国家互联网应急中心

2021 年第 27 期

6 月 28 日-7 月 4 日

网络安全信息与动态周报

CNCERT/CC

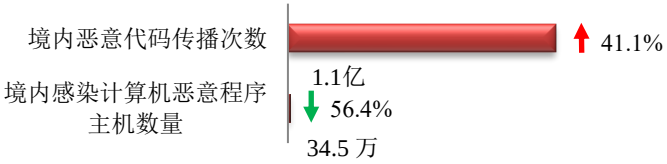
本周网络安全基本态势

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	•1.1亿 •34.5万	↑41.1% ↓56.4%
境内被篡改网站总数 其中政府网站数量	•2592 •13	↑2.3% ↓23.5%
境内被植入后门网站总数 其中政府网站数量	•503 •1	↓63.8% ↓66.7%
针对境内网站的仿冒页面数量	•171	↓63.5%
新增信息安全漏洞数量 其中高危漏洞数量	•608 •107	↑0.5% ↓36.3%

= 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

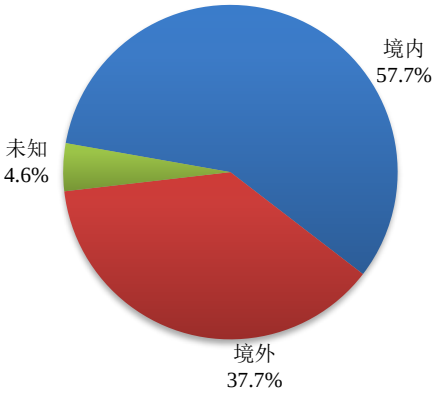
本周网络病毒活动情况

境内计算机恶意程序传播次数约为 1.106 亿次，境内感染计算机恶意程序主机数量约为 34.5 万个。

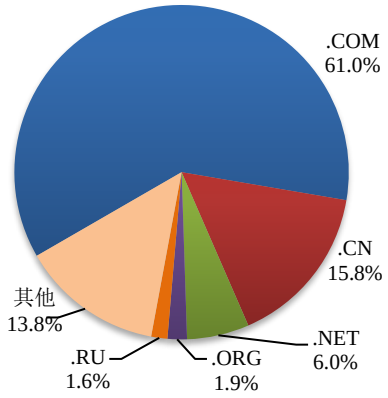


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1280 个，涉及 IP 地址 5333 个。在 1280 个域名中，有 37.7%为境外注册，且顶级域为.com 的约占 61.0%；在 5333 个 IP 中，有约 34.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 171 个。

本周放马站点域名注册所属境内外分布
(6/28-7/4)



本周放马站点域名注册所属顶级域分布
(6/28-7/4)



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。

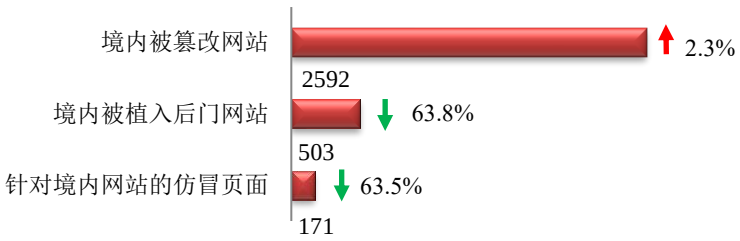
ANVA网络安全威胁信息共享平台

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。

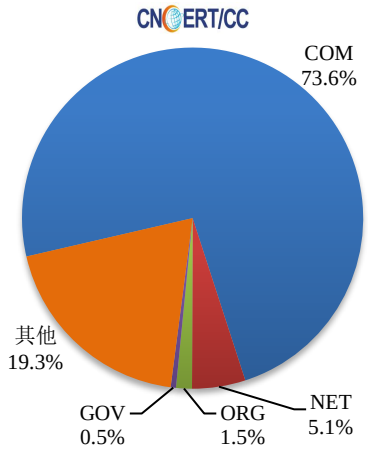
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 2592 个；被植入后门的网站数量为 503 个；针对境内网站的仿冒页面数量为 171 个。

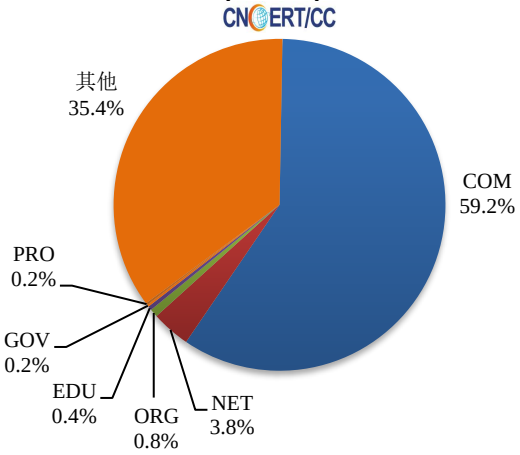


本周境内被篡改政府网站（GOV 类）数量为 13 个（约占境内 0.5%），与上周下降了 23.5%；境内被植入后门的政府网站（GOV 类）数量为 1 个（约占境内 0.2%），与上周相比下降了 66.7%。

本周我国境内篡改网站按类型分布
(6/28-7/4)

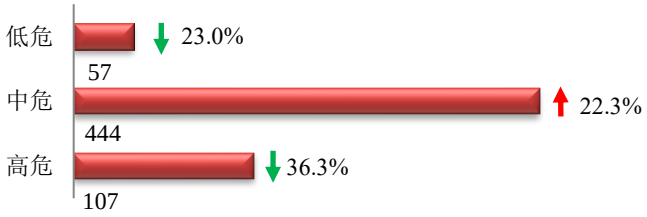


本周我国境内被植入后门网站按类型分布
(6/28-7/4)

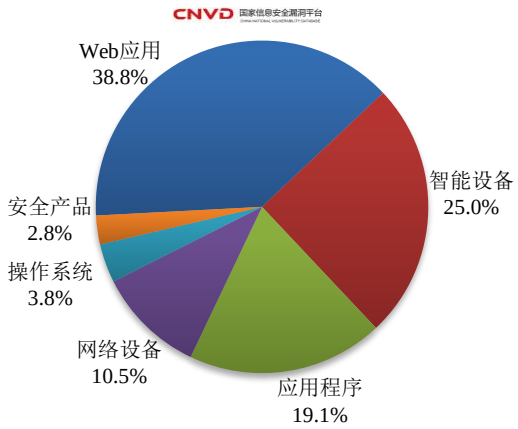


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 608 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
(6/28-7/4)



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

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

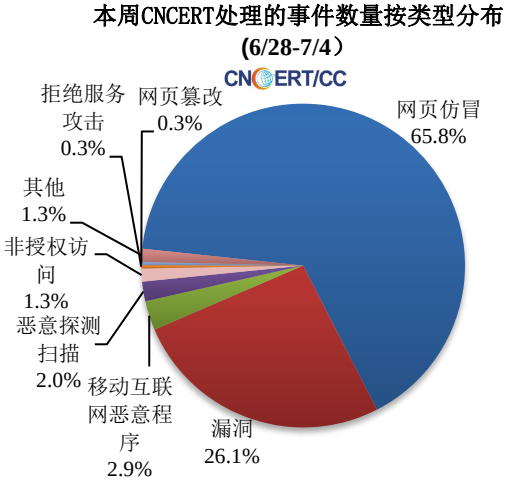
CNVD漏洞周报发布地址

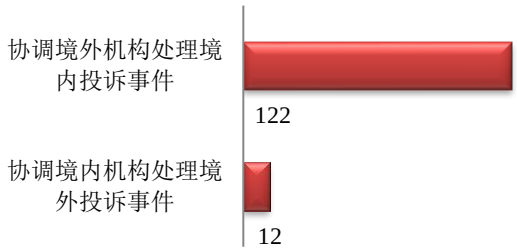
http://www.cnvd.org.cn/webinfo/list?type=4

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。

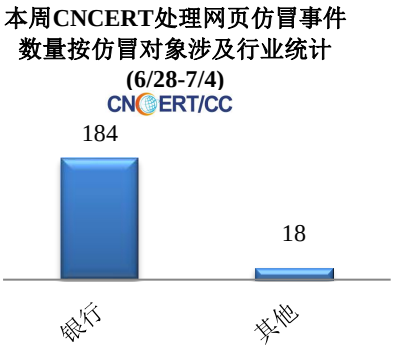
本周事件处理情况

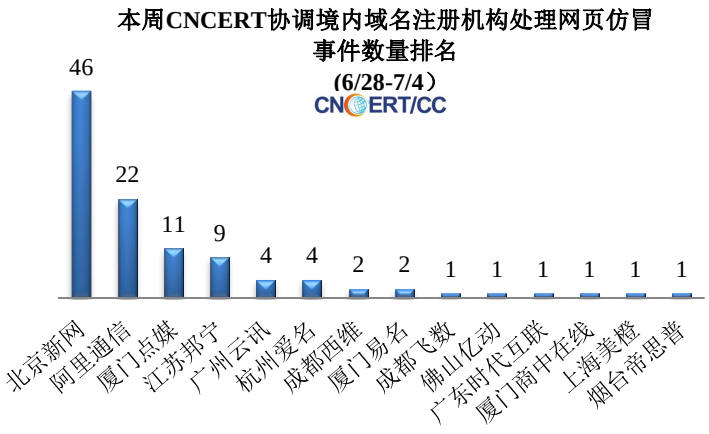
本周，CNCERT 协调云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 307 起，其中跨境网络安全事件 134 起。



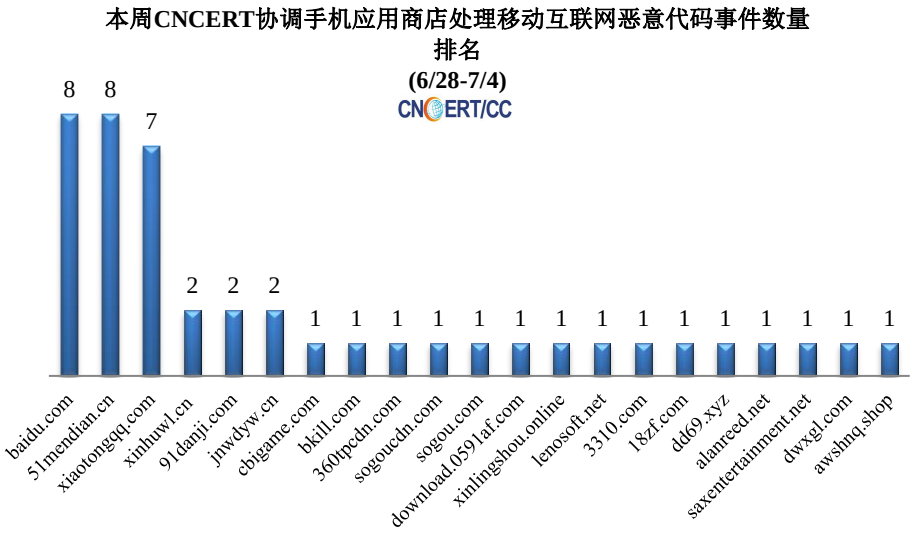


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理 202 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，银行仿冒事件 184 起，其他事件 18 起。





本周，CNCERT 协调 21 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 44 个。



业界新闻速递

1. 关于下架“滴滴出行”App 的通报

2021 年 7 月 4 日，据中国网信网消息，根据举报，经检测核实，“滴滴出行”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“滴滴出行”App，要求滴滴出行科技有限公司严格按照法律要求，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。

2. 关于遴选第九届 CNCERT 网络安全应急服务支撑单位的通知

2021 年 7 月 2 日，国家互联网应急中心（以下简称 CNCERT）组织开展第九届 CNCERT 网络安全应急服务支撑单位（以下简称“支撑单位”）遴选工作。本次遴选面向国家网络安全保障需要，按照开放、合作、自愿、共享的发展理念，坚持公平公正、开放竞争，面向全国企事业单位公开遴选，凝聚全国技术力量共同维护国家网络安全。第九届支撑单位拟遴选类别分为：国家级、省级、反网络诈骗（重点技术领域）、APT 监测分析（重点技术领域）。各类别说明详见《CNCERT 网络安全应急服务支撑单位申报指南》。

3. CNCERT 发布《2021 年开源软件供应链安全风险研究报告》

2021 年 6 月 30 日，国家互联网应急中心(CNCERT)发布《2021 年开源软件供应链安全风险研究报告》。CNCERT 联合棱镜七彩开源安全研究团队持续对开源软件供应链安全进行跟踪分析。《2019 年开源软件风险研究报告》主要从 GitHub 热门开源软件视角出发，对开源软件安全风险进行了分

析。本报告从全新视角带来开源安全风险新的发现与突破。报告共分为五部分，第一部分，首先介绍开源漏洞的发展现状及趋势；第二部分，聚焦开源组件生态库的安全风险；第三部分，重点围绕组件按依赖层级漏洞传播范围分析；第四部分，对文件级漏洞潜在安全风险及波及范围进行讨论；第五部分，对开源使用者和关注者如何在开源领域蓬勃发展下，更安全的拥抱开源生态提出了建设性意见。本报告详细内容参见 CNCERT 官网。

4. CNCERT 发布《关于新型 P2P 僵尸网络 PBot 的分析报告》

2021 年 6 月 28 日，国家互联网应急中心（CNCERT）与北京奇虎科技有限公司（360）共同发布《关于新型 P2P 僵尸网络 PBot 的分析报告》。CNCERT 监测发现从 2020 年以来 P2P 僵尸网络异常活跃，如 Mozi、Pinkbot 等 P2P 僵尸网络家族在 2020 年均异常活跃，感染规模大、追溯源头难且难以治理，给网络空间带来较大威胁。2021 年 5 月 31 日，CNCERT 和 360 捕获到一个全新的使用自定义 P2P 协议的僵尸网络，其主要功能为 DDoS。当前很多杀毒引擎将其识别为 Mirai 或 Gafgyt 家族，CNCERT 和 360 将之命名 PBot。本报告详细内容参见 CNCERT 官网。

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：温森浩

网址：www.cert.org.cn

Email：cncert_report@cert.org.cn

电话：010-82990315