

网络安全信息与动态周报

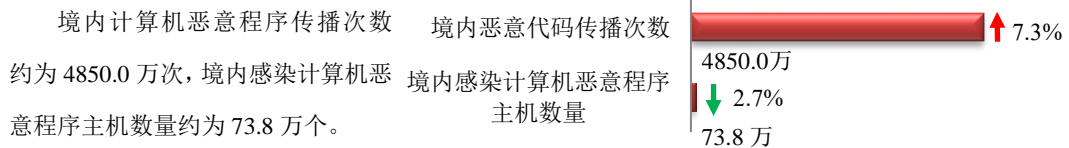
本周网络安全基本态势



境内计算机恶意程序传播次数	•4850.0万	↑ 7.3%
境内感染计算机恶意程序主机数量	•73.8万	↓ 2.7%
境内被篡改网站总数	•2637	↑ 125.4%
其中政府网站数量	•16	↑ 433.3%
境内被植入后门网站总数	•1318	↓ 1.6%
其中政府网站数量	•3	↓ 66.7%
针对境内网站的仿冒页面数量	•645	↑ 38.7%
新增信息安全漏洞数量	•600	↓ 0.7%
其中高危漏洞数量	•158	↑ 10.5%

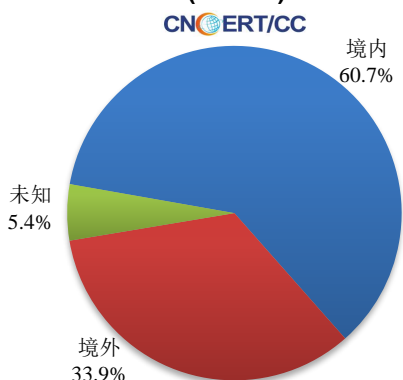
▬ 表示数量与上周相同 ↑ 表示数量较上周环比增加 ↓ 表示数量较上周环比减少

本周网络病毒活动情况

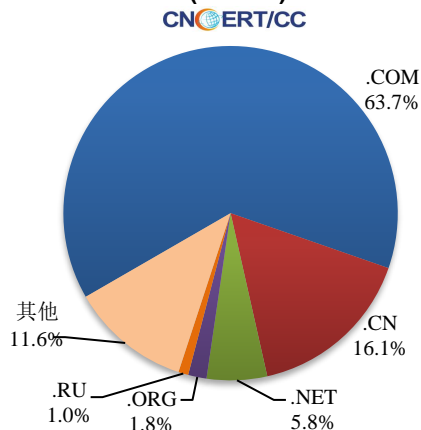


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 2697 个，涉及 IP 地址 11535 个。在 2697 个域名中，有 33.9%为境外注册，且顶级域为.com 的约占 63.7%；在 11535 个 IP 中，有约 52.3%于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 294 个。

本周放马站点域名注册所属境内外分布
(5/31-6/6)



本周放马站点域名注册所属顶级域分布
(5/31-6/6)



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。

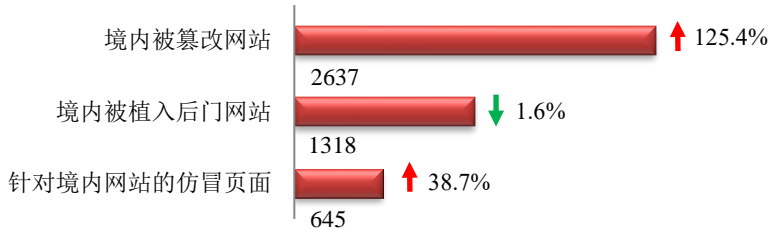
ANVA网络安全威胁信息共享平台

<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。

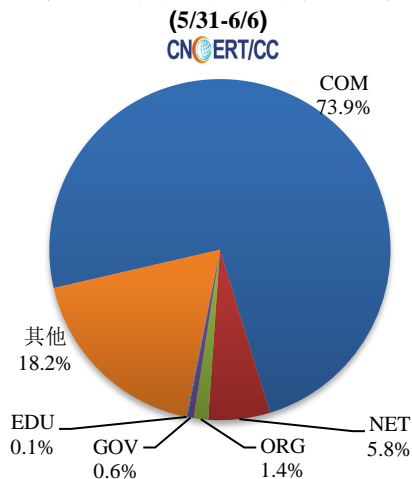
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 2637 个；被植入后门的网站数量为 1318 个；针对境内网站的仿冒页面数量为 645 个。

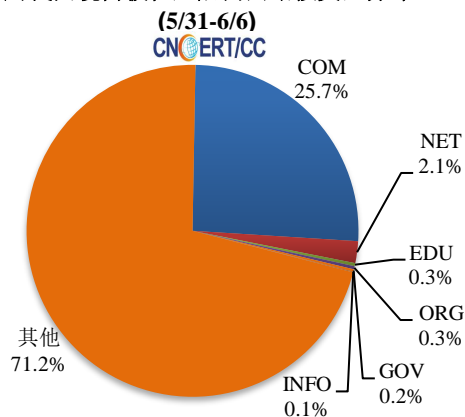


本周境内被篡改政府网站（GOV类）数量为16个（约占境内0.6%），与上周相比上升了433.3%；境内被植入后门的政府网站（GOV类）数量为3个（约占境内0.2%），与上周相比下降了66.7%。

本周我国境内篡改网站按类型分布

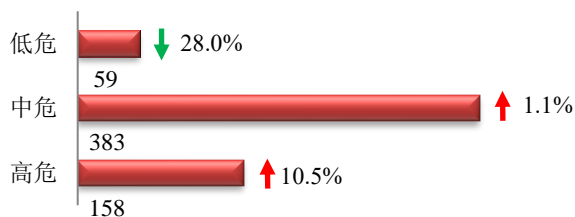


本周我国境内被植入后门网站按类型分布

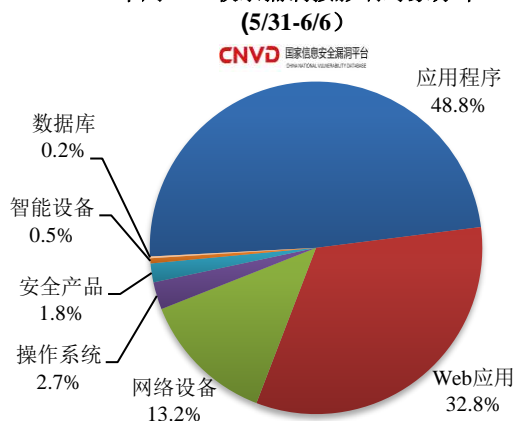


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞600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



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

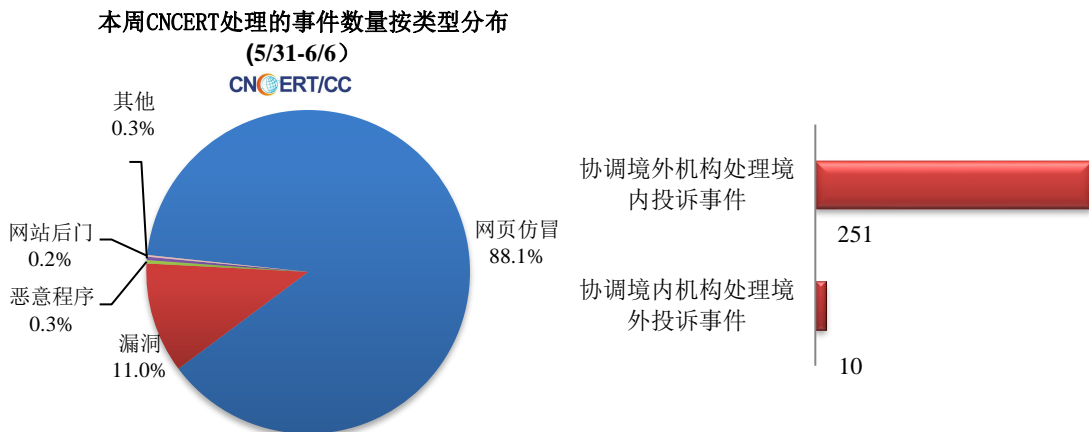
<http://www.cnvd.org.cn/webinfo/list?type=4>

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。

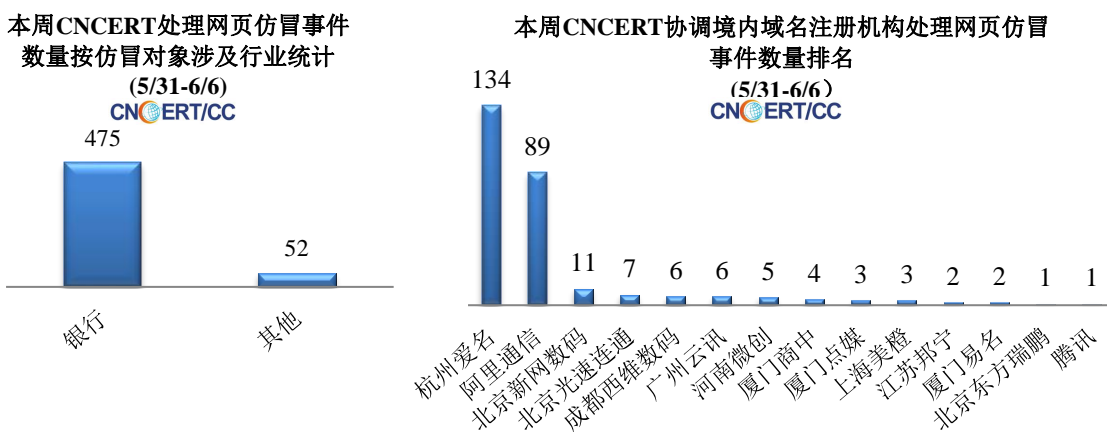


本周事件处理情况

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 598 起，其中跨境网络安全事件 261 起。

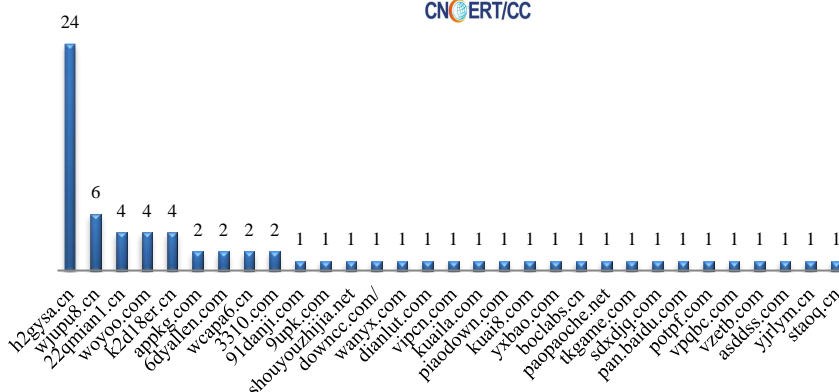


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理 527 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，银行仿冒事件 475 起，其他事件 52 起。



本周，CNCERT 协调 31 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 72 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 (5/31-6/6)
CNCERT/CC



业界新闻速递

1. 工信部、中央网信办印发《关于加快推动区块链技术应用和产业发展的指导意见》

2021年6月7日，据中国网信网消息，工业和信息化部、中央网络安全和信息化委员会办公室近日联合发布《关于加快推动区块链技术应用和产业发展的指导意见》。明确到2025年，区块链产业综合实力达到世界先进水平，产业初具规模。区块链应用渗透到经济社会多个领域，在产品溯源、数据流通、供应链管理等领域培育一批知名产品，形成场景化示范应用。培育3~5家具有国际竞争力的骨干企业和一批创新引领型企业，打造3~5个区块链产业发展集聚区。区块链标准体系初步建立。形成支撑产业发展的专业队伍，区块链产业生态基本完善。区块链有效支撑制造强国、网络强国、数字中国战略，为推进国家治理体系和治理能力现代化发挥重要作用。到2030年，区块链产业综合实力持续提升，产业规模进一步壮大。区块链与互联网、大数据、人工智能等新一代信息技术深度融合，在各领域实现普遍应用，培育形成若干具有国际领先水平的企业和产业集群，产业生态体系趋于完善。区块链成为建设制造强国和网络强国，发展数字经济，实现国家治理体系和治理能力现代化的重要支撑。

2. 全国人大法工委：数据安全法草案三次审议稿拟加大对违法行为的处罚力度

2021年6月4日，据中国新闻网消息，全国人大常委会法制工作委员会发言人臧铁伟表示，《数据安全法草案》三次审议稿拟作五项修改，包括进一步完善保障政务数据安全方面的规定、加大对违法行为的处罚力度等。根据各方面意见，提请本次常委会会议审议的草案三次审议稿拟作如下主要修改：一是，建立工作协调机制，加强对数据安全工作的统筹。二是，明确对关系国家安全、国民经济命脉、重要民生、重大公共利益等数据实行更严格的管理制度。三是，要求提供智能化公

共服务应当充分考虑老年人、残疾人的需求，不得对老年人、残疾人的日常生活造成障碍。四是，进一步完善保障政务数据安全方面的规定。五是，加大对违法行为的处罚力度。

3. 关于用友 NC BeanShell 存在远程代码执行漏洞的安全公告

2021年6月3日，据国家信息安全漏洞共享平台（CNVD）消息，4月12日，CNVD收录了用友 NC BeanShell 远程代码执行漏洞（CNVD-2021-30167）。该漏洞的综合评级为“高危”。攻击者利用该漏洞，可在未授权的情况下远程执行代码，该漏洞对部署于公共互联网上的用友 NC 6.5 系统构成一定的安全风险。目前，漏洞利用细节已公开，用友公司已发布版本补丁完成修复，并通过服务渠道推送解决方案，授权用户可以通过访问链接进行下载。CNVD 建议该产品用户立即通过官方网站安装最新补丁，及时消除漏洞隐患。

4. 国家标准《信息安全技术 网络安全态势感知通用技术要求》征求意见稿征求意见

2021年6月3日，据全国信息安全标准化技术委员会网站消息，全国信安标委归口的《信息安全技术 网络安全态势感知通用技术要求》国家标准现已形成标准征求意见稿。根据《全国信息安全标准化技术委员会标准制修订工作程序》要求，现将该国家标准（征求意见稿）面向社会公开征求意见。标准相关材料已发布在信安标委网站（网址：<https://www.tc260.org.cn/front/bzzqList.html?start=0&length=10>），如有意见或建议请于2021年8月2日24:00前反馈至委员会秘书处。

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：李志辉

网址：www.cert.org.cn

Email：cncert_report@cert.org.cn

电话：010-82990315