国家互联网应急中心

网络安全信息与动态周报

2020 年第 52 期

12 月 21 日-12 月 27 日

CNCERT/CC

本周网络安全基本态势

境内被木马或僵尸程序控制主机数量	•52.3万	↓ 25.5%
境内被篡改网站总数 其中政府网站数量	•4453 •20	↑ 2.9% ↓ 20.0%
境内被植入后门网站总数 其中政府网站数量	•1498 •38	↑ 78.5% ↑ 1800.0%
针对境内网站的仿冒页面数量	•4942	↑ 13.0%
新增信息安全漏洞数量 其中高危漏洞数量	•298 •117	↑ 39.3% ↑ 46.3%

= 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

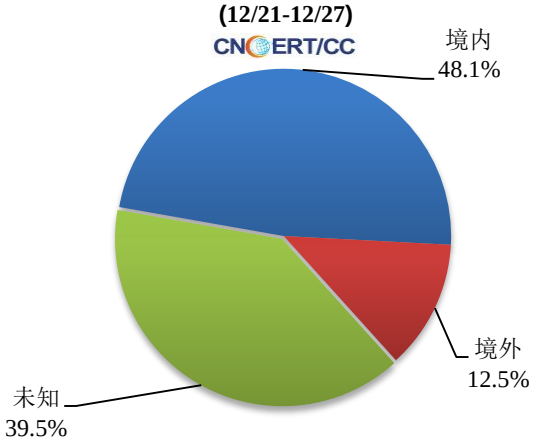
本周境内被木马或僵尸程序控制主机数量约为 52.3 万个。

被植入木马僵尸数量

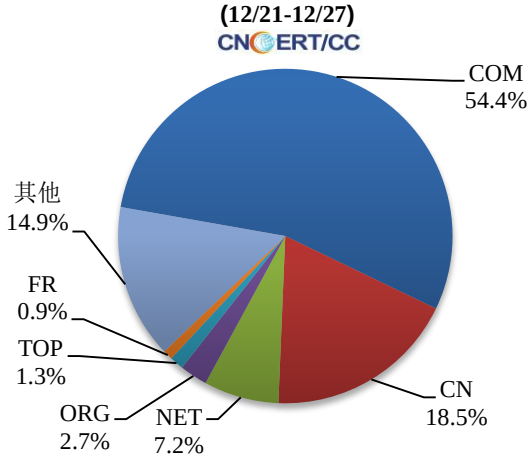
↓ 25.5%

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 745 个，涉及 IP 地址 3178 个。在 745 个域名中，有 12.5%为境外注册，且顶级域为.com 的约占 54.4%；在 3178 个 IP 中，有约 16.7%位于境外。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 289 个 IP。

本周放马站点域名注册所属境内外分布
(12/21-12/27)



本周放马站点域名注册所属顶级域分布
(12/21-12/27)



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。

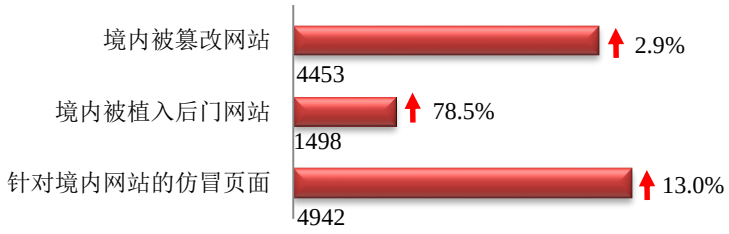
ANVA网络安全威胁信息共享平台

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

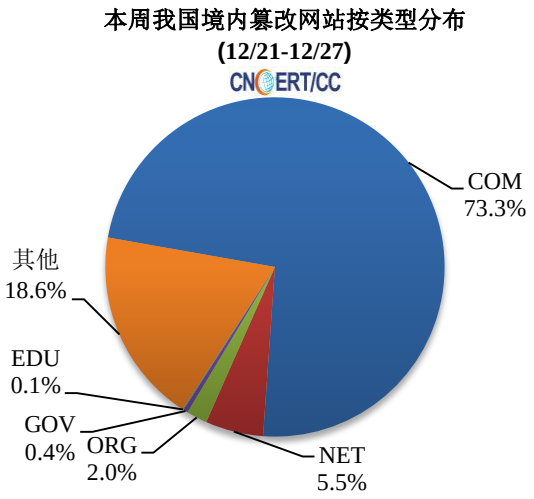
中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由 CNCERT 发起并组织运作的行业联盟。

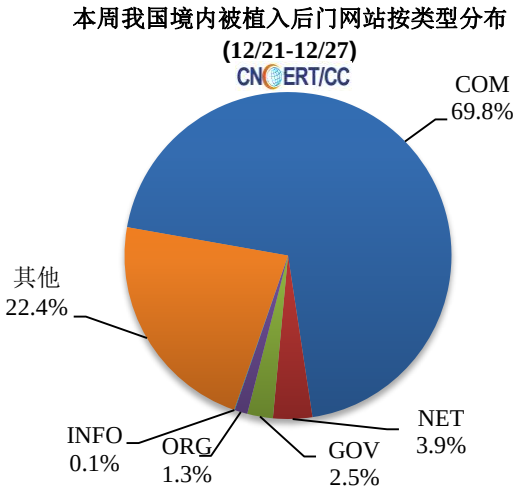
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 4453 个；被植入后门的网站数量为 1498 个；针对境内网站的仿冒页面数量为 4942 个。



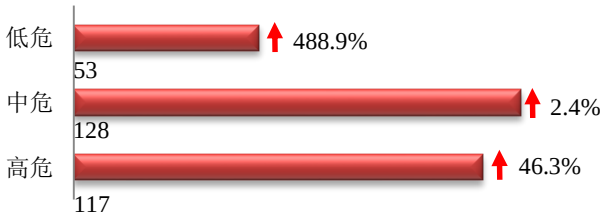
本周境内被篡改政府网站（GOV 类）数量为 20 个（约占境内 0.4%），较上周下降了 20.0%；境内被植入后门的政府网站（GOV 类）数量为 38 个（约占境内 2.5%），较上周上涨了 1800.0%。

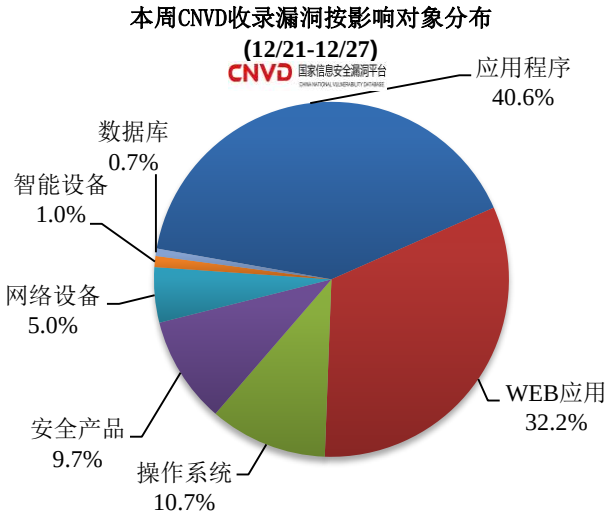




本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 298 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 应用和操作系统。

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

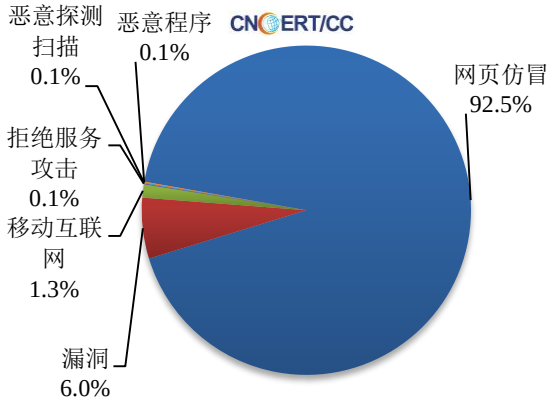
http://www.cnvd.org.cn/webinfo/list?type=4

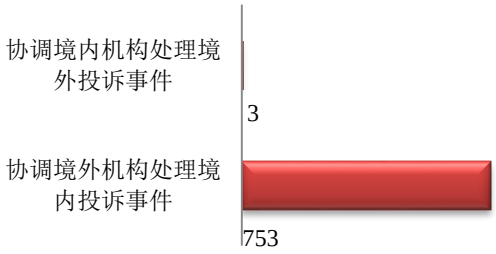
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

本周事件处理情况

本周，CNCERT 协调基础电信企业、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 1157 起，其中跨境网络安全事件 756 起。

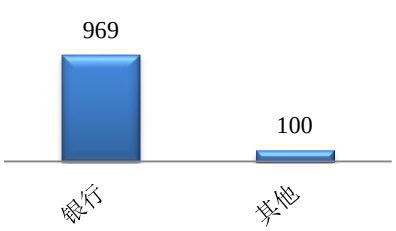
本周CNCERT处理的事件数量按类型分布
(12/21-12/27)



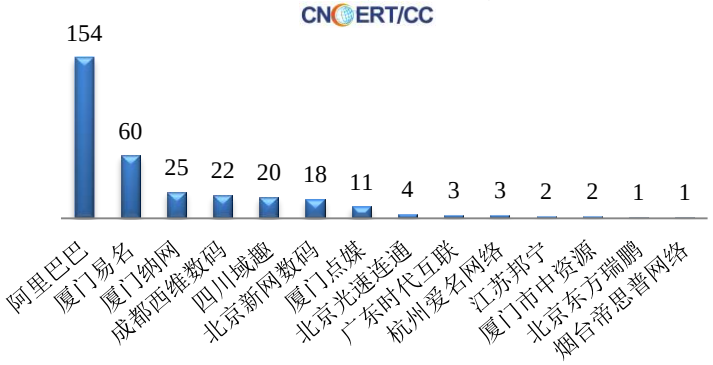


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1069 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 969 起以及其他事件 100 起。

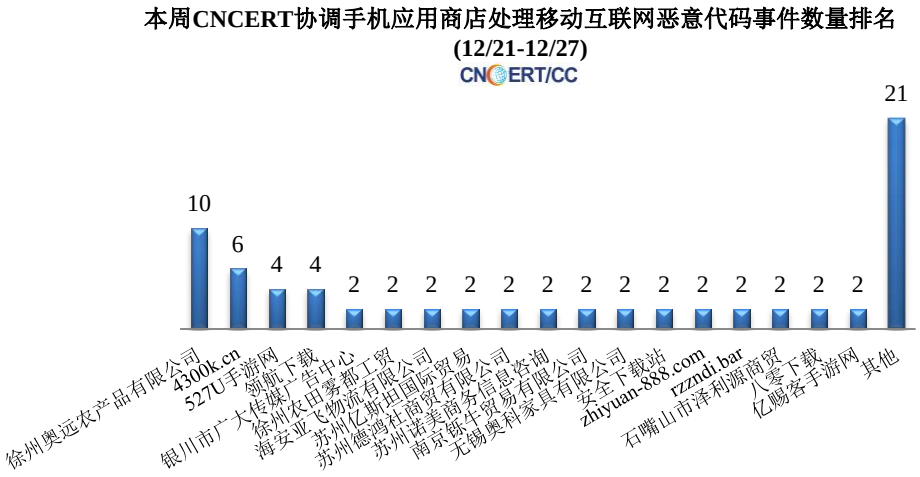
本周CNCERT处理网页仿冒事件
数量按仿冒对象涉及行业统计
(12/21-12/27)



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 (12/21-12/27)



本周，CNCERT 协调 39 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 73 个。



业界新闻速递

1. CNCERT 应急响应国际合作伙伴 2020 年视频会议成功举办

2020 年 12 月 16 日，由国家计算机网络应急技术处理协调中心（CNCERT/CC）主办的 CNCERT 应急响应国际合作伙伴 2020 年视频会议在线上成功举办。来自全球近 20 个国家和地区的 30 余个组织的 80 多名代表参加了此次会议，CNCERT/CC 副书记卢卫参会并致辞。

卢卫副书记指出，当前以互联网为代表的信息技术日新月异，世界正进入数字化连接的时代，特别是今年新冠肺炎疫情发生以来，互联网对促进各国经济复苏、保障社会运行、推动国际抗疫合作发挥了重要作用。但与此同时，与疫情相关的网络安全事件频频出现，利用跨国资源开展的网络攻击时有发生。各国 CERT 组织与国际合作伙伴应共同努力，在网络安全领域积极沟通合作，合力应对挑战。坚持深化共识，增进包容互信。利用国际交流平台，深化信任、扩大共识，倡导尊重各国网络空间主权，尊重各国自主选择网络治理模式、互联网公共政策和平等参与网络空间国际治理的权利。坚持合作共济，维护和平安全。加强在疫情防控条件下网络安全领域的沟通协商、信息共享、协调处置，让互联网成为助力全球抗疫的和平之网、合作之网、安全之网。坚持携手共进，加快创新发展。及时交流网络安全应急响应领域的新技术、新想法、新理念，带动网络安全技术创新进步，共享全球网络安全成果。坚持多边共治，构建良好秩序。多边参与、多方参与，共同完善网络安全应急响应对话协商协作机制，共同构建更加公正合理的网络空间安全秩序。

本次会议以“疫情下的网络安全应急响应合作”为主题，设置“国际合作”和“技术经验”两个板块。会上，来自 CNCERT/CC、马来西亚网络安全中心、柬埔寨邮政通信部通信技术局、亚太互联网络信息中心（APNIC）、斯里兰卡 CERT、巴基斯坦信息安全协会、日本 CERT、卡巴斯基工业控制系统 CERT 的 8 位嘉宾重点围绕网络安全应急响应国际合作、疫情期间 CERT 跨境响应合作实践、疫情相关

网络安全事件协作经验、应急响应组织居家办公实践经验、疫情下工业网络安全趋势与挑战等方面发言交流。

2. 关于侵害用户权益行为的 APP 通报（2020 年第七批）

12 月 21 日，工信部官网消息，依据《网络安全法》《电信条例》《电信和互联网用户个人信息保护规定》等法律法规，按照《关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》（工信部信管〔2020〕164 号）工作部署，工信部近期组织第三方检测机构对手机应用软件进行检查，督促存在问题的企业进行整改。截至目前，尚有 63 款 APP 未完成整改，上述 APP 应在 12 月 28 日前完成整改落实工作。

此次检测发现，APP 未经用户同意，私自收集设备 MAC 地址信息；将用户个人信息发送给第三方 SDK 的问题较多。部分头部企业 APP 检测仍发现问题，且未按工信部要求时限整改完成。部分应用商店及移动应用分发平台对利用技术对抗、更换“马甲”等方式故意逃避我部监管的企业，监测发现和处置力度不够。后续工信部将对上述问题突出、有令不行、整改不彻底的相关企业，采取全面下架、停止接入、行政处罚以及纳入电信业务经营不良名单或失信名单等措施，依法严厉处置。

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 2019 年，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。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：贾子骁

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315