我国联网智能设备安全情况报告

（2018 年第一季度）

国家计算机网络应急技术处理协调中心

2018 年 4 月

2018 年第一季度，CNCERT 继续对联网智能设备安全情况开展跟踪监测和数据分析，发现联网智能设备（以下简称“智能设备”或“IOT 设备”）在安全漏洞、恶意代码攻击活动等方面主要表现出如下特点:

1、在安全漏洞方面，智能设备漏洞数量继续大幅增加。国家信息安全漏洞共享平台（CNVD）2018 年第一季度公开收录智能设备通用型漏洞 644 个，较去年同期增长 76%。按漏洞类型统计,权限绕过、信息泄露、命令执行漏洞数量位列前三，分别占公开收录漏洞总数的 20%、17%、16%。手机设备、路由器、网络摄像头、智能监控平台、防火墙等类型设备漏洞数量较多，是漏洞利用的重要目标。

2、在恶意代码攻击活动方面，境外控制服务器控制了我国境内大量智能设备，每日活跃受控设备 IP 地址和控制服务器 IP 地址的数量较 2017 年下半年有所上升。CNCERT 抽样监测发现 2018 年第一季度我国境内感染恶意代码的智能设备 IP 地址数量约 52.7 万，位于浙江、河南、山东、江苏、河北的 IP 地址占比较大。控制我国智能设备的境外控制服务器 IP 地址数量约 1.08 万个，位于美国、俄罗斯、日本的 IP 地址占比较大。受控设备规模在 1 万以上的智能设备僵尸网络有 13 个，受控设备规模在 5 万以上的僵尸网络有 3 个。每日活跃的受控智能设备 IP 地址平均数量约 2.8 万个、控制服务器 IP 地址平均数量 288 个，分别较 2017 年下半年有所上升。

一、智能设备漏洞收录情况

智能设备存在的软硬件漏洞可能导致设备数据和用户信息泄露、设备瘫痪、感染木马僵尸网络恶意代码、被用作跳板攻击内网主机或其他信息基础设施等安全风险。2018 年第一季度，CNVD 持续对智能设备（IOT 设备）漏洞开展跟踪、收录和通报处置。

（一）通用型漏洞收录情况

通用型漏洞一般是指对某类软硬件产品都会构成安全威胁的漏洞。2018 年第一季度 CNVD 收录通用型 IOT 设备漏洞 644 个，与去年同期的 366 个相比增长 76%。按收录漏洞所涉及厂商、漏洞的类型、影响的设备类型统计如下:

漏洞涉及厂商包括谷歌、华为、思科、普联、施耐德等厂商。其中，收录谷歌 IOT 设备漏洞 164 条，占全季度 IOT 设备漏洞的 25%；华为位列第二，共收录 82 条；思科和普联分列第三和第四，如图 1 所示。

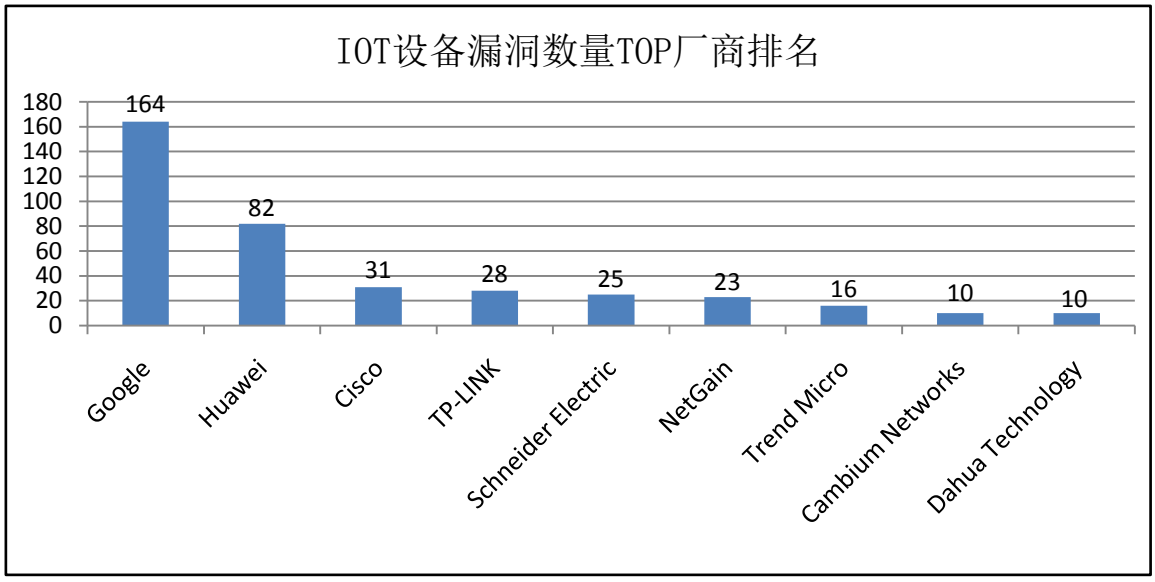

图 1 IOT 设备漏洞数量 TOP 厂商排名

漏洞类型包括权限绕过、信息泄露、命令执行、跨站、拒绝服务、缓冲区溢出、SQL 注入、文件上传、设计缺陷等漏洞。其中，权限绕过、信息泄露、命令执行漏洞数量位列前三，分别占公开收录漏洞总数的 20%、17%、16%，如图 2 所示。

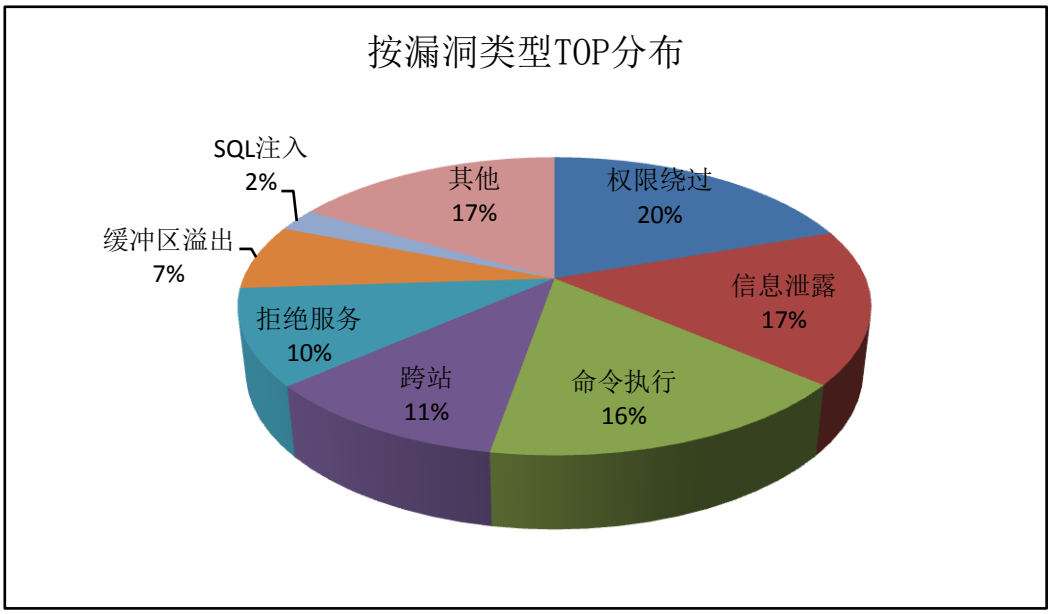

图 2 按漏洞类型 TOP 分布

漏洞影响的设备类型包括手机设备、路由器、网络摄像头、

智能监控平台、防火墙、网关设备、交换机、会议系统等。其中，手机设备、路由器、网络摄像头的数量位列前三，分别占公开收录漏洞总数的 28%、18%、17%，如图 3 所示。

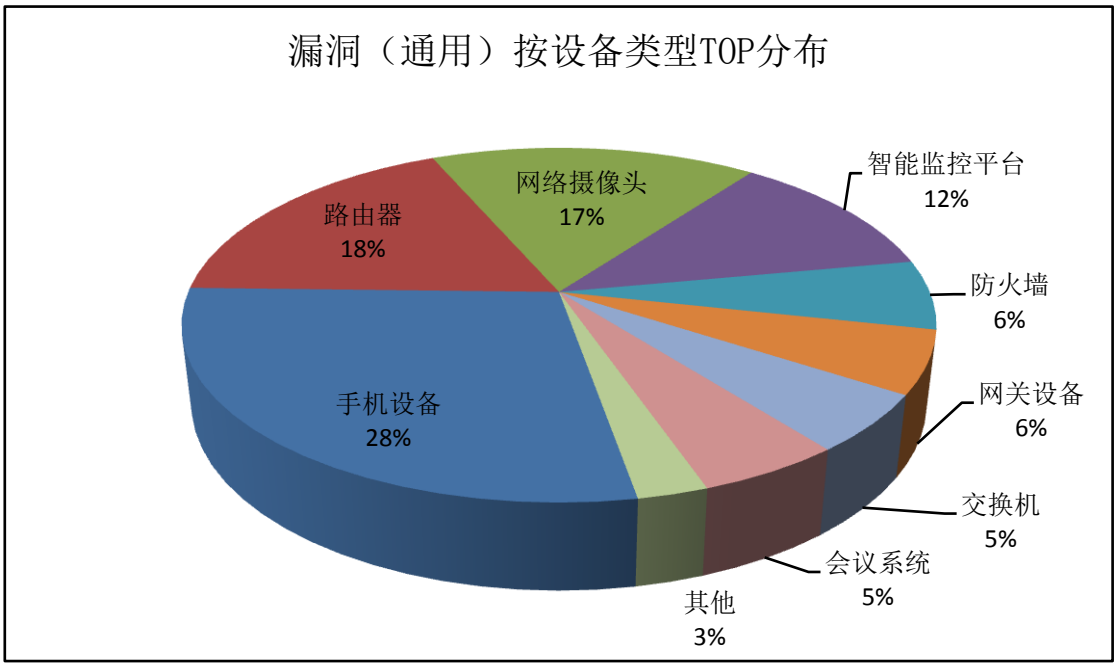

图 3 漏洞（通用）按设备类型 TOP 分布

（二）事件型漏洞收录情况

事件型漏洞一般是指对一个具体应用构成安全威胁的漏洞。2018 年第一季度 CNVD 收录 IOT 设备事件型漏洞 44 个，影响的设备包括智能监控平台、网络摄像头、GPS 设备、路由器、网关设备、防火墙、会议系统、一卡通、打印机、交换机等。其中，智能监控平台、网络摄像头、会议系统漏洞数量位列前三，分别占公开收录漏洞总数的 27%，18%，15%，如图 4 所示。

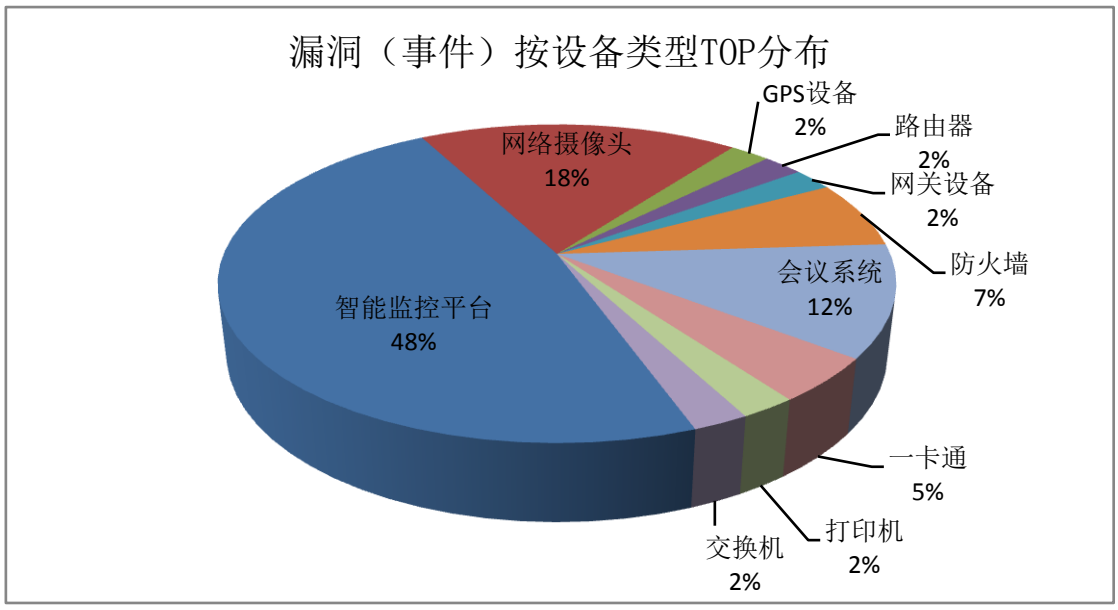

图 4 漏洞（事件型）按设备类型 TOP 分布

二、智能设备恶意代码攻击活动情况

（一）恶意代码活动总体监测情况

2018 年第一季度，CNCERT 继续对智能设备相关的 Gafgyt、MrBlack、Tsunami、Mirai、Reaper、Ddostf、Satori、TheMoon 等流行恶意代码的网络攻击活动开展抽样监测，详细情况如下。

1、恶意代码控制服务器数量及分布情况

2018 年第一季度 CNCERT 抽样监测发现智能设备恶意代码控制服务器 IP 地址累计数量约 1.23 万个，位于境外的控制服务器 IP 地址约占 88.1%，该比例较去年有所上升，其中位于美国（3696 个）、俄罗斯（740 个）和日本（725 个）的 IP 地址位列前三，详细分布如图 5 所示。位于我国境内的控制服务

器 IP 地址数量为 1467 个，排名前三的省市依次是河南 273 个、北京 156 个、广东 130 个。

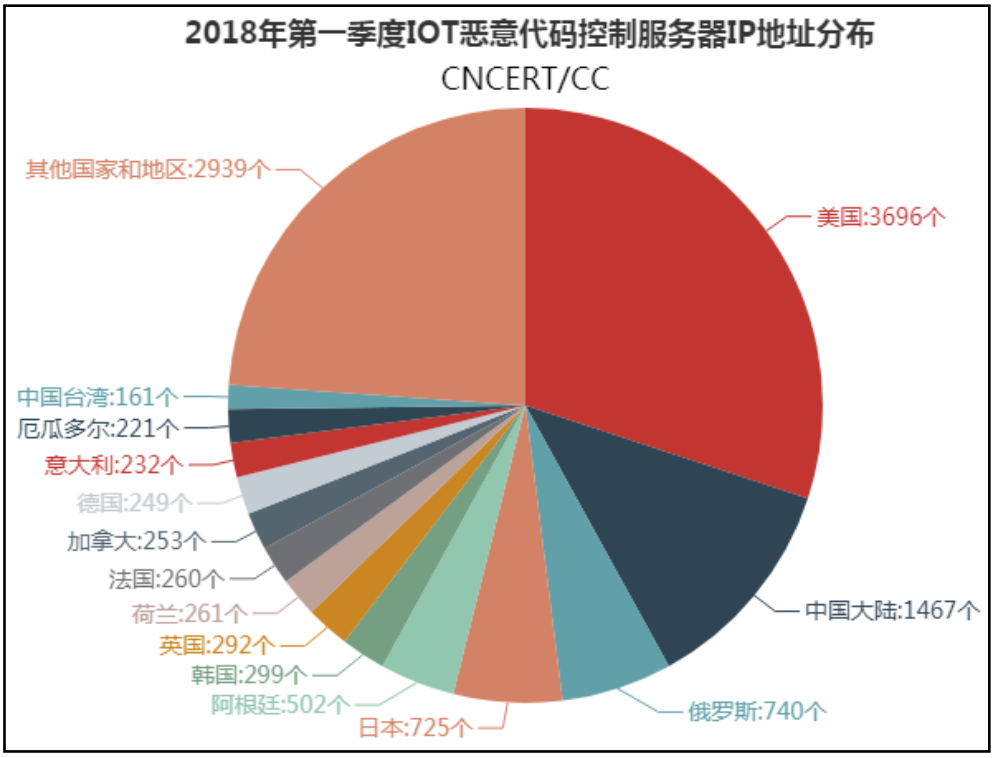

图 5 2018 年第一季度 IOT 恶意代码控制服务器 IP 地址分布

2、受控设备数量及分布情况

2018 年第一季度，CNCERT 抽样监测发现的受控智能设备 IP 地址累计数量为 159.5 万个，位于我国境内的受控 IP 数量为 52.7 万，占比约 33.1%，其中受控 IP 地址数量在 2 万以上的地区依次是浙江、河南、山东、江苏、河北、辽宁、广东、重庆，详细分布如图 6 所示。

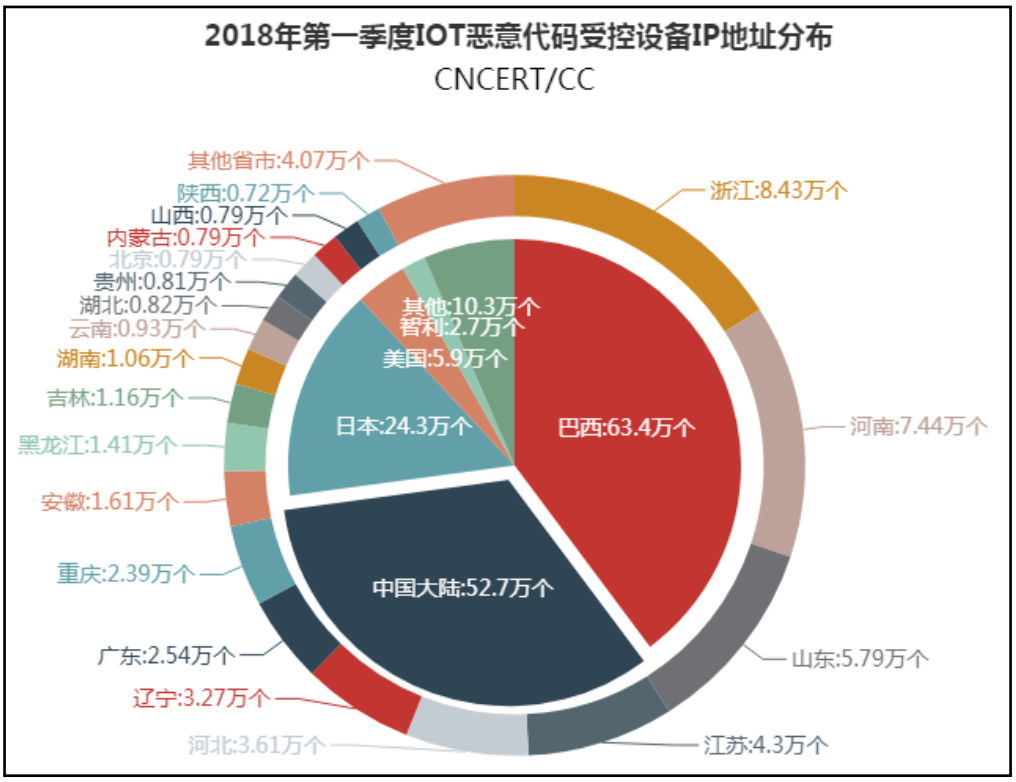

图 6 2018 年第一季度 IOT 恶意代码受控设备 IP 地址分布

3、木马僵尸网络规模统计分析

CNCERT 对智能设备木马僵尸网络规模进行分析，2018 年第一季度智能设备木马僵尸网络控制规模(单个控制服务器所控制的受控设备 IP 地址的累计数量）在 1 千以上的僵尸网络有 143 个，在 1 万以上的僵尸网络有 13 个，在 5 万以上的僵尸网络有 3 个。规模较大的僵尸网络控制端主要分布在荷兰、西班牙、俄罗斯、美国、法国、加拿大、意大利、中国大陆等国家或地区，详细情况见表 1。

表 1　2018 年第一季度智能设备木马僵尸网络控制规模统计情况

木马僵尸网络控制规模	木马僵尸网络个数（按控制端 IP 地址统计）	木马僵尸网络控制端 IP 地址地理位置分布
5 万以上	3	荷兰、西班牙和中国大陆各 1 个
1 万至 5 万	10	俄罗斯 3 个、中国大陆 2 个，罗马尼亚、意大利、加拿大、荷兰和瑞典各 1 个
5 千至 1 万	13	法国 4 个、加拿大 3 个、俄罗斯 2 个，卢森堡、荷兰、泰国和南非各 1 个
1 千至 5 千	117	美国 40 个、荷兰 15 个、法国 13 个、加拿大 11 个、俄罗斯 10 个、意大利 8 个、英国 3 个、欧盟 3 个、罗马尼亚 2 个、新加坡 2 个、中国 2 个，摩尔多瓦、拉脱维亚、保加利亚、西班牙、乌克兰、韩国、波兰、捷克各 1 个
100 至 1000	297	美国 129 个、意大利 39 个、荷兰 21 个、加拿大 19 个、法国 18 个、俄罗斯 16 个、德国 9 个、罗马尼亚 7 个、英国 6 个、印度 5 个、西班牙 4 个、新加坡 4 个、欧盟 4 个、中国大陆 4 个、保加利亚 3 个、瑞士 2 个，巴布亚新几内亚、澳大利亚、拉脱维亚、葡萄牙、立陶宛、孟加拉、乌克兰各 1 个

4、恶意代码攻击活动变化趋势

2018 年第一季度，CNCERT 抽样监测发现每日活跃的受控智能设备 IP 地址平均数量约 2.8 万个、控制服务器 IP 地址平均数量 288 个，分别较 2017 年下半年有所上升。恶意代码攻击活动处于持续活跃态势，1 月 10 日至 1 月 12 日、1 月 22 日至 1 月 24 日、2 月 8 日至 2 月 15 日恶意代码攻击活动更加频繁，其中 1 月 10 日的单日活跃受控 IP 地址数量达到峰值 35731 个、2 月 14 日的单日活跃控制服务器 IP 地址数量达到峰值 550 个，如图 7 所示。

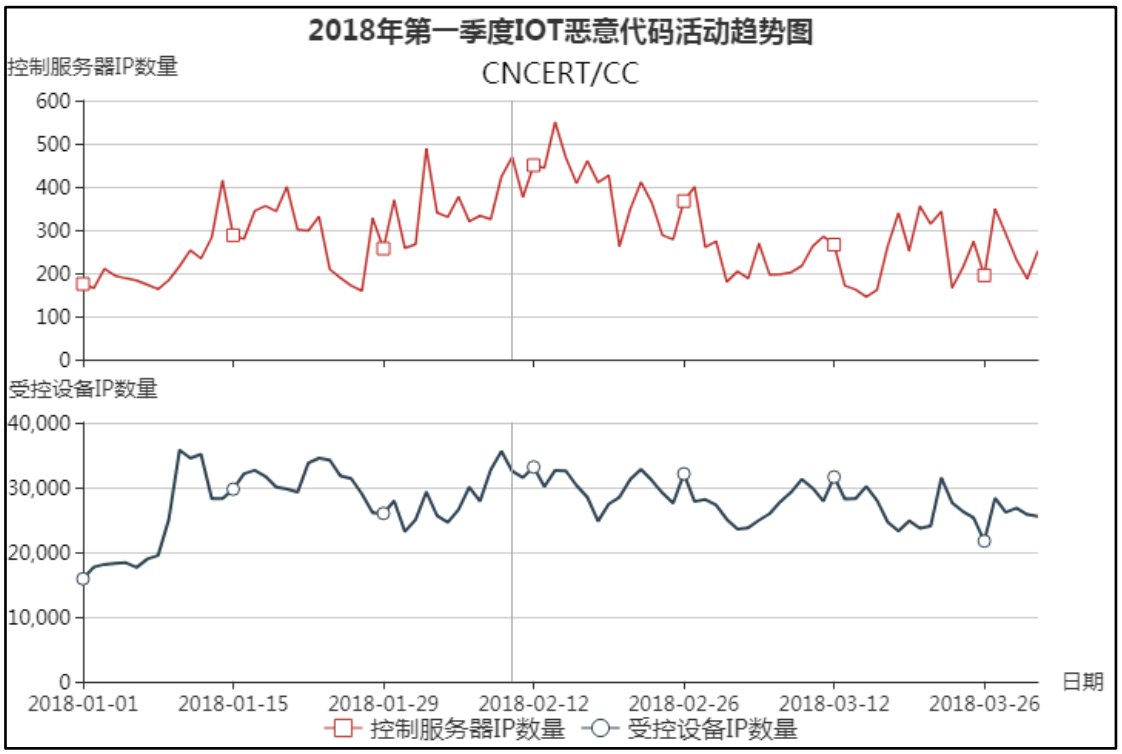

图 7 2018 年第一季度 IOT 恶意代码攻击活动变化趋势

（二）典型恶意代码活动的监测情况

以下是在境内感染量较大的 Gafgyt、Mirai 等典型恶意代码的网络攻击监测情况。

1、Gafgyt 恶意代码监测情况

Gafgyt 恶意代码的通用命名为 Backdoor.Linux.Gafgyt。2018 年第一季度，CNCERT 对 Gafgyt 僵尸网络攻击活动开展抽样监测，共发现活跃控制服务器 IP 地址 990 个，疑似被控 IP 地址 27.32 万个。这些控制服务器向疑似被控 IP 地址发送 DDoS 攻击指令，分别对境内外约 3.8 万个 IP 地址实施 UDP Flood（占比 89.7%）、TCP SYN Flood（占比 10.2%）等类型分布式拒绝服务攻击。

CNCERT 抽样监测数据显示，Gafgyt 木马僵尸网络的受控端 IP 地址绝大多数位于境内，约 27 万个（占比高达 98.8%），其中位于山东、河南、浙江、辽宁、河北等省受控端 IP 地址规模都在 2 万以上，国内各省（市、区）具体分布如图 8 所示。

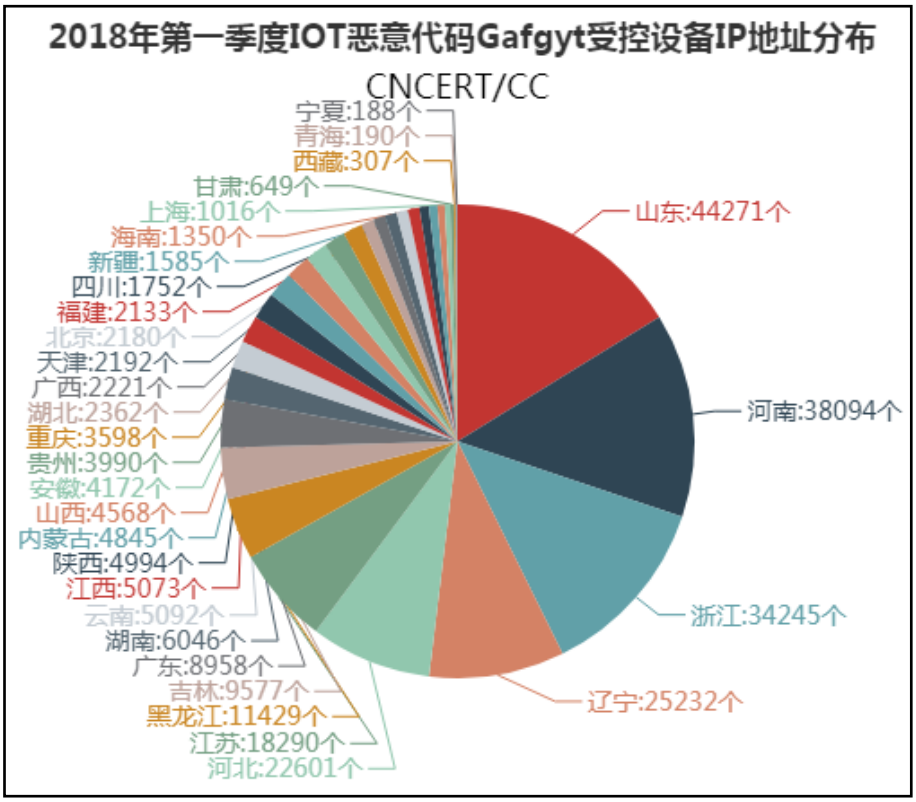

图 8 2018 年第一季度 IOT 恶意代码 Gafgyt 受控设备 IP 地址分布

Gafgyt 木马僵尸网络控制服务器 IP 地址绝大多数位于境外，主要分布在美国、意大利、荷兰、加拿大等国家或地区，主要分布情况与 2017 年下半年大致相同，详细数据见图 9。

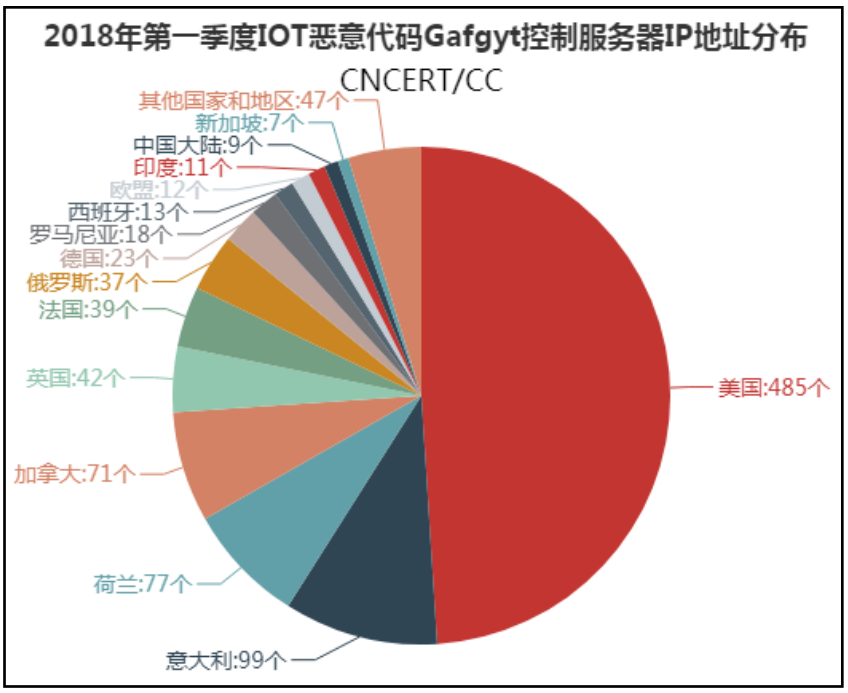

图 9 2018 年第一季度 IOT 恶意代码 Gafgyt 控制服务器 IP 地址按国家或地区分布

2、Mirai 恶意代码监测情况

Mirai 恶意代码的通用命名为 Trojan[DDoS]/Linux.Mi-rai。2018 年第一季度，CNCERT 对 Linux.Mirai 木马僵尸程序网络攻击情况进行抽样监测，共发现控制服务器 IP 地址 1052 0 个，疑似被控智能设备 IP 地址约 18.8 万个，主要恶意代码下载服务器 IP 地址 260 个。恶意代码下载方式主要为 telnet 远程执行 wget 或 tftp 下载，下载文件恶意代码文件名主要是 mirai.arm7、mirai.arm、mirai.mips、mirai.x86 和 mirai.ppc，恶意代码下载后启动名称主要包括 dvrHelper（占比 47.5%）、dvrpelper（占比 44.5%）、Wordmemy（占比 6.7%）、WsGA4@F6F（<1%）、McLuvin（<1%）、zxcvbnm（<1%）。从 Mirai 源代码和恶意代码文件名上可以看出 Mirai 支持多种硬件平

台。

CNCERT 监测发现的 Mirai 木马僵尸受控端 IP 地址绝大多数位于境内，如图 10 所示，受控端 IP 地址数量最多的是位于浙江、河南、重庆、江苏、广东、河北等省市，受控端 IP 地址数量均在 1 万以上，其中位于河南受控端数量增长趋势明显。境外受控端 IP 地址数量相对较多的是位于美国（2642 个）、日本（390 个）和英国（215 个）。

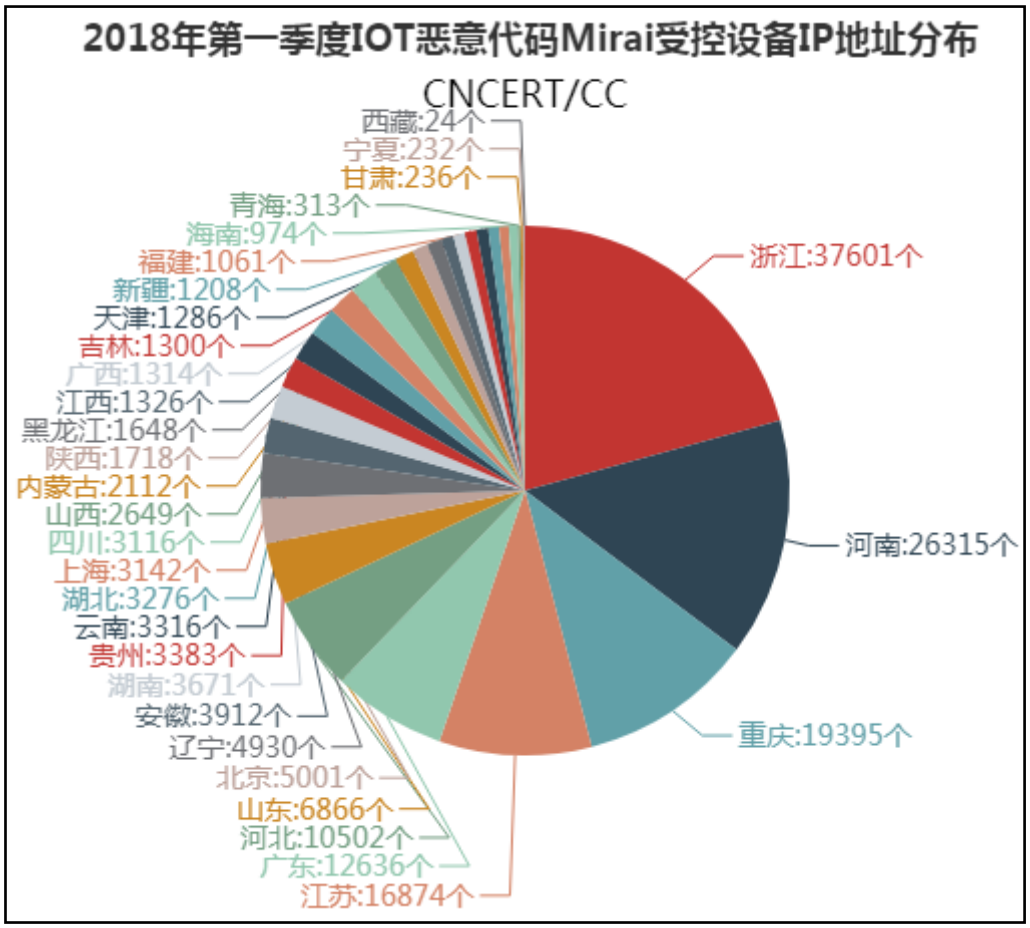

图 10 2018 年第一季度 Mirai 恶意代码受控设备 IP 地址分布

Mirai 木马僵尸程序控制端 IP 地址主要位于境外，排名前三的是美国 3066 个、日本 716 个、俄罗斯 696 个，如图 11 所示。位于中国大陆控制端 IP 地址 1084 个，主要分布在北京、

广东、江苏、浙江、上海、山东、辽宁等省市。

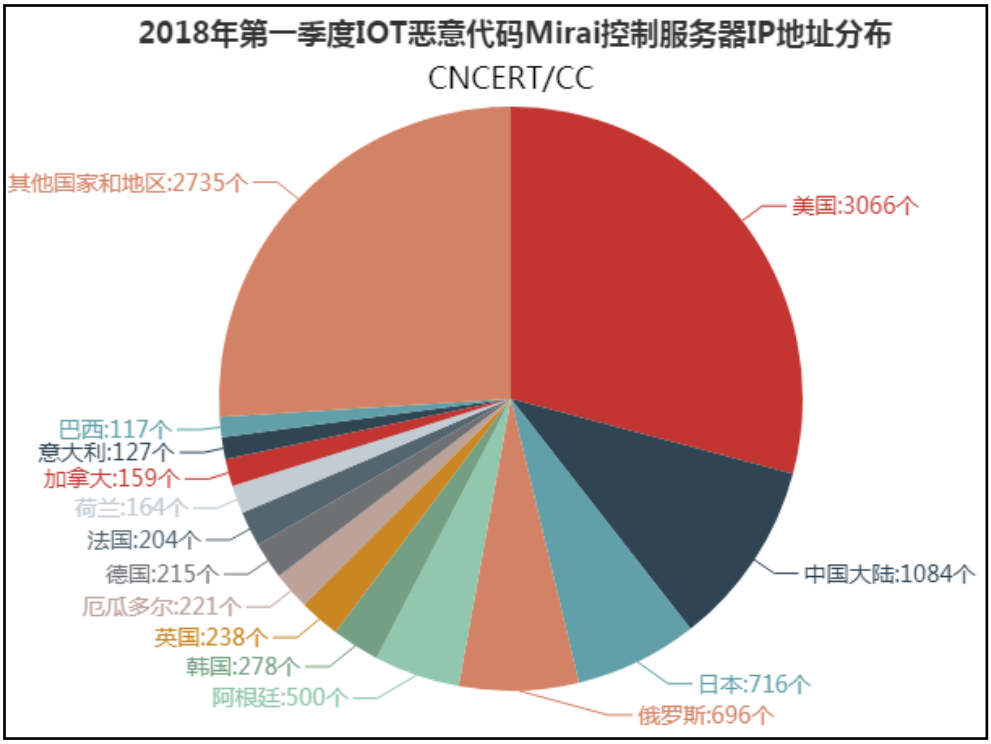

图 11　2018 年第一季度 Mirai 恶意代码控制服务器 IP 地址分布图