国家互联网应急中心

网络安全信息与动态周报

2021 年第 46 期

11 月 8 日-11 月 14 日

CNCERT/CC

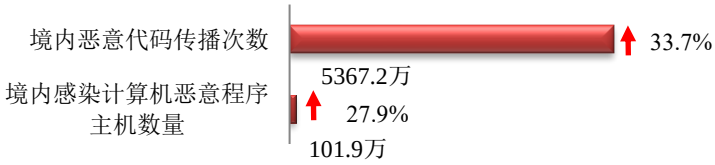
本周网络安全基本态势

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	• 5367.2万 • 101.9万	↑ 33.7% ↑ 27.9%
境内被篡改网站总数 其中政府网站数量	• 1543 • 10	↑ 196.7% ↑ 66.7%
境内被植入后门网站总数 其中政府网站数量	• 942 • 6	↑ 36.3% ↑ 100.0%
针对境内网站的仿冒页面数量	• 73	↓ 66.0%
新增信息安全漏洞数量 其中高危漏洞数量	• 484 • 104	↓ 8.2%. ↓ 18.1%

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

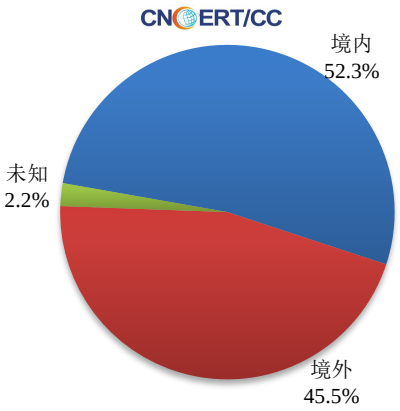
本周网络病毒活动情况

境内计算机恶意程序传播次数约为 5367.2 万次，境内感染计算机恶意程序主机数量约为 101.9 万个。

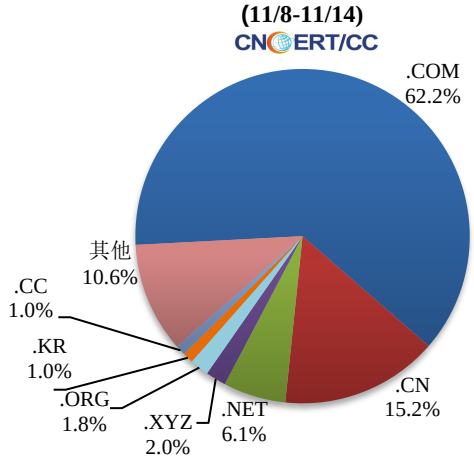


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 5371 个，涉及 IP 地址 22507 个。在 5371 个域名中，有 45.5%为境外注册，且顶级域为.com 的约占 62.3%；在 22506 个 IP 中，有约 45.5%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 563 个。

本周放马站点域名注册所属境内外分布
(11/8-11/14)



本周放马站点域名注册所属顶级域分布
(11/8-11/14)



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。

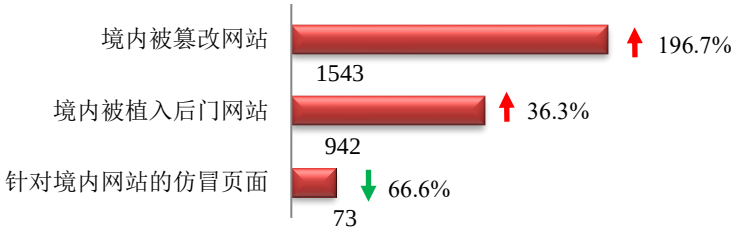
ANVA网络安全威胁信息共享平台

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。

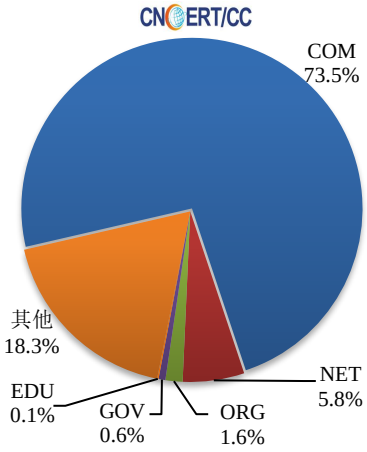
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 1543 个；被植入后门的网站数量为 942 个；针对境内网站的仿冒页面数量为 73 个。

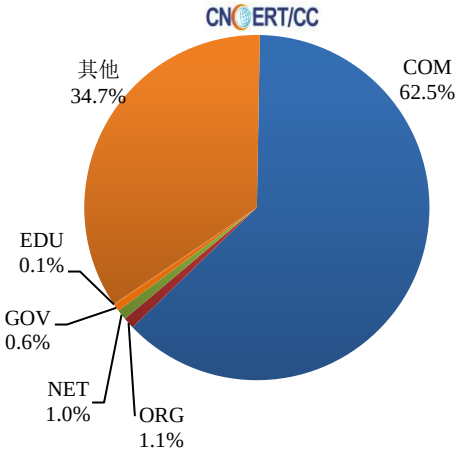


本周境内被篡改政府网站（GOV 类）数量为 10 个（约占境内 0.6%）,与上周相比上升 66.7%；境内被植入后门的政府网站（GOV 类）数量为 6 个（约占境内 0.6%），与上周相比上升 100.0%。

本周我国境内篡改网站按类型分布
(11/8-11/14)

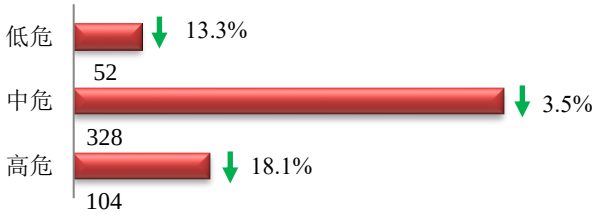


本周我国境内被植入后门网站按类型分布
(11/8-11/14)

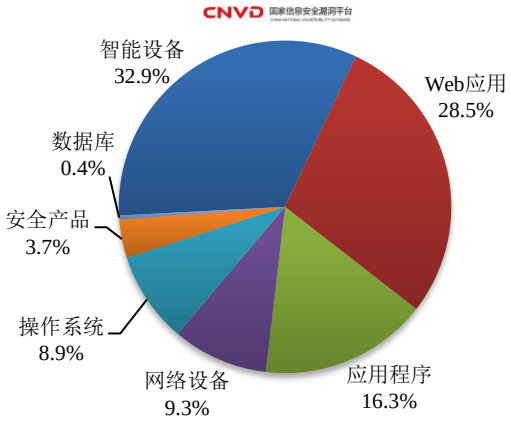


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 484 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
(11/8-11/14)



本周 CNVD 发布的网络安全漏洞中，智能设备占比最高，其次是 Web 应用和应用程序。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

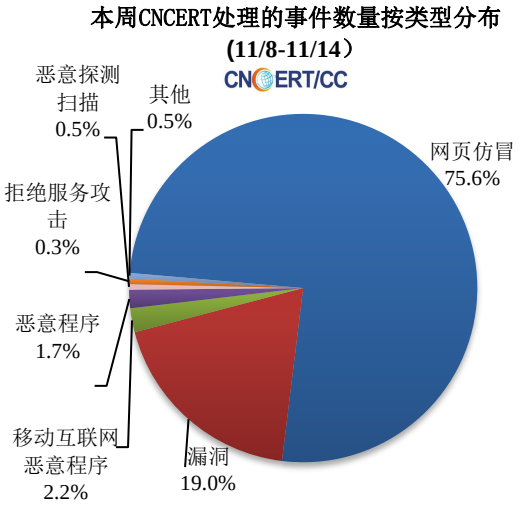
CNVD漏洞周报发布地址

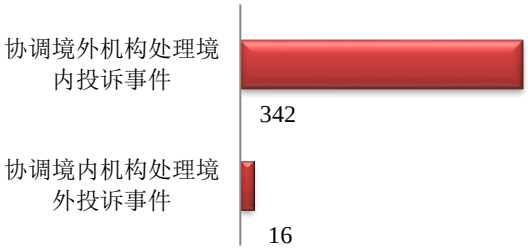
http://www.cnvd.org.cn/webinfo/list?type=4

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。

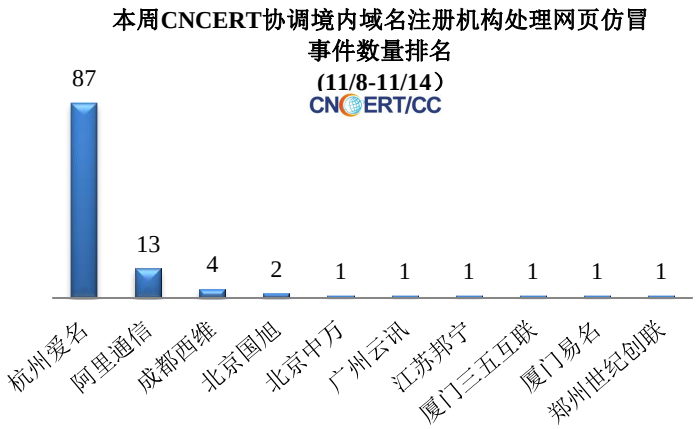
本周事件处理情况

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网络安全事件 585 起，其中跨境网络安全事件 358 起。

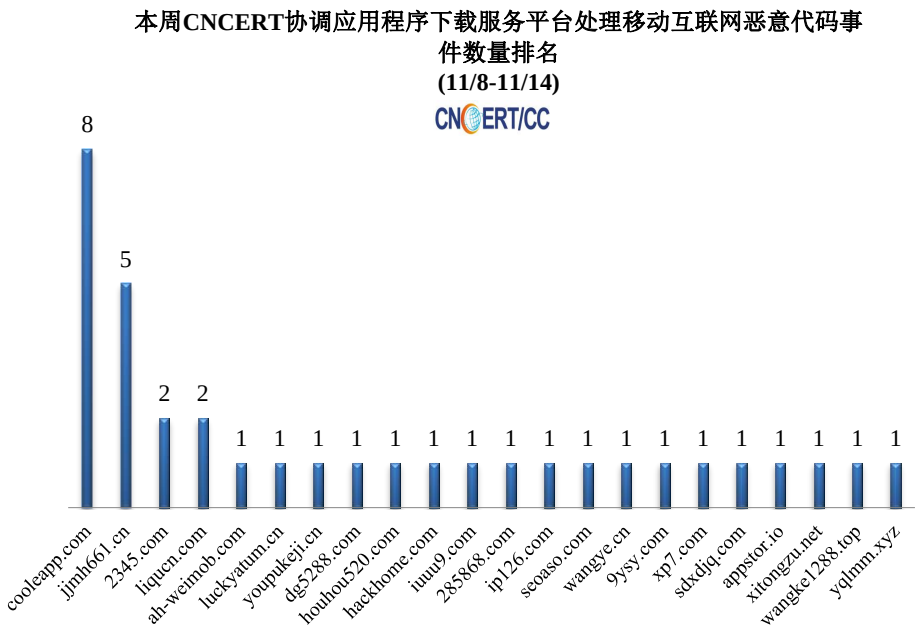




本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理 442 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，银行仿冒事 423 起，其他事件 19 起。



本周，CNCERT 协调 22 个提供恶意移动应用程序下载服务的平台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 35 个。



业界新闻速递

1. 2021 年 CNCERT 国际合作伙伴非洲区域视频会议成功举办

2021 年 11 月 3 日，由国家计算机网络应急技术处理协调中心（CNCERT/CC）主办的 2021 年 CNCERT 国际合作伙伴非洲区域视频会议在线上成功举办。来自中非 17 个组织的 30 余名代表参加了此次会议。本次会议设置“应急协作”、“技术经验”和“交流讨论”三个板块，CNCERT/CC 负责同志卢卫参会并致辞。会上，来 CNCERT/CC、非洲 CERT 联盟、贝宁 bjCSIRT、毛里求斯 CERT-MU、中国联通、华为、奇安信、绿盟科技、恒安嘉新、深信服的 10 位嘉宾重点围绕应急响应国际合作与能力建设、CERT 组织发展，以及云设施安全、AI 使能的威胁检测与应急响应、网络安全攻防、工业互联网安全、勒索病毒应对处置等合作与技术经验发言交流。此次会议是 CNCERT 国际合作论坛机制下针对非洲合作伙伴开展的区域性会议，今年以视频形式召开。该论坛为我中心、国际伙伴和网络安全企业提供了一个在网络安全领域交流的平台，进一步增进互信，相互学习，建立紧密的联系渠道，优化网络安全事件应急响应，加强信息和数据共享，开展应急能力建设，促进开展全方面的网络安全合作。

2. 国家互联网信息办公室对《网络数据安全管理条例（征求意见稿）》公开征求意见

2021 年 11 月 14 日，据中国网信网消息，为落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律关于数据安全管理的规定，规范网络数据处理活动，保护个人、组织在网络空间的合法权益，维护国家安全和公共利益，根据国务院 2021 年立法计划，国家互联网信息办公室会同相关部门研究起草《网络数据安全管理条例（征求意见稿）》，现向社

会公开征求意见。公众可通过以下途径和方式反馈意见：1.通过电子邮件将意见发送至：shujuju@cac.gov.cn。2.通过信函将意见寄至：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数据管理局，邮编：100044，并在信封上注明“网络数据安全管理条例征求意见”。意见反馈截止时间为 2021 年 12 月 13 日。

3. Microsoft 发布 2021 年 11 月安全更新

2021 年 11 月 11 日，据国家信息安全漏洞共享平台 CNVD 消息，11 月 10 日，微软发布了 2021 年 11 月份的月度例行安全公告，修复了其多款产品存在的 55 个安全漏洞。受影响的产品包括 3D Viewer 等 36 个产品。利用上述漏洞，攻击者可进行欺骗，绕过安全功能限制，获取敏感信息，提升权限，执行远程代码，或发起拒绝服务攻击等。CNVD 提醒广大 Microsoft 用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

4. 中央网信办等部门联合印发《关于开展 IPv6 技术创新和融合应用试点工作的通知》

2021 年 11 月 10 日，据中国网信网消息，近日，中央网信办、国家发展改革委、工业和信息化部、教育部、科技部、公安部、财政部、住房和城乡建设部、水利部、中国人民银行、国务院国资委、国家广电总局印发《关于开展 IPv6 技术创新和融合应用试点工作的通知》，联合组织开展 IPv6 技术创新和融合应用试点工作，聚焦重点领域，优先方向和瓶颈问题，探索 IPv6 全链条、全业务、全场景部署和创新应用，以点促面，整体提升 IPv6 规模部署和应用水平。 《通知》明确到 2023 年底，IPv6 技术创新和融合应用试点工作取得明显成效。IPv6 关键技术创新、应用创新、服务创新、管理创新持续突破，IPv6 标准体系更加完善，基本形成 IPv6 技术创新生态体系。IPv6 端到端贯通能力显著增强，关键环节不畅、应用程度不深、终端支持不足等瓶颈问题得到有效解决。5G 网络 IPv6 单栈试点应用范围和场景不断扩展，物联网、工业互联网、智慧家庭等重点领域 IPv6 应用更加广泛，政务、教育、金融、广电、水利等行业 IPv6 融合应用水平大幅提升。IPv6 网络安全保障体系更加完善。综合试点城市率先实现网络、平台、应用、终端及各行业全面支持 IPv6，在 IPv6 整体规划实施、网络改造建设、技术融合应用、产业生态培育等方面形成一批可复制、可推广的做法经验，为全国深入推进 IPv6 规模部署和应用奠定良好基础。

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：周彧

网址： www.cert.org.cn

Email：cncert_report@cert.org.cn

电话： 010-82990315