

网络安全信息与动态周报



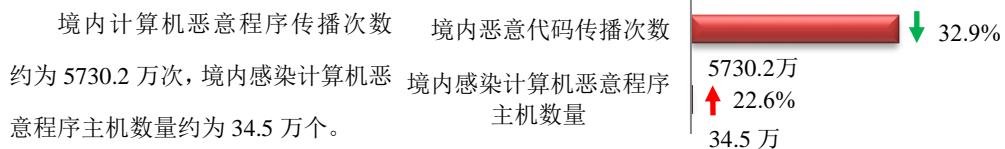
本周网络安全基本态势



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	• 5730.2万 • 34.5万	↓ 32.9% ↑ 22.6%
境内被篡改网站总数 其中政府网站数量	• 2525 • 13	↓ 13.1% =
境内被植入后门网站总数 其中政府网站数量	• 570 • 1	↑ 56.2% =
针对境内网站的仿冒页面数量	• 182	↓ 48.3%
新增信息安全漏洞数量 其中高危漏洞数量	• 575 • 158	↑ 6.3% ↑ 22.5%

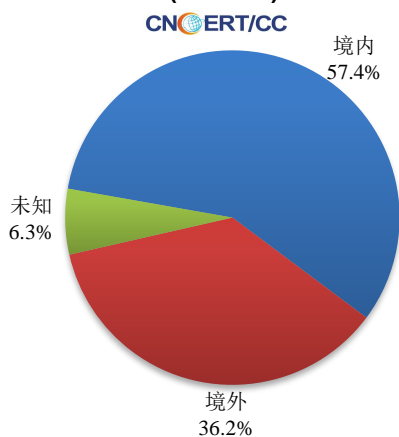
▬ 表示数量与上周相同 ↑ 表示数量较上周环比增加 ↓ 表示数量较上周环比减少

本周网络病毒活动情况

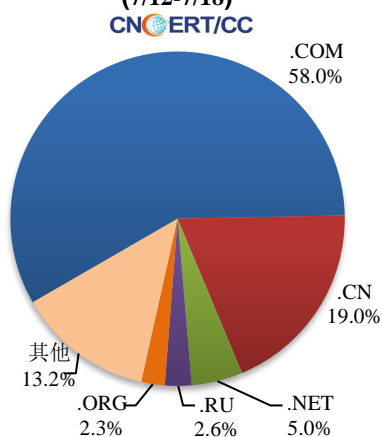


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1010 个，涉及 IP 地址 5361 个。在 1010 个域名中，有 36.2% 为境外注册，且顶级域为 .com 的约占 58.0%；在 5361 个 IP 中，有约 30.3% 位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 192 个。

本周放马站点域名注册所属境内外分布
(7/12-7/18)



本周放马站点域名注册所属顶级域分布
(7/12-7/18)



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。

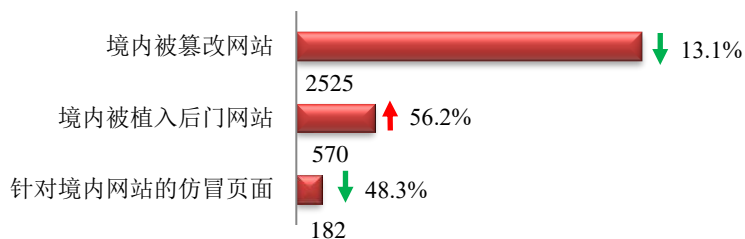
ANVA 网络安全威胁信息共享平台

<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。

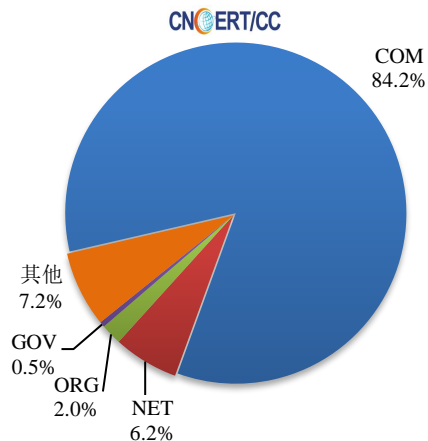
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 2525 个；被植入后门的网站数量为 570 个；针对境内网站的仿冒页面数量为 182 个。

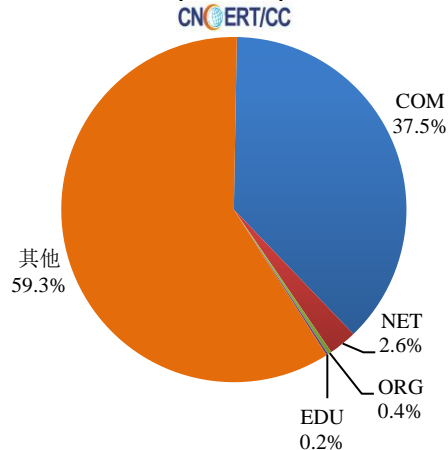


本周境内被篡改政府网站（GOV类）数量为13个（约占境内1.2%），与上周持平；境内被植入后门的政府网站（GOV类）数量为1个（约占境内0.1%），与上周持平。

本周我国境内篡改网站按类型分布
(7/12-7/18)

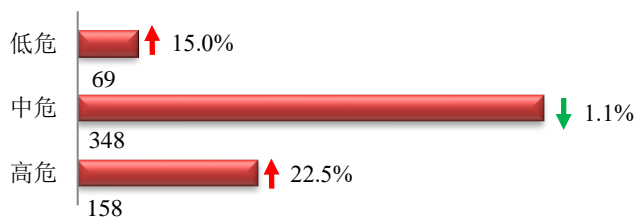


本周我国境内被植入后门网站按类型分布
(7/12-7/18)

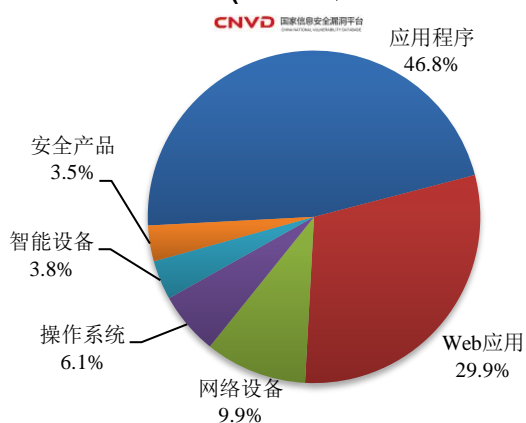


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞575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
(7/12-7/18)



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>

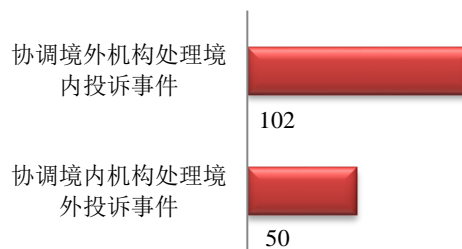
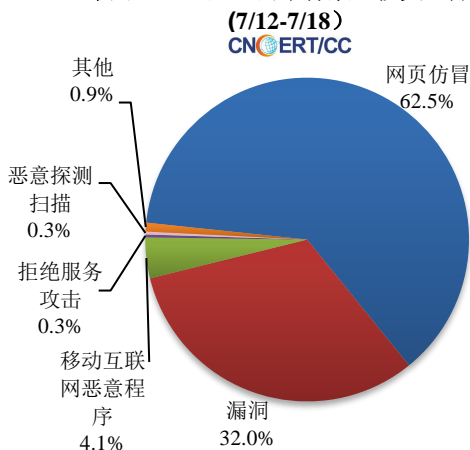
国家信息安全漏洞共享平台(缩写CNVD)是CNCERT联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。



本周事件处理情况

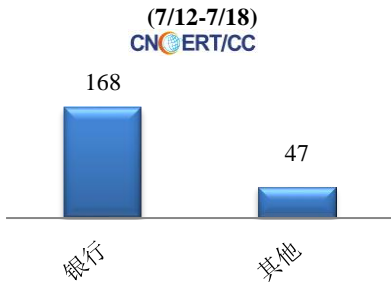
本周，CNCERT 协调云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 344 起，其中跨境网络安全事件 152 起。

本周CNCERT处理的事件数量按类型分布

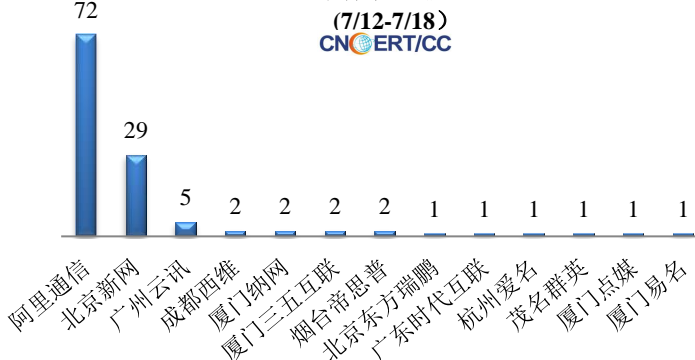


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理 215 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，银行仿冒事件 168 起，其他事件 47 起。

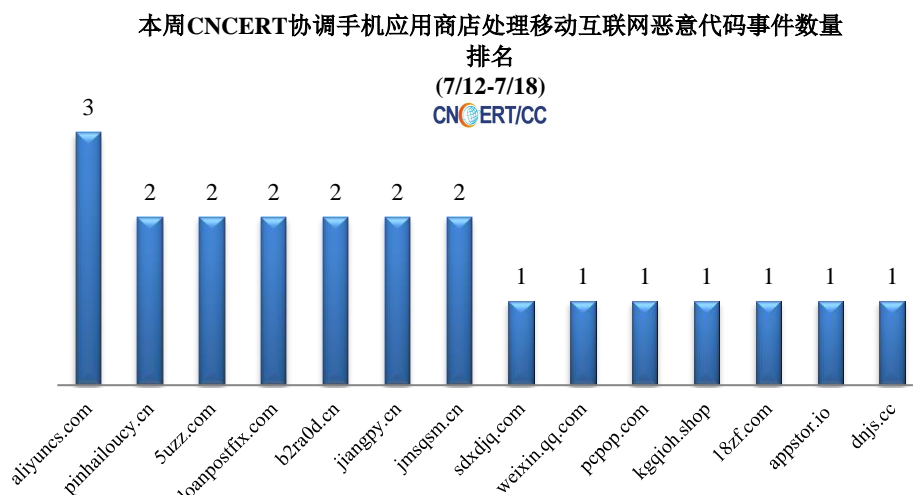
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计



本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名



本周，CNCERT 协调 14 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 22 个。



业界新闻速递

1. 工信部发布《网络安全产业高质量发展三年行动计划（2021-2023年）（征求意见稿）》

2021年7月12日，据工业和信息化部网站消息，为深入贯彻党中央、国务院关于制造强国和网络强国的战略决策部署，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，加快推动网络安全产业高质量发展，提升网络安全产业综合实力，工业和信息化部起草了《网络安全产业高质量发展三年行动计划（2021-2023年）（征求意见稿）》。为进一步听取社会各界意见，予以公示。

2. 工信部关于下架侵害用户权益APP名单的通报

2021年7月12日，据工信部网站消息，工信部公开通报第5批（总第14批）APP，经第三方检测机构核查复检，截至目前尚有18款APP未按照工信部要求完成整改。上海、安徽、广东、四川省（市）通信管理局检查发现共有30款APP仍未完成整改依据《网络安全法》《电信和互联网用户个人信息保护规定》《移动智能终端应用软件预置和分发管理暂行规定》等法律和规范性文件要求，工信部组织对上述48款APP进行下架。相关应用商店应在本通报发布后，立即组织对名单中应用软件进行下架处理。

3. 工信部、国家网信办、公安部联合印发《网络产品安全漏洞管理规定》

2021年7月13日，据中国网信网消息，工信部、国家网信办和公安部联合发布《网络产品安全漏洞管理规定》。该规定自2021年9月1日起施行。中华人民共和国境内的网络产品（含硬件、软件）提供者和网络运营者，以及从事网络产品安全漏洞发现、收集、发布等活动的组织或者

个人，均应遵守本规定。此外规定细化了相关政府职能部门分工：国家互联网信息办公室负责统筹协调网络产品安全漏洞管理工作。工业和信息化部负责网络产品安全漏洞综合管理，承担电信和互联网行业网络产品安全漏洞监督管理。公安部负责网络产品安全漏洞监督管理，依法打击利用网络产品安全漏洞实施的违法犯罪活动。有关主管部门加强跨部门协同配合，实现网络产品安全漏洞信息实时共享，对重大网络产品安全漏洞风险开展联合评估和处置。

4. “2021 年中国网络安全年会” 正式启动注册

7月13日，据CNCERT官网消息，“2021年中国网络安全年会”将于7月20-21日举办。本次年会以“携手应对数据安全威胁挑战”为主题，设置1个主论坛和7个分论坛，聚焦国内外网络安全工作新情况、新形势与新挑战，邀请党政机关有关部门负责同志，知名院士、专家学者，知名网络安全机构和企业负责人等嘉宾，以网络安全年会为平台，共话数据安全未来发展趋势，共谋数据安全深入合作，全方位、多角度分享网络安全前沿洞察，带来智慧风暴。

5. 国家互联网信息办公室等七部门进驻滴滴出行科技有限公司开展网络安全审查

7月16日，据中国网信网消息，按照网络安全审查工作安排，国家网信办会同公安部、国家安全部、自然资源部、交通运输部、税务总局、市场监管总局等部门联合进驻滴滴出行科技有限公司，开展网络安全审查。

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：朱芸茜

网址：www.cert.org.cn

Email: cncert_report@cert.org.cn

电话：010-82990315