国家互联网应急中心

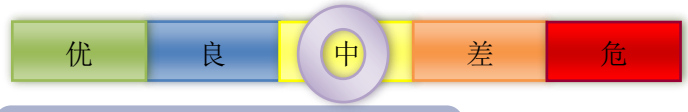
网络安全信息与动态周报

2021 年第 24 期

6 月 7 日-6 月 13 日

CNCERT/CC

本周网络安全基本态势

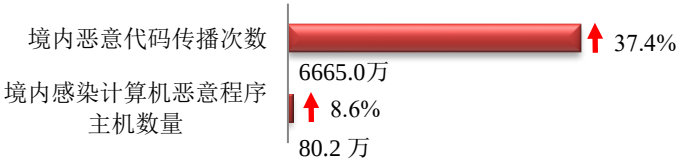


境内计算机恶意程序传播次数 境内感染计算机恶意程序主机数量	•6665.0万 •80.2万	↑37.4% ↑8.6%
境内被篡改网站总数 其中政府网站数量	•3387 •11	↑28.4% ↓31.3%
境内被植入后门网站总数 其中政府网站数量	•1249 •10	↓5.2% ↑233.3%
针对境内网站的仿冒页面数量	•349	↓45.9%
新增信息安全漏洞数量 其中高危漏洞数量	•602 •227	↑0.3% ↑43.7%

= 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

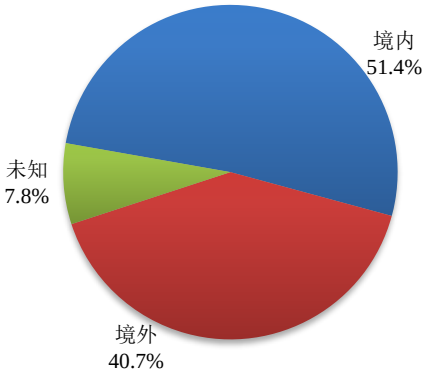
本周网络病毒活动情况

境内计算机恶意程序传播次数约为 6665.0 万次，境内感染计算机恶意程序主机数量约为 80.2 万个。

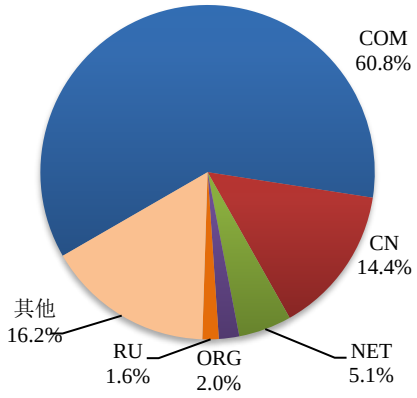


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1524 个，涉及 IP 地址 8807 个。在 1524 个域名中，有 40.7%为境外注册，且顶级域为.com 的约占 60.8%；在 8807 个 IP 中，有约 41.7%于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 182 个。

本周放马站点域名注册所属境内外分布
(6/7-6/13)



本周放马站点域名注册所属顶级域分布
(6/7-6/13)



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。

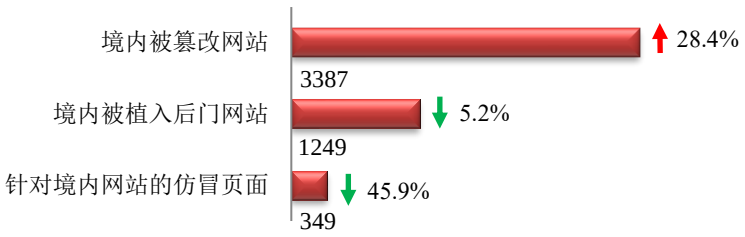
ANVA网络安全威胁信息共享平台

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。

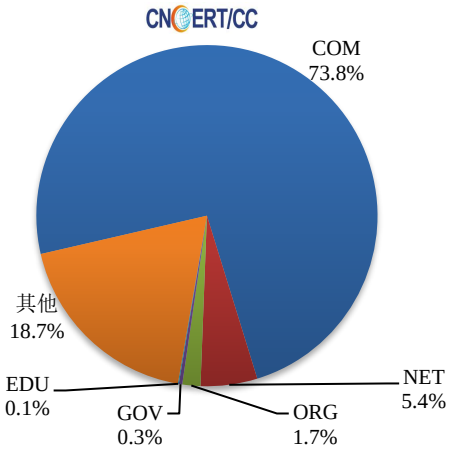
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 3387 个；被植入后门的网站数量为 1249 个；针对境内网站的仿冒页面数量为 349 个。

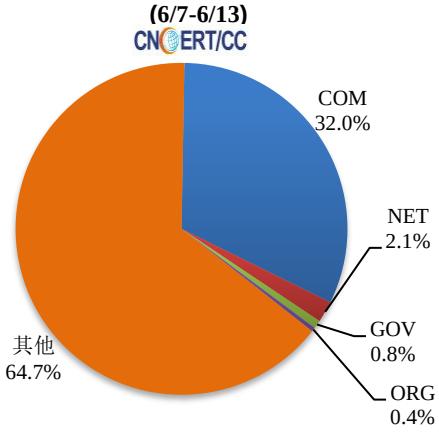


本周境内被篡改政府网站（GOV 类）数量为 11 个（约占境内 0.3%），与上周相比下降了 31.3%；境内被植入后门的政府网站（GOV 类）数量为 10 个（约占境内 0.8%），与上周相比上升了 233.3%。

本周我国境内篡改网站按类型分布
(6/7-6/13)

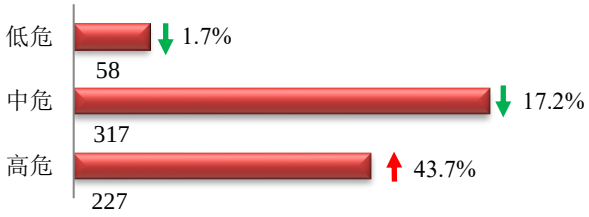


本周我国境内被植入后门网站按类型分布
(6/7-6/13)

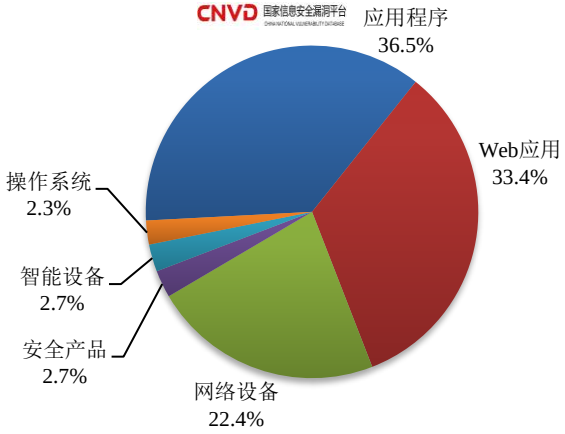


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 602 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
(6/7-6/13）



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。

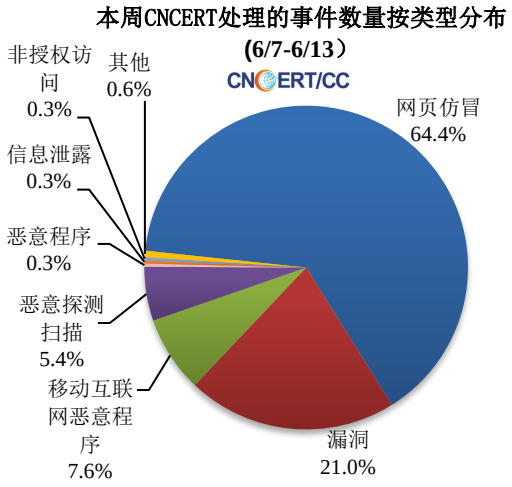
CNVD漏洞周报发布地址

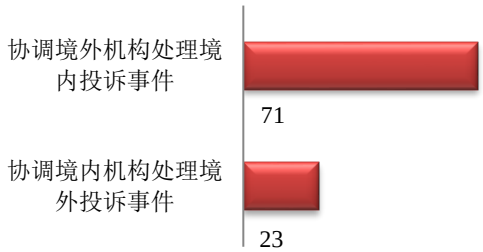
http://www.cnvd.org.cn/webinfo/list?type=4

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。

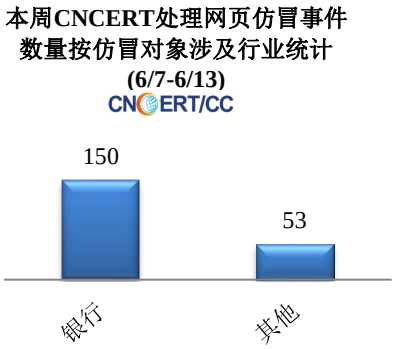
本周事件处理情况

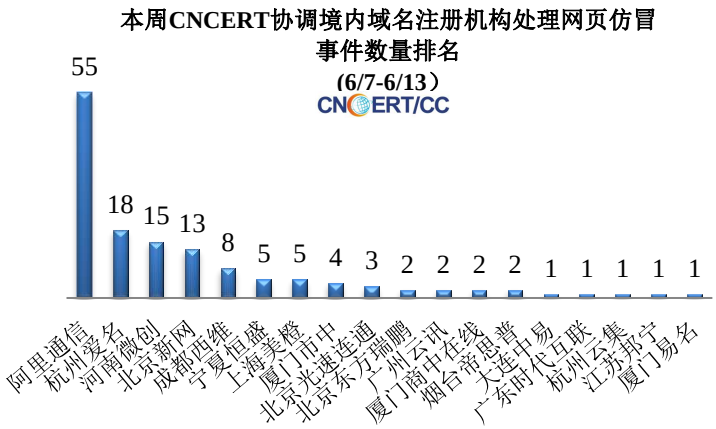
本周，CNCERT 协调云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 315 起，其中跨境网络安全事件 94 起。



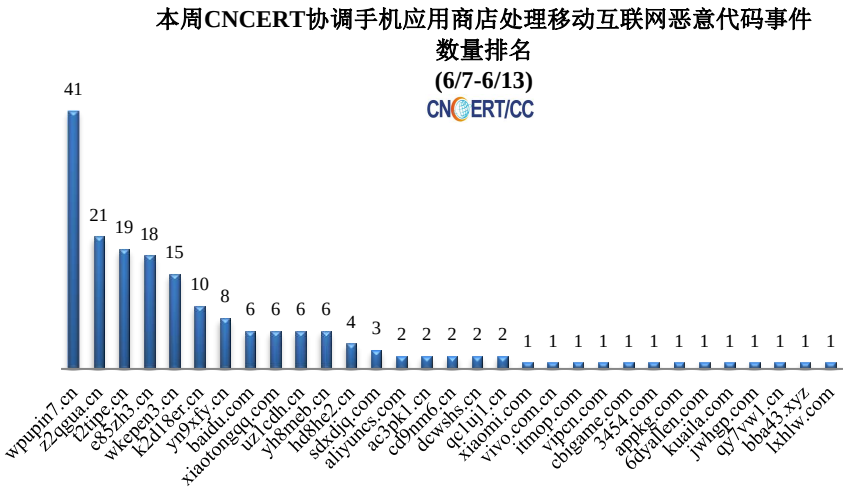


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理 203 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，银行仿冒事件 150 起，其他事件 53 起。





本周，CNCERT 协调 34 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 189 个。



业界新闻速递

1. 中华人民共和国数据安全法获表决通过

2021 年 6 月 10 日，据中国人大网消息，《中华人民共和国数据安全法》已由中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议于 2021 年 6 月 10 日通过，自 2021 年 9 月 1 日起施行。数据是国家基础性战略资源，没有数据安全就没有国家安全。数据安全法贯彻落实总体国家安全观，聚焦数据安全领域的风险隐患，加强国家数据安全工作的统筹协调，确立了数据分类分级管理、数据安全审查、数据安全风险评估、监测预警和应急处置等基本制度。通过建立健全各项制度措施，提升国家数据安全保障能力，有效应对数据这一非传统领域的国家安全风险与挑战，切实维护国家主权、安全和发展利益。

2. 国家网信办通报 129 款违法违规收集使用个人信息 App

2021 年 6 月 11 日，据国家网信办消息，针对人民群众反映强烈的 App 非法获取、超范围收集、过度索权等侵害个人信息的现象，国家互联网信息办公室依据《中华人民共和国网络安全法》《App 违法违规收集使用个人信息行为认定方法》《常见类型移动互联网应用程序必要个人信息范围规定》等法律和有关规定，组织对运动健身、新闻资讯、网络直播、应用商店、女性健康等常见类型公众大量使用的部分 App 的个人信息收集使用情况进行了检测。针对检测发现的问题，相关 App 运营者应当于本通报发布之日起 15 个工作日内完成整改，并将整改报告加盖公章发至电子邮箱：Appzhili@cac.gov.cn。各地网信办应指导督促本地区 App 运营者按要求限期进行整改。逾期未完成整改的国家网信办将依法予以处置。

3. 工信部通报 291 款侵害用户权益 APP

2021 年 6 月 8 日，据工信部网站消息，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》（工信部信管函〔2020〕164 号）工作部署，工业和信息化部近期组织第三方检测机构对手机应用软件进行检查，重点督促用户反映问题较多的实用工具、学习教育、生活出行、求职招聘、运动健身等五类企业进行整改，并进一步加大对 APP 弹窗信息关不掉或者未显著提供关闭功能标识，开屏信息、弹窗信息利用文字、图片、视频等方式欺骗误导用户跳转至其他页面等突出问题的整治力度，充分保障用户的知情权和选择权。截至目前，尚有 83 款 APP 未完成整改。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，天津市、上海市、江苏省、浙江省、广东省、四川省通信管理局检查发现仍有 208 款 APP 未完成整改。上述 APP 应在 6 月 16 日前完成整改落实工作。逾期不整改的，工业和信息化部将依法依规组织开展相关处置工作。

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：朱天

网址：www.cert.org.cn

Email：cncert_report@cert.org.cn

电话：010-82990315