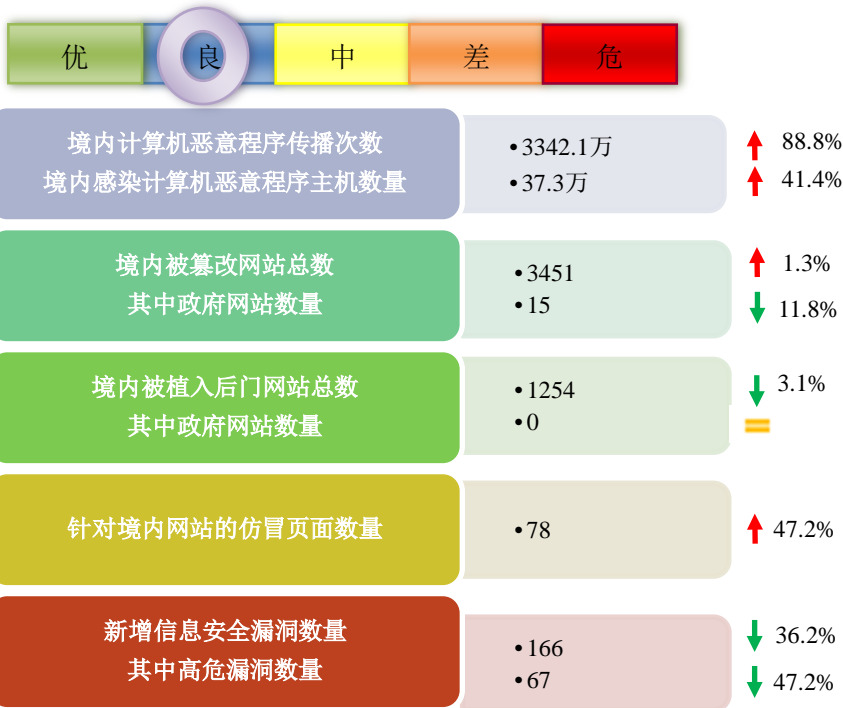


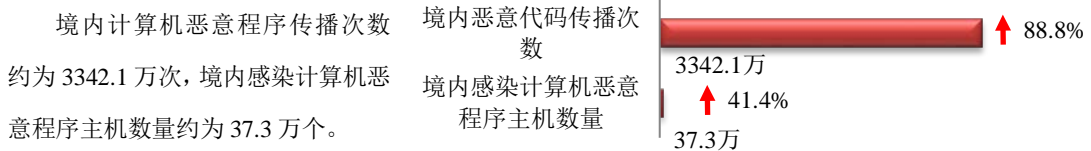
网络安全信息与动态周报

本周网络安全基本态势

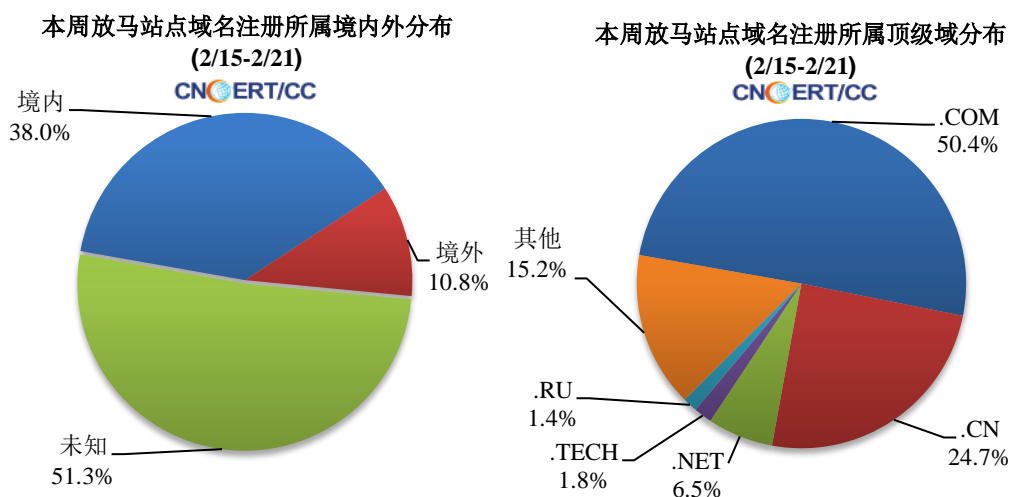


■ 表示数量与上周相同
 ↑ 表示数量较上周环比增加
 ↓ 表示数量较上周环比减少

本周网络病毒活动情况



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 558 个，涉及 IP 地址 3605 个。在 558 个域名中，有 10.8% 为境外注册，且顶级域为 .com 的约占 50.4%；在 3605 个 IP 中，有约 12.3% 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 547 个 IP。



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。

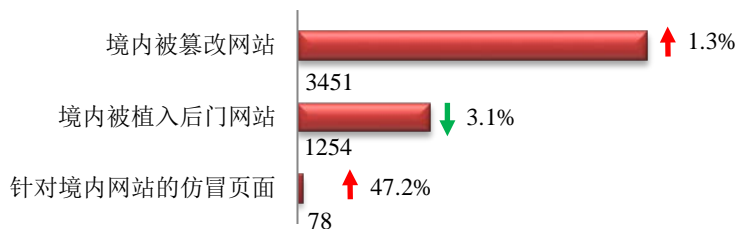
ANVA 网络安全威胁信息共享平台

<https://share.anva.org.cn/web/publicity/listurl>

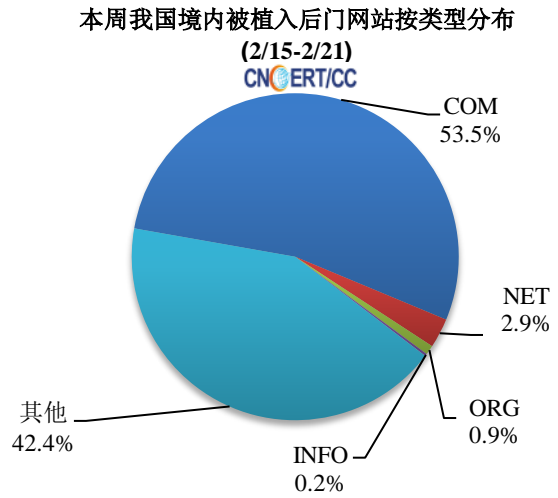
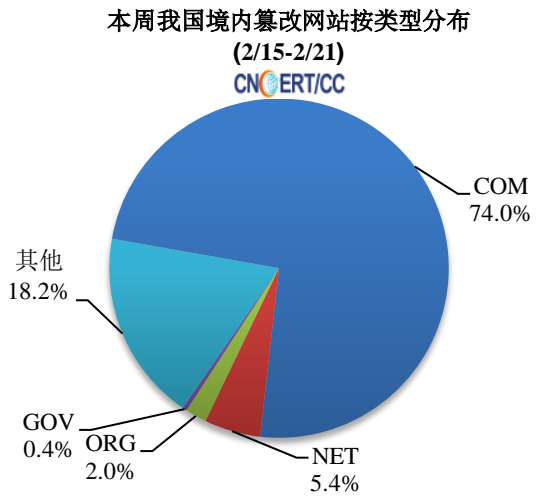
中国反网络病毒联盟 (Anti Network-Virus Alliance of China, 缩写 ANVA) 是由 CNCERT 发起并组织运作的行业联盟。

本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 3451 个；被植入后门的网站数量为 1254 个；针对境内网站的仿冒页面数量为 78 个。

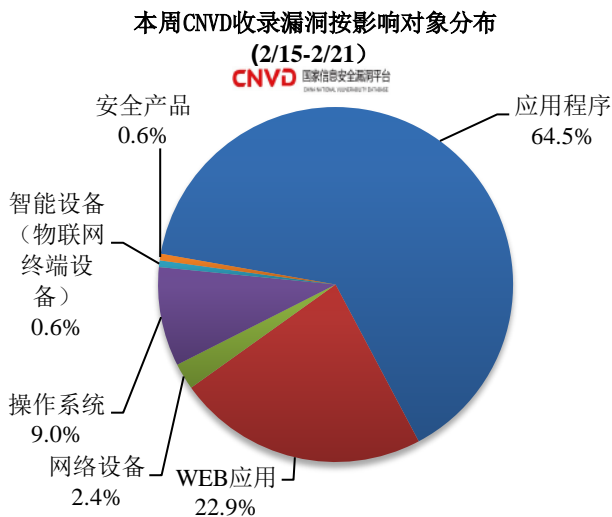
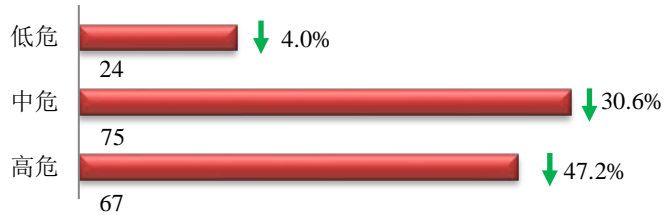


本周境内被篡改政府网站（GOV类）数量为15个（约占境内0.5%），较上周下降了11.8%；境内被植入后门的政府网站（GOV类）数量为0个。



本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞166个，信息安全漏洞威胁整体评价级别为中。



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应用和操作系统。

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

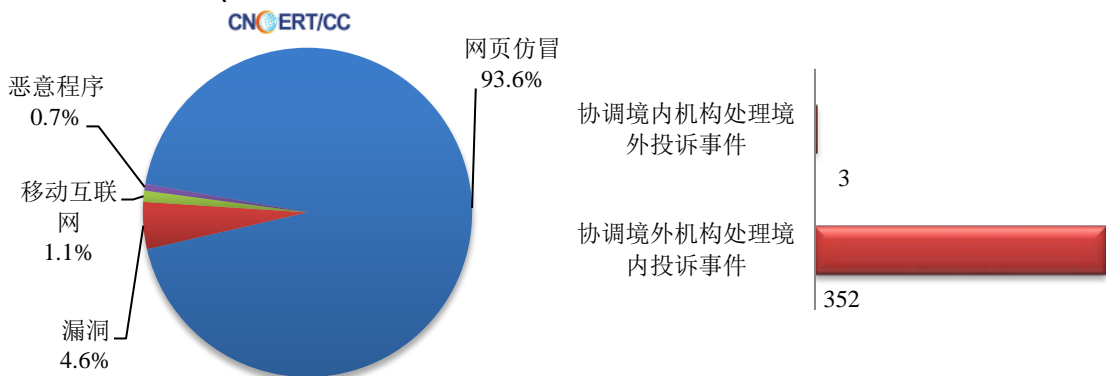
<http://www.cnvd.org.cn/webinfo/list?type=4>

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

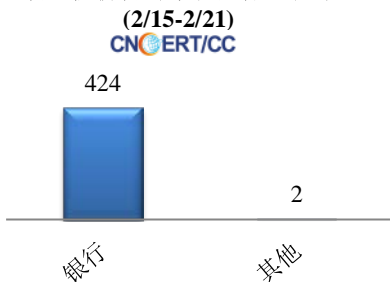
本周，CNCERT 协调云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 455 起，其中跨境网络安全事件 355 起。

本周CNCERT处理的事件数量按类型分布
(2/15-2/21)

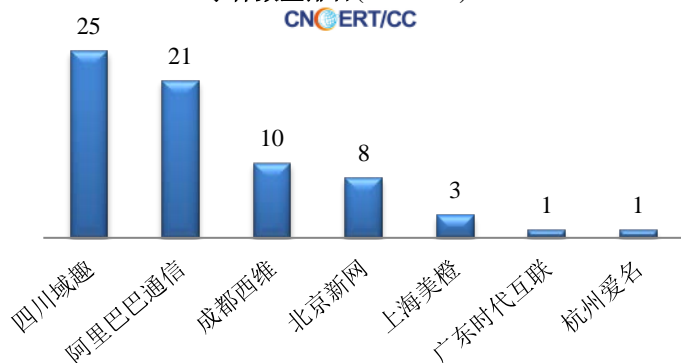


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理 426 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，银行仿冒事件 424 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计
(2/15-2/21)

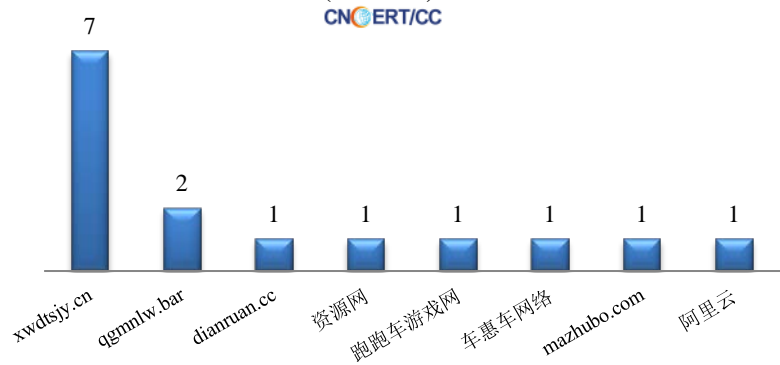


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名(2/15-2/21)



本周, CNCERT 协调 8 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 15 个。

本周CNCERT协调手机应用商店处理移动互联网恶意代码事件数量排名
(2/15-2/21)



业界新闻速递

1. 强制性国家标准《网络关键设备安全通用要求》发布

2月20日, 据中国通信标准化协会消息, 国家市场监督管理总局(国家标准化管理委员会)发布2021年第1号公告, 批准了7项强制性国家标准和1项强制性国家标准修改单, 其中包含1项通信领域的强制性国家标准: GB 40050-2021《网络关键设备安全通用要求》。

GB 40050-2021《网络关键设备安全通用要求》是工业和信息化部网络安全管理局为落实《中华人民共和国网络安全法》中有关网络关键设备安全的要求, 组织相关研究机构编制的一项重要标准。标准主要包括安全功能要求和安全保障要求。安全功能要求聚焦于保障和提升设备的安全技术能力, 主要包括设备标识安全、冗余备份恢复与异常检测、漏洞和恶意程序防范、预装软件启动及更新安全、用户身份标识与鉴别、访问控制安全、日志审计安全、通信安全、数据安全以及密码要求10个部分。安全保障要求聚焦于规范网络关键设备提供者在设备全生命周期的安全保障能力, 主要包括设计和开发、生产和交付、运行和维护三个环节的要求。

强制性国家标准 GB 40050-2021《网络关键设备安全通用要求》将于2021年8月1日正式实施。为配合本标准的正式实施, 后续中国通信标准化协会将在工业和信息化部网络安全管理局的指导下, 加强标准宣贯, 帮助相关主体提升网络关键设备安全能力以符合标准的要求。

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：高川

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315