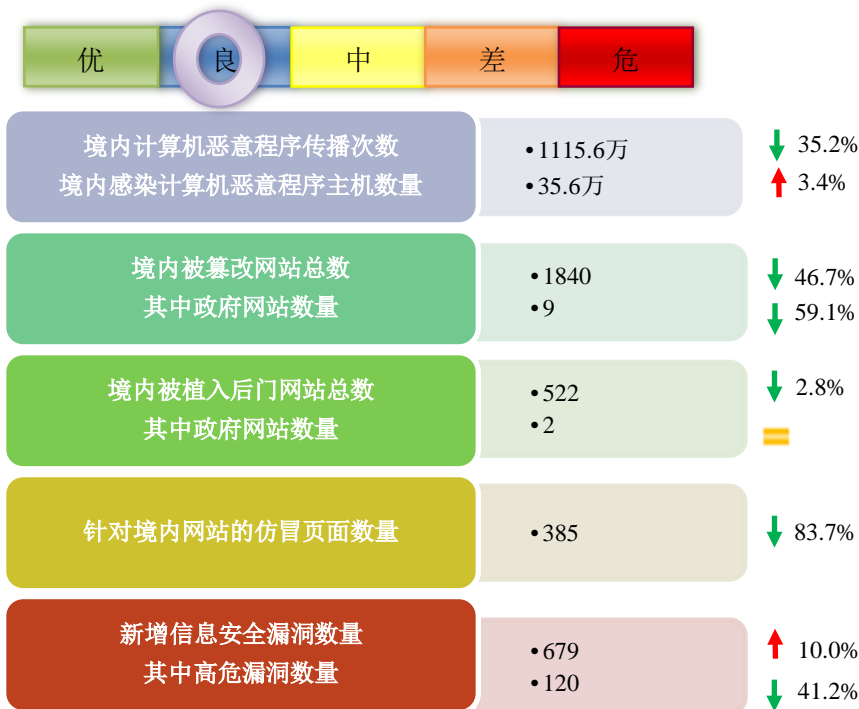


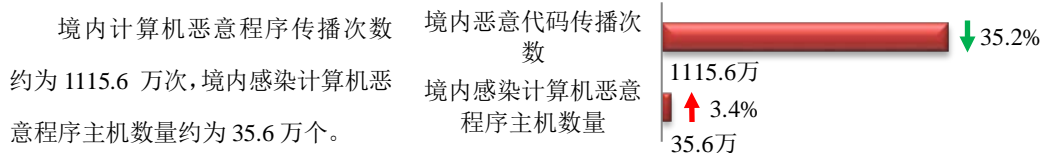
# 网络安全信息与动态周报

## 本周网络安全基本态势



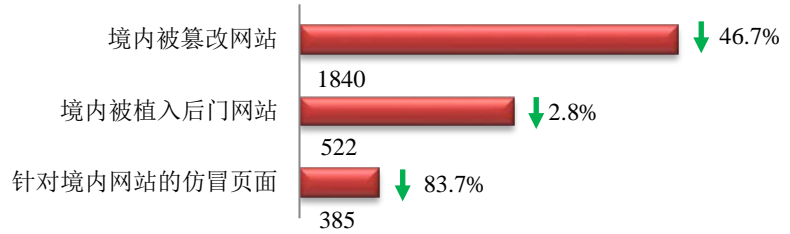
▬ 表示数量与上周相同    ↑ 表示数量较上周环比增加    ↓ 表示数量较上周环比减少

## 本周网络病毒活动情况



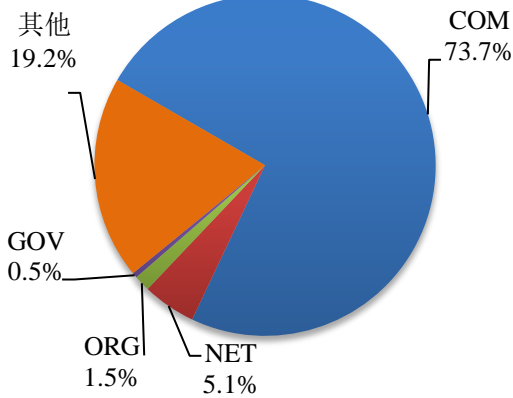
## 本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 1840 个；被植入后门的网站数量为 522 个；针对境内网站的仿冒页面数量为 385 个。

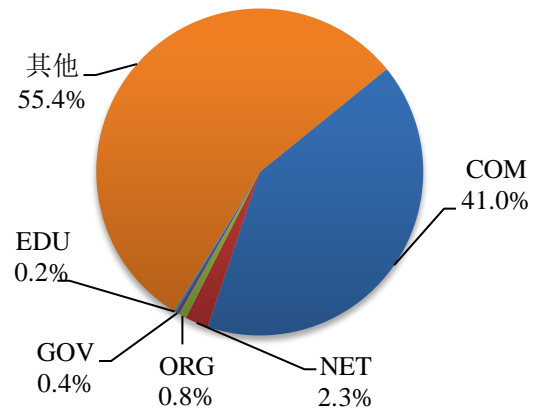


本周境内被篡改政府网站（GOV 类）数量为 9 个（约占境内 0.5%），较上周下降了 59.1%；境内被植入后门的政府网站（GOV 类）数量为 2 个。

本周我国境内篡改网站按类型分布  
(3/15-3/21)  
CNCERT/CC

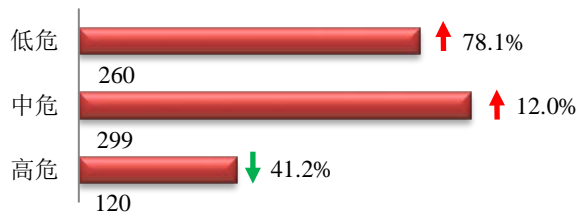


本周我国境内被植入后门网站按类型分布  
(3/15-3/21)  
CNCERT/CC

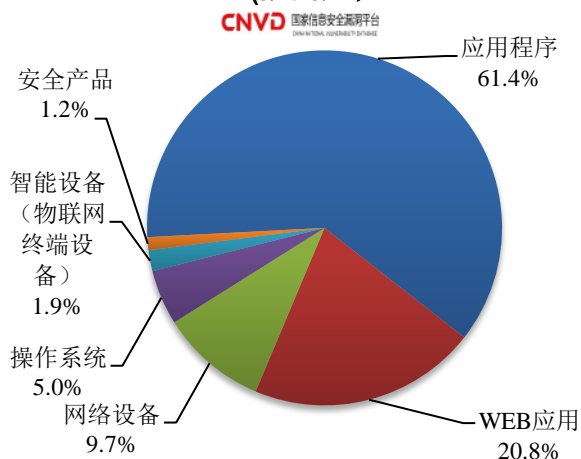


## 本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 679 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  
(3/15-3/21)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，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

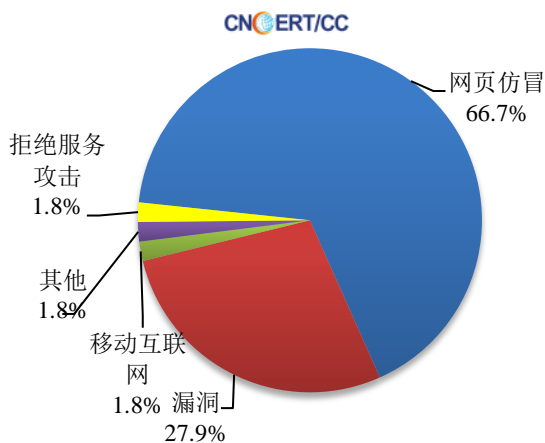
<http://www.cnvd.org.cn/webinfo/list?type=4>

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 219 起，其中跨境网络安全事件 87 起。

本周CNCERT处理的事件数量按类型分布  
(3/15-3/21)



协调境内机构处理境外投诉事件

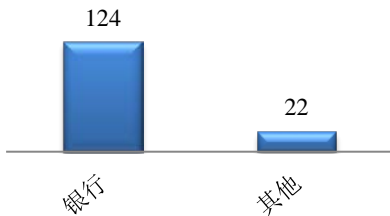
4

协调境外机构处理境内投诉事件

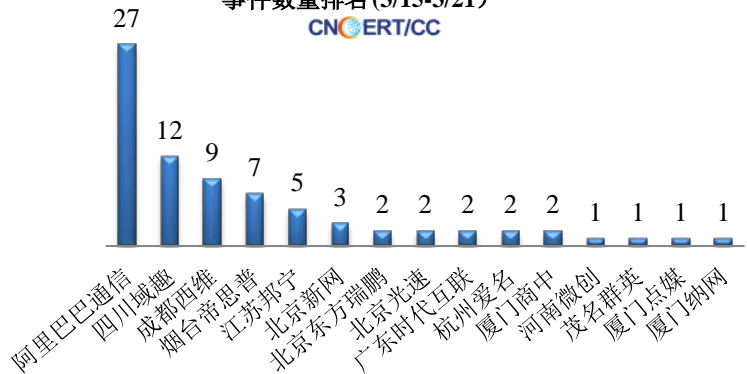
83

本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理 146 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 124 起，其他事件 22 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 (3/15-3/21)  
CNCERT/CC

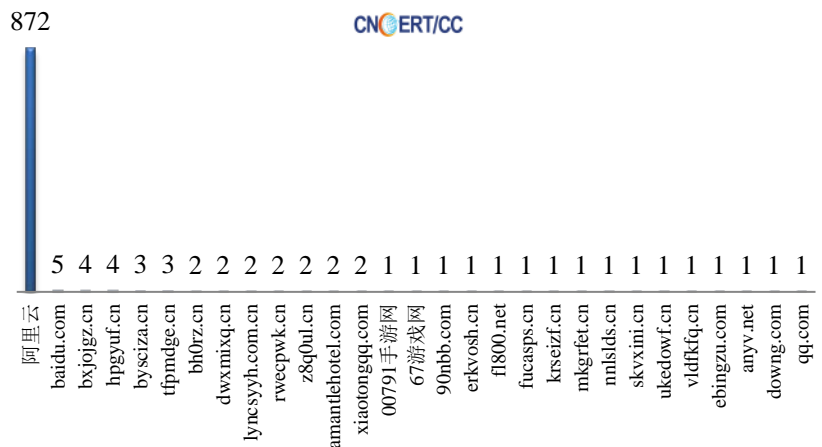


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (3/15-3/21)  
CNCERT/CC



本周，CNCERT 协调 28 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 921 个。

本周CNCERT协调手机应用商店处理移动互联网恶意代码 (3/15-3/21)  
CNCERT/CC



## 业界新闻速递

### 1. 国家网信办等四部委发布关于《常见类型移动互联网应用程序必要个人信息范围规定》的通知

3月22日，据国家网信办网站消息，为贯彻落实《中华人民共和国网络安全法》关于“网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则”“网络运营者不得收集与其提供的服务无关的个人信息”等规定，国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局联合制定了《常见类型移动互联网应用程序必要个人信息范围规定》，明确移动互联网

应用程序（App）运营者不得因用户不同意收集非必要个人信息，而拒绝用户使用 App 基本功能服务。

## 2. CNCERT 发布《2020 年联网智能设备安全态势报告》

3 月 23 日，CNCERT 发布了《2020 年联网智能设备安全态势报告》。2020 年，CNCERT 运营的 CNVD 漏洞平台（国家信息安全漏洞共享平台）新增收录的通用联网智能设备漏洞数量呈显著增长趋势，同比增长 28%。联网智能设备恶意程序通过 P2P 方式传播非常活跃，具有传播速度快、感染规模大、追溯源头难的特点，预计将被越来越多的恶意程序所采用。联网智能设备僵尸网络控制规模增大，部分大型僵尸网络通过 P2P 传播方式与集中控制方式相结合对受控端进行控制，给治理工作带来一定难度。

## 3. 工信部严厉查处“3·15”晚会曝光“诱导老年人下载 APP”“APP 违规收集老年人个人信息”等违规行为

3 月 16 日，据工信部网站消息，工业和信息化部高度重视 APP 用户权益保护工作，连续两年开展 APP 侵害用户权益专项整治行动，重点整治包括 APP 违规收集使用个人信息、欺骗误导用户下载在内的四方面十大类问题。截至 2021 年 3 月，共完成 73 万款 APP 的技术检测工作，连续发布 12 批次对外通报，责令整改 3046 款违规 APP，下架 179 款拒不整改的 APP，治理工作取得了积极成效。针对 2021 年中央广播电视总台“3.15”晚会曝光的内存优化大师、智能清理大师、超强清理大师、手机管家 pro 四款 APP，工业和信息化部第一时间组织开展技术检测，查实其存在欺骗误导用户下载、违规处理个人信息等问题，已要求主要应用商店予以下架，并组织北京、天津、上海、广东四省市通信管理局对涉事企业主体进行调查处理。前期专项整治行动中，工业和信息化部针对存在欺骗误导用户下载问题的 APP，责令整改 300 款、公开通报 37 款、下架 3 款；针对存在违规处理个人信息问题的手机管家、内存优化、垃圾清理类 APP，责令整改 75 款、公开通报 20 款、下架 1 款。

## 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：文静

网址：[www.cert.org.cn](http://www.cert.org.cn)

email：[cncert\\_report@cert.org.cn](mailto:cncert_report@cert.org.cn)

电话：010-82990315