国家互联网应急中心

2021 年第 31 期

7 月 26 日-8 月 1 日

网络安全信息与动态周报

CNCERT/CC

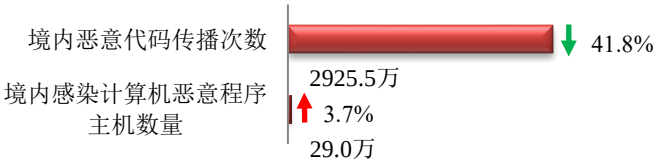
本周网络安全基本态势

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	•2925.5万 •29.0 万	↓ 41.8% ↑ 3.7%
境内被篡改网站总数 其中政府网站数量	•1070 •3	↓ 68.4% ↓ 81.3%
境内被植入后门网站总数 其中政府网站数量	•633 •0	↑ 67.9% ↓ 100%
针对境内网站的仿冒页面数量	•142	↓ 30.4%
新增信息安全漏洞数量 其中高危漏洞数量	•484 •131	↓ 18.5% ↓ 19.1%

= 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

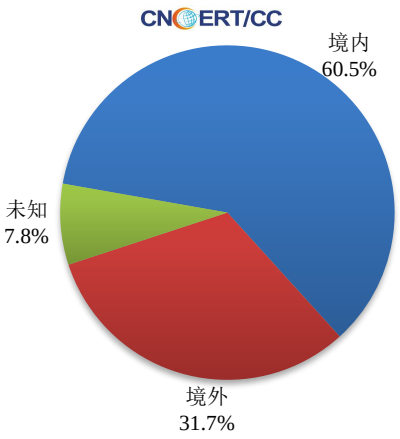
本周网络病毒活动情况

境内计算机恶意程序传播次数约为 2925.5 万次，境内感染计算机恶意程序主机数量约为 29.0 万个。

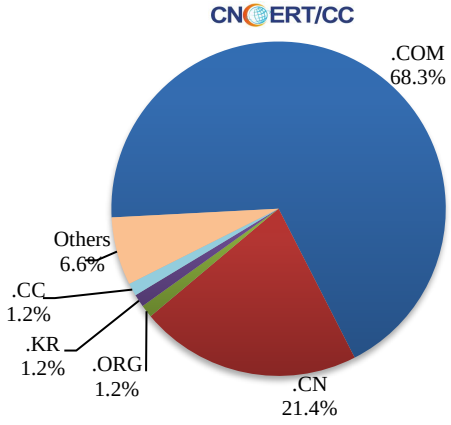


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 243 个，涉及 IP 地址 1082 个。在 243 个域名中，有 31.7%为境外注册，且顶级域为.com 的约占 68.3%；在 1082 个 IP 中，有约 24.5%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 93 个。

本周放马站点域名注册所属境内外分布
(7/26-8/1)



本周放马站点域名注册所属顶级域分布
(7/26-8/1)



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。

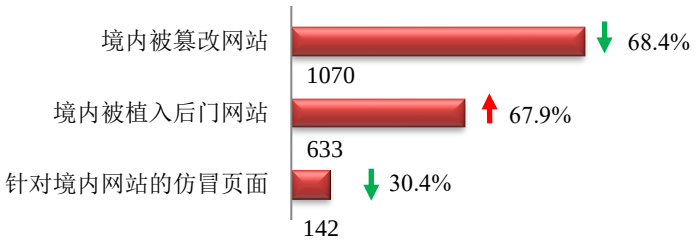
ANVA网络安全威胁信息共享平台

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。

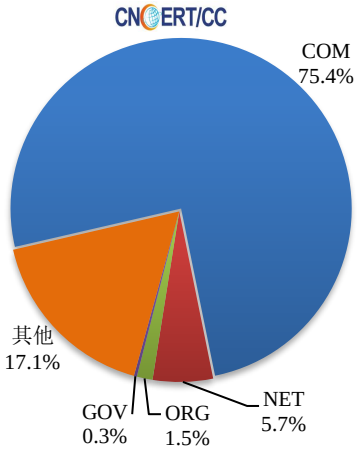
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 1070 个；被植入后门的网站数量为 633 个；针对境内网站的仿冒页面数量为 142 个。

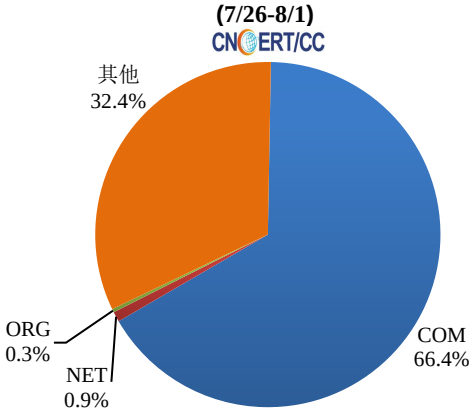


本周境内被篡改政府网站（GOV 类）数量为 3 个（约占境内 0.3%），与上周相比下降 81.3%；境内被植入后门的政府网站（GOV 类）数量为 0 个，与上周相比下降 100.0%。

本周我国境内篡改网站按类型分布
(7/26-8/1)

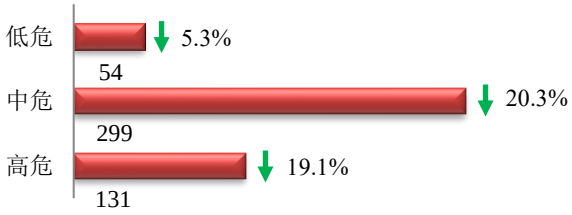


本周我国境内被植入后门网站按类型分布
(7/26-8/1)

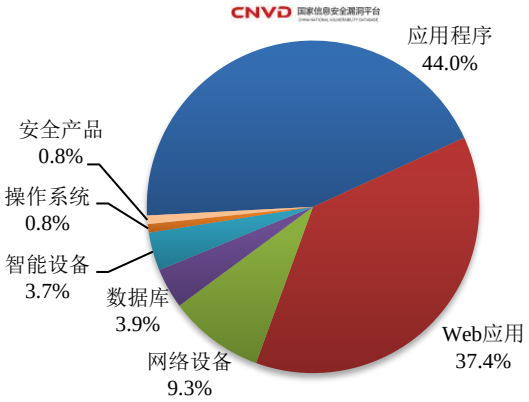


本周重要漏洞情况

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
(7/26-8/1）



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。

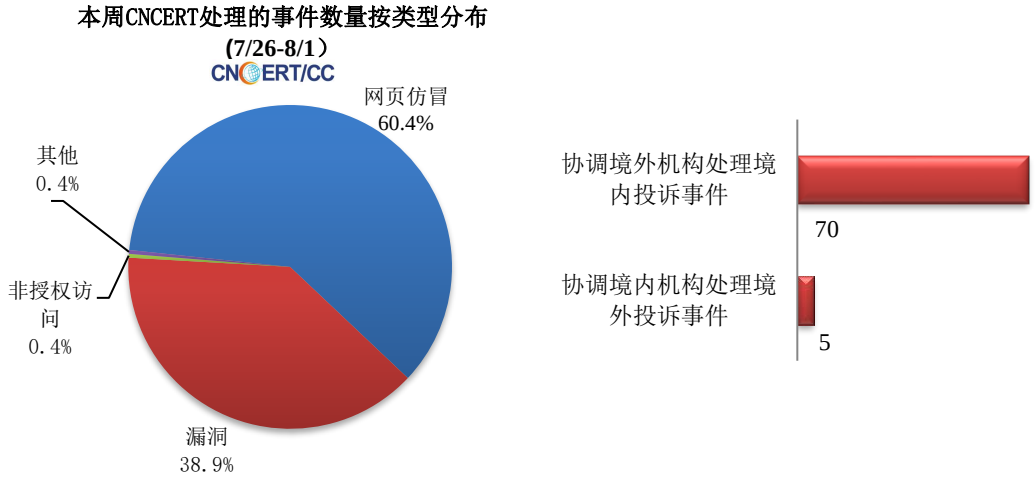
CNVD漏洞周报发布地址

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

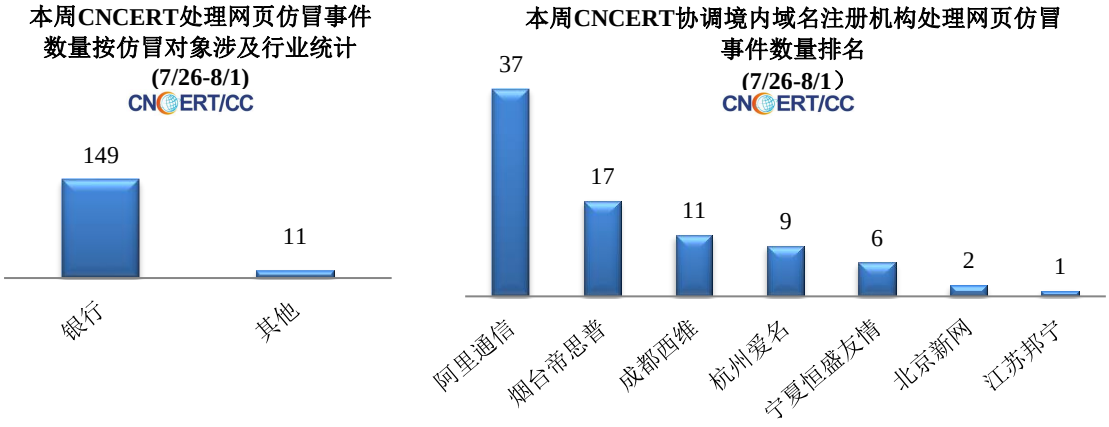
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

本周事件处理情况

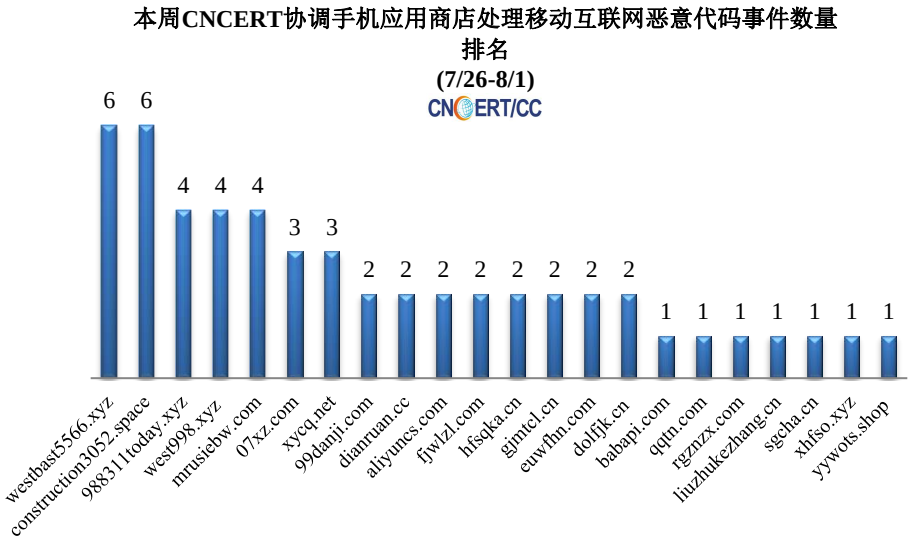
本周，CNCERT 协调云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 265 起，其中跨境网络安全事件 75 起。



本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理 160 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 149 起，其他事件 11 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 53 个。



业界新闻速递

1. CNCERT 发布《2021 年上半年我国互联网网络安全监测数据分析报告》

2021 年 7 月 31 日，CNCERT 发布《2021 年上半年我国互联网网络安全监测数据分析报告》。CNCERT 对上半年监测数据进行了梳理，形成了监测数据分析报告，报告全面反映了 2021 年上半年我国互联网在恶意程序传播、漏洞风险、DDoS 攻击、网站安全等方面的情况。

2. 工信部通报 14 款未严格落实开屏弹窗信息骚扰用户问题整改要求的 APP

2021 年 7 月 28 日，据工业和信息化部网站消息，前期工业和信息化部针对用户反映强烈投诉较多的开屏弹窗信息骚扰用户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、整屏图片、视频等方式欺骗误导用户跳转等问题。近期，工业和信息化部在对该问题“回头看”中，依然发现部分企业“有令不行、有禁不止”，存在问题整改不彻底、将整改过的问题改回原样、采取技术手段对抗针对不同地区差异化整改的情况。检测发现，14 款 APP 未严格落实整改要求，上述 APP 需在 8 月 3 日前完成彻底整改工作。逾期不整改的或整改不到位的，工业和信息化部将依法依规组织开展相关处置工作。

3. 最高人民法院发布《关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》

2021 年 7 月 28 日，据最高人民法院官网消息，为正确审理使用人脸识别技术处理个人信息相关民事案件，保护当事人合法权益，促进数字经济健康发展，根据《中华人民共和国民法典》《中华人民共和国网络安全法》《中华人民共和国消费者权益保护法》《中华人民共和国电子商务法》

《中华人民共和国民事诉讼法》等法律的规定，结合审判实践，最高人民法院制定本规定。因信息处理者违反法律、行政法规的规定或者双方的约定使用人脸识别技术处理人脸信息、处理基于人脸识别技术生成的人脸信息所引起的民事案件，适用本规定。人脸信息的处理包括人脸信息的收集、存储、使用、加工、传输、提供、公开等。

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：胡俊

网址： www.cert.org.cn

Email：cncert_report@cert.org.cn

电话： 010-82990315