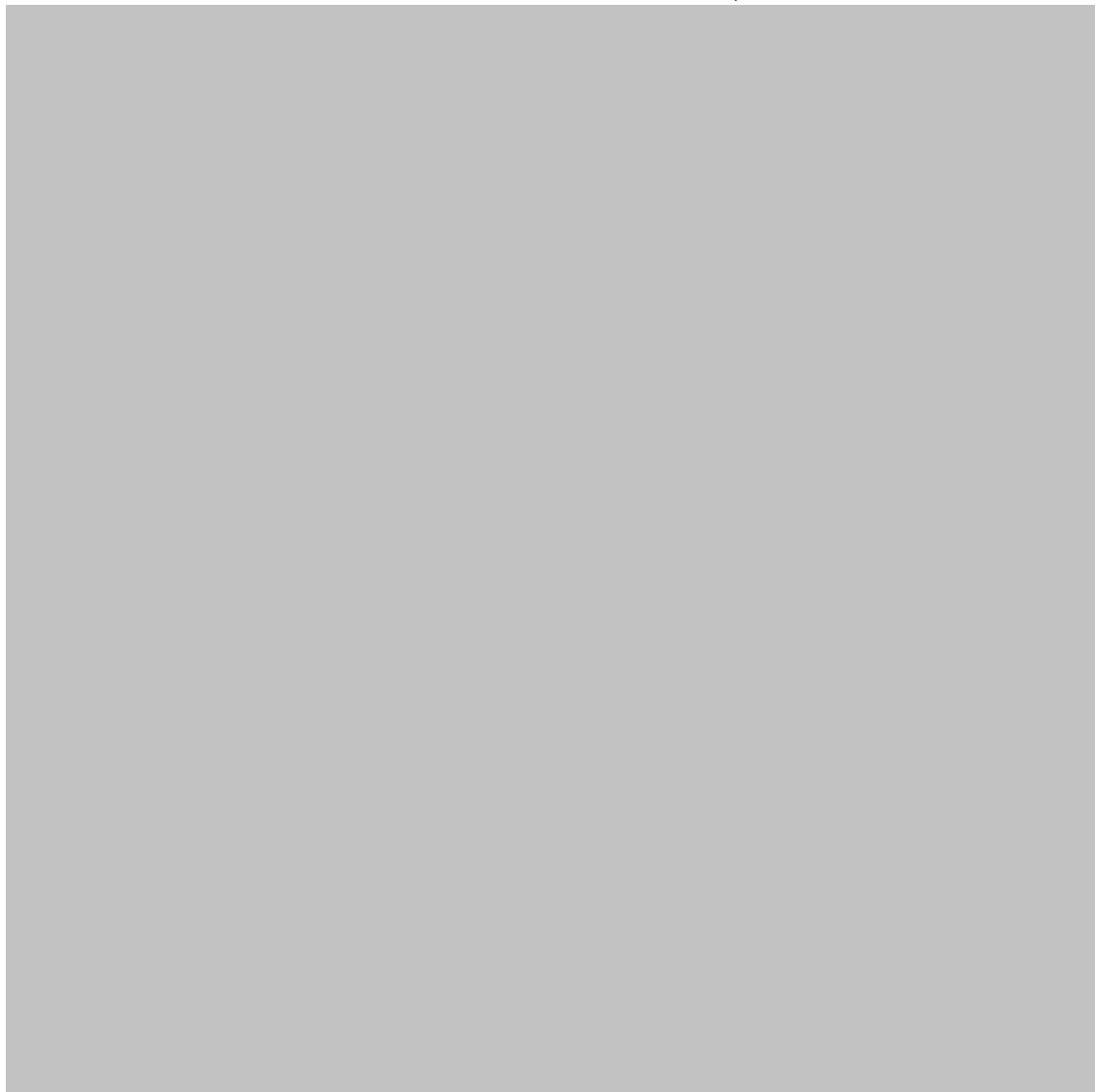


图20 BillGates家族攻击方式分布统计

3、Mayday家族

Mayday家族攻击情报走势与BillGates家族类似，但相较于BillGates家族低迷比较早，且活跃度也明显低于BillGates家族。Mayday家族的主要攻击类型仍为SYN flood，其次为TCP flood，其他的具备反射型的攻击模式并不多见。



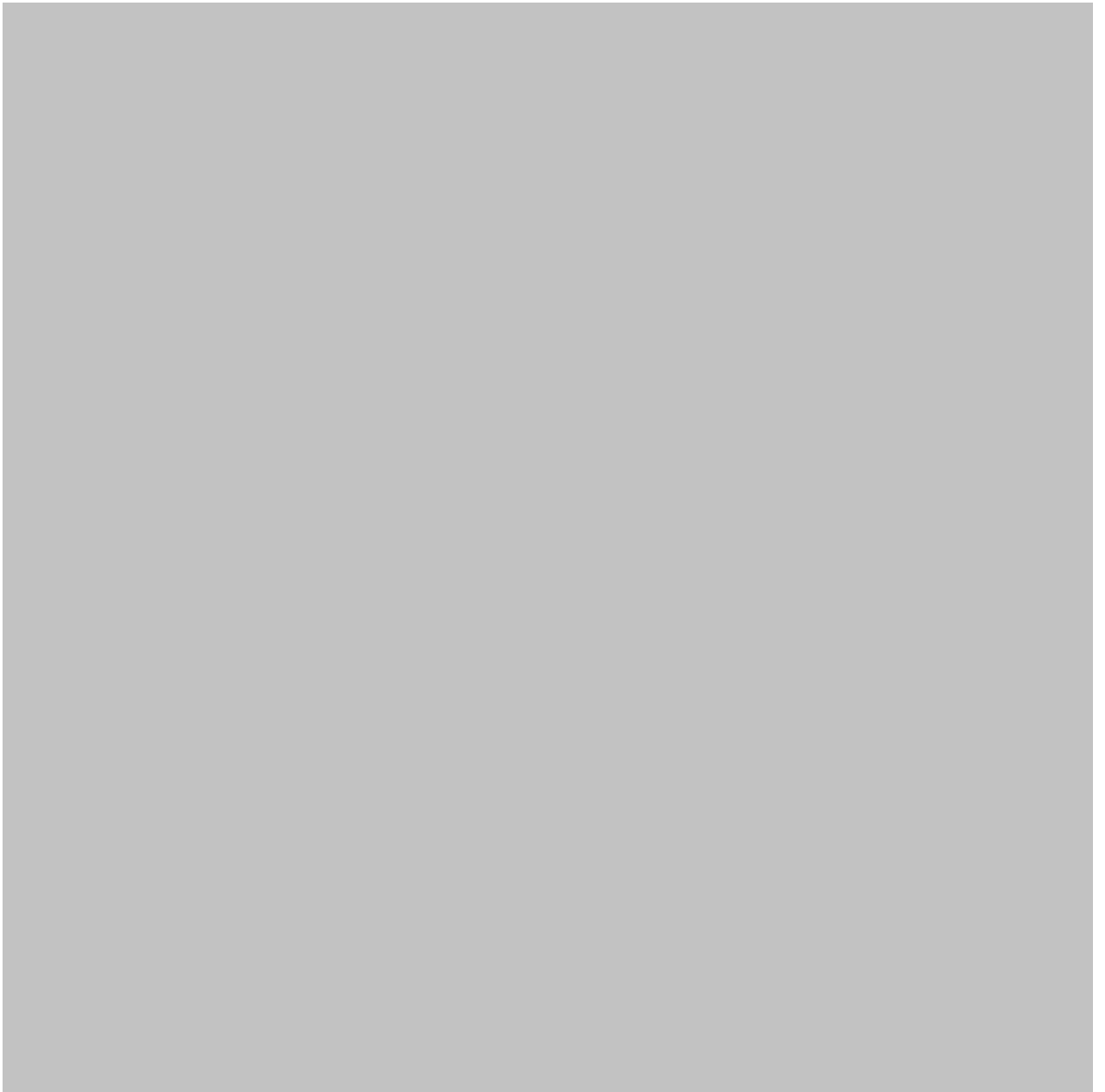


图 21 Mayday年度攻击情报时间分布



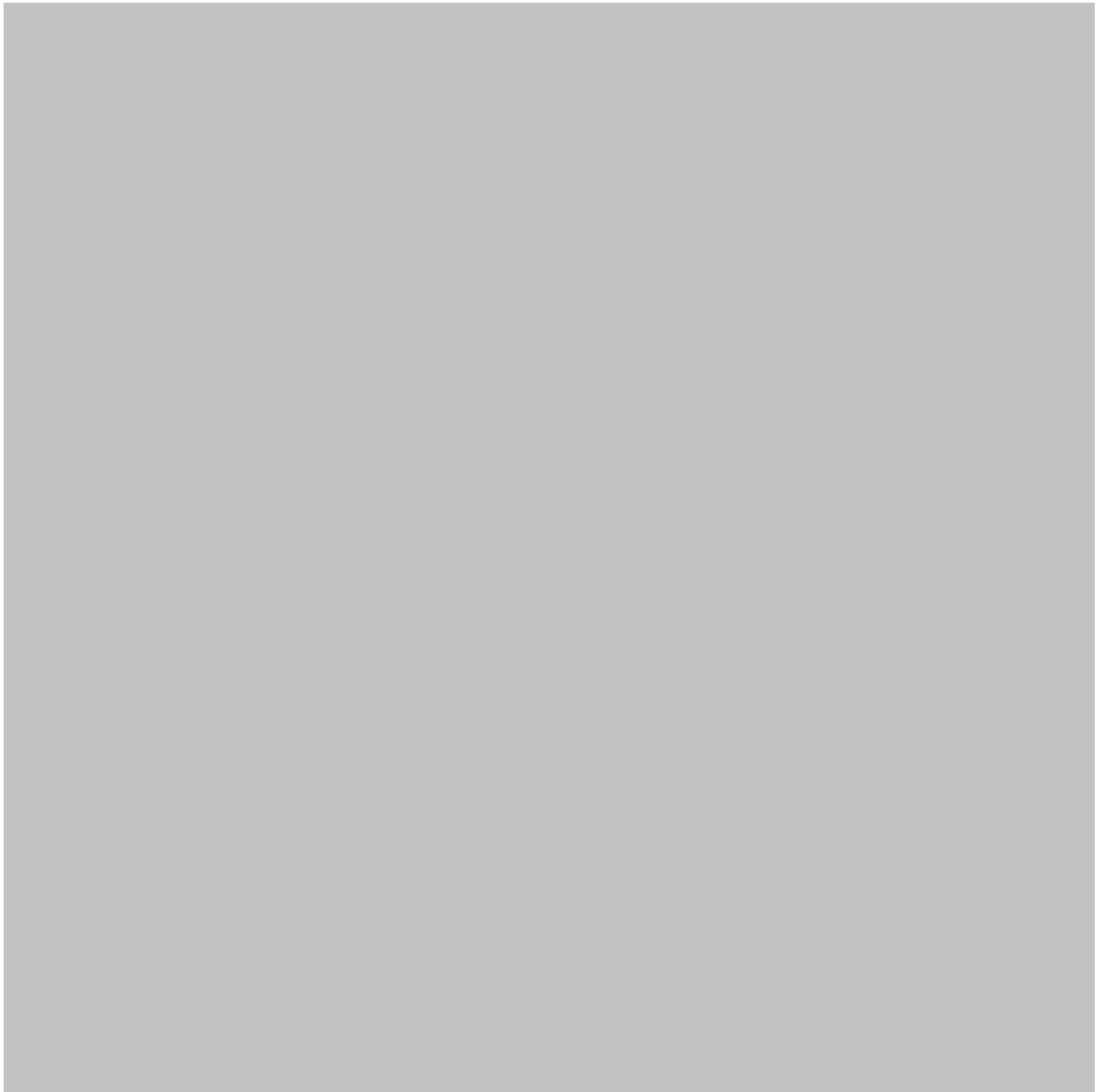


图22 Mayday家族攻击方式分布统计

4、Nitol家族

Nitol家族是目前Windows系列中最为活跃的DDoS僵尸网络，而且经过多年的发展变异，现在已经存在10多个不同的变种，并且国外有关黑客通过Nitol家族开放的源代码进行升级修改和使用。虽然Nitol家族的僵尸网络工具已经传到国外，但是其主要感染设备还是在国内，特别是NSA的“永恒之蓝”漏洞和Structs2系列的漏洞被相继爆出后，开始现通过自动化漏洞利用工具批量植入各家族恶意代码（Nitol家族包含在内）的事件。在DDoS攻击方面，最新Nitol改进版本中集成了SYN flood、TCP flood、DNS flood、C2 flood、UDP flood、HTTP flood、ICMP flood和NTP flood种攻击类型。从2017年Nitol家族系列的攻击威胁情报上看，其主要攻击方式还是倾向于HTTP flood和C2 flood，这明显区别于其他家族。





图23 Nitol年度威胁情报时间分布



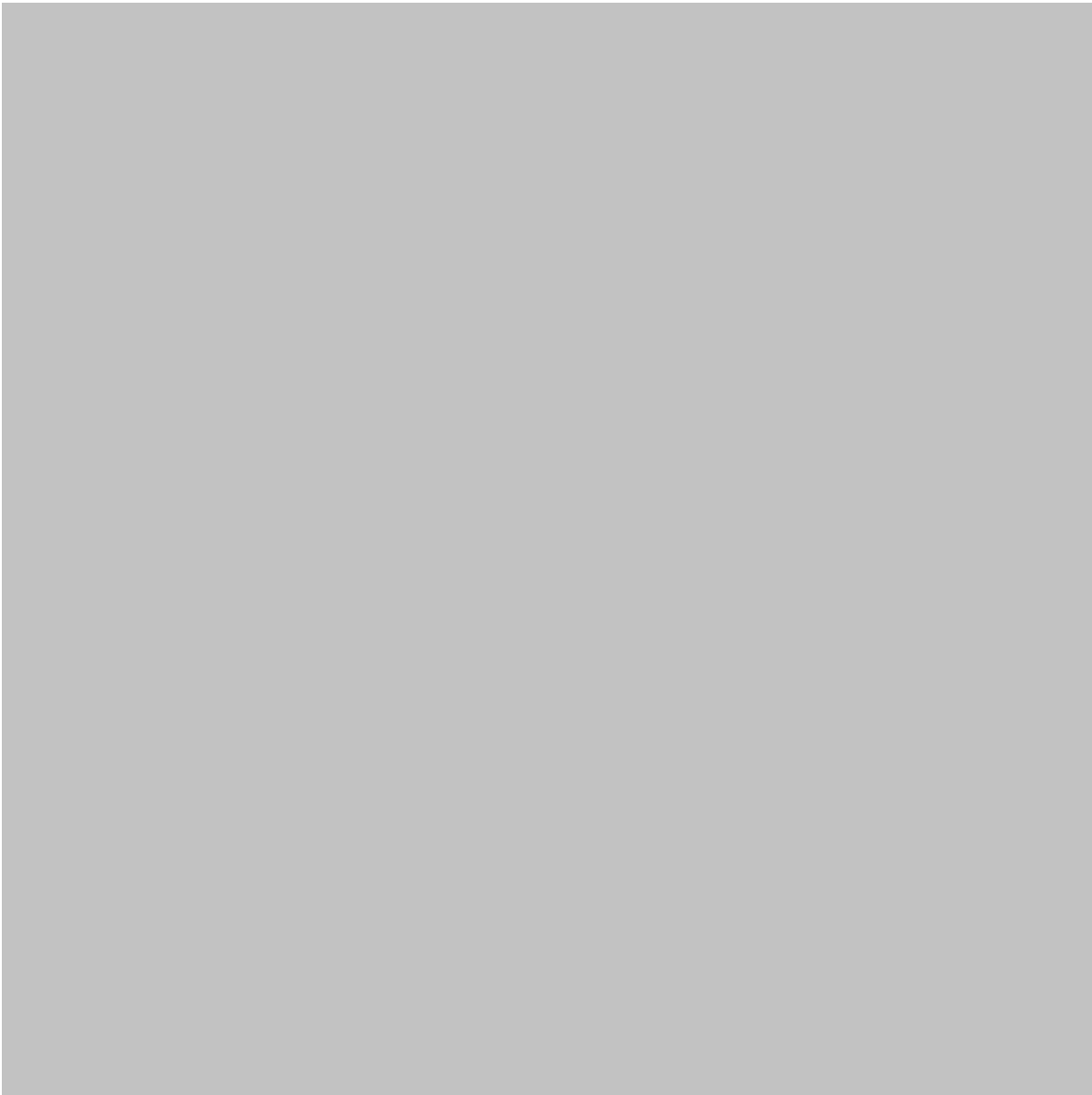


图24 Nitol家族攻击方式分布统计

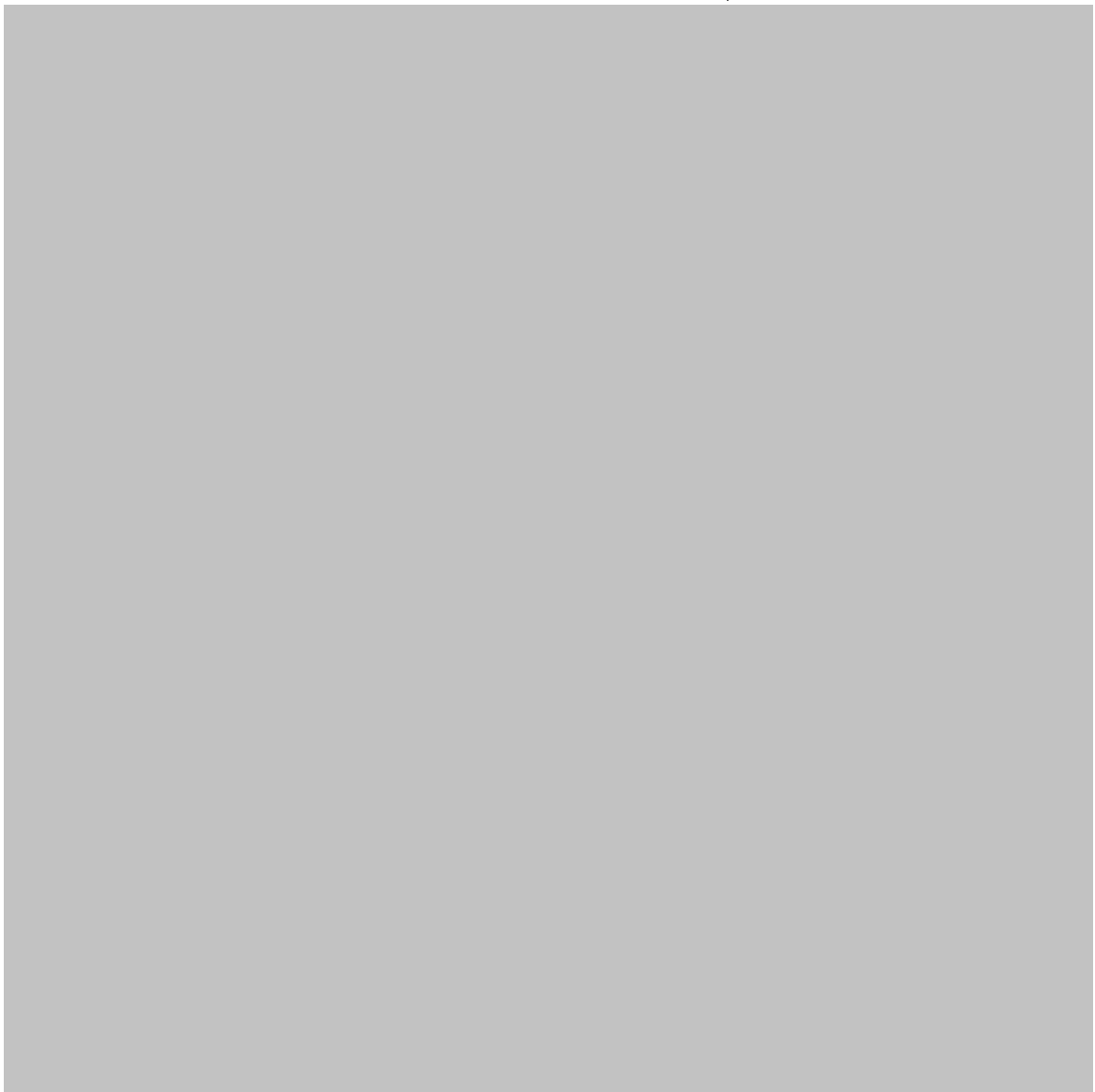


图25 Nitol家族感染设备系统版本统计

从对Nitol家族系列的僵尸网络监测拓展发现，很多控制Nitol家族系列的僵尸网络同时还控制其它RAT类型的僵尸网络，多个僵尸网络之间通过“交叉感染”方式实现“肉鸡”互通和共享。随机统计Nitol家族的3万“肉鸡”设备类型上，Nitol家族系列感染的设备系统版本主要为Windows系列的低、中档系统版本，其中主要集中在Win XP SP3系统版本（约占79.91%），其次是Win 7 SP1系统版本（约占8.27%）。目前，Win XP SP3的主要用户群集中在事业单位办公环境和企业工控环境等疏于系统升级和维护的终端设备上，也就说明Nitol家族系列感染的设备系统主要是普通配置设备系统或者互联网工控设备系统，初步统计境内每天大约有260万台Windows环境设备受Nitol家族恶意代码感染。

5、Dofloo家族

Dofloo家族无论是从数据加密算法还是攻击模式或是木马平台兼容性，都算是一个比较成熟完善的家族。Dofloo家族使用了256位AES加密算法将攻击数据加密，可以有效确保数据通信的安全性。在攻击类型上，除了常见的SYN flood、TCP flood、HTTP flood等，Dofloo家族还具备高放大倍数的DNS flood、NTP flood、ICMP flood等反射攻击类型。在兼容平台上，其木马不仅能够兼容常见的Windows、Linux等两大类型平台，同时可以兼容ARM、MIPS



过CVE-2017-8225等漏洞的自动化利用工具，实现IP网段进行批量“抓取”200多万台存在漏洞的设备。庞大的“f群”加上高倍数的放大攻击使得Dofloo家族的攻击破坏力远胜于其他家族的僵尸网络。

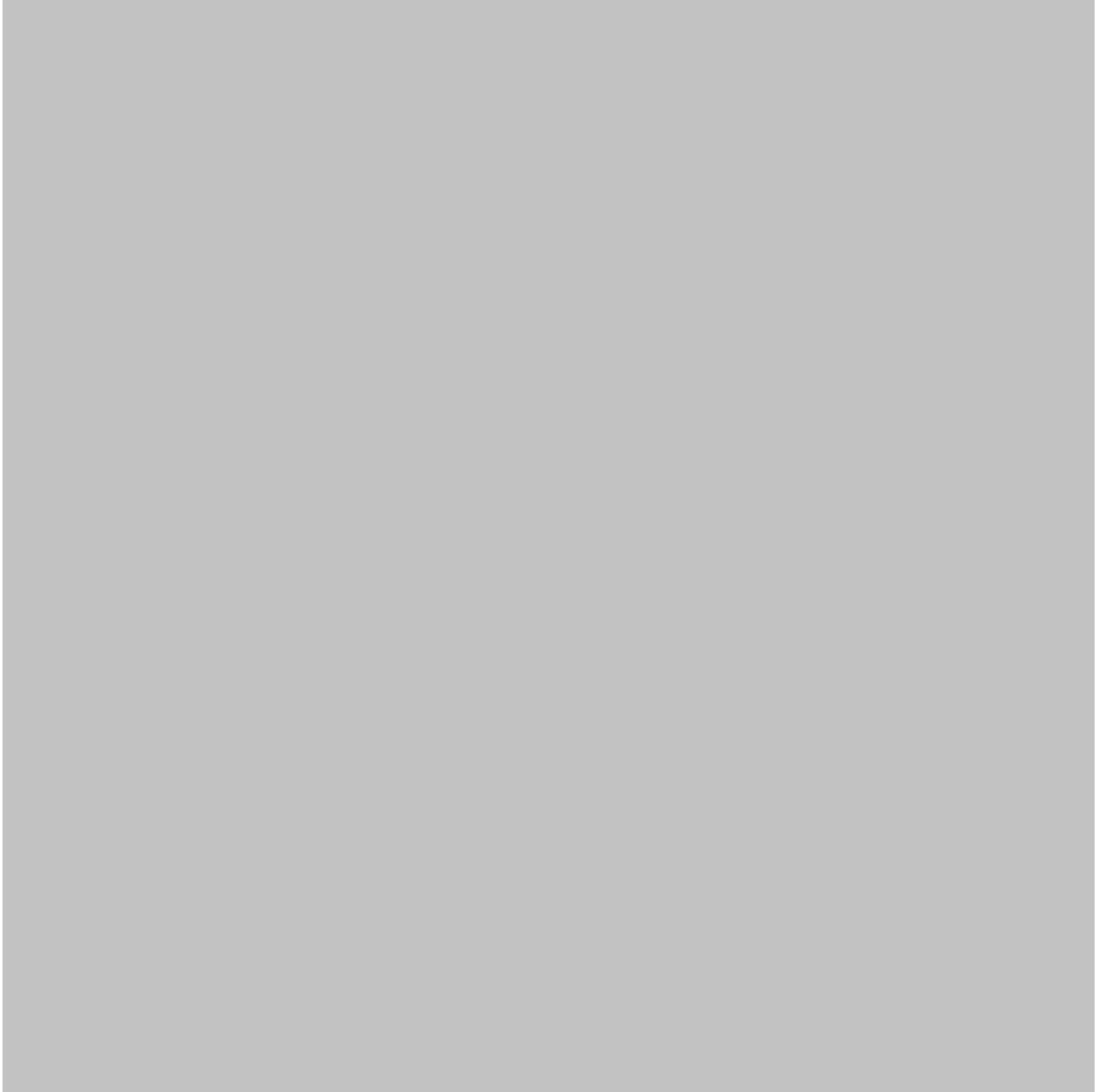


图 26 Dofloo年度威胁情报时间分布

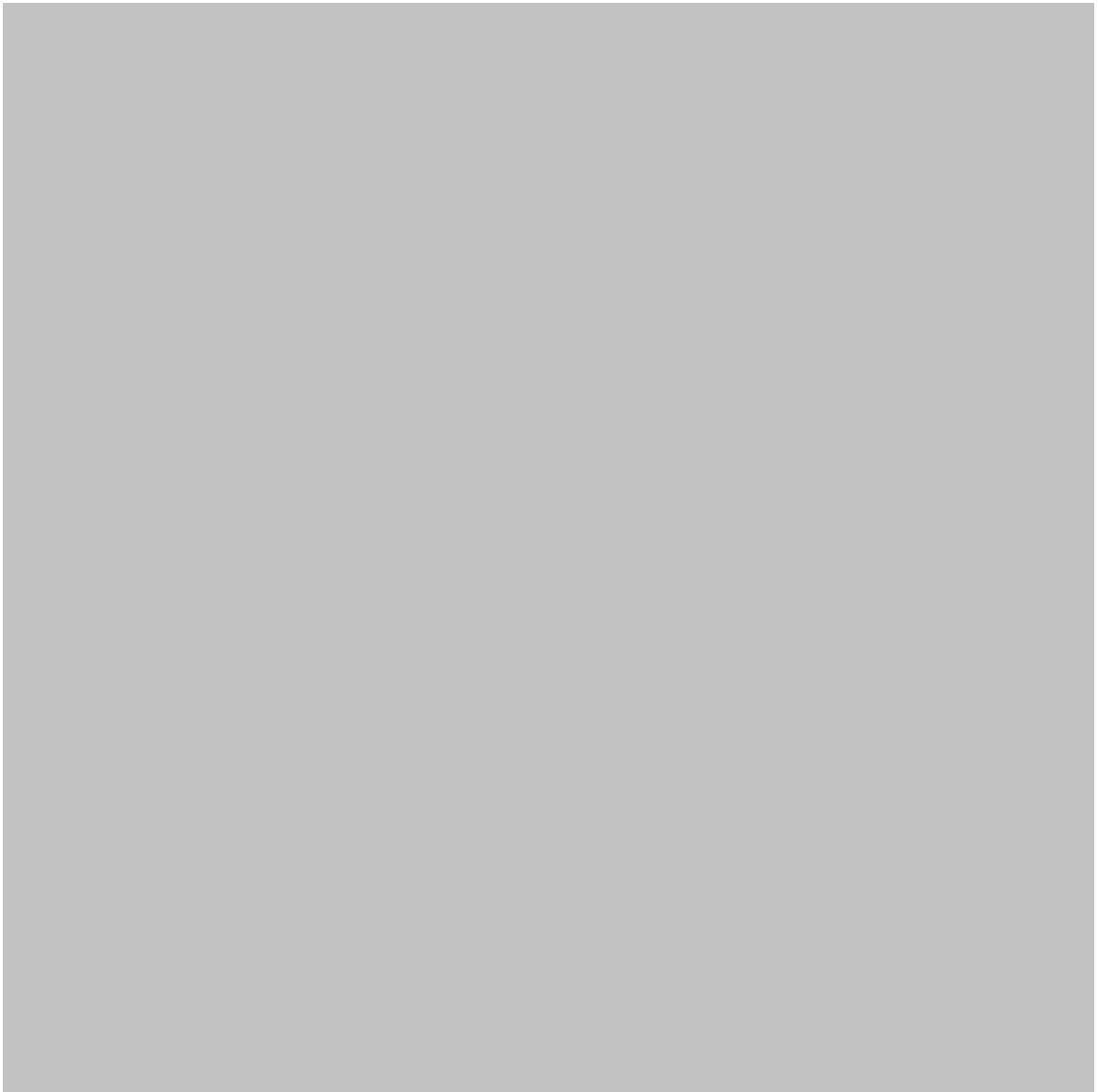


图27 Dofloo家族攻击方式分布统计

6、Mirai家族

Mirai家族出现于2016年上半年，由美国的Paras Jha（21岁）、Josiah White（20岁）和Dalton Norman（21岁）开发并运营，据悉2016年10月24日的美国域名服务商Dyn被DDoS攻击等事件就是他们所为。同时，他们为了隐藏自身、避免被执法部门追查，决定在执行攻击前以他人身份将源代码在github上公布，致使Mirai源代码迅速扩散到全球各地的黑客手中，从而引发了Mirai家族的高频率变种。

历史总是惊人的相似，灰鸽子木马开源导致delphi木马变种泛滥，Gh0st木马开源导致VC开发远控变种占据国内木马市场半壁江山。Mirai开源也引起国内黑产团伙升级改造IoT类型僵尸网络。



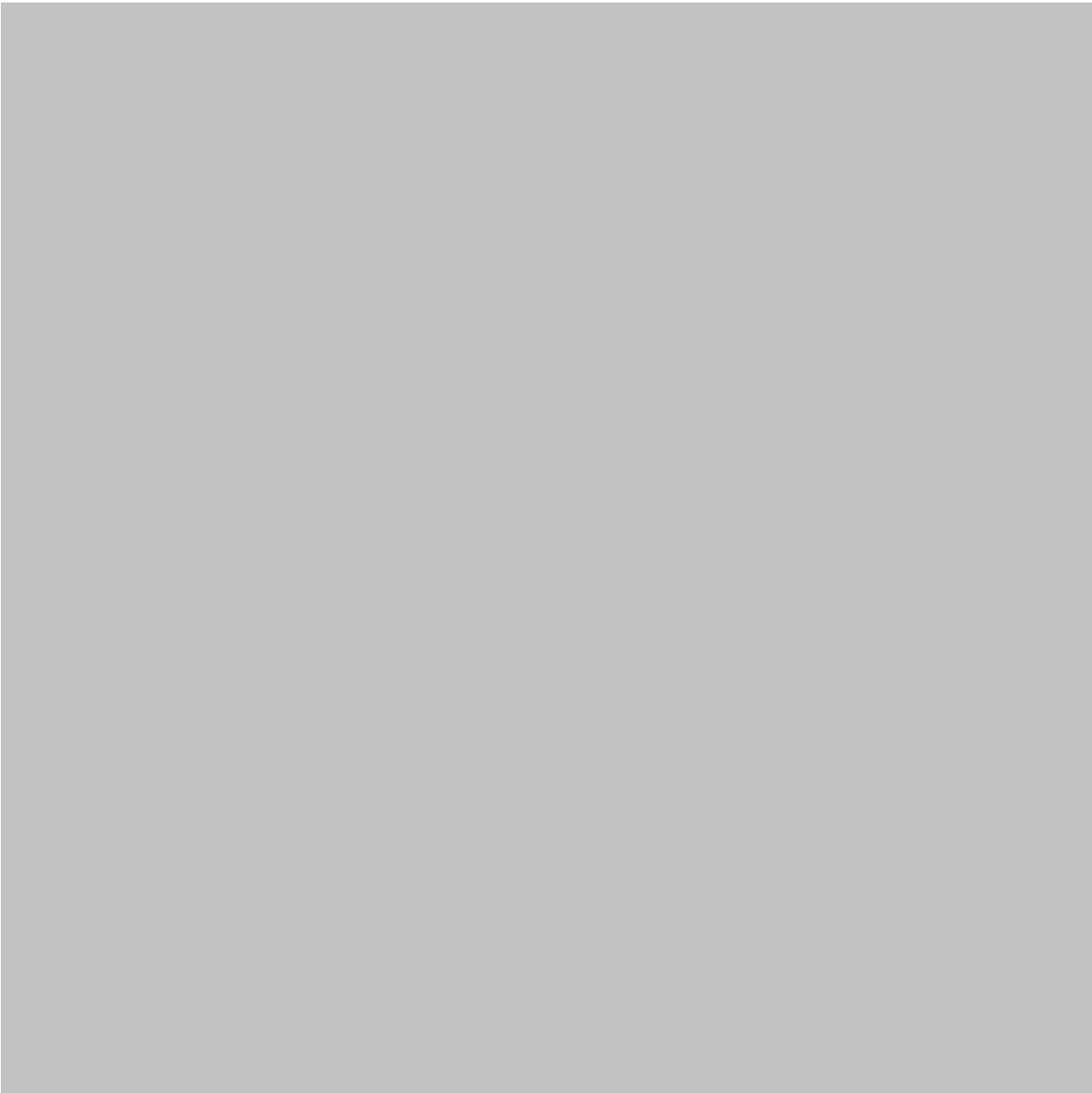


图 28 Mirai年度威胁情报分布



图 29 Mirai家族攻击方式分布统计

由于Mirai的木马具备22、23端口弱口令爆破功能，可进行各种物联网设备的漏洞利用，使得每一次Mirai变种的出现都会导致其“肉鸡”量以爆发式增长。初步统计，仅一年多的时间，Mirai家族涉及的漏洞扫描端口就有7547、5556767、37215 和52869等，涉及到的物联网设备厂商有Dahua、Huawei、D-Link、WIFICAM、Linksys、Avtec Netgear、Vacron、TP-Link等。而从2017年Mirai家族的攻击态势看，4月-9月期间攻击态势相对活跃，虽然下半年Mirai家族变种比较频繁，但并未提升攻击态势。

4.3 DDoS攻击方式

目前黑客发起DDoS攻击的方式主要有：SYN flood、TCP flood、DNS flood、C2 flood、UDP flood、HTTP flood、ICMP flood。以上七种攻击方式涵盖了所有攻击方式的99.97%，下面列出了以上七种攻击方式在2017年12个月里的分布情况。

总体来看，黑客控制僵尸网络发起的DDoS攻击在前半年中较为活跃，占全年DDoS攻击的71.96%，而在下半年活跃势逐渐减弱，直到12月份，又出现上升趋势。SYN flood攻击方式一直是黑客比较青睐的发起DDoS攻击的攻击方



在全年所有的攻击方式中SYN flood攻击方式占比最大，为91.56%。其在4月份和5月份中表现得格外活跃，在5月1以SYN flood攻击方式发起的攻击高达1586万次。



图 30 全球SYN flood攻击方式分布情况



图31 全球TCP、DNS、C2、UDP、HTTP、ICMP flood攻击方式分布统计

5 DDoS攻击情报信息

5.1 全球范围受DDoS攻击情报统计

据统计，在2017年中，受到黑客DDoS攻击的国家共130个，主要分布在亚洲，占总比的85.97%；其次是北美洲，占比的10.77%；欧洲占比2.99%；其他洲虽然占比较低，但都有被捕获的攻击数据。其中，中国成为了遭受DDoS攻击的重灾区，其被攻击总次数高达12200万次，占全球受攻击总数的84.79%，占整个亚洲地区受攻击总数的98.63%。



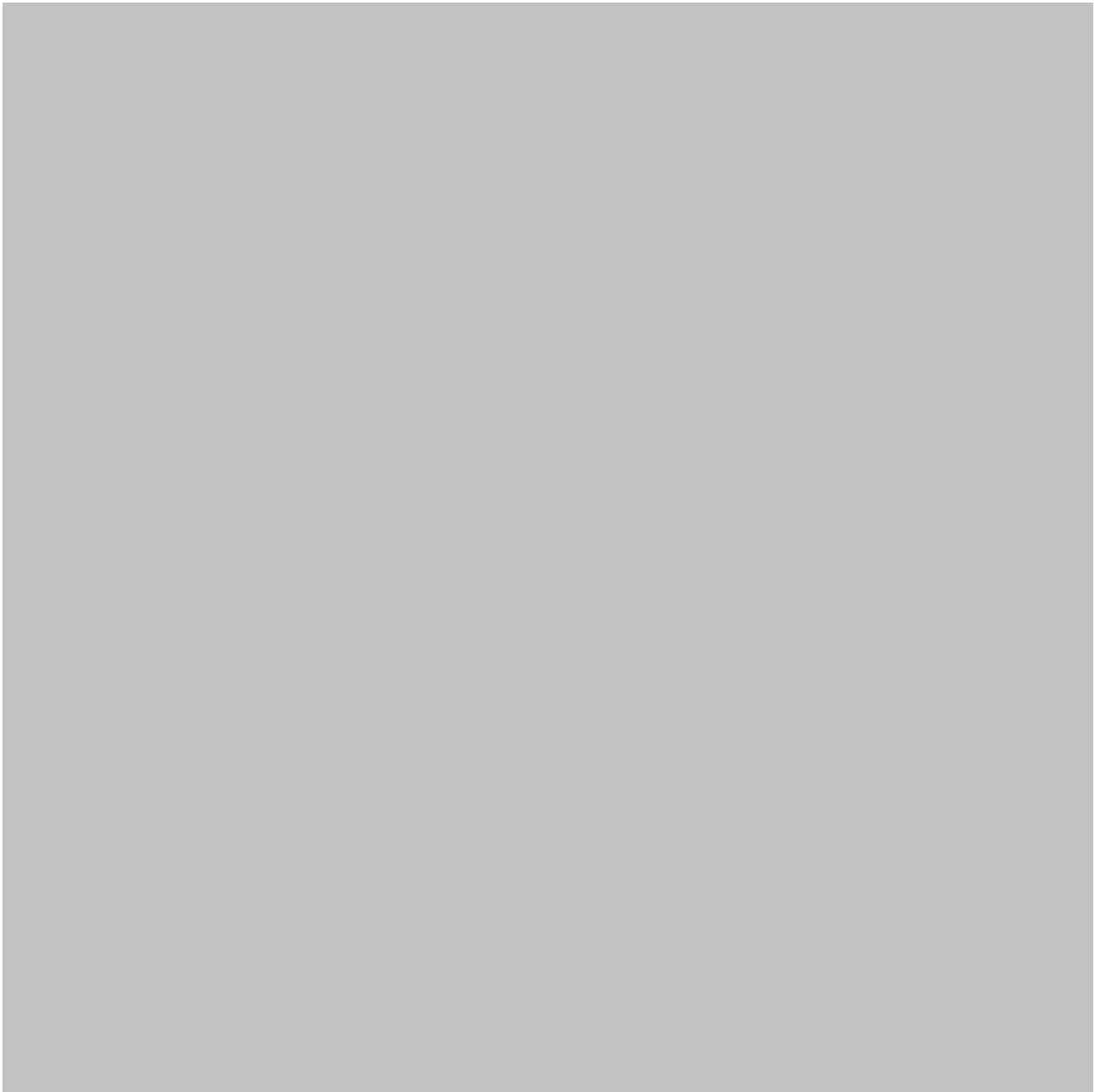


图32 受害者全球分布比例

5.2 全国受攻击DDoS攻击地区情报统计

据统计数据分析显示，2017年，国内遭受DDoS攻击的受害者地区分布情况如下，其中浙江省是国内遭受DDoS攻击的重灾区，被攻击次数为3790多万，占全国被DDoS攻击总数的31.39%；山东省位居第二，被攻击次数为2920多万，占全国被DDoS攻击总数的24.21%。



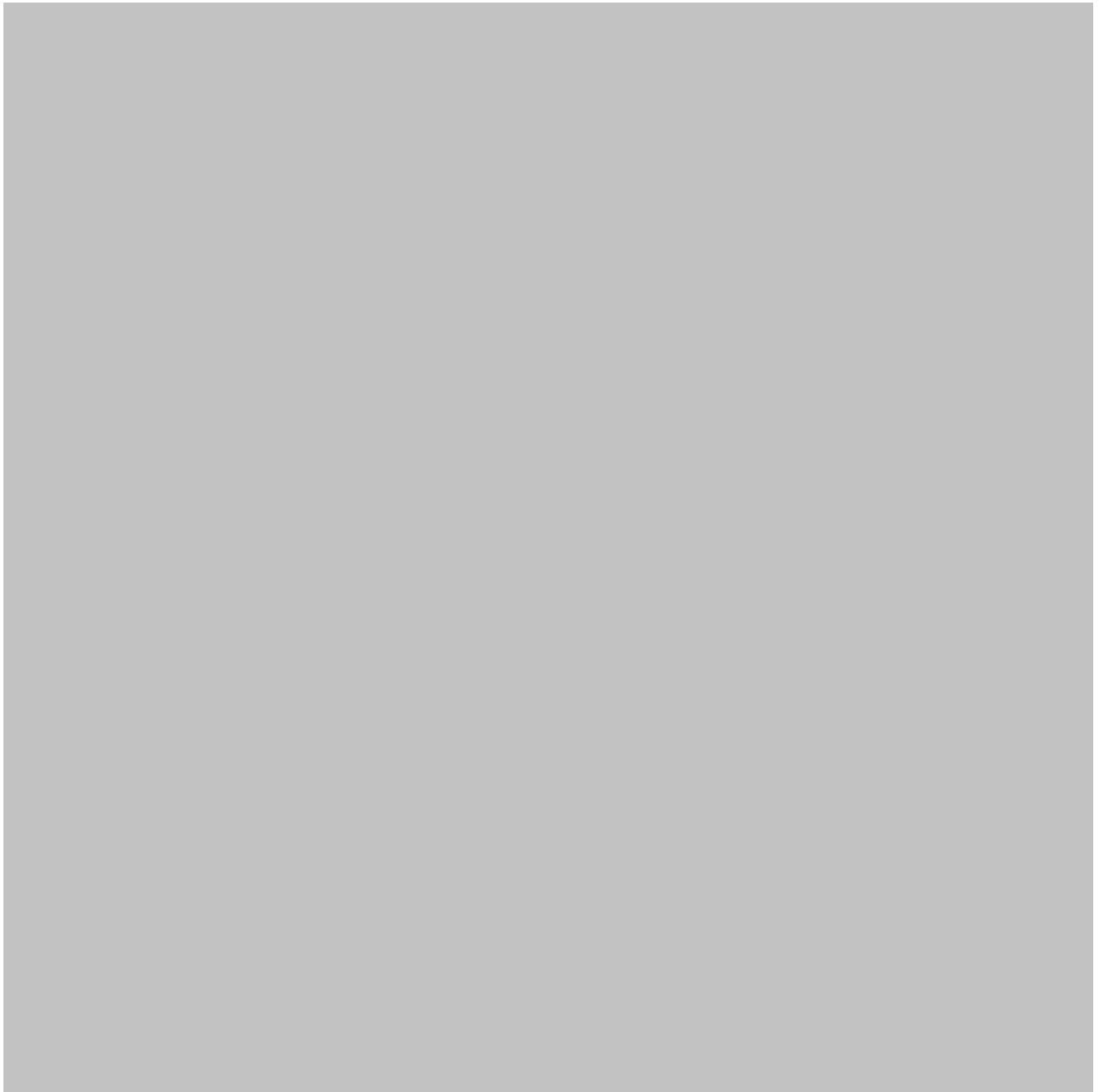


图 33 受害者在全国各地区的分布统计

5.3 攻击国内的DDoS攻击发起源情报分析

对2017年攻击国内的DDoS攻击情报进行统计分析，得到如下统计结果。其中，在美国的C2对我国国内发起的DDoS攻击总数为4600万次，在国内所遭受的所有DDoS攻击数中占比最大，为37.47%；其次，国内的C2对全国各地发起DDoS攻击，占总比的27.77%；在法国的C2对我国国内发起的攻击，占总比的23.28%；在韩国的C2对我国国内发起的攻击占总比的10.17%。



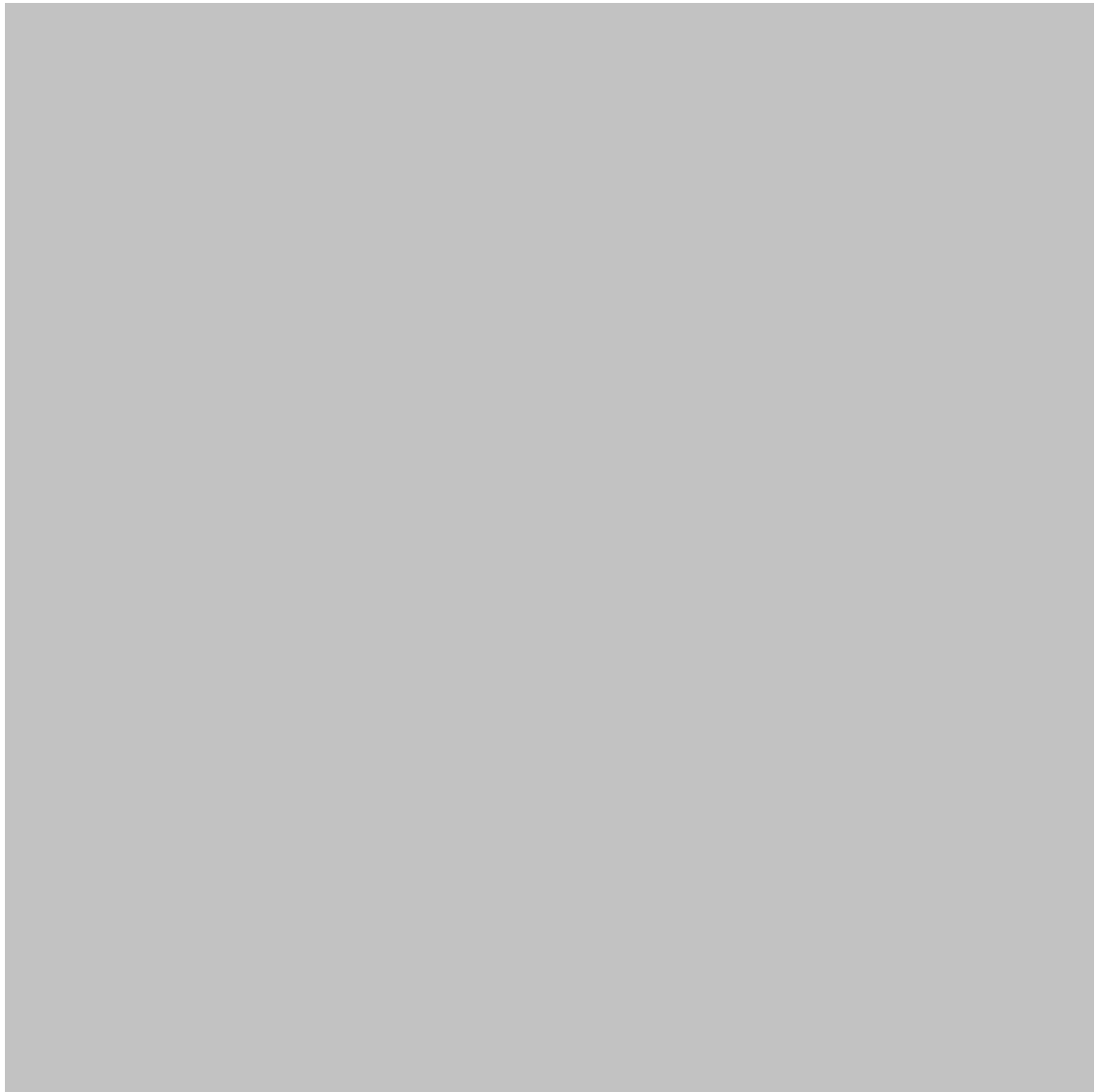


图 34 攻击国内DDoS攻击的发起源统计

5.4 受攻击行业类型

据不完全统计，黑客发起的DDoS攻击的受害行业分布如下：棋牌行业占比最高，为45.2%；游戏行业占比22.8%；学校科研占比11.5%；金融行业占比8.5%；行政单位占比5.5%；其他行业占比6.5%。

商家之间的恶性竞争或黑客的恶意勒索，是各行业遭受DDoS攻击的根本原因，游戏行业受到的影响尤为突出，在遭受DDoS攻击后，游戏公司的日损失可达数百万元人民币。

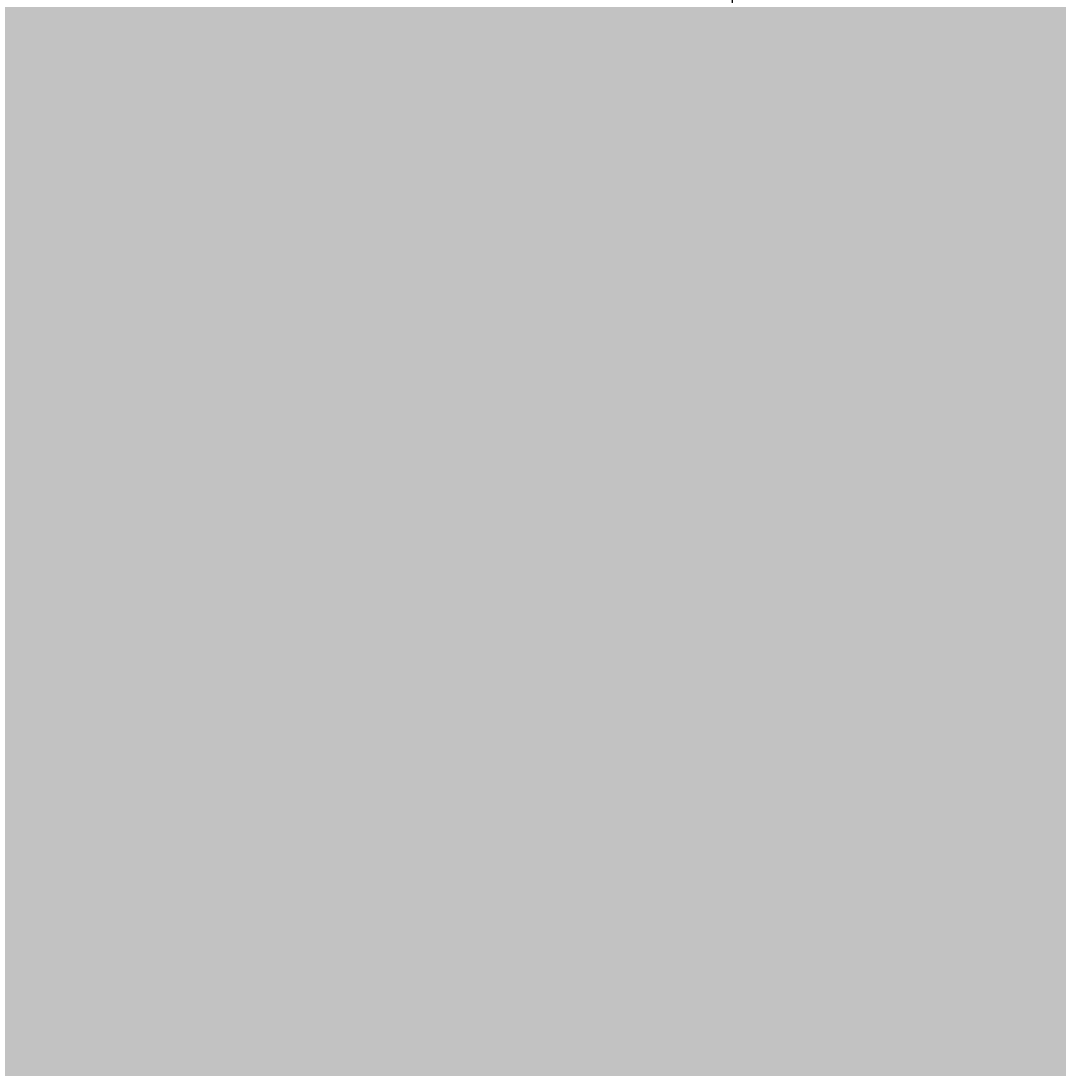


图 35 受害行业类型比例

6 国内“肉鸡”情报

2017年12月29日，随机对不同家族的11个DDoS僵尸网络C2的“肉鸡”进行了抽样，获取了国内外“肉鸡”IP 33661个。

6.1 国内DDoS僵尸网络“肉鸡”设备类型情报

通过捕获的“肉鸡”进行设备类型分析，以Windows、Linux和IoT设备作为分类范围，其中IoT设备类型的“肉鸡”占比61.37%；其次是Linux设备类型的“肉鸡”，占比20.85%，Windows设备类型“肉鸡”仅占比17.78%。

IoT设备因其漏洞较多、漏洞修复周期较长，且易于入侵、控制，而成为黑客们喜欢“抓取”的“肉鸡”类型。在统计中，涉及的IoT设备厂商包括华为、中兴、H3C、大华等，其中442个“肉鸡”设备属于华为的IoT设备，240个属于中兴的IoT设备，1142个属于H3C的IoT设备。

对于Linux设备类型，攻击者多通过22、23端口进行弱口令爆破以实现对其“肉鸡”的控制。而针对Windows设备类型的“肉鸡”，黑客多通过利用“永恒之蓝”漏洞结合各家族的病毒、木马，以实现对其“肉鸡”的“抓取”。



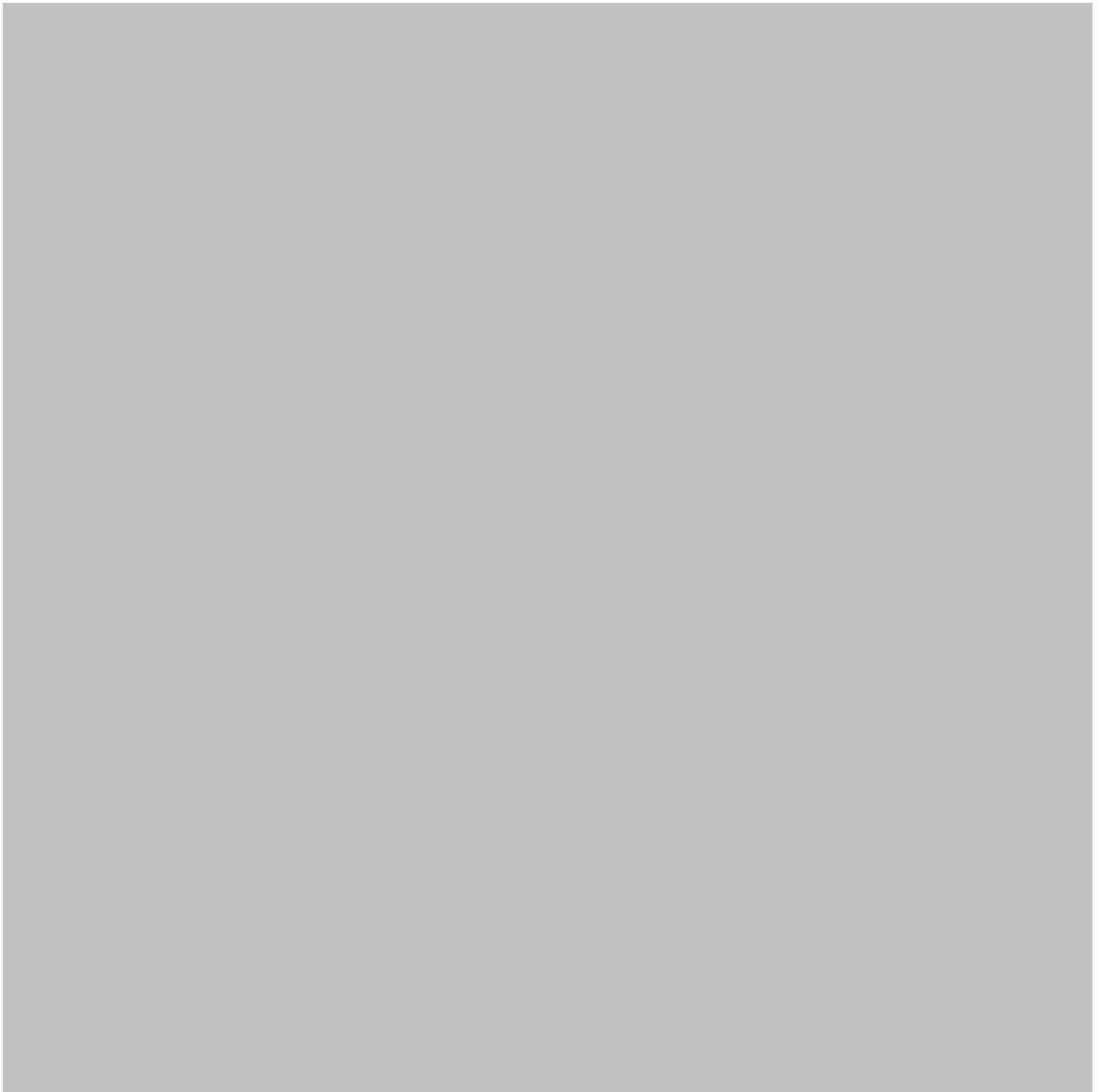


图 36 国内DDoS僵尸网络“肉鸡”设备类型统计

6.2 国内DDoS僵尸网络“肉鸡”分布地区情报

对获取到的33661个DDoS僵尸网络“肉鸡”IP进行分析定位发现，其中33555个“肉鸡”IP位于中国。对国内的“肉鸡”IP进行汇总分析，得出以下部分“肉鸡”在国内部分省份的分布情况。位于江苏和浙江的“肉鸡”IP较多，分别为5961和5899个。从地理分布上看，“肉鸡”IP多位于沿海城市，我国的沿海城市从北到南依次为山东省、江苏省、浙江省、福建省和广东省，这五个省份的“肉鸡”数量均位列前十。





图 37 国内部分DDoS僵尸网络“肉鸡”分布情报统计

7 总结

从1998年第一次真正意义上的DDoS攻击开始，其攻击带宽流量从10GB、90GB，逐渐扩大至300GB、400GB、800GB，如今已经以“T”级别来计算，DDoS攻击几乎在以飞跃式的速度增长着。受到影响的设备，从一开始的单个服务器、区域性的多个服务器，扩大到针对某行业的整个服务、甚至差点瘫痪欧洲的网络；受到影响的范围从个人、范围网络，发展到商业之间的竞争、国家金融服务，甚至国家之间的政治、军事行动等等。

从DDoS攻击的发展历程，我们不难看出，在如今这个虚拟网络已经嵌入我们现实生活的社会里，DDoS攻击无疑是个巨大的安全隐患。伴随着DDoS工具的廉价性、易获取性，以及各僵尸网络家族的快速增长，利用物联网设备组成僵尸网络发起攻击的现象日益严峻，与此同时，移动端的僵尸网络亦处于萌芽阶段，网络安全之路可谓任重道远。



[1]. 安天针对“魔鼬”木马DDoS事件分析报告

<http://www.antiy.com/response/weasel.html>

[2]. 僵尸网络团伙利用MIRAI开源代码改造升级攻击装备

<http://www.freebuf.com/articles/web/153689.html>

[3]. <https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html>

*本文作者：antiylab，转载请注明FreeBuf.COM

上一篇：[病毒分析 | 一只“蜗牛”偷梁换柱，靠锁主页进行牟利](#)

下一篇：[本篇已是最新文章](#)

已有 1 条评论

WWWWWW 2018-01-12

1楼 [回](#)

好文，学习一下

💡 亮了 1

选择文件 未选择任何文件

昵称

请输入昵称

必须 您当前尚未登录。 [登陆?](#) [注册](#)

邮箱

请输入邮箱地址

必须 (保密)

表情 插图

提交评论(Ctrl+Enter)

[取消](#)



有人回复时邮件通知我





antiylab

安天网络安全官方账号

9

文章数

1

评论数

最近文章

- 2017全球僵尸网络DDOS攻击威胁态势报告 2018.01.12
- 处理器A级漏洞Meltdown（熔毁）和Spectre（幽灵）分析报告 2018.01.05
- 对利用CVE-2017-0199漏洞的病毒变种的监测与分析 2017.12.17

浏览更多

相关阅读

[逆天而行：我们如何在云中发掘僵尸...](#)[Dorothy2：一个开源的僵尸网络分析框架](#)[“IOT幽灵”样本分析报告：物联网僵尸...](#)[爆料全球首个基于Twitter的Android僵...](#)[IoT reaper：一个正在快速扩张的新型I...](#)

特别推荐





[极客DAY：手机文件直传U盘，三步教你做一根OTG传输线](#)

[geekman](#)

2014-12-27

[量子计算从概念走入现实，公钥加密是否岌岌可危](#)

[Elaine_z](#)

2017-07-18

[独家分析：安卓“Janus”漏洞的产生原理及利用过程](#)

[顶象技术](#)

2017-12-12


[快讯：联想官网被黑，内部邮件被劫持](#)

[hujias](#)

2015-02-26



Copyright © 2018 WWW.FREEBUF.COM All Rights Reserved [沪ICP备13033796号](#)

 阿里云 提供计算与安全服务