国家互联网应急中心

网络安全信息与动态周报

2021 年第 28 期

7 月 5 日-7 月 11 日

CNCERT/CC

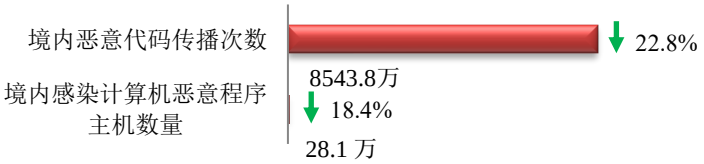
本周网络安全基本态势

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	•8543.8万 •28.1万	↓ 22.8% ↓ 18.4%
境内被篡改网站总数 其中政府网站数量	•2906 •13	↑ 12.1% =
境内被植入后门网站总数 其中政府网站数量	•365 •1	↓ 27.4% =
针对境内网站的仿冒页面数量	•352	↑ 105.8%
新增信息安全漏洞数量 其中高危漏洞数量	•541 •129	↓ 11.0% ↑ 20.6%

= 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

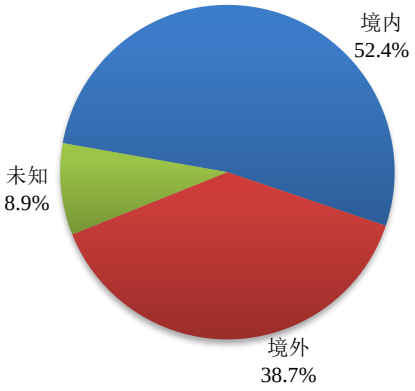
本周网络病毒活动情况

境内计算机恶意程序传播次数约为 8543.8 万次，境内感染计算机恶意程序主机数量约为 28.1 万个。

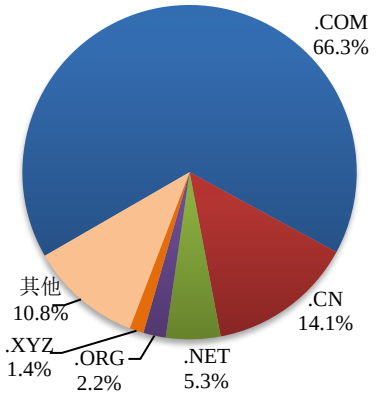


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 9632 个，涉及 IP 地址 49917 个。在 9632 个域名中，有 38.7%为境外注册，且顶级域为.com 的约占 66.3%；在 49917 个 IP 中，有约 82.1%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 639 个。

本周放马站点域名注册所属境内外分布
(7/5-7/11)



本周放马站点域名注册所属顶级域分布
(7/5-7/11)



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。

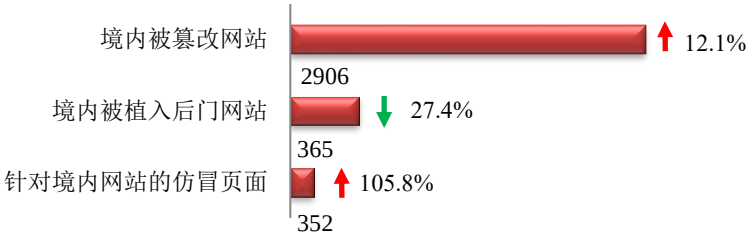
ANVA网络安全威胁信息共享平台

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。

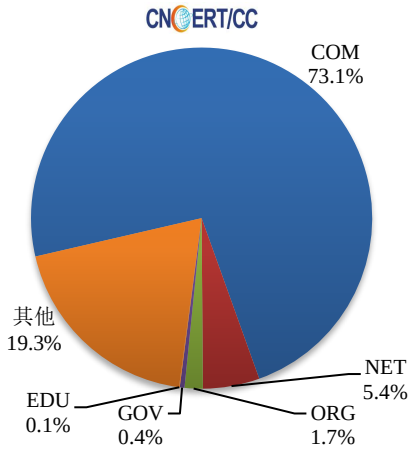
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 2906 个；被植入后门的网站数量为 365 个；针对境内网站的仿冒页面数量为 352 个。

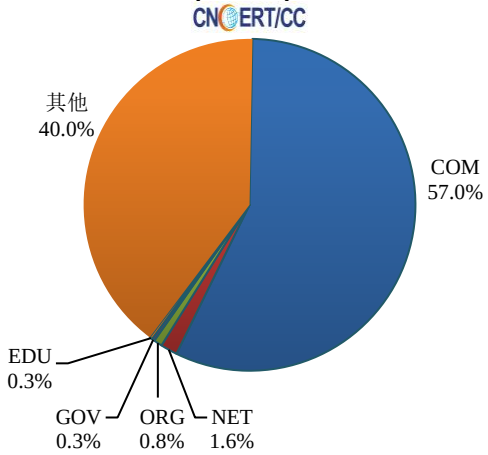


本周境内被篡改政府网站（GOV 类）数量为 13 个（约占境内 0.4%），与上周持平；境内被植入后门的政府网站（GOV 类）数量为 1 个（约占境内 0.3%），与上周持平。

本周我国境内篡改网站按类型分布
(7/5-7/11)

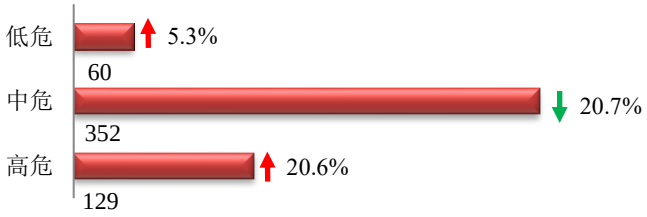


本周我国境内被植入后门网站按类型分布
(7/5-7/11)

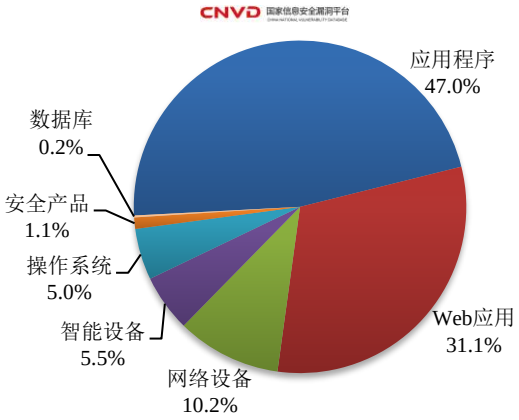


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 541 个，信息安全漏洞威胁整体评价级别为中。



本周CNVD收录漏洞按影响对象分布
(7/5-7/11）



本周 CNVD 发布的网络安全漏洞中，应用程序占比最高，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。

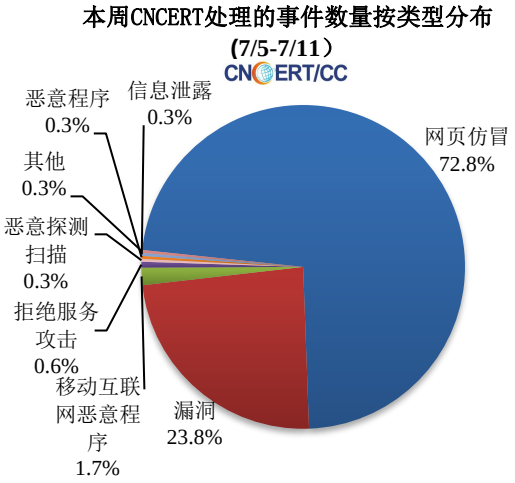
CNVD漏洞周报发布地址

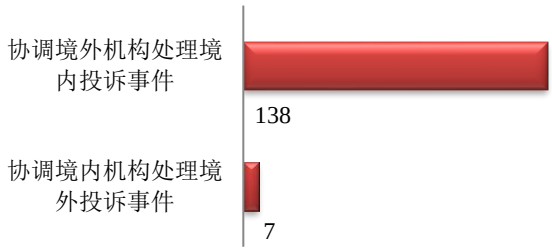
http://www.cnvd.org.cn/webinfo/list?type=4

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。

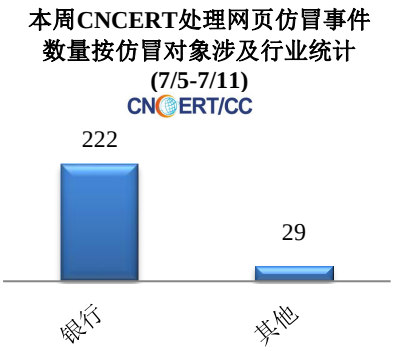
本周事件处理情况

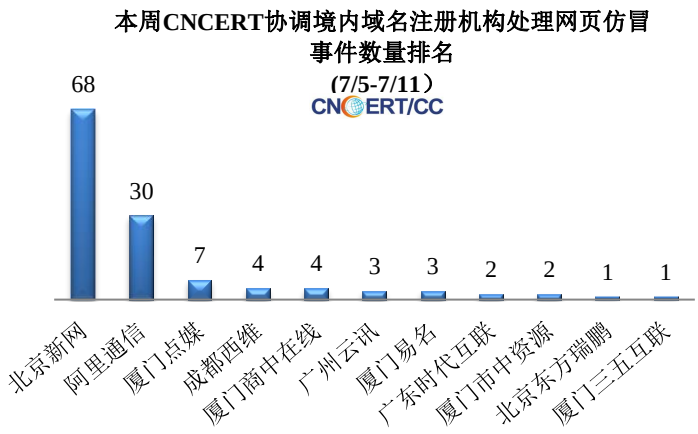
本周，CNCERT 协调云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 345 起，其中跨境网络安全事件 145 起。



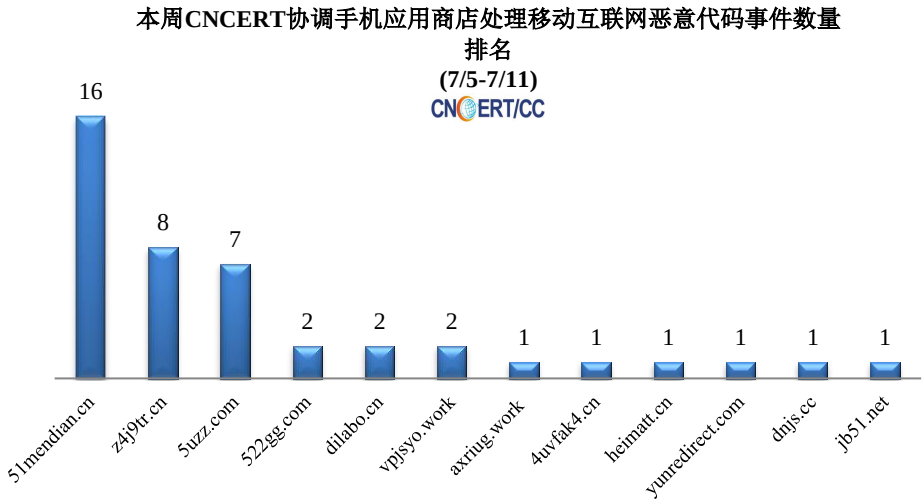


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理 251 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，银行仿冒事件 222 起，其他事件 29 起。





本周，CNCERT 协调 12 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 43 个。



业界新闻速递

1. 国家网信办关于下架“滴滴企业版”等 25 款 App 的通报

2021 年 7 月 9 日，据中国网信网消息，根据举报，经检测核实，“滴滴企业版”等 25 款 App 存在严重违法违规收集使用个人信息问题。国家互联网信息办公室依据《中华人民共和国网络安全法》相关规定，通知应用商店下架上述 25 款 App，要求相关运营者严格按照法律要求，参照国家有关标准，认真整改存在的问题，切实保障广大用户个人信息安全。各网站、平台不得为“滴滴出行”和“滴滴企业版”等上述 25 款已在应用商店下架的 App 提供访问和下载服务。

2. 《网络安全审查办法（修订草案征求意见稿）》公开征求意见

2021 年 7 月 10 日，据中国网信网消息，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》《中华人民共和国数据安全法》等法律法规，国家互联网信息办公室会同有关部门修订了《网络安全审查办法》，现向社会公开征求意见。公众可通过以下途径和方式提出反馈意见：1.登录中华人民共和国司法部 中国政府法制信息网（www.moj.gov.cn、www.chinalaw.gov.cn），进入首页主菜单的“立法意见征集”栏目提出意见。2.通过电子邮件方式发送至：shencha@cac.gov.cn。3.通过信函方式将意见寄至：北京市西城区车公庄大街 11 号国家互联网信息办公室网络安全协调局，邮编 100044，并在信封上注明“网络安全审查办法征求意见”。意见反馈截止日期为 2021 年 7 月 25 日。

3. 中国-东盟网络安全应急响应能力建设研讨会暨 CNCERT 国际合作伙伴东盟区域视频会议成功举办

2021 年 6 月 29 日，由国家计算机网络应急技术处理协调中心（CNCERT/CC）主办的中国-东盟网络安全应急响应能力建设研讨会暨 CNCERT 国际合作伙伴东盟区域视频会议在线上成功举办。来自国内外 10 余个组织的 30 多名代表参加了此次会议，CNCERT/CC 有关代表参会并致辞。CNCERT/CC 指出，5G、大数据、物联网、人工智能等新技术正在影响社会生产新变革，创造了生活新空间，提供了社会经济繁荣进步与快速发展的新动力。但与此同时，世界面临的不稳定不确定因素正在增加，以网络安全为代表的非传统安全威胁等持续蔓延。利用跨国资源开展网络攻击时有发生，网络安全已超越一国国界，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。

2021 年，是中国-东盟建立对话关系 30 周年。CNCERT/CC 愿与各东盟 CERT 组织继续加强合作。深化共识，充分利用本次会议在内的国际交流平台，深化信任、扩大共识，倡导尊重各国在网络空间的主权，致力于共同维护网络空间的和平与安全。强化合作，加强网络安全领域的沟通协商，推动信息共享，及时协调处置网络安全事件。多边共治，坚持多边参与、多方参与，共同完善网络安全应急响应对话协商协作机制，促进全球互联网治理体系更加公正合理。开放发展，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。

4. “2021 年中国网络安全年会”即将举办 期待您的参与

7 月 20 日，“2021 年中国网络安全年会”即将在线上线下同期举办，专业、权威、精彩的网络安全盛宴即将呈现。本届中国网络安全年会在国家互联网信息办公室指导下，由国家互联网应急中心（CNCERT/CC）主办。 本届网络安全年会有三大亮点：一是主题鲜明，聚焦当前网络安全新形势与新挑战。本次网络安全年会围绕“携手应对数据安全威胁挑战”这一主题，聚焦当前国内外网络安全工作新情况、新形势与新挑战，特别是数据安全这一当前的热门领域，共话数据安全未来发展趋势，共谋数据安全深入合作，促进政府部门、重要信息系统单位与网络安全产业界间交流，普及宣传网络安全知识技能，提升社会网络安全意识，并肩应对潜在威胁与风险，携手营造安全健康网络空间。二是议题丰富，多维度多领域深度探讨解读网络安全热点问题。本届网络安全年会将设置 1 个主论坛和 7 个分论坛，主论坛将由国家互联网应急中心和联合主办单位共同主办，分论坛由联合主办单位负责，分享探讨产、学、研、用新情况，交流应对网络安全问题新思路。三是专家云集，邀请权威顶级业界专家带来智慧风暴。

5. 工信部大力推进 APP 开屏弹窗信息骚扰用户问题整治

2021 年 7 月 8 日，据工信部网站消息，工业和信息化部近期对用户反映强烈投诉较多的“弹窗信息标识近于无形、关闭按钮小如蝼蚁、页面伪装瞒天过海、诱导点击暗度陈仓”等违规行为进行了集中整治，督促企业重视用户诉求，解决好在开屏信息页面中存在利用文字、图片、视频等方式欺骗误导用户跳转等问题。截至目前，百度、阿里、腾讯、字节跳动、新浪微博、爱奇艺等 68 家

头部互联网企业已按要求完成整改。2021 年第二季度，开屏弹窗信息用户投诉举报数量环比下降 50%，误导用户点击跳转第三方页面问题同比下降 80%。

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：姚力

网址：www.cert.org.cn

Email：cncert_report@cert.org.cn

电话：010-82990315