2017 全球僵尸网络 DDOS 攻击威胁态势报告

联合编写：安天捕风团队、电信云堤

初稿完成时间：2018 年 1 月 9 日 08 时

首次发布时间：2018 年 1 月 9 日 08 时

本版更新时间：2018 年 1 月 9 日 08 时

文章分享二维码

目 录

1 概述 3

2 DDoS 僵尸网络攻击情报 4

2.1 DDoS 僵尸网络 DDoS 攻击情报全球分布情况 5

2.2 DDoS 僵尸网络发起 DDoS 攻击全国分布情报 6

3 DDoS 攻击带宽流量情报信息 6

4 DDoS 僵尸网络 C2 情报信息 9

4.1 DDoS 僵尸网络 C2 攻击情报 9

4.1.1 DDoS 僵尸网络 C2 分布 9

4.1.2 DDoS 僵尸网络 C2 存活时间 12

4.2 黑客攻击工具 12

4.2.1 DDoS 僵尸网络木马传播 12

4.2.2 全球各 DDoS 家族僵尸网络威胁情报 15

4.3 DDoS 攻击方式 22

5 DDoS 攻击情报信息 23

5.1 全球范围受 DDoS 攻击情报统计 23

5.2 全国受攻击 DDoS 攻击地区情报统计 24

5.3 攻击国内的 DDoS 攻击发起源情报分析 25

5.4 受攻击行业类型 26

6 国内“肉鸡“情报 27

6.1 国内 DDoS 僵尸网络“肉鸡”设备类型情报 27

6.2 国内 DDoS 僵尸网络“肉鸡”分布地区情报 27

7 总结 28

附录一 参考资料 29

附录二 关于安天 30

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，针对 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发起 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详细分析。

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%；而中国则成为了遭受 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、BillGates、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，也快速向 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、IoT 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，网络服务需求与日俱增，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。

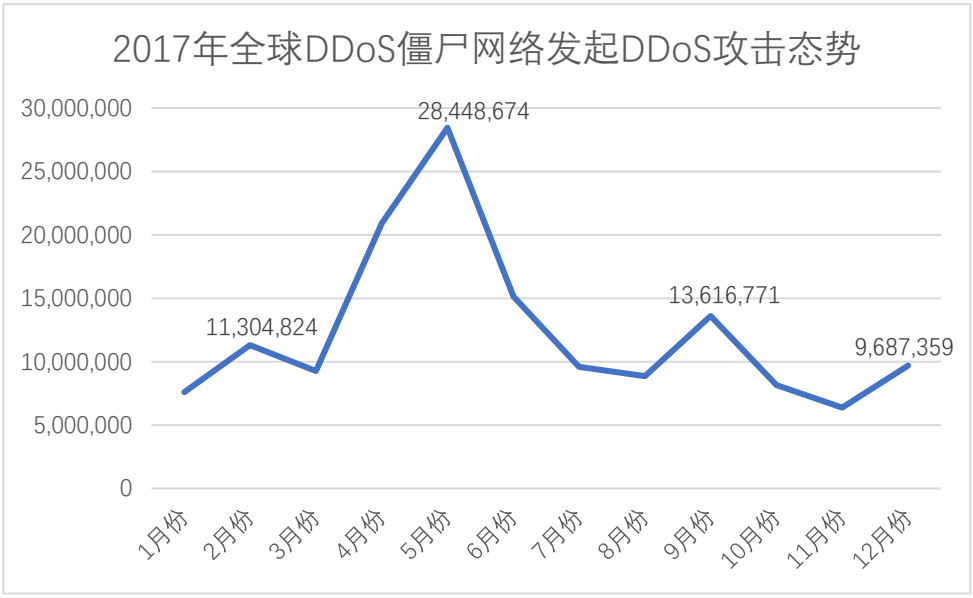

图 1　2017 年全球 DDoS 僵尸网络发起 DDoS 攻击态势

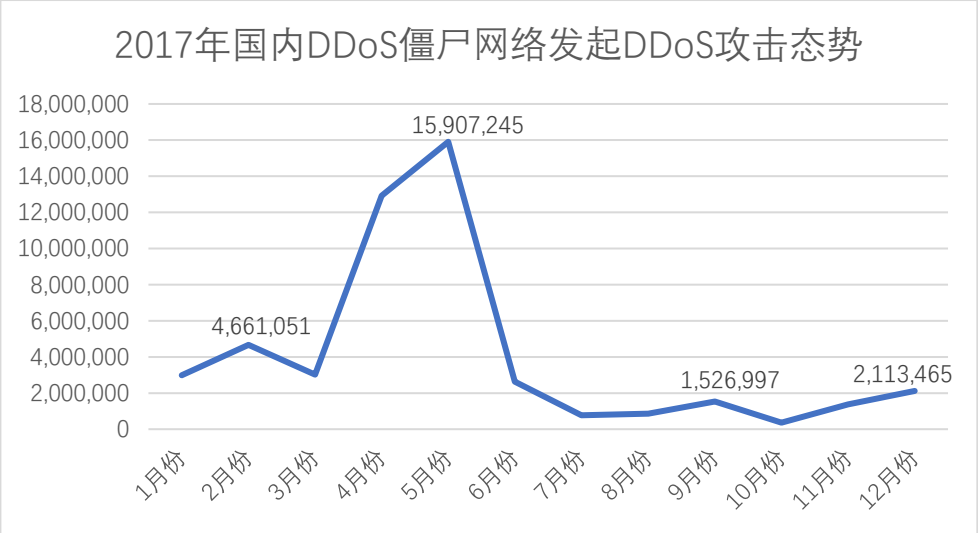

图 2　2017 年国内 DDoS 僵尸网络 DDoS 攻击态势

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的 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 攻击占总比的 34.19%；C2 位于法国境内对各国发起的 DDoS 攻击占比 19.10%。

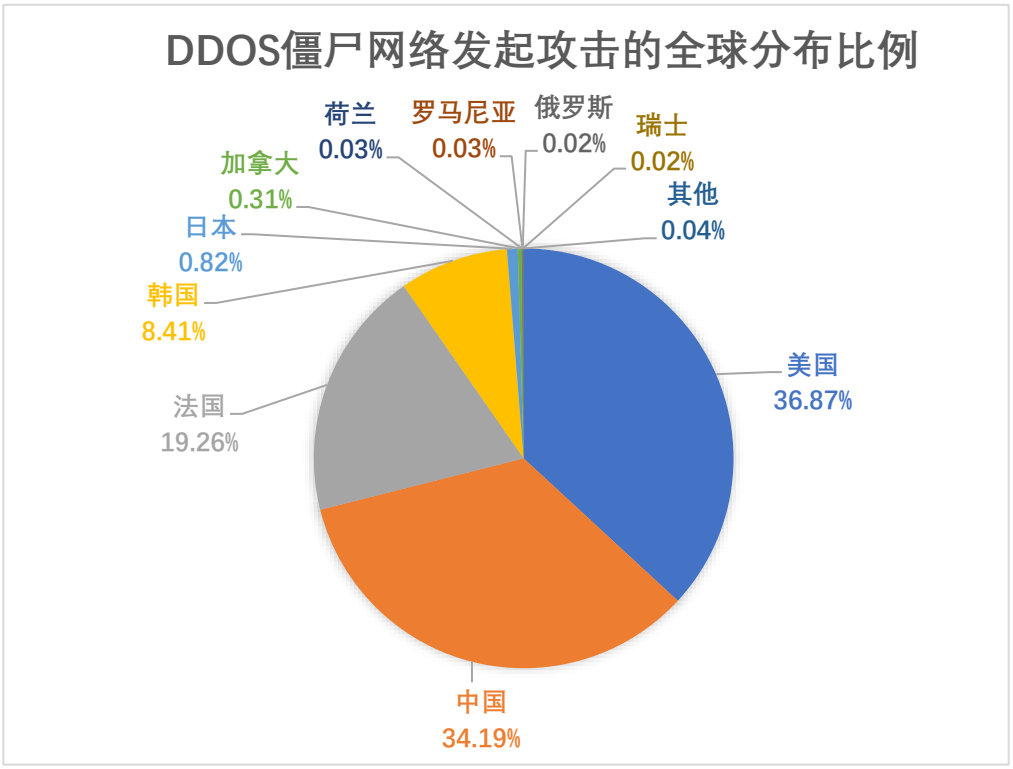

图 3　DDoS 僵尸网络发起攻击的全球分布比例

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，江西省内发起的 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 1300 多万，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，为 23.12%。

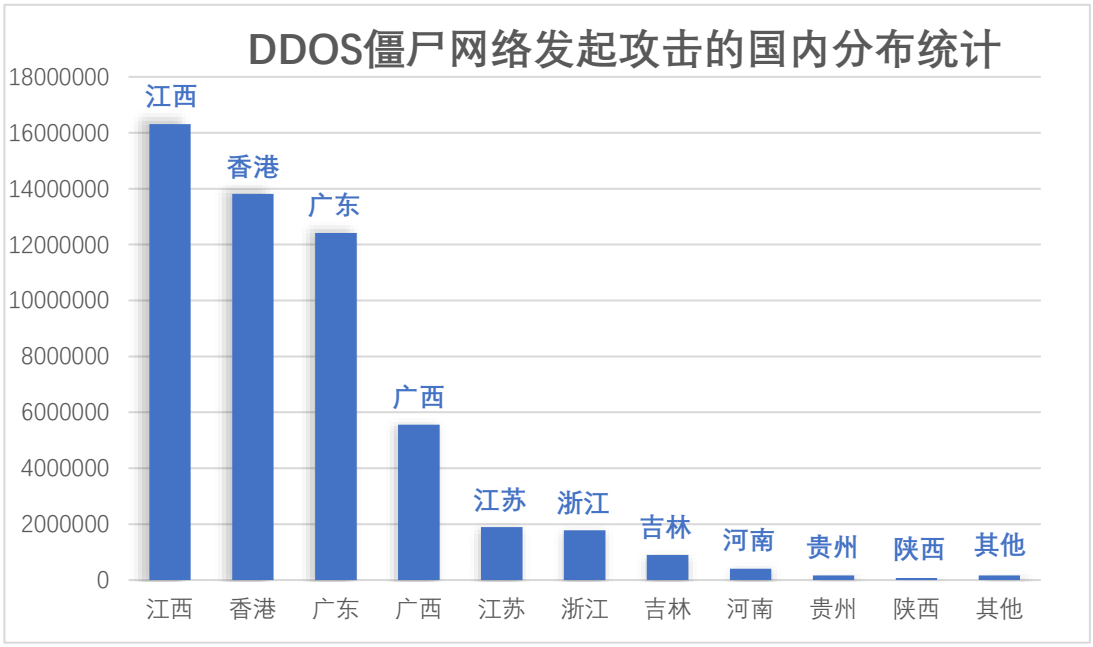

图 4　DDoS 僵尸网络发起攻击的国内分布统计

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。

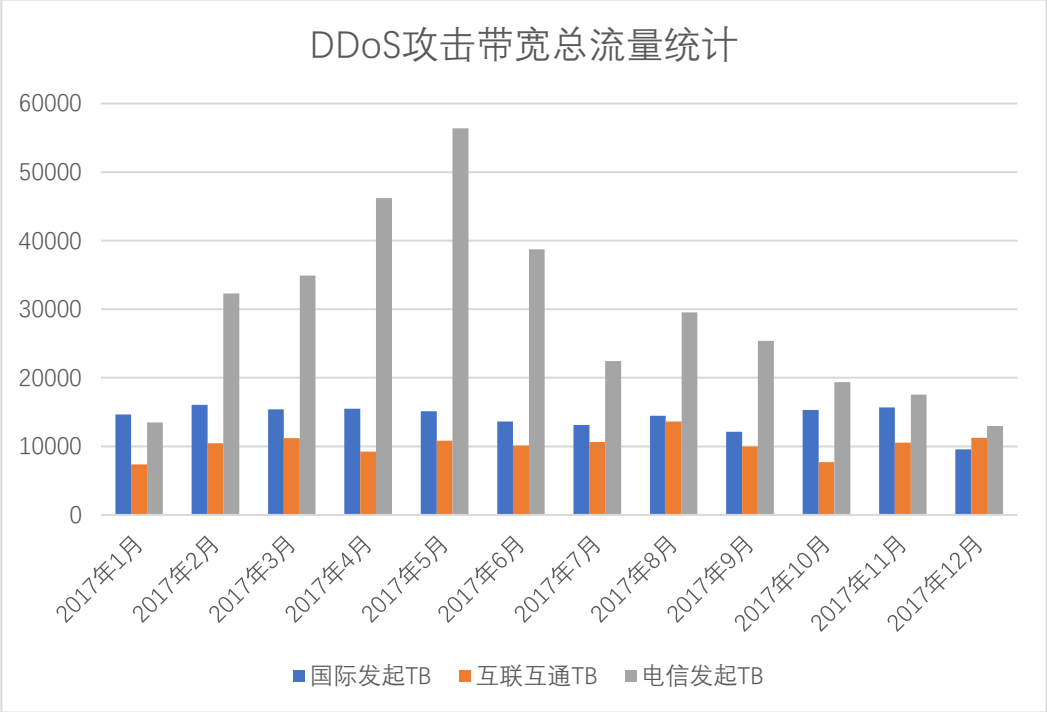

图 5　DDoS 攻击带宽总流量统计

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。

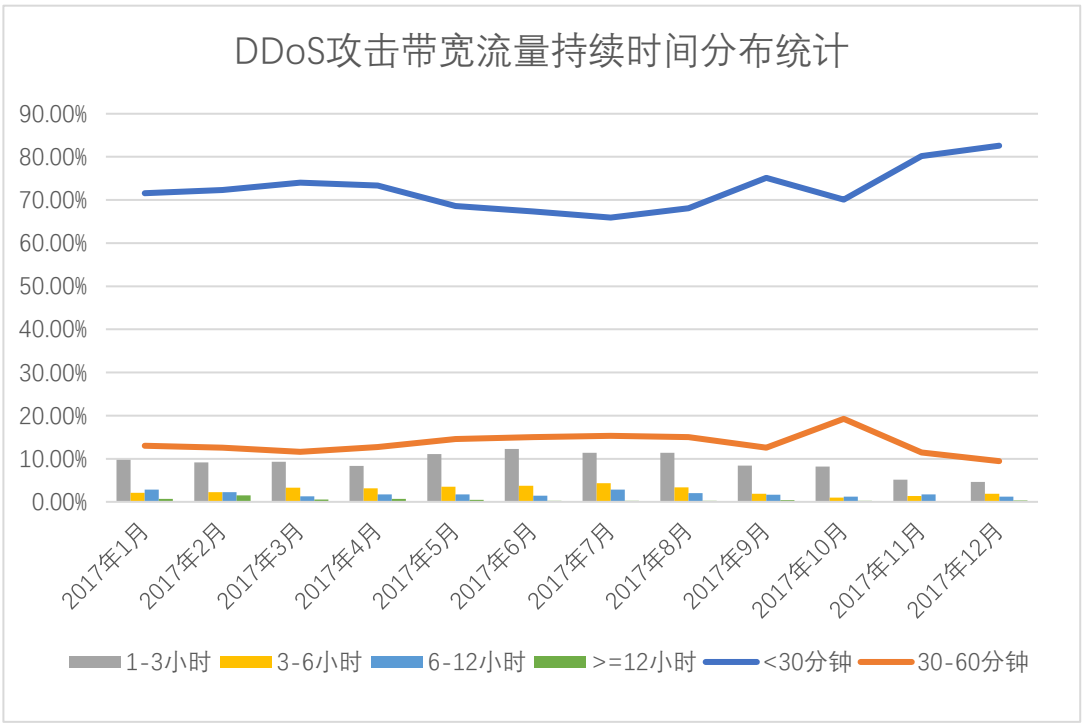

图 6 DDoS 攻击带宽流量持续时间分布统计

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。

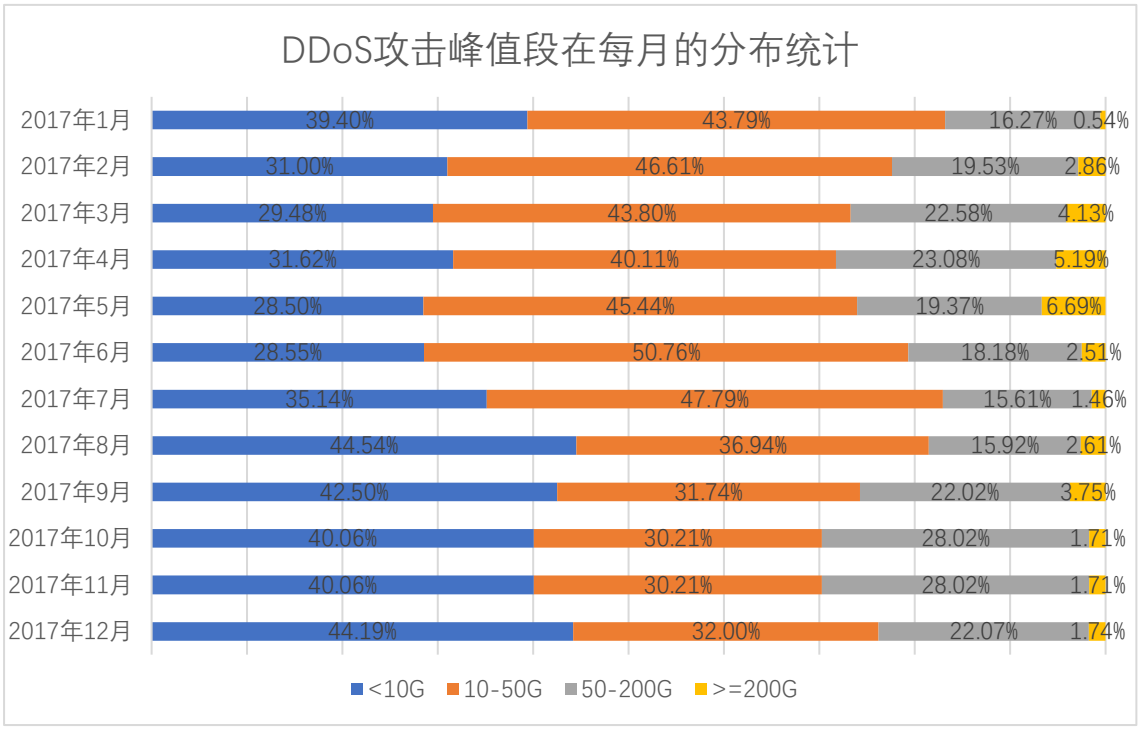

图 7 DDoS 攻击峰值段在每月的分布统计

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。

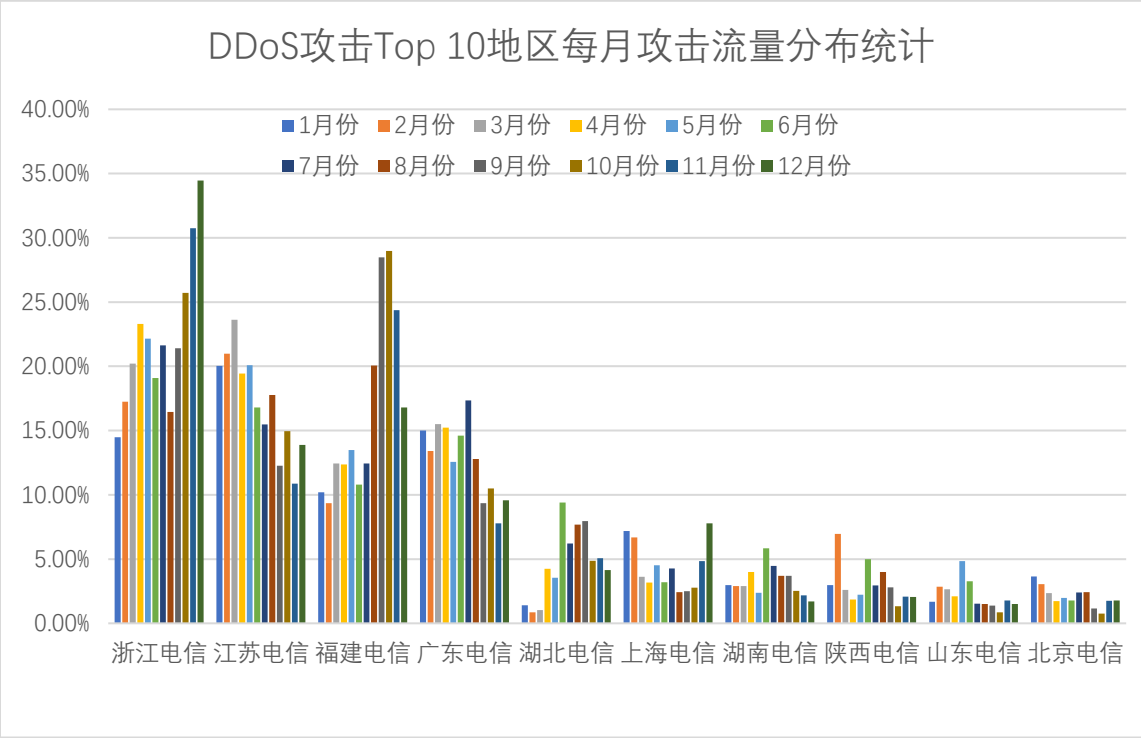

图 8 DDoS 攻击 Top 10 地区每月攻击带宽流量分布统计

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%；排在第三位的是韩国，位于韩国的 C2 有 1039 个，占比全球 C2 分布的 4.11%。

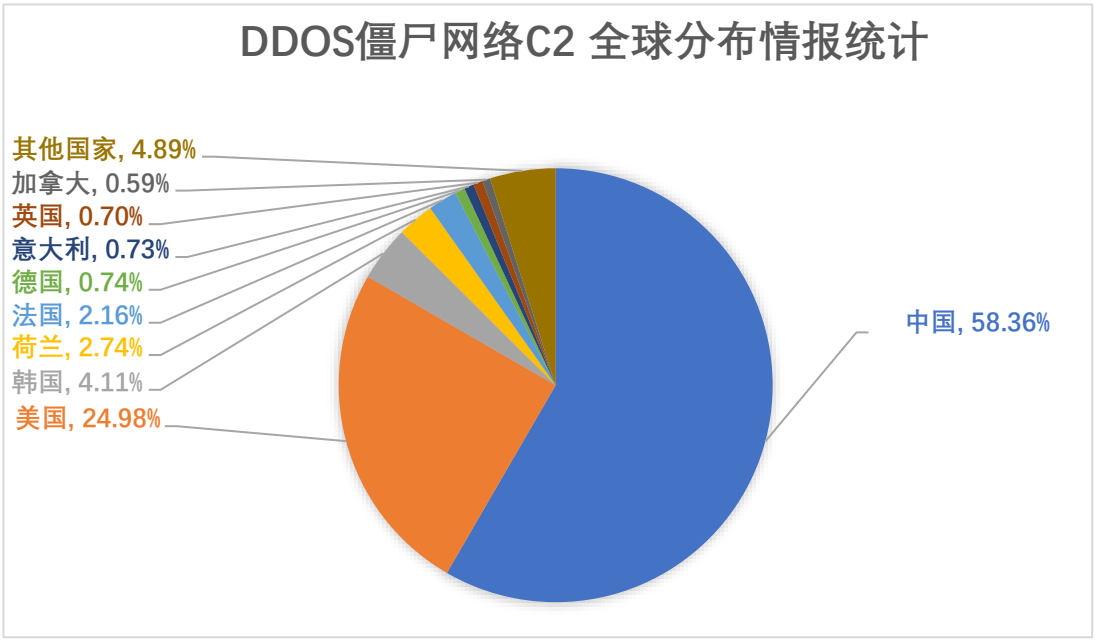

图 9 DDoS 僵尸网络 C2 全球的分布情报统计

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，各国 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。

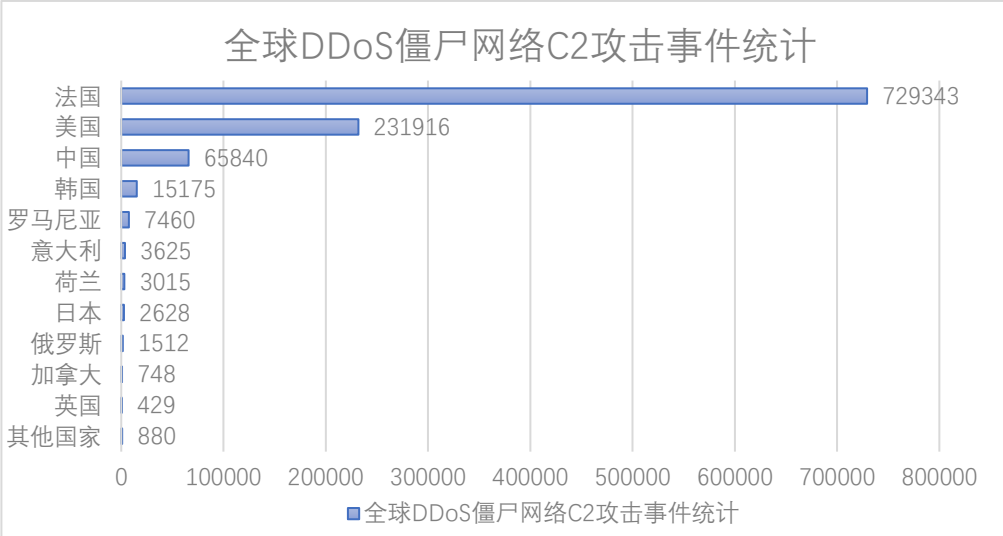

图 10　全球 DDoS 僵尸网络 C2 攻击目标统计

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%。

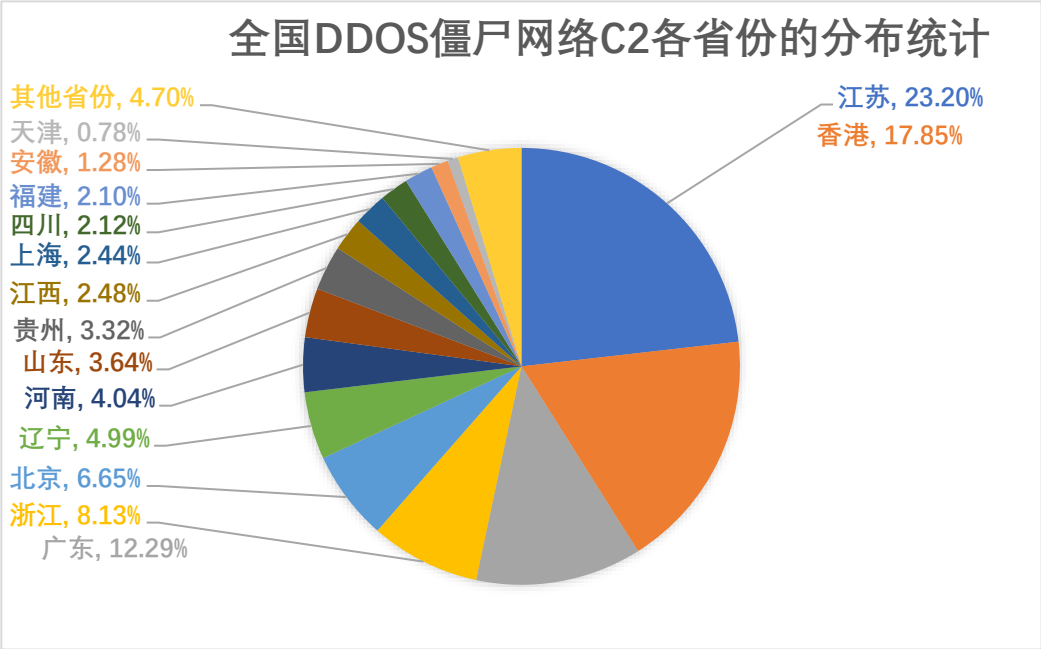

图 11　全国 DDoS 僵尸网络 C2 各省份的分布统计

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的省份，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，该 C2 的存活时间为 508.05 个小时。

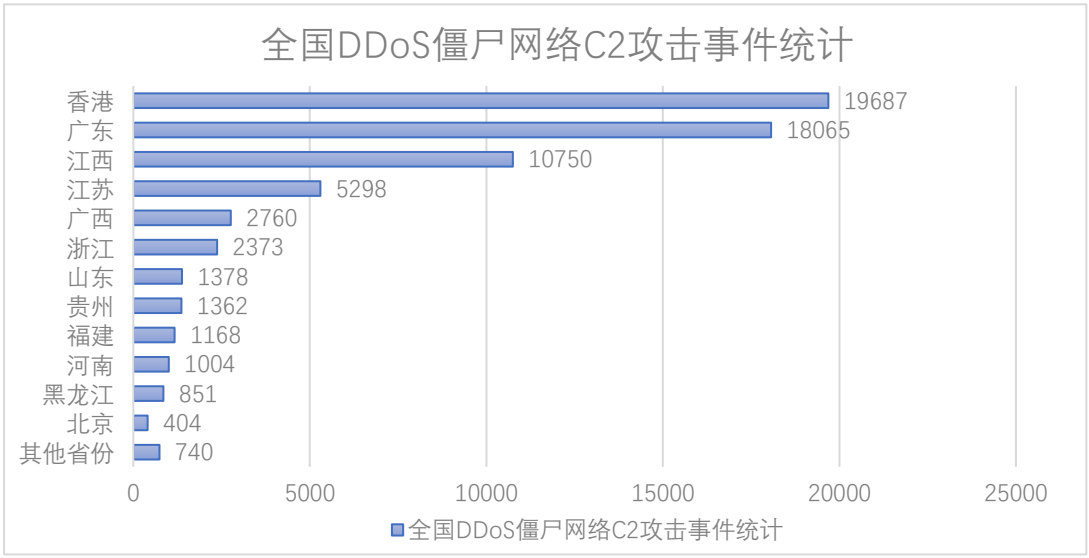

图 12　全国 DDoS 僵尸网络 C2 攻击事件统计

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 小时以内的占比 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。

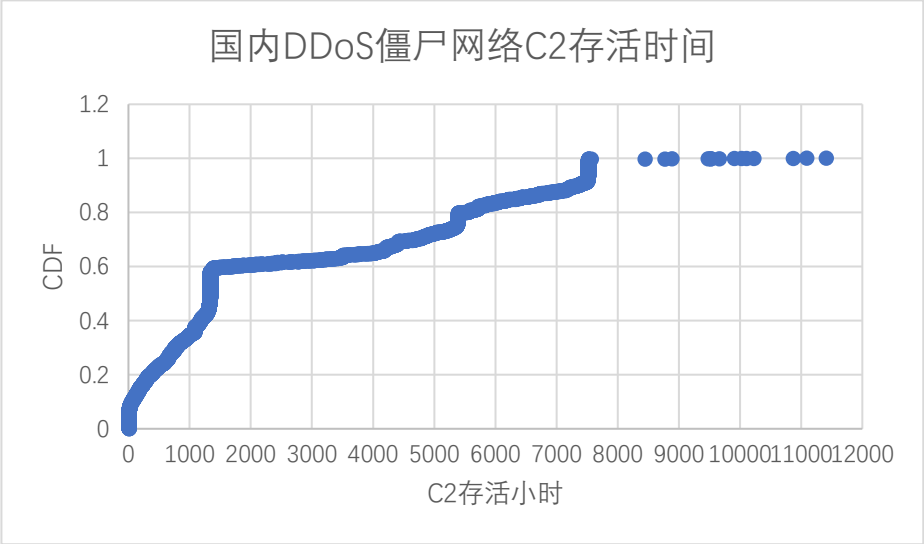

图 13　国内 DDoS 僵尸网络 C2 存活时间

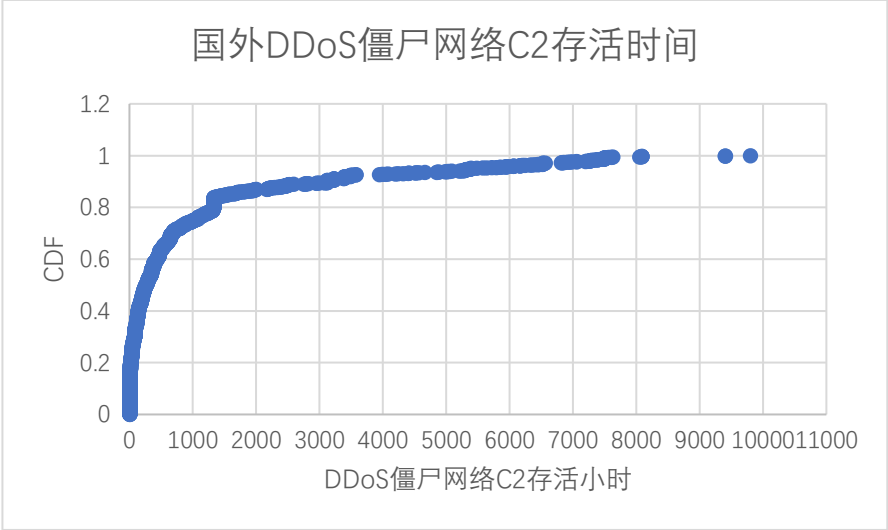

图 14　国外 DDoS 僵尸网络 C2 存活时间

4.2 黑客攻击工具

4.2.1 DDoS 僵尸网络木马传播

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，而常见的“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，且每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较常见。

表格 1 扫描端口可疑 IP

端口	月均独立扫描 IP （单位：万）
23	75
2323	73
445	10
22	6.7
80	2.3
1433	2
3389	2
81	2
3306	0.3

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经展示得淋漓尽致。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

厂商名称	漏洞编号	估计受影响设备
SENRIO	CVE-2017-9765	100 万+ IoT 设备
Goahead	CVE-2017-8225	250 万+ IoT 设备
Huawei	CVE-2017-17215	250 万+ 路由设备

Dlink	CNVD-2017-20002、 CNVD-2017-20001	250 万+ 路由设备
Netgear	CVE-2017-5521	…… 路由设备
Linksys	CVE-2017-17411、 CVE-2014-8244	300 万路由器

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，在易受攻击的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 协议插入到 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接收来自互联网的 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 其共享对象的有效 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、可以在多个平台运行的嵌入式 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。

磊科后门利用是 2014 年爆出的后门利用方法，目前在捕获的攻击数据中依旧有出现。

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）设备的漏洞。

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不断感染设备拓展“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，所以通过这种传播方式形成的僵尸网络，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成型的僵尸网络，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，捕获样本为 10667 个。如下图所示：

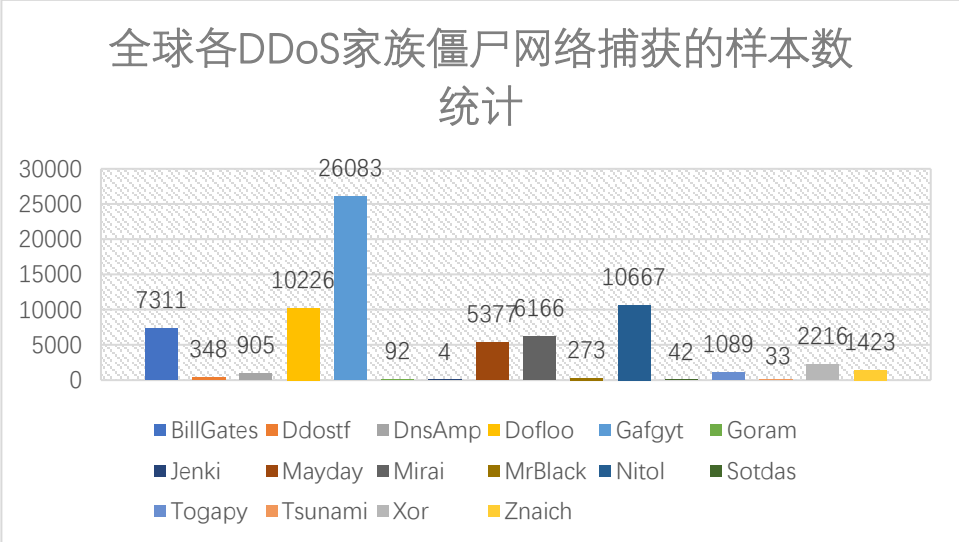

图 15　全球各 DDoS 家族僵尸网络捕获的样本数统计

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%。

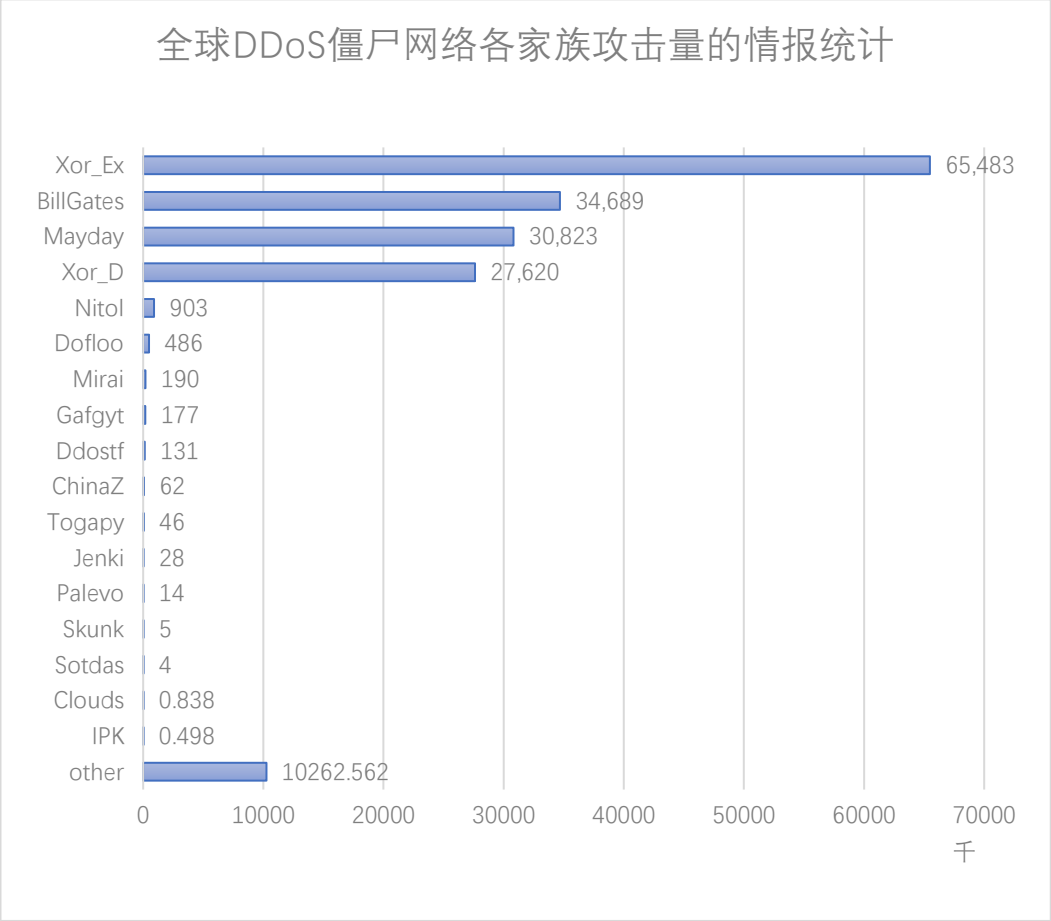

图 16　全球 DDoS 僵尸网络各家族攻击量的情报统计

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 家族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 对应的设备基本是通过非法渠道获取远程控制权限进行部署，极大增加了对黑客的溯源难度。

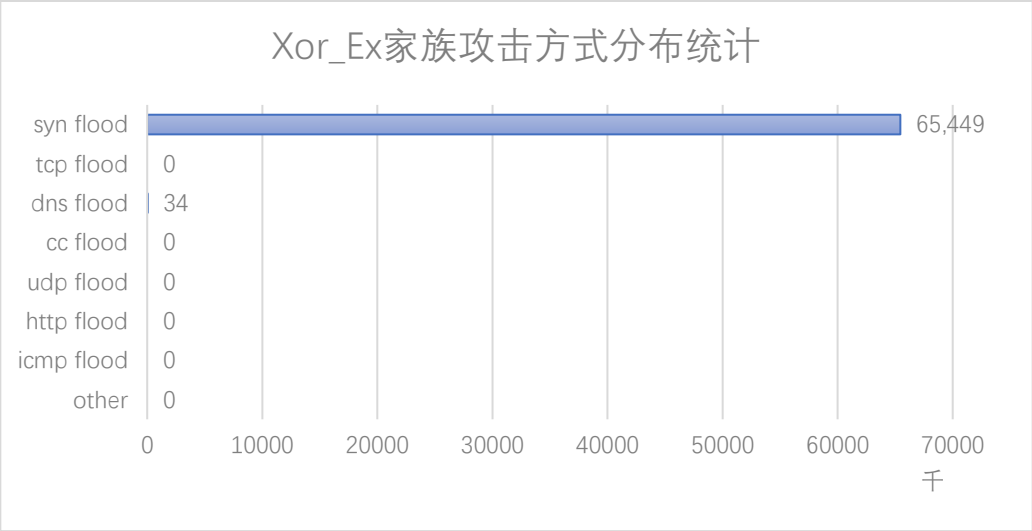

图 17　Xor_Ex 家族攻击方式分布统计

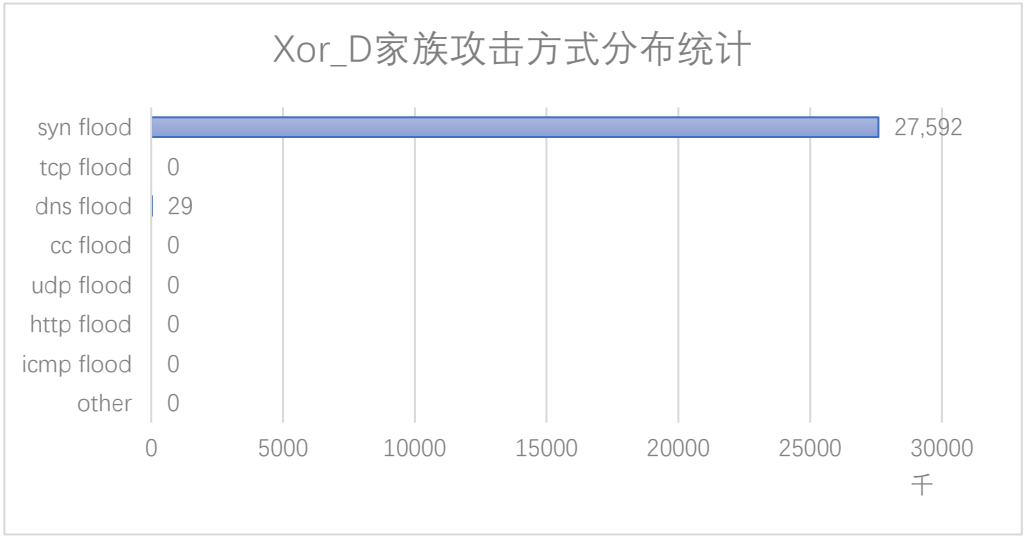

图 18　Xor_D 家族攻击方式分布统计

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，且攻击类型主要是 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换为挖矿僵尸网络从事挖矿。

图 19　BillGates 年度攻击情报时间分布

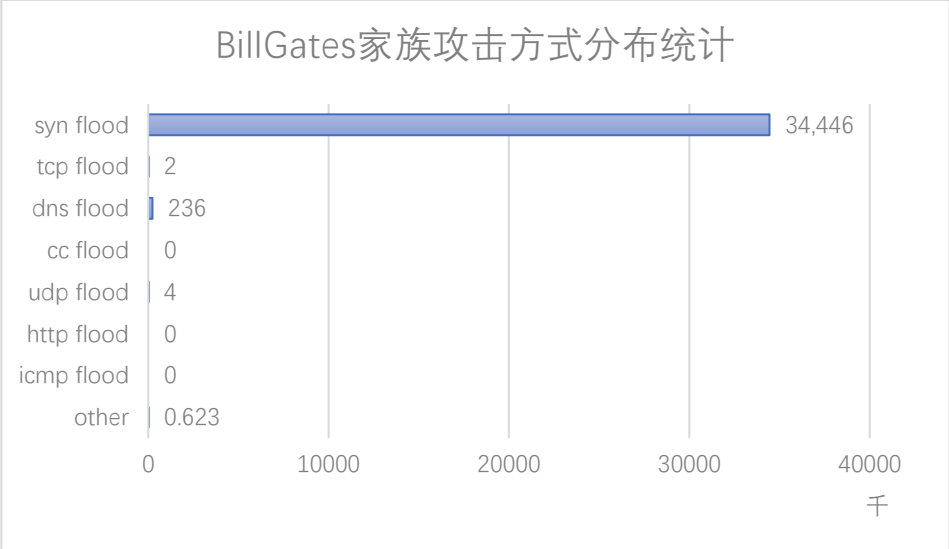

图 20　BillGates 家族攻击方式分布统计

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

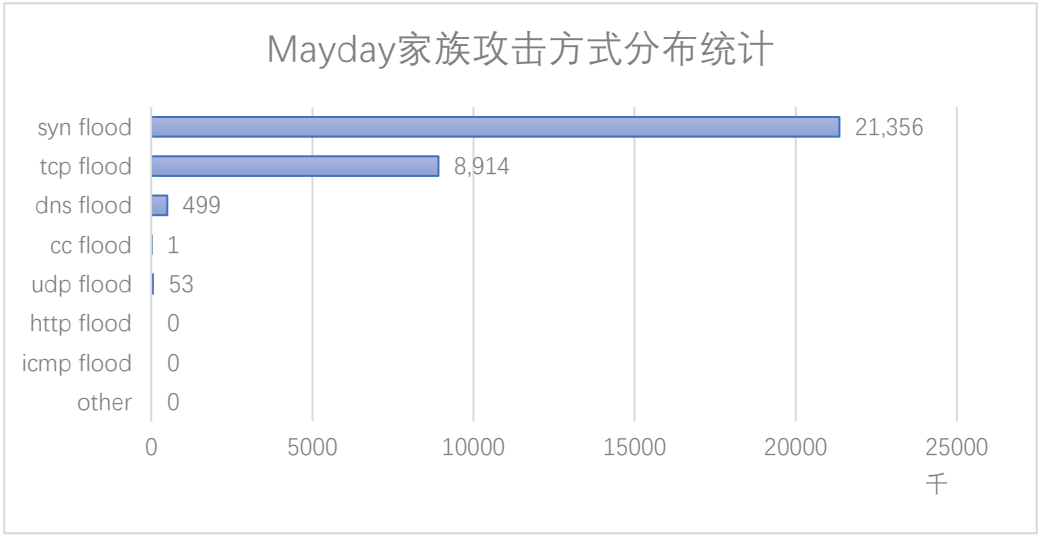

图 22　Mayday 家族攻击方式分布统计

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 多个不同协议的变种，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扩散到国外，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，开始出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 的改进版本中集成了 SYN flood、TCP flood、DNS flood、C2 flood、UDP flood、HTTP flood、ICMP flood 和 NTP flood 等 8 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，这点明显区别于其他家族。

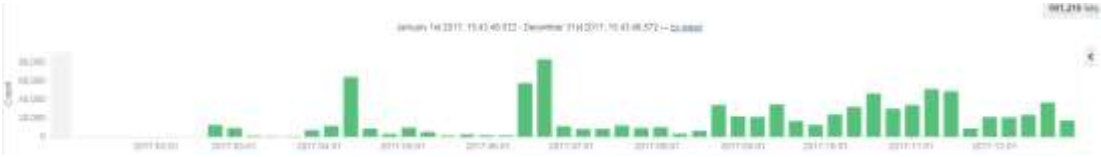

图 23　Nitol 年度威胁情报时间分布

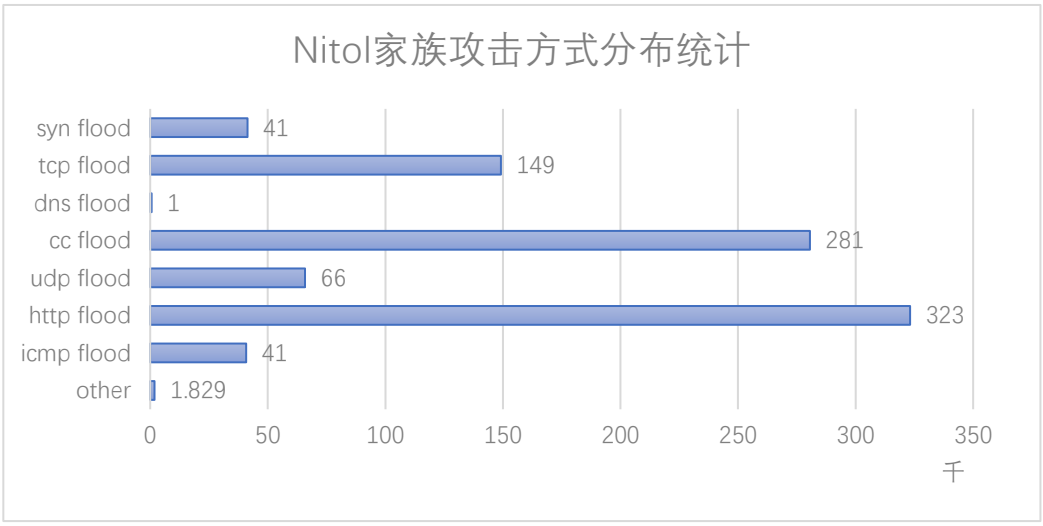

图 24　Nitol 家族攻击方式分布统计

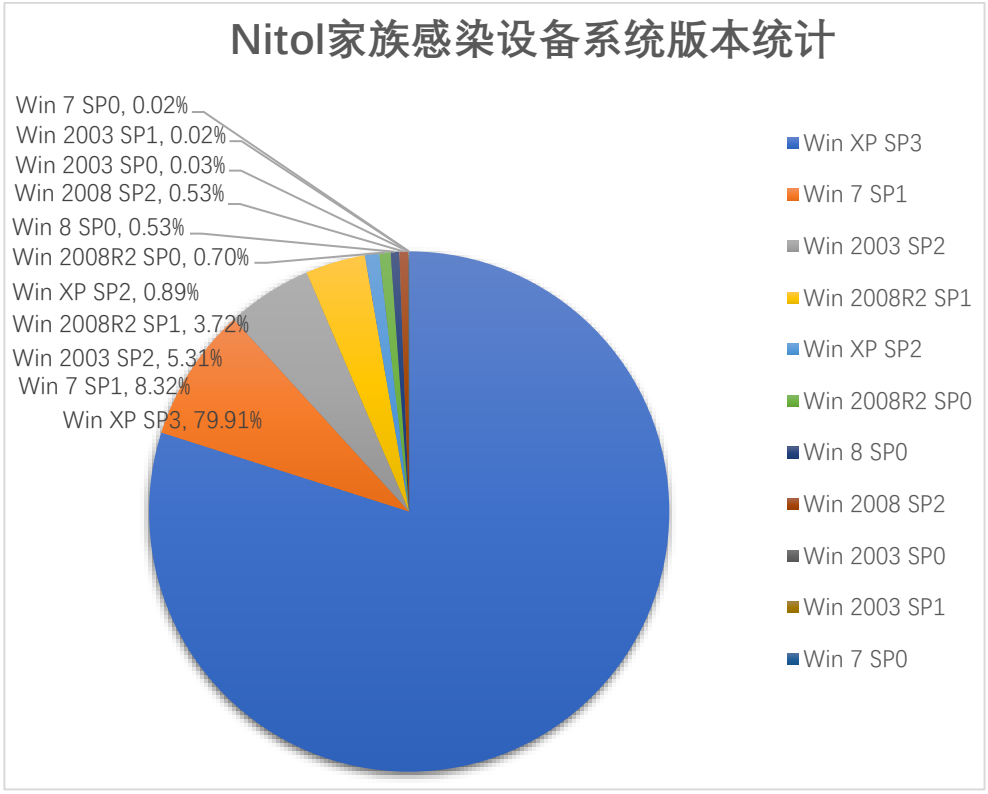

图 25　Nitol 家族感染设备系统版本统计

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”设备类型上看，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 系统版本上（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办公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、SIMPLE 等物联网系统架构。因此，平台的兼容性为 Dofloo 家族的僵尸网络“肉鸡”基数放大不少；同时，还发现黑客通过 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“肉鸡群”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。

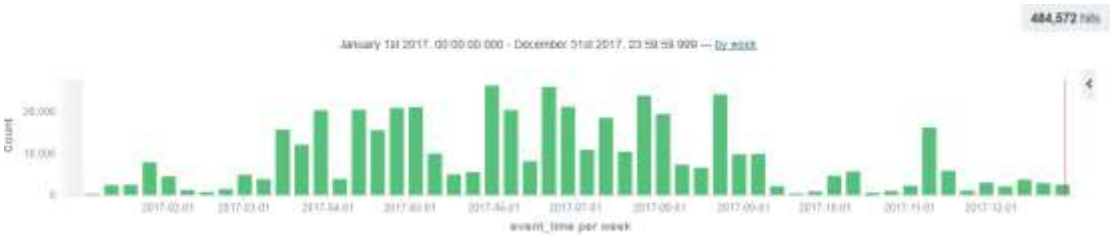

图 26 Dofloo 年度威胁情报时间分布

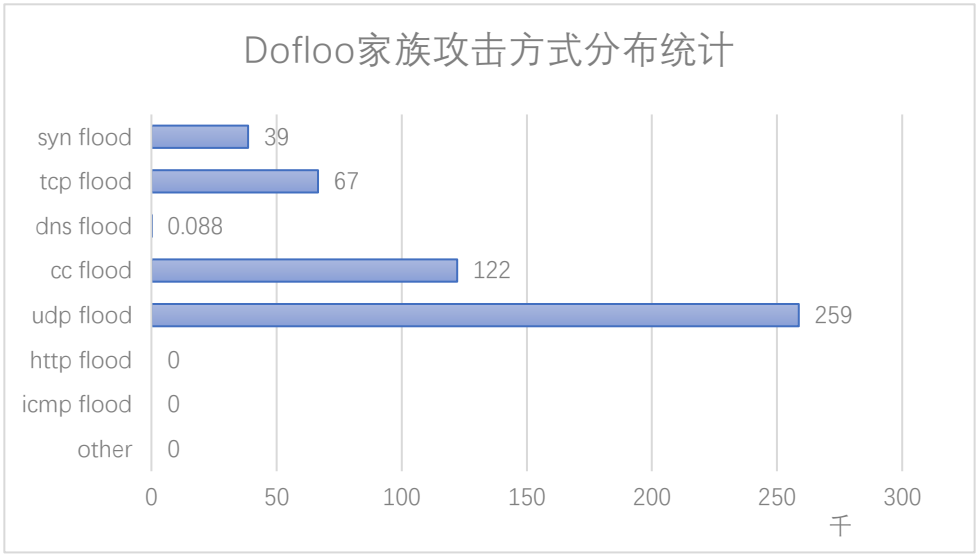

图 27 Dofloo 家族攻击方式分布统计

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。

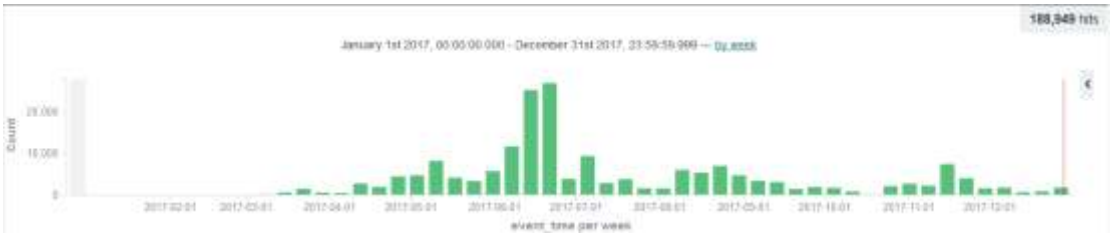

图 28 Mirai 年度威胁情报分布

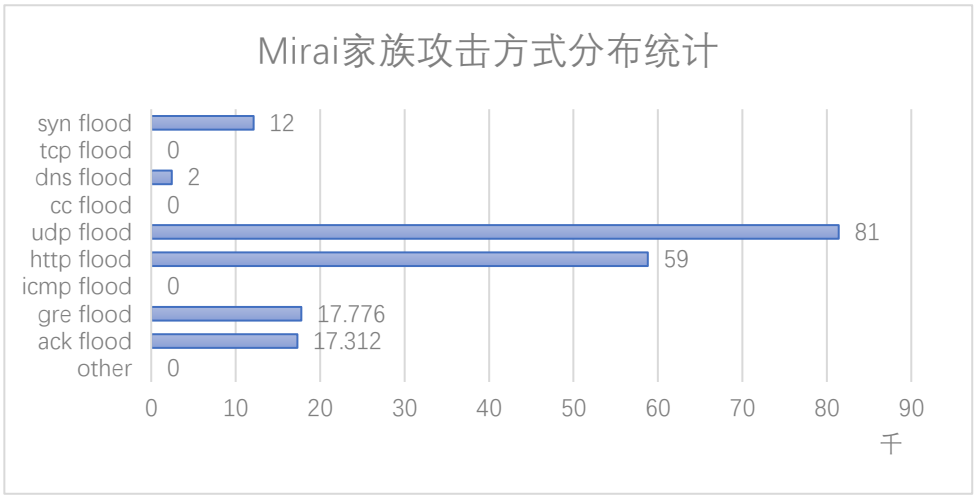

图 29 Mirai 家族攻击方式分布统计

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、5555、6767、37215 和 52869 等，涉及到的物联网设备厂商有 Dahua、Huawei、D-Link、WIFICAM、Linksys、Avtech、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，虽然下半年的 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%，而在后半年活跃趋势逐渐减弱，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 攻击的攻击方式，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 月份，以 SYN flood 攻击方式发起的攻击高达 1586 万次。

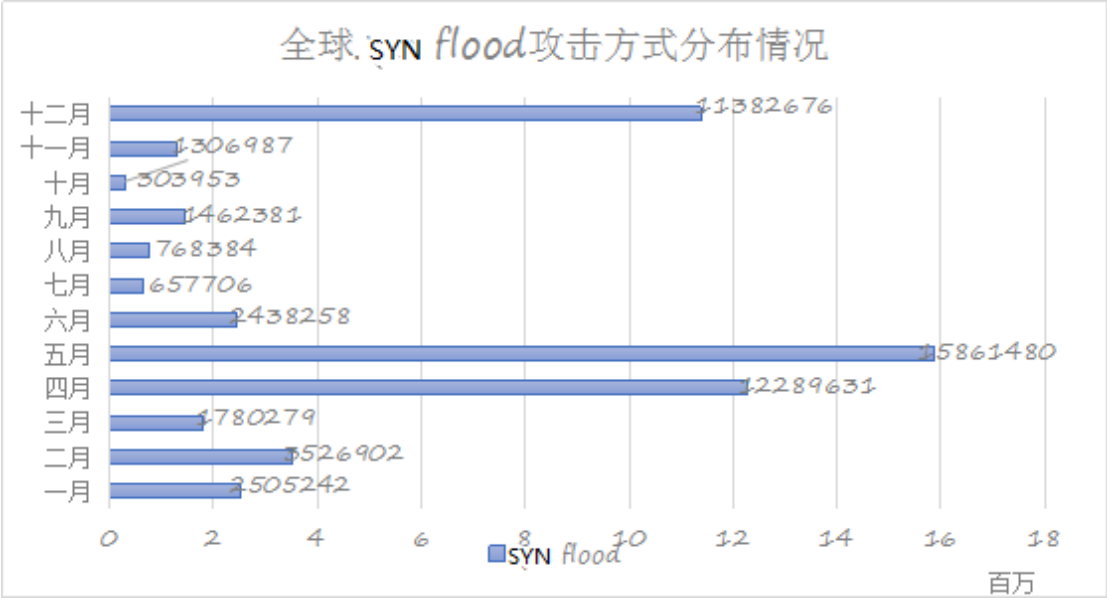

图 30　全球 SYN flood 攻击方式分布情况

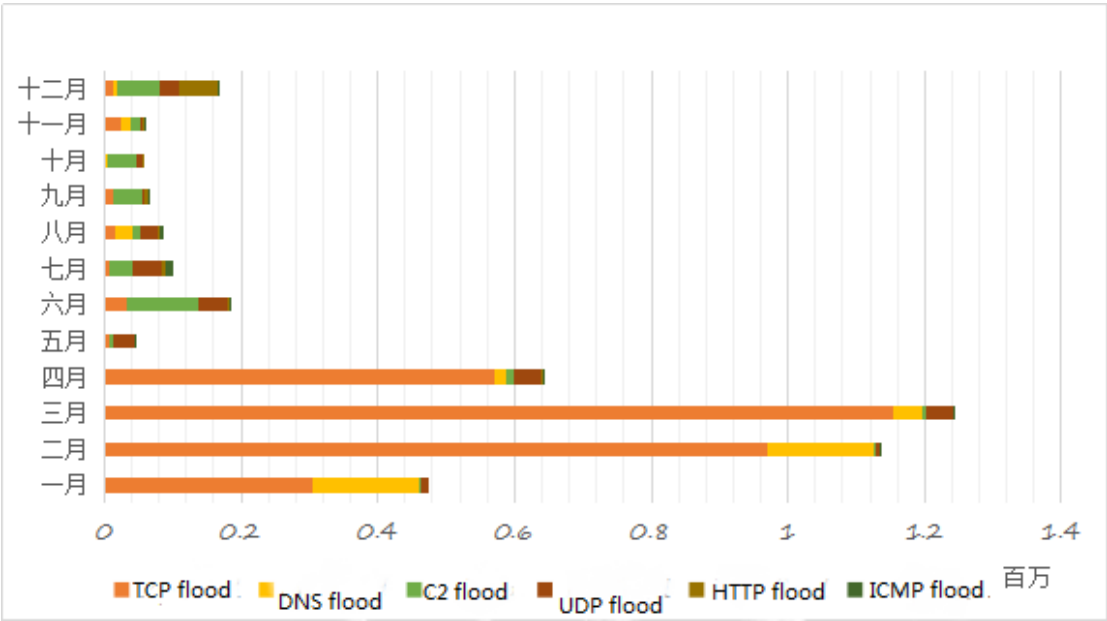

图 31　全球 TCP、DNS、C2、UDP、HTTP、ICMP flood 攻击方式分布统计

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，占总比的 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%。

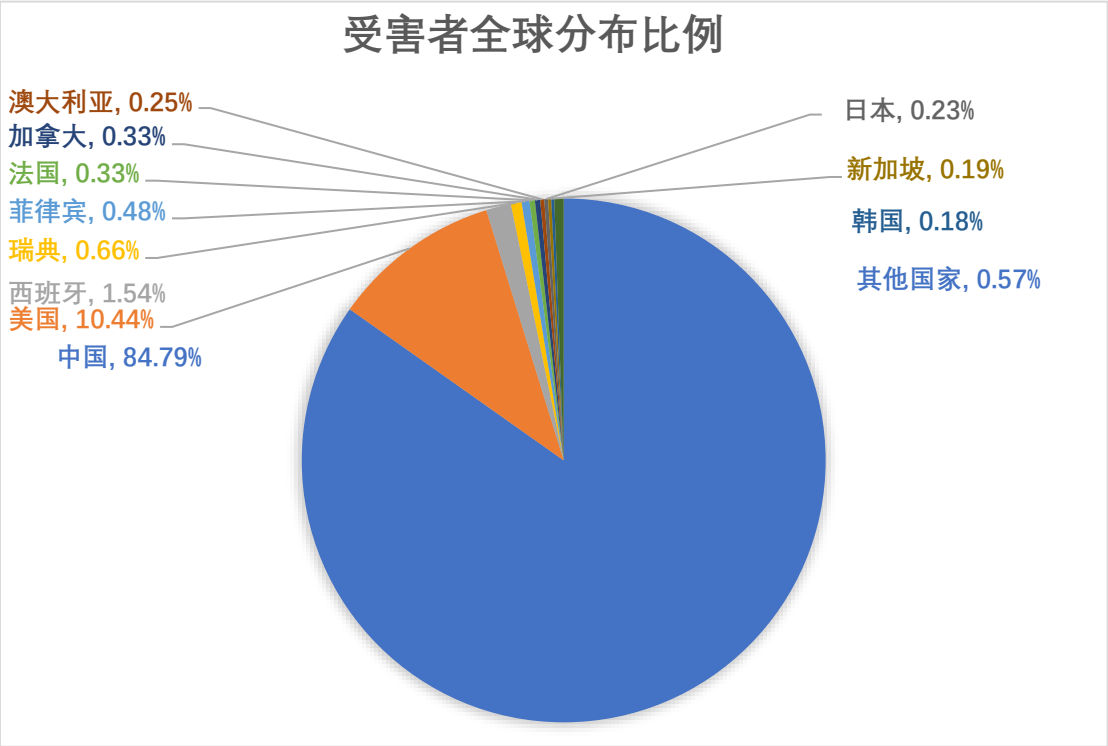

图 32　受害者全球分布比例

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%。

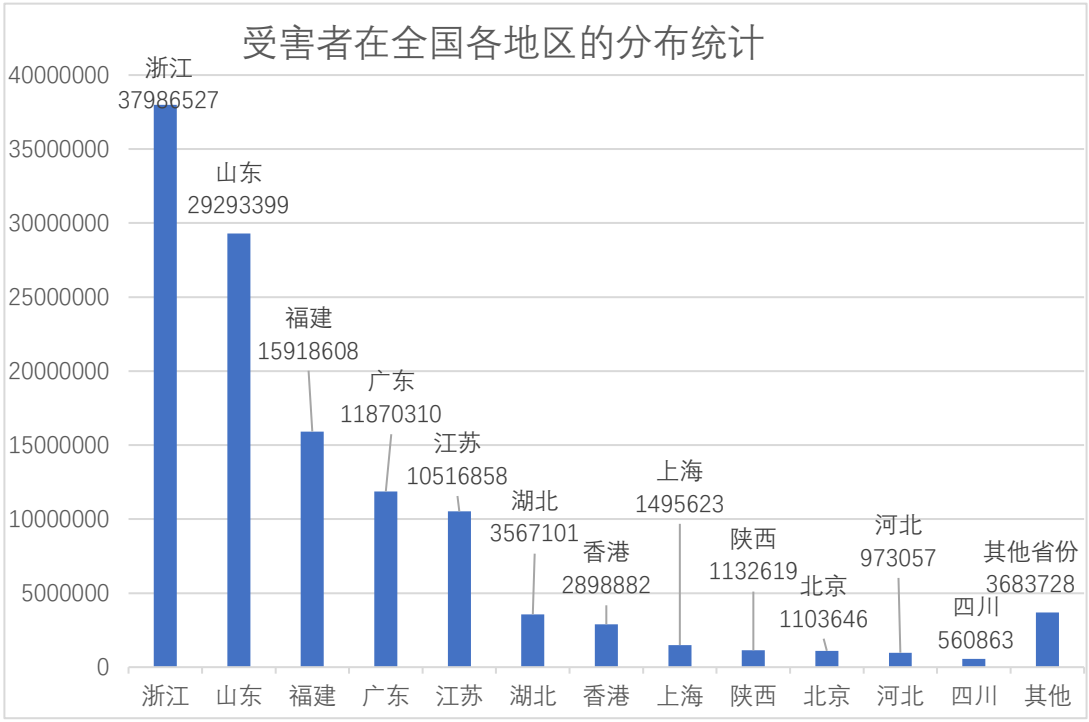

图 33　受害者在全国各地区的分布统计

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 对全国各地发起的 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%。

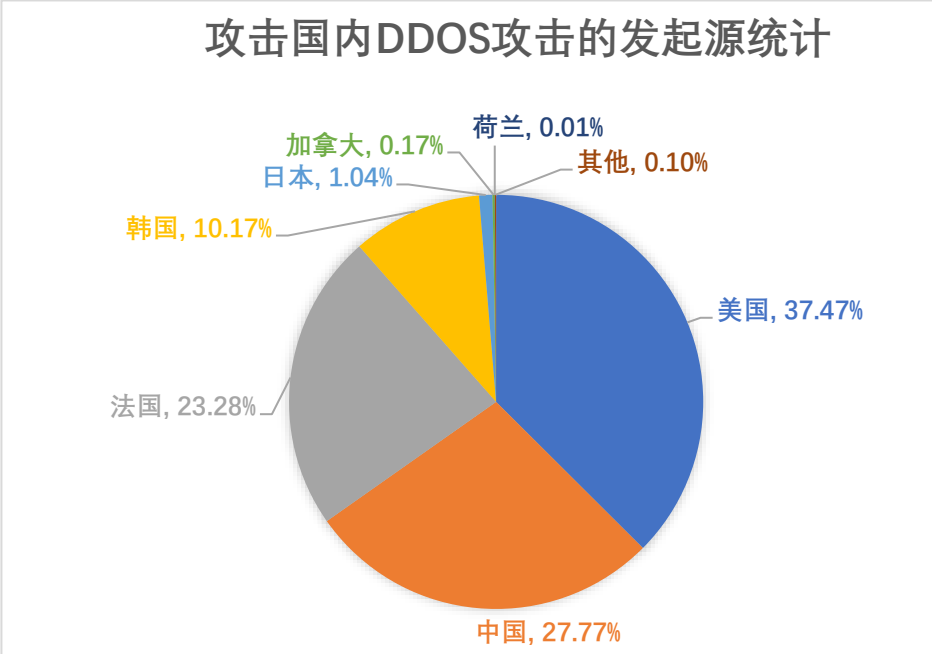

图 34　攻击国内 DDoS 攻击的发起源统计

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%。

商家之间的恶意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。

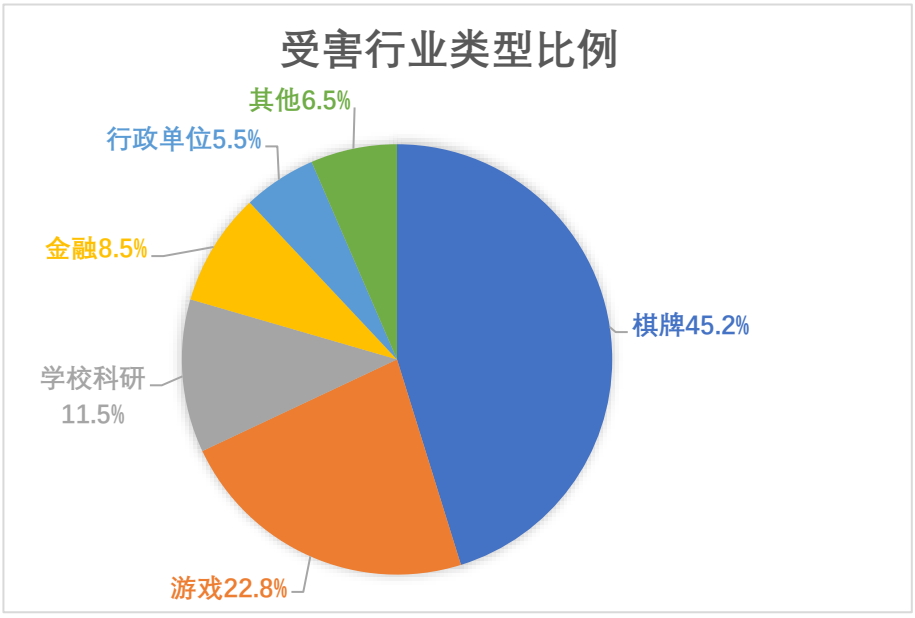

图 35　受害行业类型比例

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”最多，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。在统计数据中，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“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“肉鸡”的“抓取”。

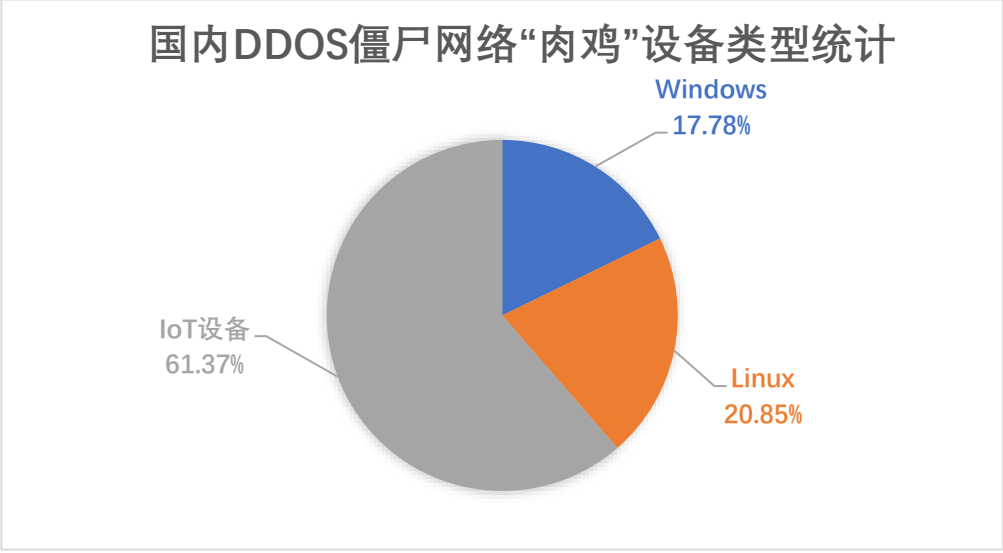

图 37 国内 DDoS 僵尸网络“肉鸡”设备类型统计

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 定位进行汇总分析，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 个和 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。

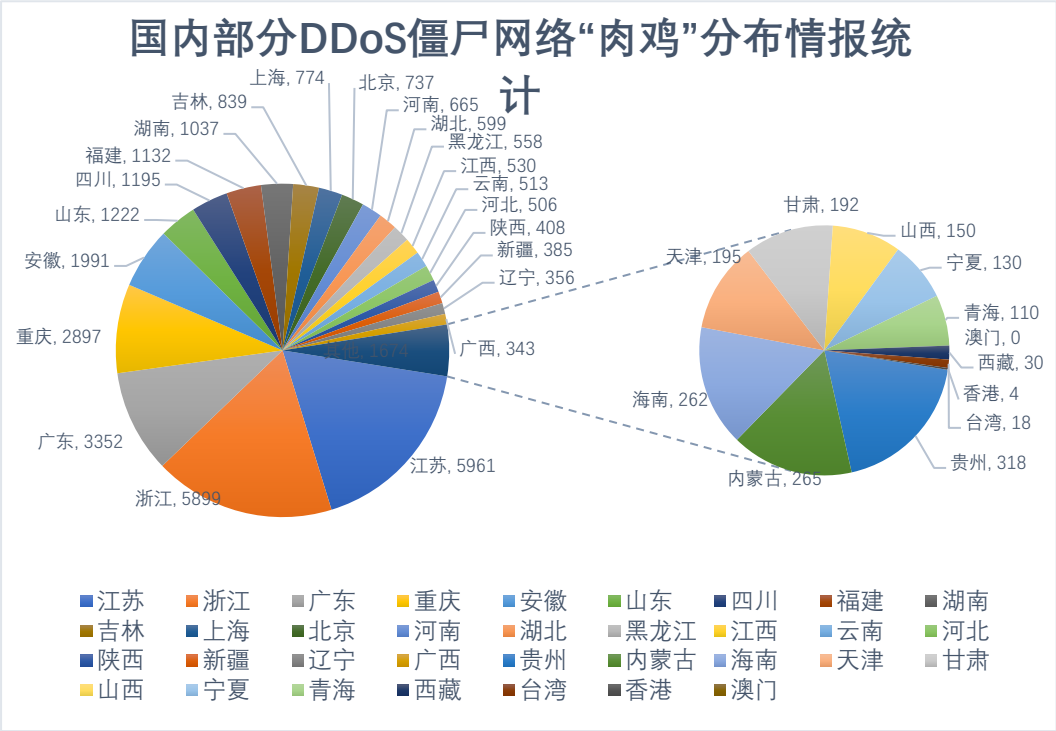

图 38　国内部分 DDoS 僵尸网络“肉鸡”分布情报统计

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、小范围网络，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 攻击无疑是一个巨大的安全隐患。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，利用物联网设备组建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。

附录一 参考资料

[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

附录二 关于安天

安天是专注于威胁检测防御技术的领导厂商。安天以提升用户应对网络空间威胁的核心能力、改善用户对威胁的认知为企业使命，依托自主先进的威胁检测引擎等系列核心技术和专家团队，为用户提供端点防护、流量监测、深度分析、威胁情报和态势感知等相关产品、解决方案与服务。

安天的监控预警能力覆盖全国、产品与服务辐射多个国家。安天将大数据分析、安全可视化等方面的技术与产品体系有效结合，以海量样本自动化分析平台延展分析师团队作业能力、缩短产品响应周期。安天结合多年积累的海量安全威胁知识库，综合应用大数据分析、安全可视化等方面经验，推出了可抵御各类已知和未知威胁的多样化解决方案。

全球超过一百家以上的著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的威胁检测引擎目前已为全球近十万台网络设备和网络安全设备、超过八亿部移动终端设备提供安全防护，其中安天移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品，并在国际权威认证机构 AV-C 的 2015 年度移动安全产品测评中，成为全球唯一两次检出率均为 100%的产品。

安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续五届蝉联国家级网络安全应急服务支撑单位资质，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。

安天是中国应急响应体系中重要的企业节点，在红色代码 II、口令蠕虫、震网、破壳、沙虫、方程式、白象、魔窟等重大安全事件中，安天提供了先发预警、深度分析或系统的解决方案。

安天实验室更多信息请访问： http://www.antiy.com（中文）

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com