国家互联网应急中心

网络安全信息与动态周报

2021 年第 15 期

4 月 5 日-4 月 11 日

CNCERT/CC

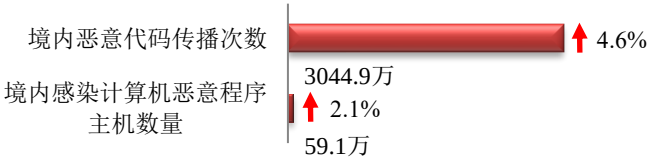
本周网络安全基本态势

境内计算机恶意程序传播次数 境内感染计算机恶意程序主机数量	•3044.9万 •59.1万	↑4.6% ↑2.1%
境内被篡改网站总数 其中政府网站数量	•1370 •3	↓56.7% ↓76.9%
境内被植入后门网站总数 其中政府网站数量	•711 •5	↑39.7% ↑66.7%
针对境内网站的仿冒页面数量	•351	↓81.3%
新增信息安全漏洞数量 其中高危漏洞数量	•671 •164	↓4.1% ↑16.3%

表示数量与上周相同　表示数量较上周环比增加　表示数量较上周环比减少

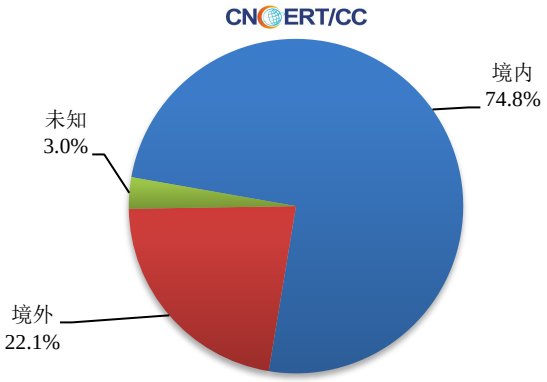
本周网络病毒活动情况

境内计算机恶意程序传播次数约为 3044.9 万次，境内感染计算机恶意程序主机数量约为 59.1 万个。

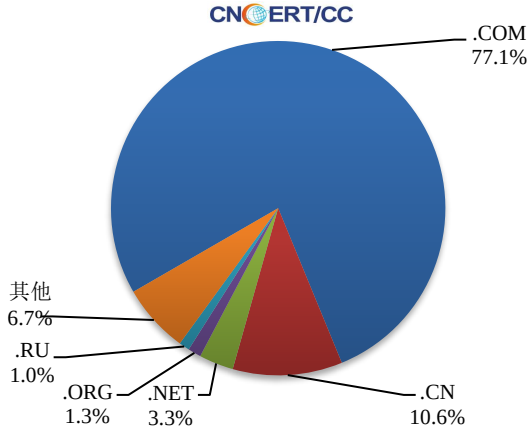


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 13779 个，涉及 IP 地址 10496 个。在 13779 个域名中，有 22.1%为境外注册，且顶级域为.com 的约占 77.1%；在 10496 个 IP 中，有约 52.9%于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 839 个。

本周放马站点域名注册所属境内外分布
(4/5-4/11)



本周放马站点域名注册所属顶级域分布
(4/5-4/11)



针对 CNCERT 自主监测发现以及各单位报送数据，CNCERT 积极协调域名注册机构等进行处理，同时通过 ANVA 在其官方网站上发布恶意地址黑名单。

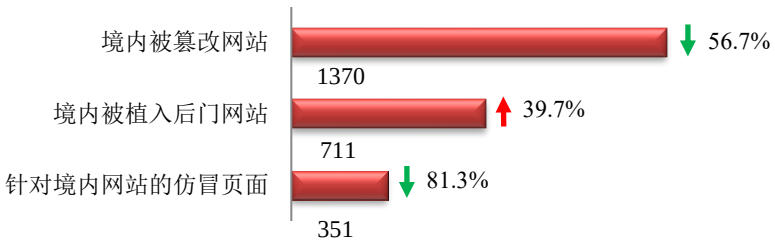
ANVA网络安全威胁信息共享平台

https://share.anva.org.cn/web/publicity/listurl

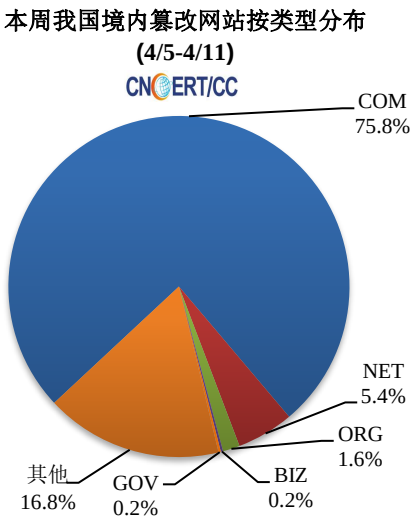
中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由 CNCERT 发起并组织运作的行业联盟。

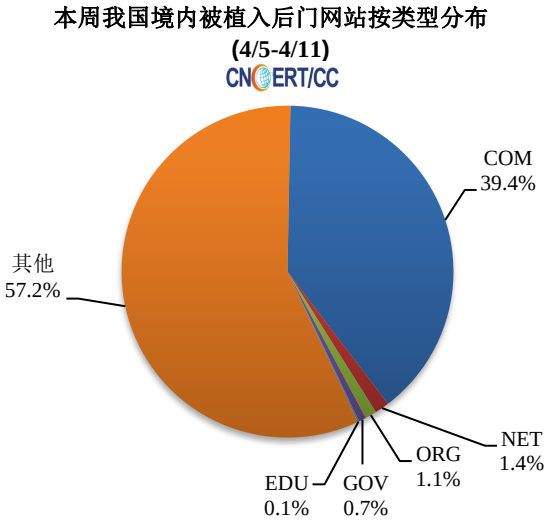
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 1370 个；被植入后门的网站数量为 711 个；针对境内网站的仿冒页面数量为 351 个。



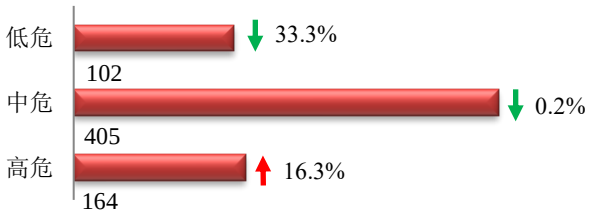
本周境内被篡改政府网站（GOV 类）数量为 3 个（约占境内 0.2%），与上周相比下降了 76.9%；境内被植入后门的政府网站（GOV 类）数量为 5 个，与上周相比上升了 66.7%。

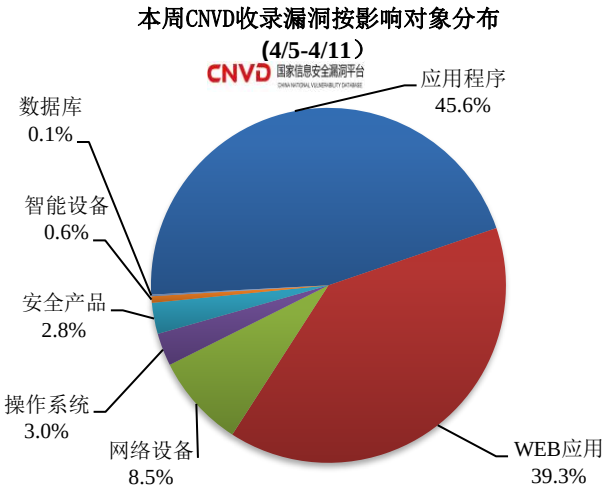




本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 671 个，信息安全漏洞威胁整体评价级别为中。





本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是 WEB 应用和网络设备。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

CNVD漏洞周报发布地址

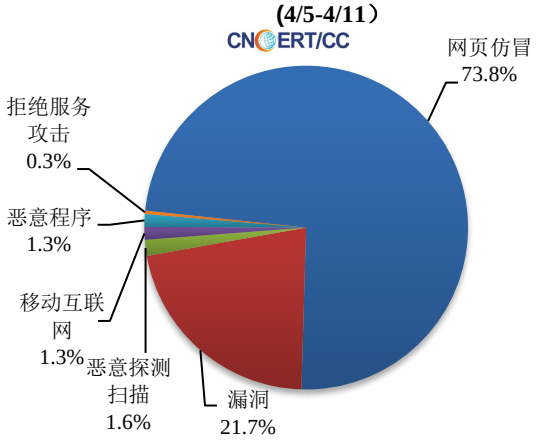
http://www.cnvd.org.cn/webinfo/list?type=4

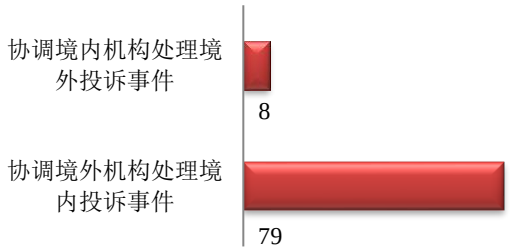
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

本周事件处理情况

本周，CNCERT 协调云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 313 起，其中跨境网络安全事件 87 起。

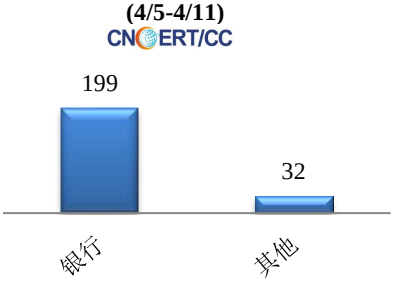
本周CNCERT处理的事件数量按类型分布 (4/5-4/11）



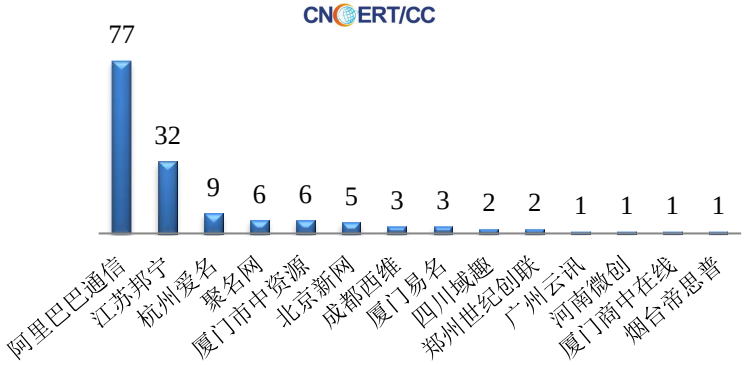


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理 231 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，银行仿冒事件 199 起，其他事件 32 起。

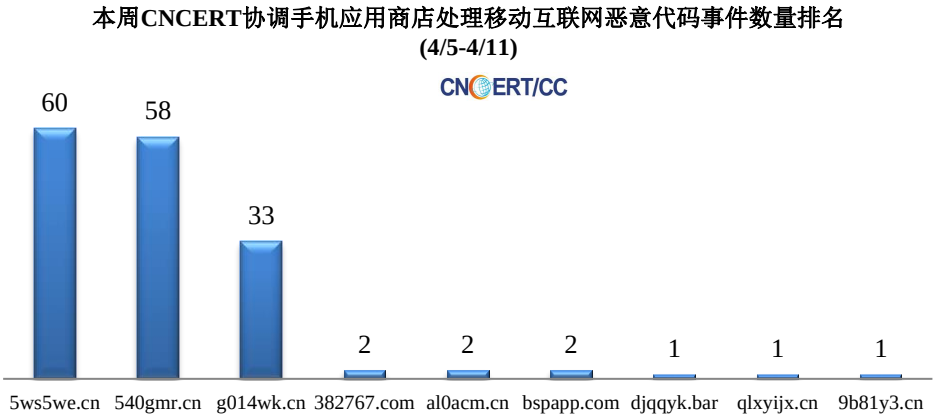
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (4/5-4/11)



本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (4/5-4/11）



本周，CNCERT 协调 9 个应用商店及挂载恶意程序的域名开展移动互联网恶意代码处理工作，共处理传播移动互联网恶意代码的恶意 URL 链接 160 个。



业界新闻速递

1. 工信部通报下架 60 款侵害用户权益 APP

2021 年 4 月 6 日，据工信部网站消息，工业和信息化部向社会通报了 136 家存在侵害用户权益行为 APP 企业的名单。截至目前，经第三方检测机构核查复检，尚有 53 款 APP 未按照工业和信息化部要求完成整改。各通信管理局按工业和信息化部 APP 整治行动部署，积极开展手机应用软件监督检查，此次浙江省通信管理局检查发现仍有 7 款 APP 未完成整改。依据《网络安全法》和《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407 号）等法律和规范性文件要求，工业和信息化部组织对上述 60 款 APP 进行下架。

2. 最高人民检察院披露 2020 年涉嫌网络犯罪大数据

2021 年 4 月 7 日，来自最高人民检察院网站消息，统计数据显示，2020 年，全国检察机关起诉涉嫌网络犯罪（含利用网络和利用电信实施的犯罪及其上下游关联犯罪）14.2 万人，同比上升 47.9%。当前，传统犯罪加速向网络空间蔓延，特别是利用网络实施的诈骗和赌博犯罪持续高发，2020 年已占网络犯罪总数的 64.4%。随机诈骗与精准诈骗相互交织，冒充公检法人员诈骗、交友诈骗、退款诈骗、信用卡贷款提额诈骗、刷单诈骗等较为突出。为赌博网站“洗白”资金的“跑分平台”、非法收集公民个人信息的“流氓软件”、扰乱网络市场秩序的“恶意刷单”等案件层出不穷。最高检披露，规模庞大的地下黑灰产业密切配合，为网络犯罪持续“输血供粮”，成为该类犯罪多发高发的重要原因。网络犯罪往往形成较为固定的犯罪利益链条：上游为犯罪团伙提供技术工具、收集个人信息等；中游实施诈骗或开设赌场等网络犯罪；下游利用支付通道“洗白”资金。数据显示，有近四分之一的网络诈骗是在获取公民个人信息后“精准出手”，有

针对性实施犯罪，侵犯公民个人信息已成为网络犯罪黑灰产业的关键环节。另外，网络犯罪集团化、跨境化特征凸显，犯罪主体呈现低年龄、低学历、低收入的“三低”趋势，老年人与年轻人更易成为受害对象。

3. 国家医疗保障局发布关于印发加强网络安全和数据保护工作指导意见的通知

2021 年 4 月 9 日，据国家医保局网站消息，国家医疗保障局发布了关于印发加强网络安全和数据保护工作指导意见的通知。意见指出：医疗保障信息化是医疗保障事业高质量发展的基础，是医保治理体系和治理能力现代化的重要支撑。为全面落实习近平总书记关于网络强国战略、大数据战略、数字经济的重要指示批示精神，以及党中央关于网络安全工作的总体部署，扎实推进医疗保障信息平台建设及运营维护，防范化解医疗保障系统数据安全风险，促进数据合理安全开发利用。

关于国家互联网应急中心（CNCERT）

国家计算机网络应急技术处理协调中心（英文简称 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，运行和管理国家信息安全漏洞共享平台（CNVD），维护公共互联网安全，保障关键信息基础设施的安全运行。

CNCERT/CC 在中国大陆 31 个省、自治区、直辖市设有分支机构，并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）。

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

联系我们

如果您对 CNCERT《网络安全信息与动态周报》有何意见或建议，欢迎与我们的编辑交流。

本期编辑：王毓骏

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315