国家互联网应急中心

网络安全信息与动态周报

2021 年第 30 期

7 月 19 日-7 月 25 日

CNCERT/CC

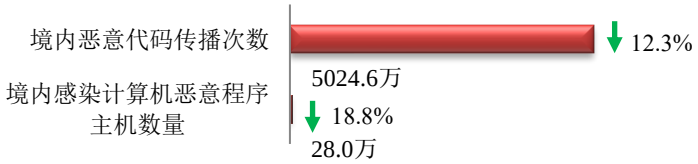
本周网络安全基本态势

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	•5024.6万 •28.0 万	↓ 12.3% ↓ 18.8%
境内被篡改网站总数 其中政府网站数量	•3381 •16	↑ 33.9% ↑ 23.1%
境内被植入后门网站总数 其中政府网站数量	•377 •4	↓ 33.9% ↑ 300%
针对境内网站的仿冒页面数量	•204	↑ 12.1%
新增信息安全漏洞数量 其中高危漏洞数量	•594 •162	↑ 3.3% ↑ 2.5%

= 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

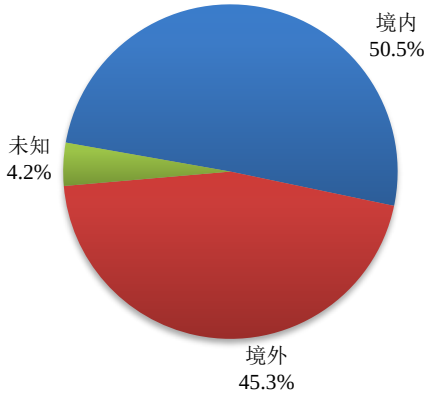
本周网络病毒活动情况

境内计算机恶意程序传播次数约为 5024.6 万次，境内感染计算机恶意程序主机数量约为 28.0 万个。

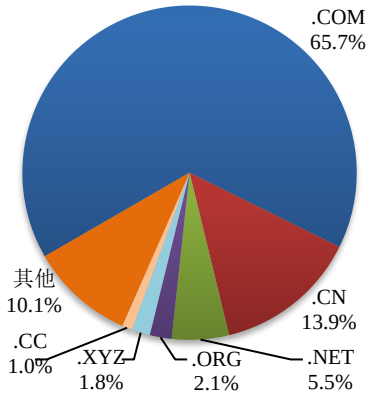


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 6094 个，涉及 IP 地址 25586 个。在 6094 个域名中，有 45.3%为境外注册，且顶级域为.com 的约占 65.7%；在 25586 个 IP 中，有约 75.0%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 603 个。

本周放马站点域名注册所属境内外分布
(7/19-7/25)



本周放马站点域名注册所属顶级域分布
(7/19-7/25)



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。

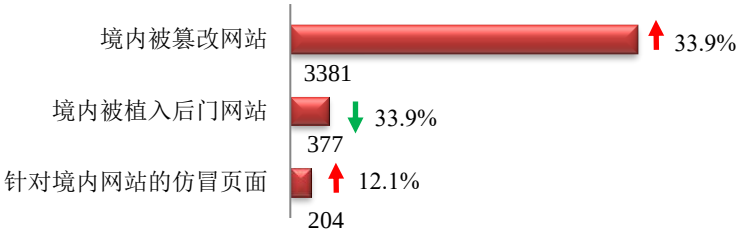
ANVA网络安全威胁信息共享平台

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。

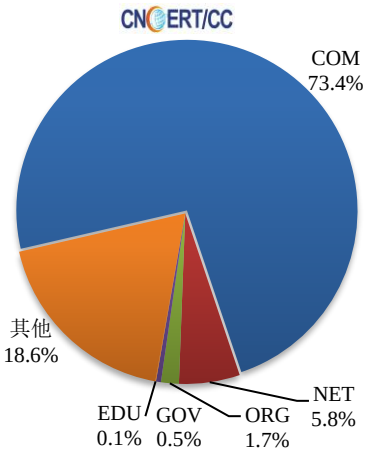
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 3381 个；被植入后门的网站数量为 377 个；针对境内网站的仿冒页面数量为 204 个。

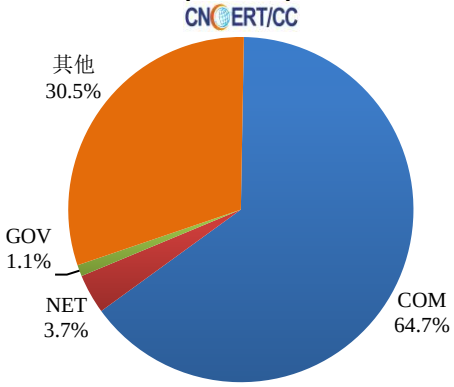


本周境内被篡改政府网站（GOV 类）数量为 16 个（约占境内 0.5%），与上周相比上升 23.1%；境内被植入后门的政府网站（GOV 类）数量为 4 个（约占境内 1.1%），与上周上升 300.0%。

本周我国境内篡改网站按类型分布
(7/19-7/25)

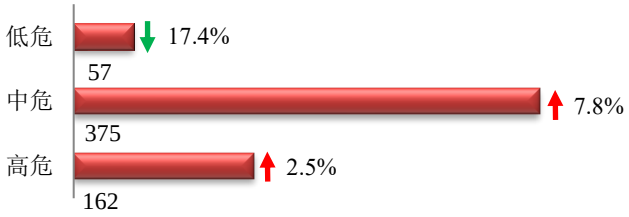


本周我国境内被植入后门网站按类型分布
(7/19-7/25)

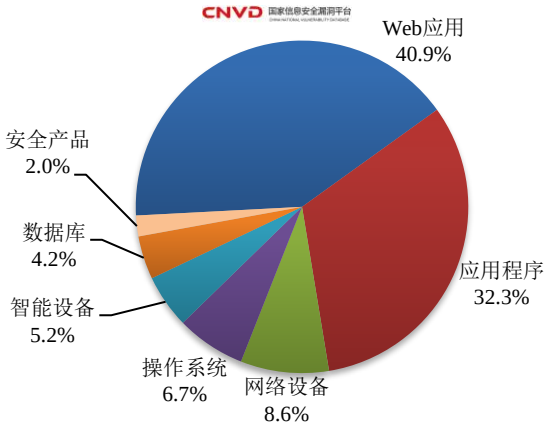


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 594 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
(7/19-7/25）



本周 CNVD 发布的网络安全漏洞中，Web 应用占比最高，其次是应用程序和网络设备。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

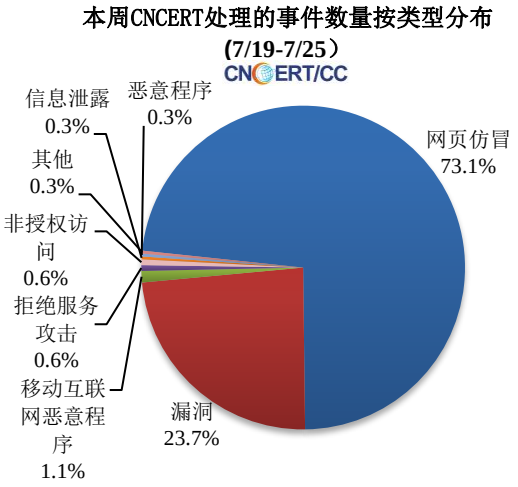
CNVD漏洞周报发布地址

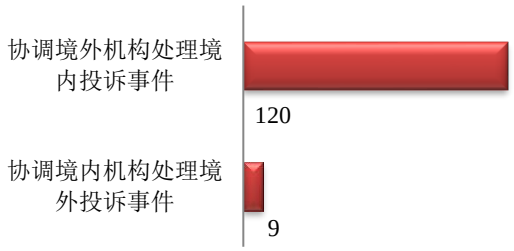
http://www.cnvd.org.cn/webinfo/list?type=4

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。

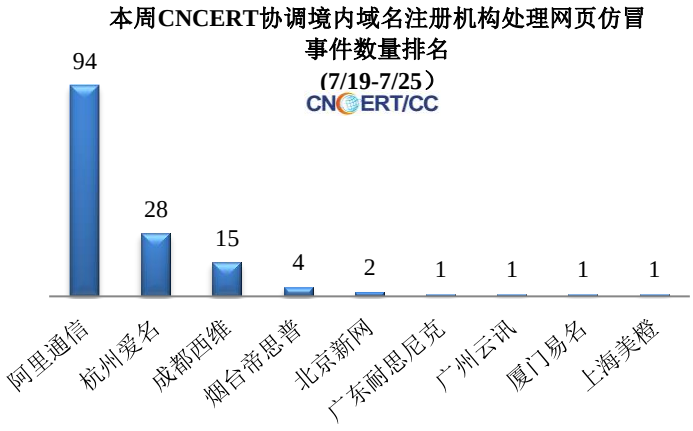
本周事件处理情况

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 350 起，其中跨境网络安全事件 129 起。

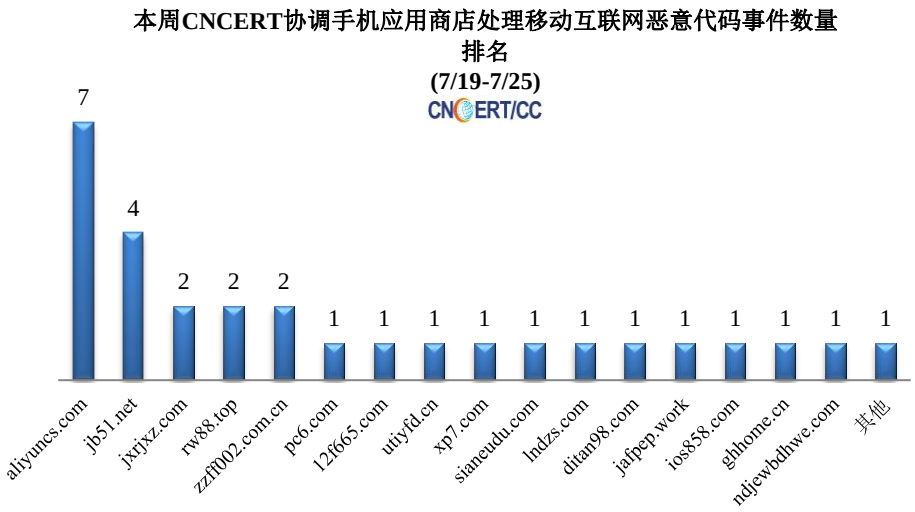




本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理 255 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，银行仿冒事件 249 起，其他事件 6 起。



本周，CNCERT 协调 17 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 28 个。



业界新闻速递

1. 中央网信办、国家发展改革委、工业和信息化部印发《关于加快推进互联网协议第六版（IPv6）规模部署和应用工作的通知》

2021 年 7 月 23 日，据中国网信网消息，近日，中央网信办、国家发展改革委、工业和信息化部印发《关于加快推进互联网协议第六版（IPv6）规模部署和应用工作的通知》（以下简称《通知》）。《通知》落实《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》有关要求，明确了“十四五”时期深入推进 IPv6 规模部署和应用的主要目标、重点任务和时间表，是各地区、各部门推进 IPv6 部署应用工作的指导性文件。《通知》指出，互联网协议第六版（IPv6）是互联网升级演进的必然趋势、网络技术创新的重要方向、网络强国建设的基础支撑。“十四五”时期是加快数字化发展、建设网络强国和数字中国的重要战略机遇期，我国 IPv6 发展处于攻坚克难、跨越拐点的关键阶段，要立足新发展阶段，贯彻新发展理念，构建新发展格局，落实高质量发展要求，坚定不移推进 IPv6 规模部署和应用。

2. CNCERT 发布《勒索软件防范指南》

2021 年 7 月 23 日，国家计算机网络应急技术处理协调中心（CNCERT/CC）发布《勒索软件防护指南》（以下简称“指南”）。近年来，勒索软件活跃程度居高不下，勒索方式和技术手段不断升级，且以大型高价值机构为攻击目标。根据 CNCERT 发布的数据显示，2019 年捕获的勒索软件数量较 2018 年增长超过 4 倍，2020 年较 2019 年增长 6.8%。2021 年上半年，勒索软件攻击愈发频繁，国内外发生多起重大事件。为有效防范勒索软件的危害，指南提出了勒索软件防范做到的“九要”“四不要”，并指出了遭勒索软件攻击后的应急处置方法。

3. CNCERT 发布《2020 年中国互联网网络安全报告》

2021 年 7 月 20 日，国家计算机网络应急技术处理协调中心（CNCERT/CC）编写的《2020 年中国互联网网络安全报告》正式发布。自 2008 年起，CNCERT 持续编写发布中国互联网网络安全年度报告，依托 CNCERT 多年来从事网络安全监测、预警和应急处置等工作的实际情况，对我国互联网网络安全状况进行总体判断和趋势分析，具有重要的参考价值。该系列报告为政府部门提供监管支撑，为互联网企业提供运行管理技术支持，向社会公众普及互联网网络安全知识，对提高全社会、全民的网络安全意识发挥积极作用。《2020 年中国互联网网络安全报告》汇总分析了 CNCERT 自有网络安全监测数据和 CNCERT 网络安全应急服务支撑单位报送的数据，具有重要的参考价值，内容涵盖我国互联网网络安全态势分析、网络安全监测数据分析、网络安全事件案例详解、网络安全政策和技术动态等多个方面。其中，报告对计算机恶意程序传播和活动、移动互联网恶意程序传播和活动、网站安全监测、DDoS 攻击监测、信息安全漏洞通报与处置、网络安全事件接收与处置等情况进行深入细致的分析，并对 2020 年的典型网络安全事件进行了专题介绍。此外，本报告还对网络安全组织发展情况和 CNCERT 举办的重要网络安全会议和活动等情况进行了阶段性总结，并对 2021 年网络安全关注方向进行预测。

4. 2021 年中国网络安全年会在北京成功召开

2021 年 7 月 20 日，以“携手应对数据安全威胁挑战”为主题的 2021 年中国网络安全年会在北京成功召开。本届中国网络安全年会由国家互联网信息办公室指导，国家计算机网络应急技术处理协调中心（CNCERT/CC）主办，深信服科技、安天、绿盟科技、恒安嘉新、杭州安恒、奇安信、长安通信、中国电信集成、阿里云、360 政企安全、天融信、启明星辰、亚信安全公司联合主办，新华网、中国通信学会协办。中央网信办副总工程师、国家计算机网络应急技术处理协调中心主任李湘宁致欢迎辞并作主旨发言。中央网信办网络安全协调局局长孙蔚敏、工业和信息化部网络安全管理局副局长陶青、公安部十一局副巡视员黄小苏致辞。中国工程院院士倪光南、中国科学院院士冯登国，国家计算机网络应急技术处理协调中心党委副书记卢卫，以及多位企业代表分别作主旨报告。大会还设置了“聚力数据安全，赋能数字未来”“新一代基础设施原生安全”“网安协同联动”“数据安全新要求，风险治理新理念”“实战化安全运营”“安全能力体系建设”6 个主题分论坛和一个闭门论坛。一年一度的“中国网络安全年会”已成为国内网络安全领域的重要会议，成为国内网络安全“产、学、研、用”各界进行技术业务交流的桥梁和纽带，对于提高我国网络安全保障水平、增强全社会网络安全意识起到积极作用。

5. 工信部通报 145 款侵害用户权益行为 APP

2021 年 7 月 19 日，据工业和信息化部网站消息，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

构针对用户反映问题较多的医疗健康、电子商务、实用工具等类型手机应用软件进行了专项检查，已通知相关企业进行了整改。截至目前，尚有 71 款 APP 未完成整改。各通信管理局按工信部 APP 整治行动部署，积极开展手机应用软件监督检查，辽宁省、浙江省、广东省、四川省、宁夏回族自治区通信管理局检查发现仍有 74 款 APP 未完成整改。上述 145 款 APP 应在 7 月 26 日前完成整改落实工作，逾期不整改的，工信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：郭晶

网址： www.cert.org.cn

Email：cncert_report@cert.org.cn

电话： 010-82990315