2020 年联网智能设备安全态势报告

2020 年，国家互联网应急中心（以下简称 CNCERT）运营的 CNVD 漏洞平台（国家信息安全漏洞共享平台）新增收录的通用联网智能设备漏洞数量呈显著增长趋势，同比增长 28%。联网智能设备恶意程序通过 P2P 方式传播非常活跃，具有传播速度快、感染规模大、追溯源头难的特点，预计将被越来越多的恶意程序所采用。联网智能设备僵尸网络控制规模增大，部分大型僵尸网络通过 P2P 传播方式与集中控制方式相结合对受控端进行控制，给治理工作带来一定难度。

1、联网智能设备漏洞态势

联网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、感染僵尸木马程序、被用作跳板攻击内网主机和其他信息基础设施等安全风险和问题。CNCERT 通过 CNVD 持续对联网智能设备的漏洞开展跟踪、收录和通报处置，主要情况如下。

1.1 通用型漏洞收录情况

2020 年，CNVD 收录通用型联网智能设备漏洞 3047 个（同比上升 28%）。按收录漏洞的类型、影响的设备类型统计如下：

联网智能设备通用型漏洞数量按漏洞类型分类，排名前三位的是权限绕过、信息泄露和缓冲区溢出漏洞，分别占公开收录漏洞总数的 17.03%、13.32%、12.54%，如图 1 所示。

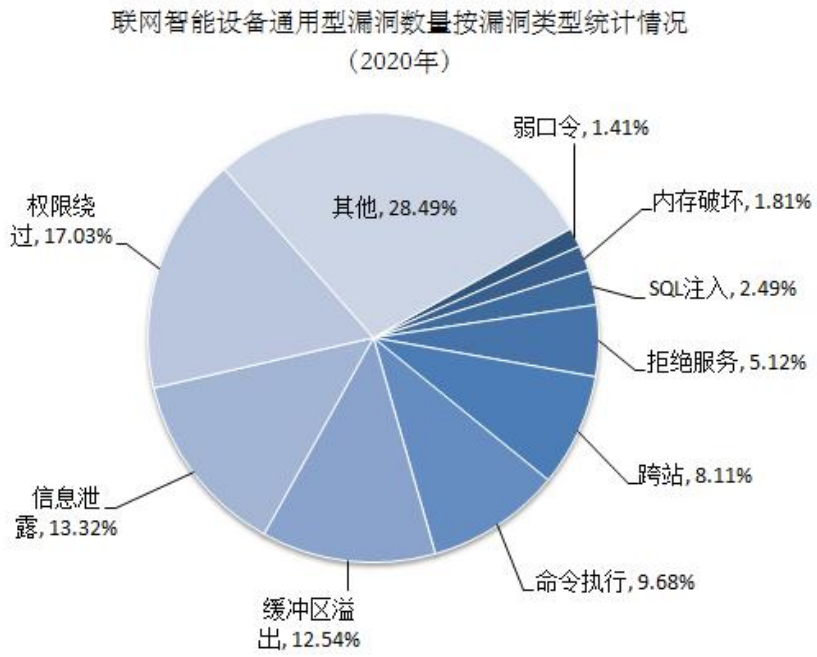

图 1 联网智能设备通用型漏洞数量按漏洞类型统计情况（2020 年）

联网智能设备通用型漏洞数量按设备类型分类，排名前三位的是手机设备、路由器和智能监控平台，分别占公开收录漏洞总数的38.33%、20.97%、19.53%，如图 2 所示。

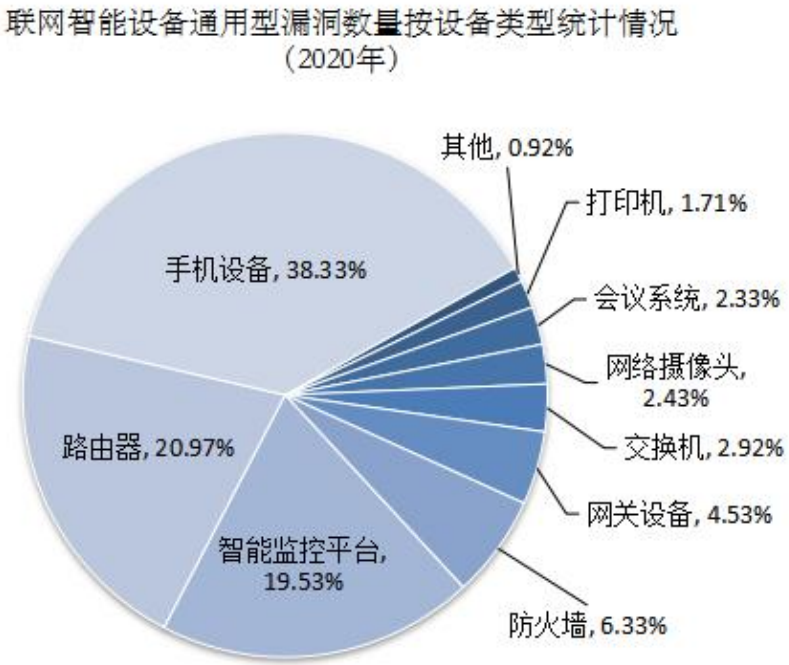

图 2 联网智能设备通用型漏洞数量按设备类型统计情况

1.2、事件型漏洞收录情况

2020 年，CNVD 收录联网智能设备事件型漏洞 2141 个。按设备类型分类，排名前三位的是智能监控平台、网络摄像头和防火墙，分别占公开收录漏洞总数的 44.84%、31.62%、9.34%，如图 3 所示。

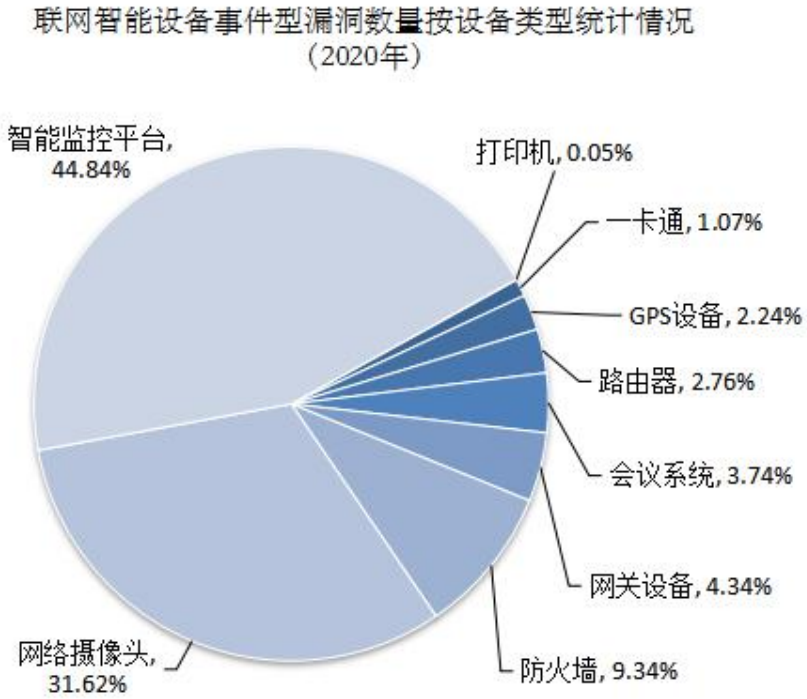

图 3 联网智能设备事件型漏洞数量按设备类型统计情况

2、联网智能设备恶意程序传播态势

CNCERT 对可用于感染、控制联网智能设备的恶意程序开展抽样监测分析，主要情况如下。

2.1 样本捕获情况

2020 年，CNCERT 捕获 341.10 万个联网智能设备恶意样本（同比上升 5.25%）。其中，排名前两位的为 Mirai、Gafgyt 家族及其变

种，占比分别为 77.48%和 13.86%,其他样本数量较多的家族还有 Tsunami、Mozi、Darknexus、Loligang、Hajime、Yakuza、Muhstik、Vpnfilter、Chalubo 等，如图 4 所示。

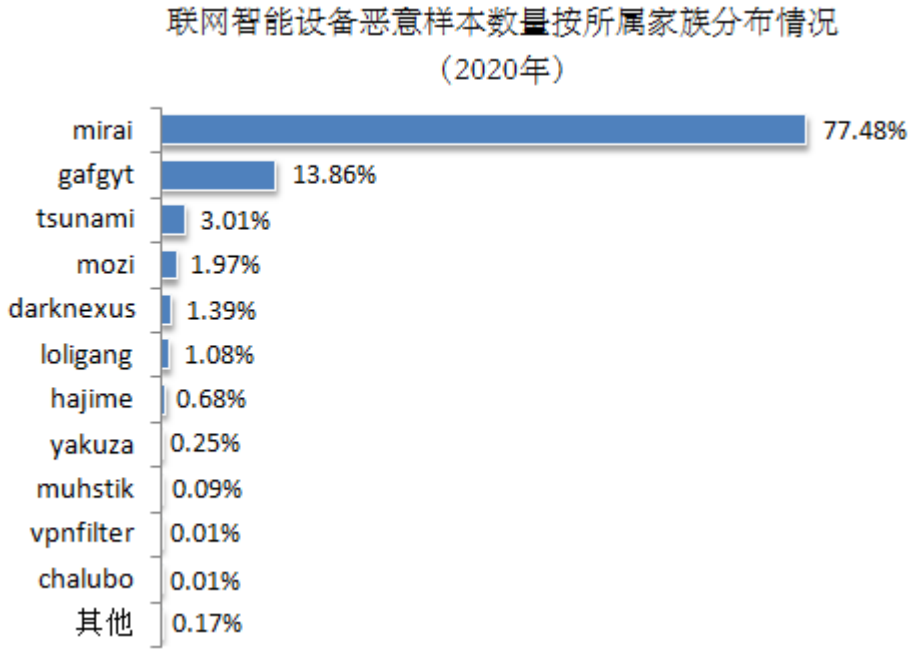

图 4 联网智能设备恶意样本数量按所属家族分布情况（2020 年）

联网智能设备恶意样本数量整体呈现上升态势，在 10 月出现峰值 74.94 万个（较 2019 年月度峰值增长 44.37%），如图 5 所示。

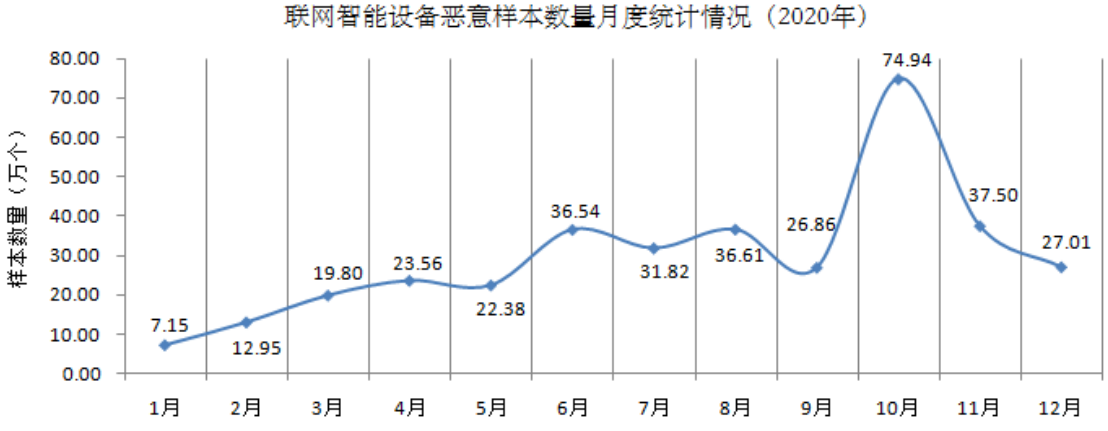

图 5 联网智能设备恶意样本数量按月统计情况（2020 年）

2.2 传播源监测情况

2020 年，CNCERT 监测发现 51.99 万个联网智能设备恶意程序传播源 IP 地址。2020 年境外传播源 IP 数量大幅增长（同比上升 9 倍），其中 Mozi 家族通过 P2P 传播方式迅速扩大感染规模，成为境外传播源 IP 数量最多的家族，境外传播源 IP 数量较多的家族还包括 Mirai、Gafgyt、Hajime 等，如图 6 所示。

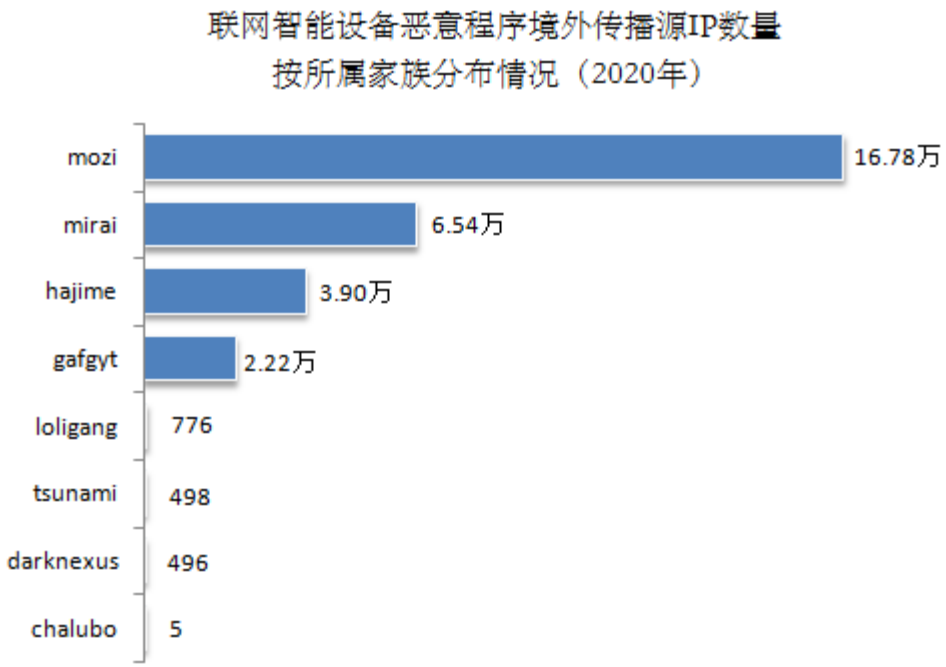

图 6 联网智能设备恶意程序传播源 IP 数量按所属家族分布情况（2020 年）

从境外传播源 IP 数量的趋势来看，9 月 Mozi 家族境外传播源 IP 数量突增，同一时期 Mirai 家族的境外传播源 IP 数量也显著增加（由于 Mozi 家族样本复用 Mirai 部分代码），如图 7 所示。

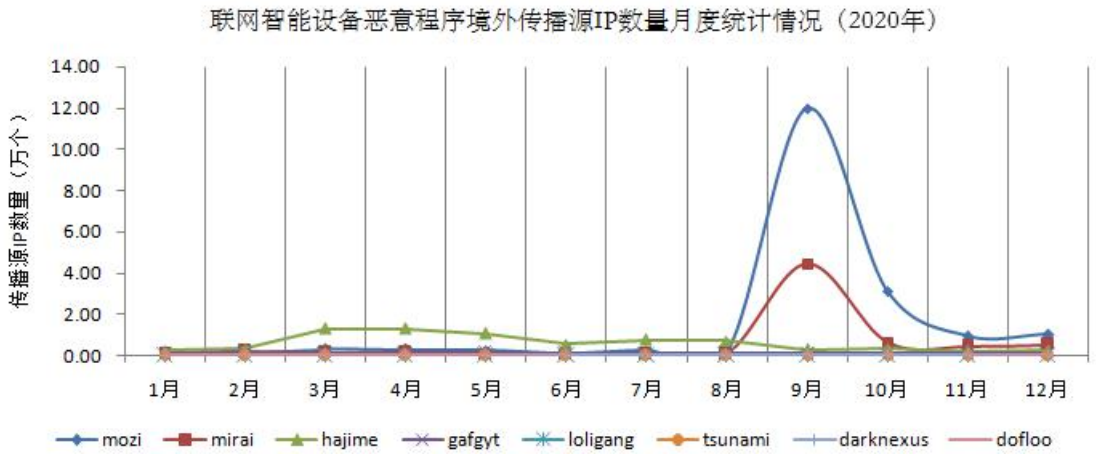

图 7 联网智能设备恶意程序境外传播源 IP 数量月度统计情况（2020 年）

2.3 下载端监测情况

2020 年，CNCERT 监测发现 132.18 万个境内 IP 地址下载联网智能设备恶意程序（同比下降 35.14%）。其中，排名前四位的为 Mirai、Gafgyt、Mozi、Hajime 家族及其变种，如图 8 所示。

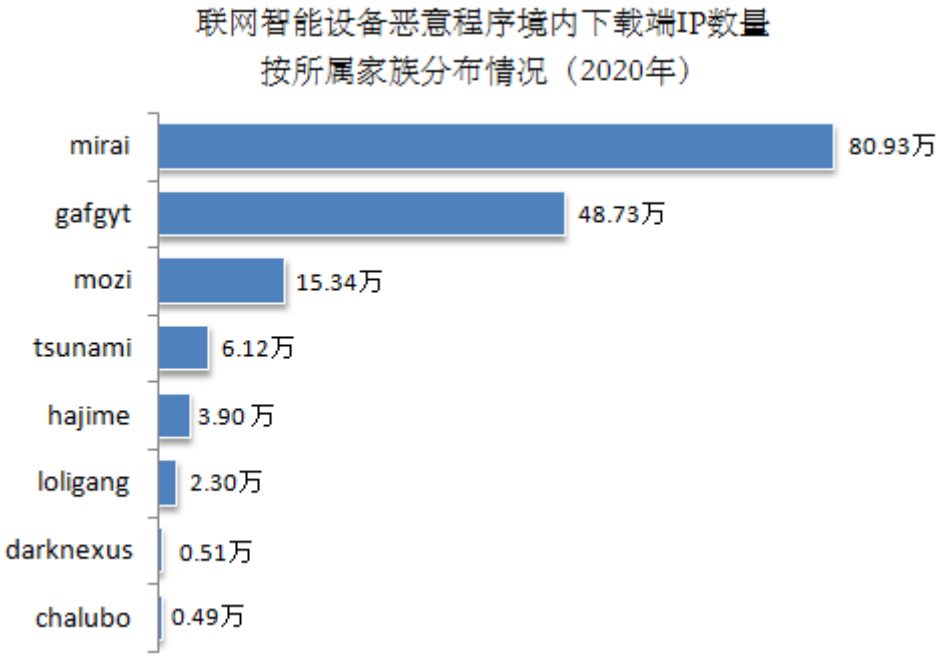

图 8 联网智能设备恶意程序境内下载端 IP 数量按所属家族分布情况（2020 年）

从下载端 IP 数量的趋势来看，Mirai、Gafgyt 家族的境内下载端 IP 数量呈缓慢下降趋势，Mozi 家族的境内下载端 IP 数量 3 至 4

月、9 至 12 月均处于较高水平，如图 9 所示。

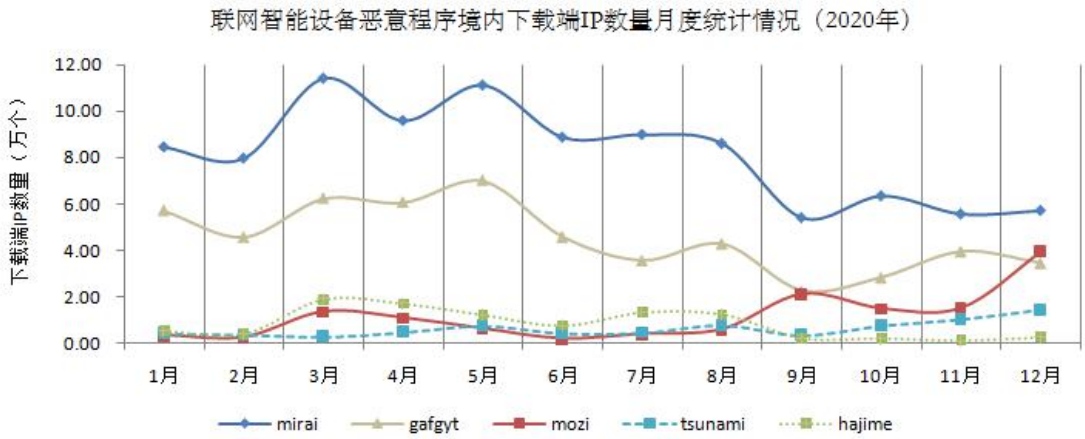

图 9 联网智能设备恶意程序境内下载端 IP 数量月度统计情况（2020 年）

境内下载端 IP 地址主要分布在江苏、浙江、安徽、山东、广东等省份，如图 10 所示。

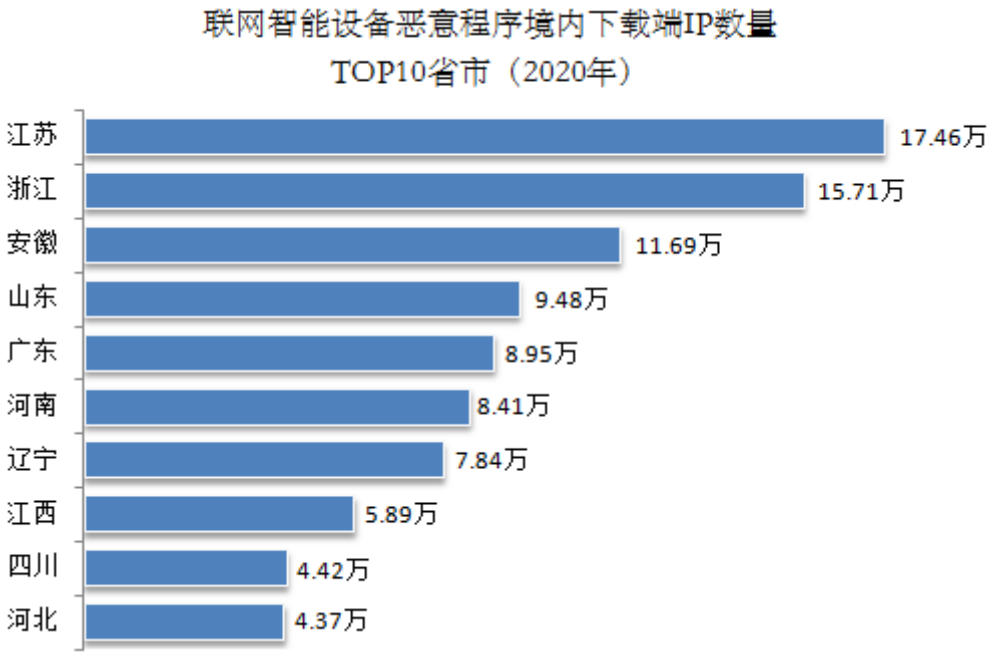

图 10 联网智能设备恶意程序境内下载端 IP 数量 TOP10 省市（2020 年）

3、联网智能设备僵尸网络活动态势

CNCERT 对联网智能设备设备感染恶意程序并被控形成的僵尸网络开展抽样监测分析，主要情况如下。

3.1 控制端监测情况

2020 年，CNCERT 监测到 20.93 万个境外控制端 IP 地址控制我国境内联网智能设备组成僵尸网络。其中，排名前三位的恶意家族为 Dofloo、Moobot、Mirai，如图 11 所示。

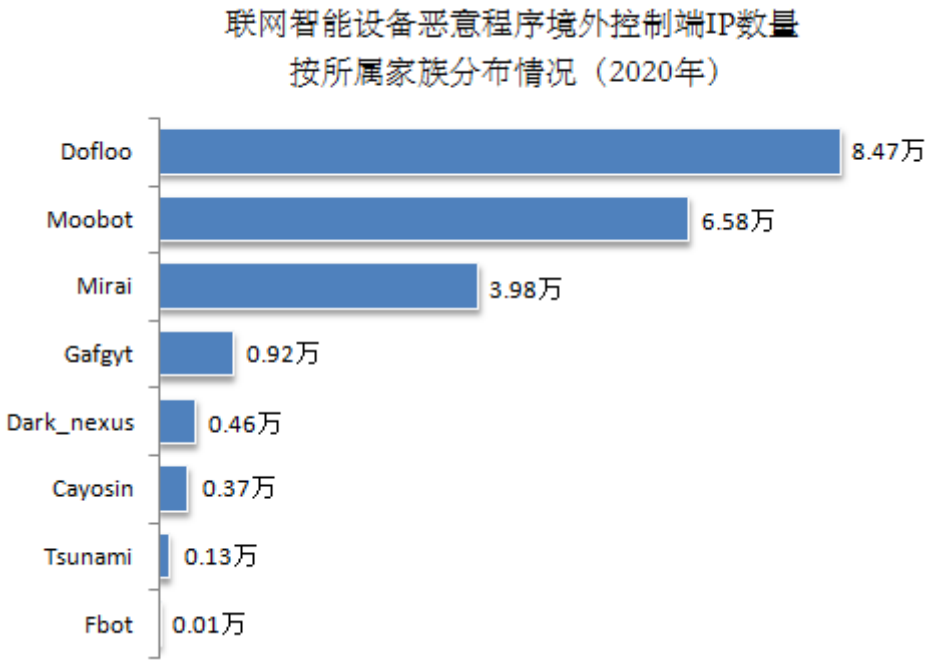

图 11 联网智能设备僵尸网络境外控制端 IP 数量按所属家族分布情况（2020 年）

2020 年上半年，在 CNCERT 对联网智能设备僵尸网络控制端的持续打击下，控制端 IP 数量趋势平稳，保持在月均 2 万个以下的水平。从 8 月开始，Moobot、Fbot 等家族僵尸网络活跃度增高，控制端 IP 数量迅速上升至月均 3 万以上。随着打击力度加大，12 月控制端 IP 数量重新下降至月均 3 万以下，如图 12 所示。

图 12 联网智能设备僵尸网络境外控制端 IP 数量按月统计情况（2020 年）

3.2 被控端监测情况

2020 年，CNCERT 监测发现 2929.73 万个境内联网智能设备 IP 地址被控制。其中，排名前三位的家族为 Pinkbot、Tsunami、Gafgyt，如图 13 所示。

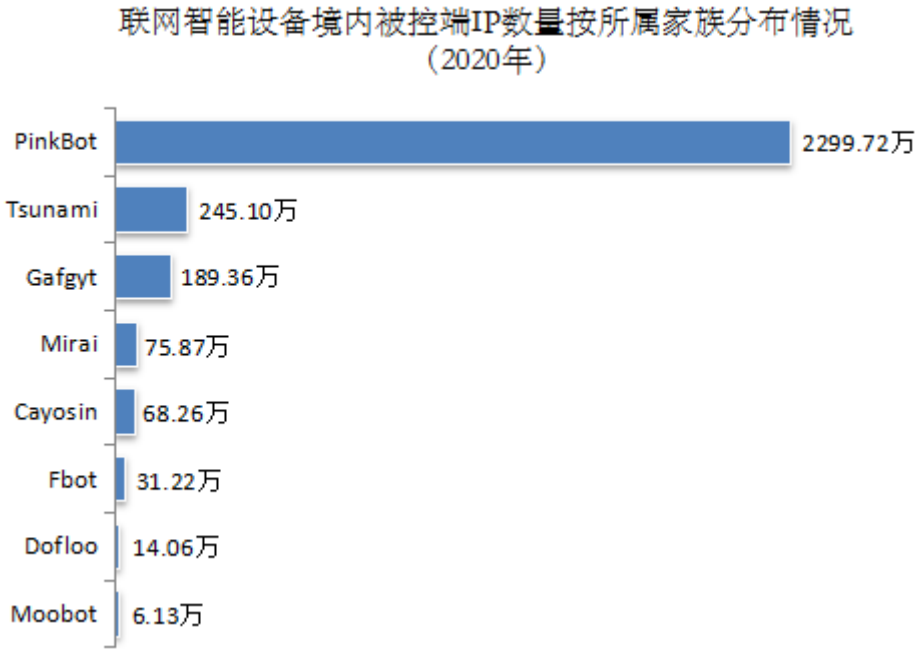

图 13 联网智能设备境内被控端 IP 数量按所属家族分布情况（2020 年）

从 3 月起，CNCERT 监测发现 Pinkbot 家族僵尸网络迅速扩张，被控端 IP 数量月均峰值超过 800 万。通过对其集中控制端的治理，从 6 月开始被控端数量持续下降。但未清理恶意程序的受感染设备之

间会继续通过 P2P 通信保持联系，截至 12 月仍能监测到约 200 万个被控端的通信行为。除此之外，其他家族的被控端 IP 数量保持平稳，约在 100 万左右规模，如图 14 所示。

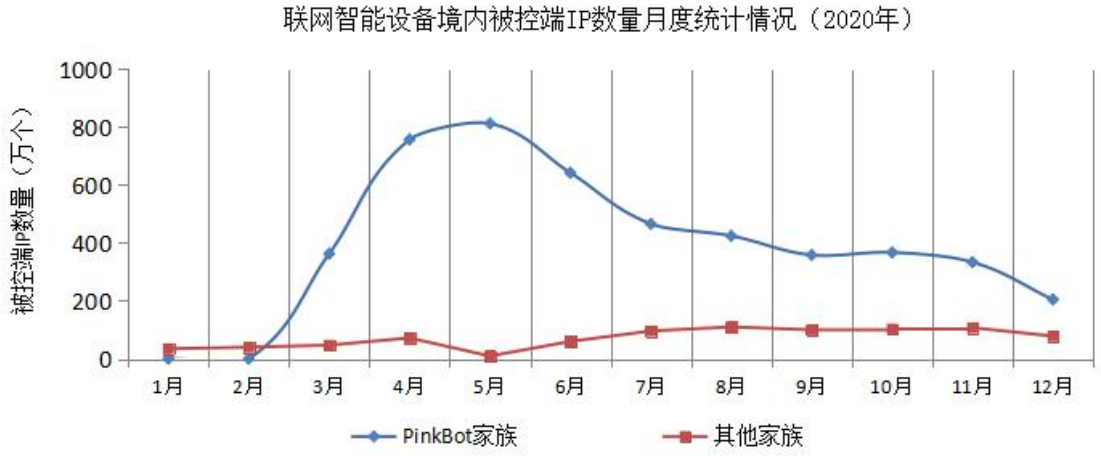

图 14 联网智能设备境内被控端 IP 数量月度统计情况（2020 年）

2020 年，通过控制联网智能设备而形成的僵尸网络规模明显增大。累计控制规模大于 10 万的僵尸网络共 53 个，1 至 10 万的共 471 个，控制规模较大的恶意家族包括 Tsunami、Gafgyt、Moobot、Cayosin、Fbot、Mirai 等。

3.3 利用联网智能设备僵尸网络进行攻击活动情况

2020 年，通过控制联网智能设备发起的 DDoS 攻击日均 3000 余起。其中，排名前四位的恶意家族为 Mirai、Gafgyt、Cayosin、Moobot，如图 15 所示。

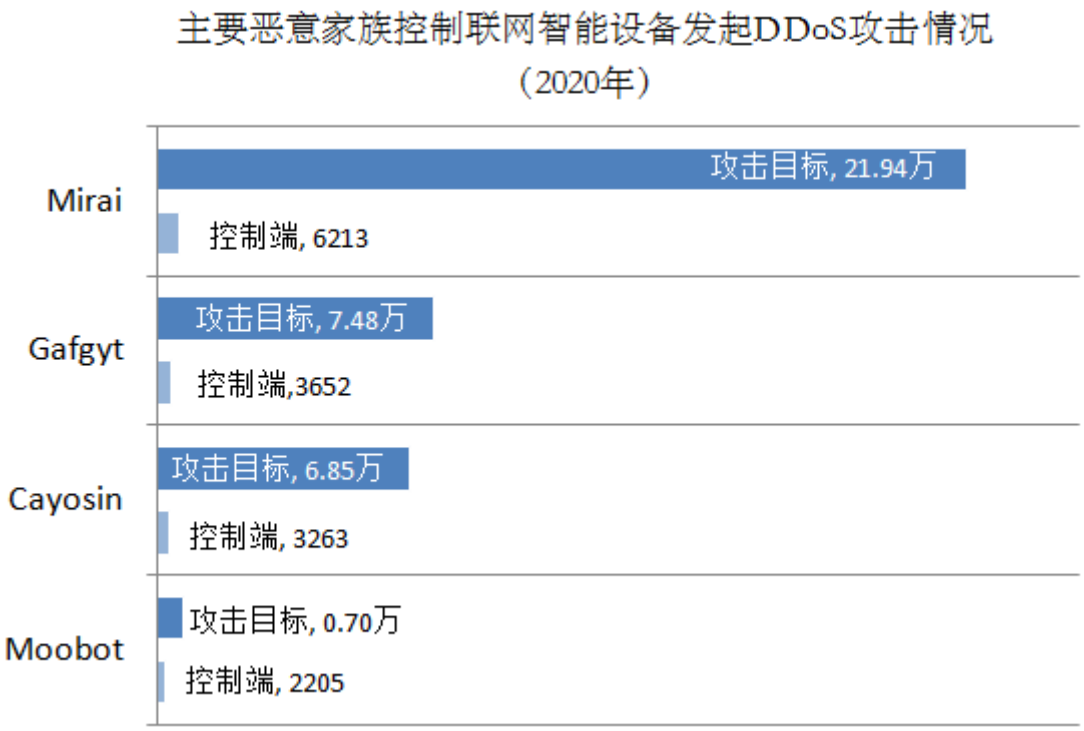

图 15 主要恶意家族控制联网智能设备发起 DDoS 攻击情况（2020 年）

本报告的撰写过程中，恒安嘉新（北京）科技股份有限公司、北京奇虎科技有限公司向 CNCERT 提供了协助和分析线索，特此致谢。