国家互联网应急中心

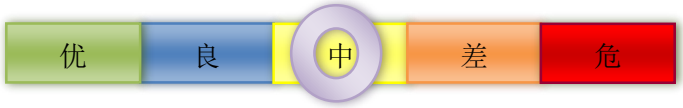
网络安全信息与动态周报

2020 年第 25 期

6 月 15 日-6 月 21 日

CNCERT/CC

本周网络安全基本态势

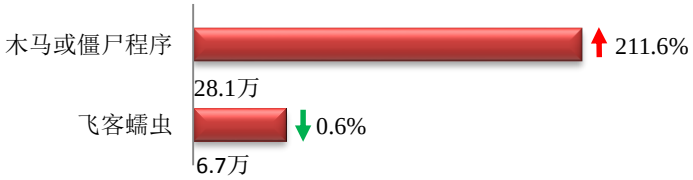


境内感染网络病毒的主机数量	•34.8万	↑ 121.0%
境内被篡改网站总数 其中政府网站数量	•8451 •28	↓ 12.0% ↓ 24.3%
境内被植入后门网站总数 其中政府网站数量	•1455 •5	↑ 13.1% ↑ 25.0%
针对境内网站的仿冒页面数量	•793	↑ 3.1%
新增信息安全漏洞数量 其中高危漏洞数量	•483 •126	↓ 14.2% ↓ 40.3%

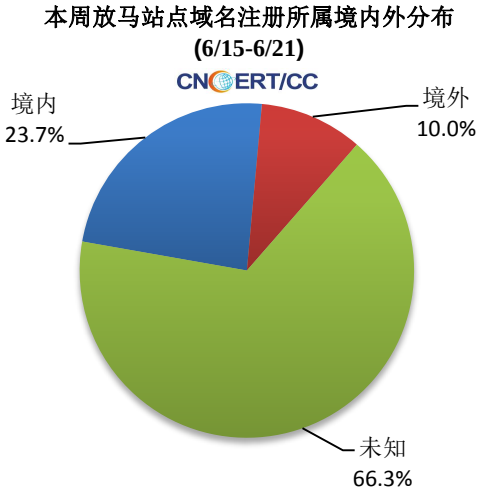
= 表示数量与上周相同　↑ 表示数量较上周环比增加　↓ 表示数量较上周环比减少

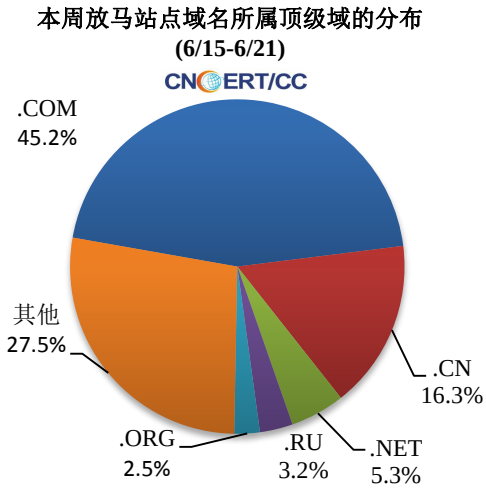
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 34.8 万个，其中包括境内被木马或被僵尸程序控制的主机约 28.1 万以及境内感染飞客（conficker）蠕虫的主机约 6.7 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 2882 个，涉及 IP 地址 5368 个。在 2882 个域名中，有 10.0%为境外注册，且顶级域为.com 的约占 45.2%；在 5368 个 IP 中，有约 60.8%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 474 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。

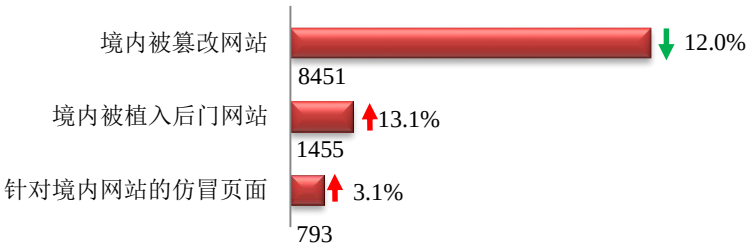
ANVA网络安全威胁信息共享平台

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。

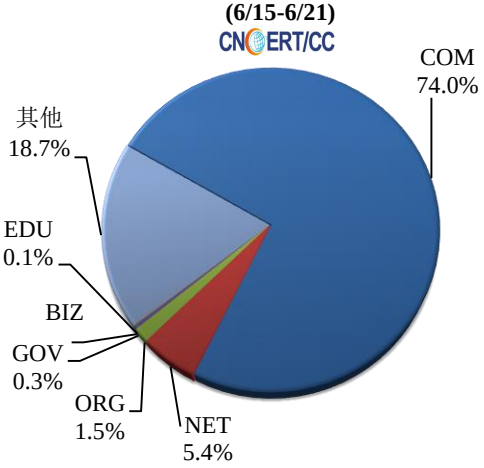
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 8451 个；被植入后门的网站数量为 1455 个；针对境内网站的仿冒页面数量 793 个。

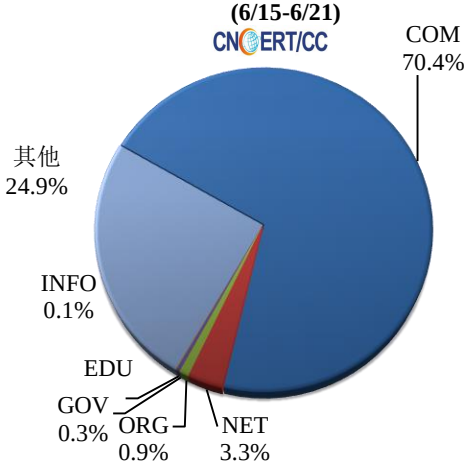


本周境内被篡改政府网站（GOV 类）数量为 28 个（约占境内 0.3%），较上周下降了 24.3%；境内被植入后门的政府网站（GOV 类）数量为 5 个（约占境内 0.3%），较上周上涨了 25.0%。

本周我国境内篡改网站按类型分布
(6/15-6/21)

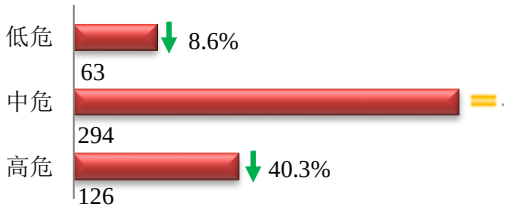


本周我国被植入后门网站按类型分布
(6/15-6/21)

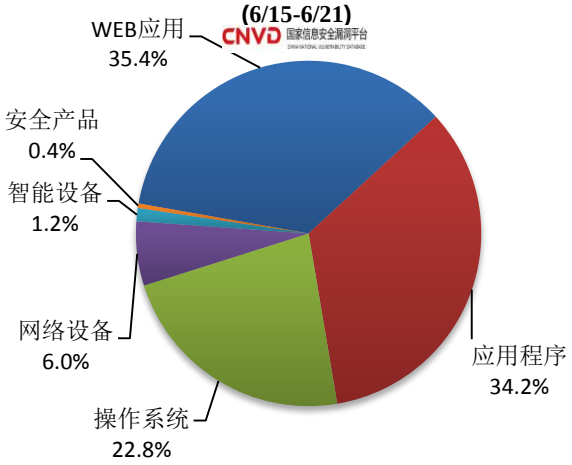


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 483 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
(6/15-6/21)



本周 CNVD 发布的网络安全漏洞中，WEB 应用漏洞占比最高，其次是应用程序和操作系统。

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

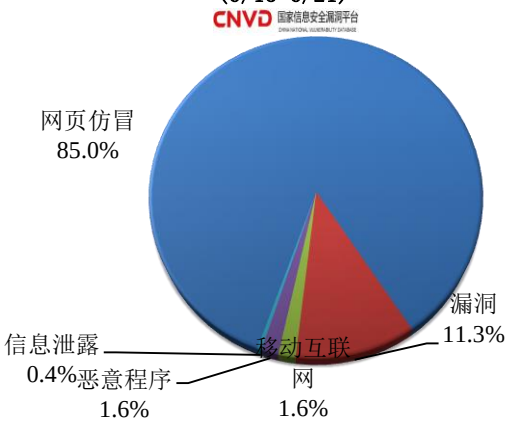
http://www.cnvd.org.cn/webinfo/list?type=4

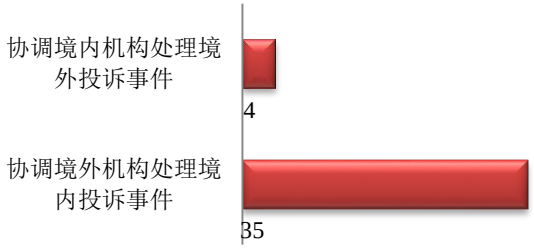
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 247 起，其中跨境网络安全事件 39 起。

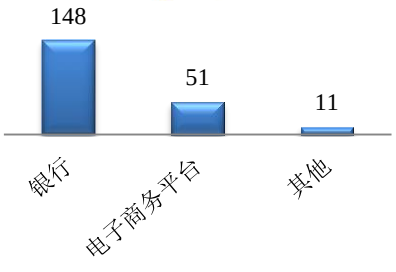
本周CNCERT处理的事件数量按类型分布
(6/15-6/21)



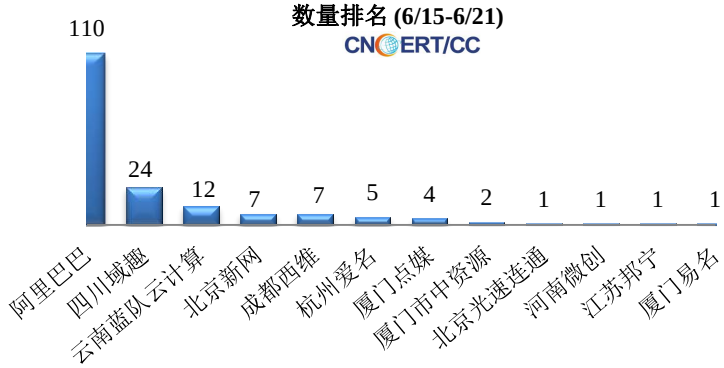


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 210 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 148 起、电子商务平台 51 起和其他事件 11 起。

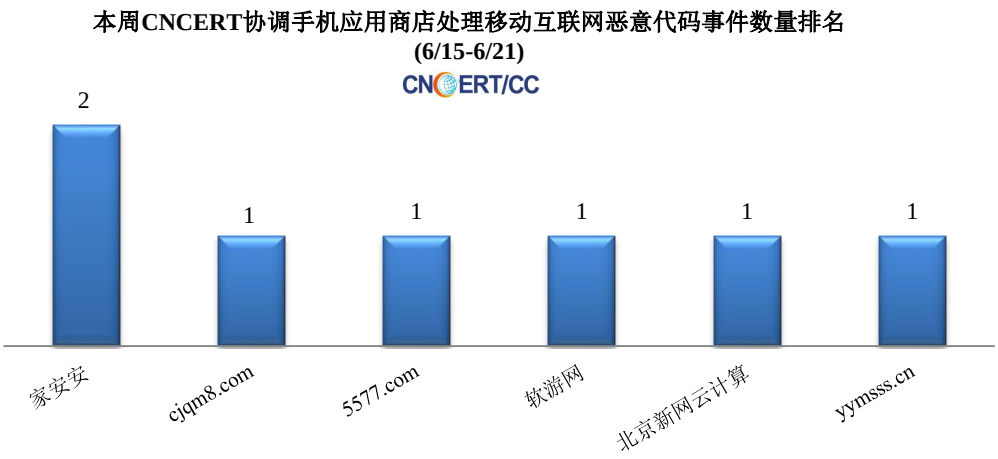
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (6/15-6/21)



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 (6/15-6/21)



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。



业界新闻速递

1、 市场监管总局等六部门联合印发《国家电子政务标准体系建设指南》

6 月 18 日，市场监管总局官网消息，市场监管总局办公厅、中共中央办公厅机要局、国务院办公厅电子政务办公室、中央网信办秘书局、国家发展改革委办公厅和工业和信息化部办公厅六部门联合印发《国家电子政务标准体系建设指南》，旨在加强电子政务领域标准化顶层设计，推动电子政务标准体系建设，支撑电子政务实施应用。该指南发布了标准体系结构图、政务数据共享开发标准子体系、公告数据资源开发利用标准子体系、电子文件标准子体系、“互联网+政务”标准子体系及电子政务现行及在研标准体系表，并明确了到 2020 年、2021 年、2022 年建设目标。

2、 工信部部署推进 2020 年电信和互联网行业网络数据安全管理工作

6 月 22 日，为切实做好 2020 年电信和互联网行业网络数据安全管理工作，工业和信息化部印发《关于做好 2020 年电信和互联网行业网络数据安全管理工作的通知》，提出深化行业网络数据安全专项治理、深入开展网络数据安全合规性评估、加快推进网络数据安全制度标准建设、提升网络数据安全技术保障能力等年度行业网络数据安全管理重点工作要求。

3、 欧盟拨款 3800 万欧元以保护关键基础设施免受网络威胁

6 月 15 日，欧盟官方网站消息，欧盟委员会宣布，将通过欧盟研究与创新计划《地

平线 2020》投入超过 3800 万欧元，支持保护关键基础设施免受网络和物理威胁以及使城市变得更智能、更安全等多个创新项目。其中，三个项目将致力于改善对地铁和铁路网络、地面空间基础设施、卫星、电子商务和传递服务的网络和物理威胁的预防、检测、响应和缓解。另外两个项目旨在增强城市基础设施和服务的弹性，并在公共场所发生安全事件时保护公民。这些项目预计将在 2020 年 6 月至 2020 年 10 月之间开始，并将运行两年。欧盟研究执行署将管理上述五个选定的项目，并已完成与利益攸关方的财政拨款协议的准备和签署。

4、 谷歌浏览器造成大规模用户安全信息泄露

6 月 18 日，据外媒报道，有网络流量分析公司表示，近日在谷歌的 Chrome 浏览器扩展程序中发现了一个恶意软件，该软件已经被下载了约 3200 万次，大量用户信息面临泄露的危险。据悉，该扩展程序会窃取用户的相关隐私，涉及电子邮件、工资单和其他敏感项。目前，谷歌已经从 Chrome Web Store 中移除了超过 70 个存在此恶意软件的扩展程序。

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：王英

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315