

网络安全信息与动态周报

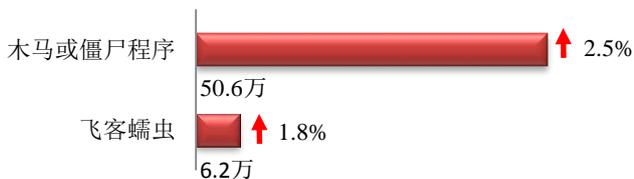
本周网络安全基本态势



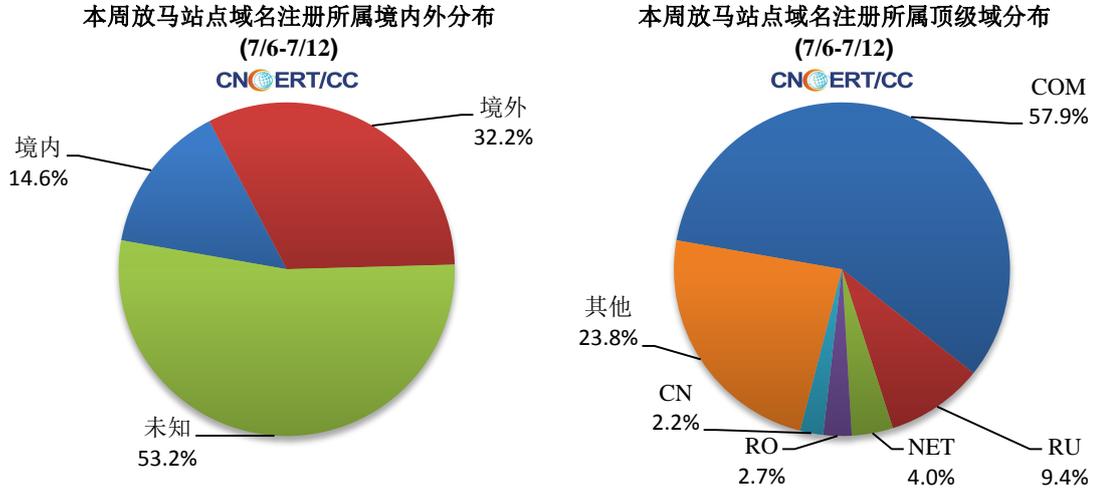
▬ 表示数量与上周相同 ↑ 表示数量较上周环比增加 ↓ 表示数量较上周环比减少

本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为56.8万个，其中包括境内被木马或被僵尸程序控制的主机约50.6万以及境内感染飞客（conficker）蠕虫的主机约6.2万。



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 404 个，涉及 IP 地址 1965 个。在 404 个域名中，有 32.2%为境外注册，且顶级域为.com 的约占 57.9%；在 1965 个 IP 中，有约 68.8%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 50 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>

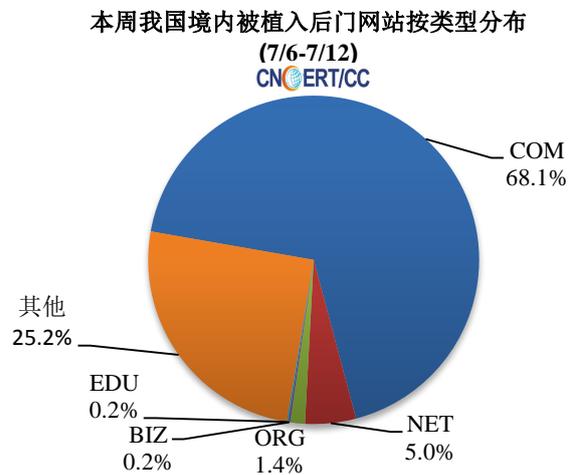
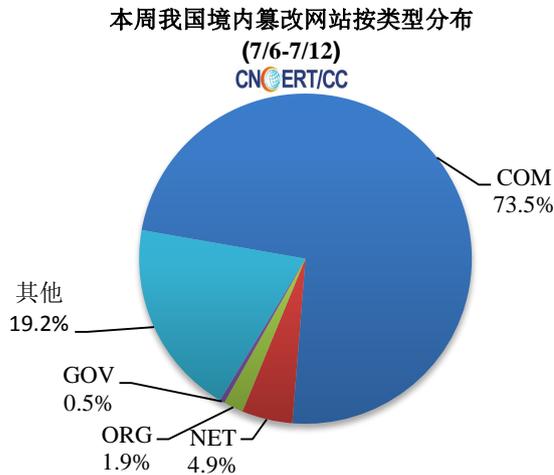
中国反网络病毒联盟 (Anti Network-Virus Alliance of China, 缩写 ANVA) 是由 CNCERT 发起并组织运作的行业联盟。

本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 4665 个；被植入后门的网站数量为 1188 个；针对境内网站的仿冒页面数量 1100 个。

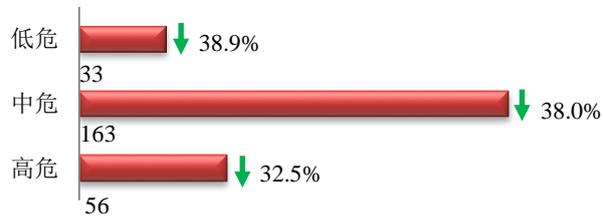


本周境内被篡改政府网站（GOV 类）数量为 22 个（约占境内 0.5%），较上周下降了 15.4%；境内被植入后门的政府网站（GOV 类）数量为 0 个（约占境内 0.0%），较上周下降了 100.0%。

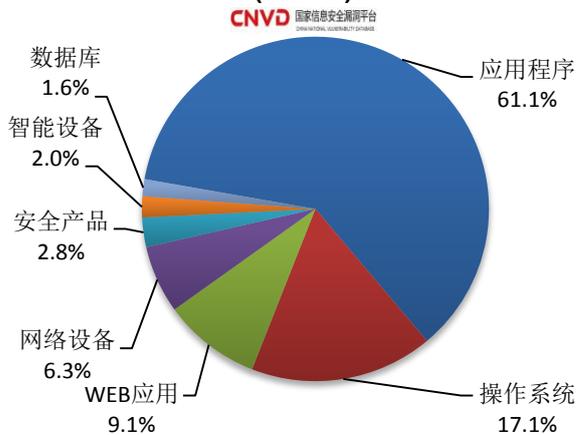


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 252 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 (7/6-7/12)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是操作系统和 WEB 应用。

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>

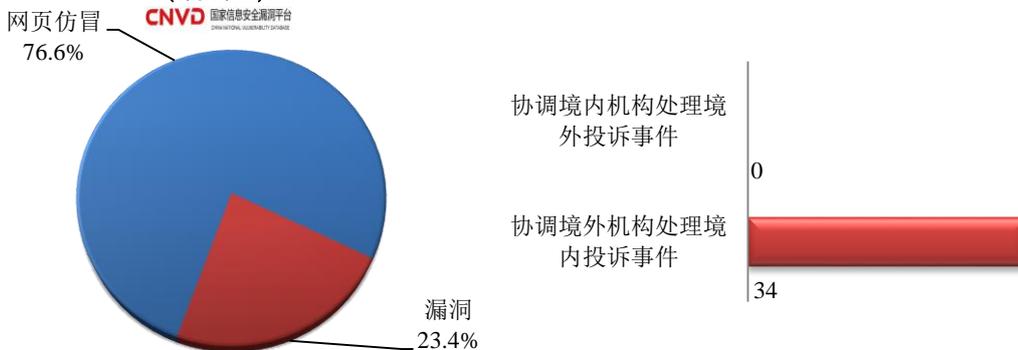
国家信息安全漏洞共享平台(缩写CNVD)是CNCERT联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

本周事件处理情况

本周，CNCERT协调基础电信企业、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278起，其中跨境网络安全事件34起。

本周CNCERT处理的事件数量按类型分布

(7/6-7/12)
CNVD 国家信息安全漏洞平台
www.cnvd.org.cn



本周，CNCERT协调境内外域名注册机构、境外CERT等机构重点处理了213起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件142起、电子商务平台51起和其他事件20起。

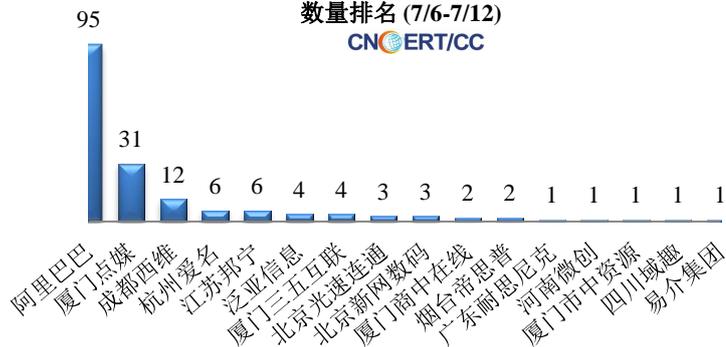
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计

(7/6-7/12)
CNCERT/CC



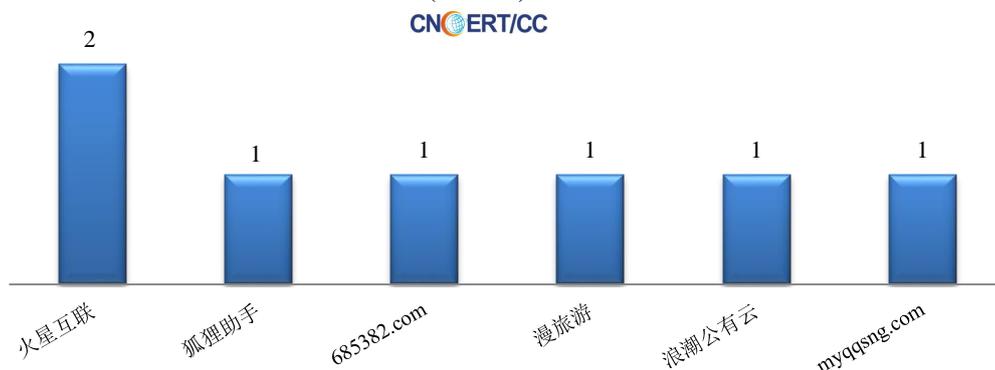
本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名

(7/6-7/12)
CNCERT/CC



本周，CNCERT 协调 6 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 7 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
(7/6-7/12)



业界新闻速递

1、国务院办公厅印发国务院 2020 年立法工作计划

7 月 8 日，国务院官网发布《国务院办公厅关于印发国务院 2020 年立法工作计划的通知》（国办发〔2020〕18 号），包括 16 件拟提请全国人大常委会审议的法律案，26 件拟制定、修订的行政法规。拟制定、修订的行政法规中，包括未成年人网络保护条例、关键信息基础设施安全保护条例。

2、工信部：今年计划推动百家龙头企业升级工业互联网内网

7 月 10 日，工信部官网发布《工业互联网专项工作组 2020 年工作计划》（下称《计划》），提出了包括提升基础设施能力、构建标识解析体系、建设工业互联网平台、突破核心技术标准、培育新模式新业态、促进产业生态融通发展、增强安全保障水平、推进开放合作、加强统筹推进、推动政策落地等 10 大任务类别共 54 项具体举措。其中第七大类增强安全保障水平，提出了健全安全管理机制、推动技术能力建设两个方面重点工作共 6 项具体举措，并明确了年度具体目标成果。

3、“云剑-2020”打击电信网络诈骗犯罪再出重拳

7 月 8 日，公安部官网消息，按照全国公安机关“云剑-2020”行动打击贷款类电信网络诈骗犯罪集群战役部署，7 月 8 日上午 10 时，在公安部统一指挥下，北京、河北、上海、江苏等 15 个省区市公安机关开展集中收网行动，依法严厉打击为贷款类电信网络

诈骗犯罪提供服务的非法网络推广团伙。截至 8 日 16 时，共捣毁非法网络推广团伙 57 个，抓获违法犯罪嫌疑人 460 余名，收网行动取得阶段性成效。

4、爆出存在 XSS 漏洞 约 10 万个网站受影响

7 月 9 日, 据外媒报道, 在 KingComposer WordPress 插件中已修复了影响 100,000 个网站的反映的跨站点脚本 (XSS) 漏洞。据悉, KingComposer 是用于基于 WordPress 的域的拖放页面生成器, 无需对由内容管理系统 (CMS) 驱动的网站进行编程或直接编码。该漏洞反映的 XSS 漏洞依赖于受害者执行特定操作以触发攻击。这可以通过提供需要单击的恶意链接来实现, 如果成功, 则可能导致浏览器会话劫持或恶意软件下载和执行。Wordfence 威胁情报团队于 6 月 26 日与 KingComposer 开发人员取得了联系, 6 月 29 日 KingComposer 发布了该补丁的修补版本 2.9.5。截至目前, 仍有 37.9% 启用了 KingComposer 的网站存在被利用风险。

关于国家互联网应急中心（CNCERT）

国家互联网应急中心是国家计算机网络应急技术处理协调中心的简称（英文简称为 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，是一个非政府非盈利的网络安全技术协调组织，主要任务是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展中国互联网上网络安全事件的预防、发现、预警和协调处置等工作，以维护中国公共互联网环境的安全、保障基础信息网络和网上重要信息系统的安全运行。目前，CNCERT 在我国大陆 31 个省、自治区、直辖市设有分中心。

同时，CNCERT 积极开展国际合作，是中国处理网络安全事件的对外窗口。CNCERT 是国际著名网络安全合作组织 FIRST 正式成员，也是 APCERT 的发起人之一，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 2019 年，CNCERT 已与 78 个国家和地区的 260 个组织建立了“CNCERT 国际合作伙伴”关系。CNCERT 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：王毓骏

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315