国家互联网应急中心

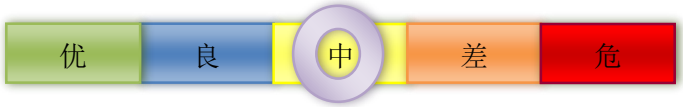
网络安全信息与动态周报

2020 年第 31 期

7 月 27 日-8 月 2 日

CNCERT/CC

本周网络安全基本态势

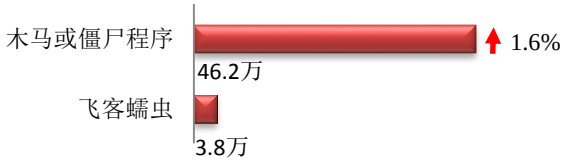


境内感染网络病毒的主机数量	•50.0万	↑ 10.0%
境内被篡改网站总数 其中政府网站数量	•4715 •18	↓ 5.0% =
境内被植入后门网站总数 其中政府网站数量	•1298 •3	↑ 5.6% =
针对境内网站的仿冒页面数量	•7900	↑ 559.4%
新增信息安全漏洞数量 其中高危漏洞数量	•292 •82	↓ 39.3% ↓ 44.2%

= 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

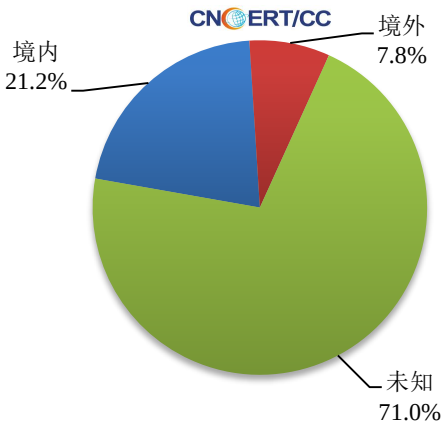
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 50.0 万个，其中包括境内被木马或被僵尸程序控制的主机约 46.2 万以及境内感染飞客（conficker）蠕虫的主机约 3.8 万。

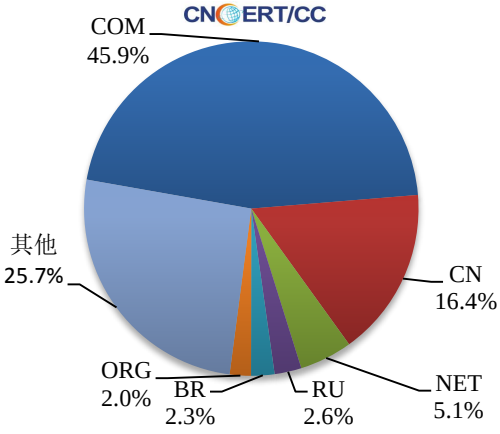


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 2879 个，涉及 IP 地址 5594 个。在 2879 个域名中，有 7.8%为境外注册，且顶级域为.com 的约占 45.9%；在 5594 个 IP 中，有约 65.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 415 个 IP。

本周放马站点域名注册所属境内外分布 (7/27-8/2)



本周放马站点域名注册所属顶级域分布 (7/27-8/2)



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。

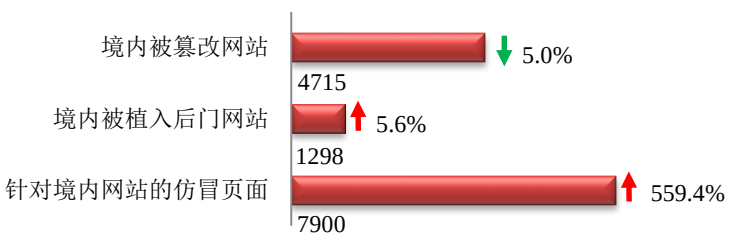
ANVA网络安全威胁信息共享平台

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。

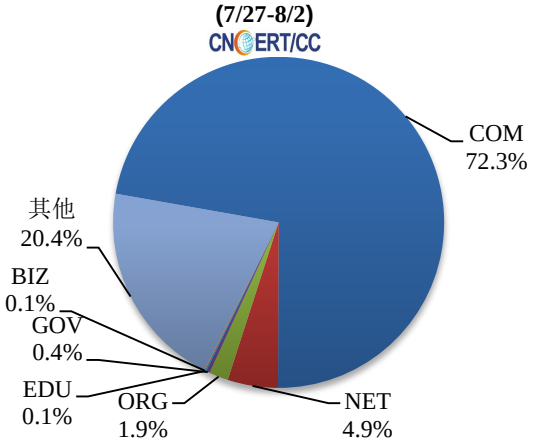
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 4715 个；被植入后门的网站数量为 1298 个；针对境内网站的仿冒页面数量 7900 个。

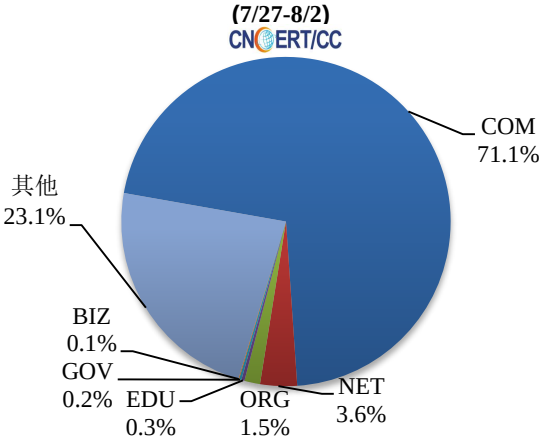


本周境内被篡改政府网站（GOV 类）数量为 18 个（约占境内 0.4%），与上周持平；境内被植入后门的政府网站（GOV 类）数量为 3 个（约占境内 0.2%），与上周持平。

本周我国境内篡改网站按类型分布
(7/27-8/2)

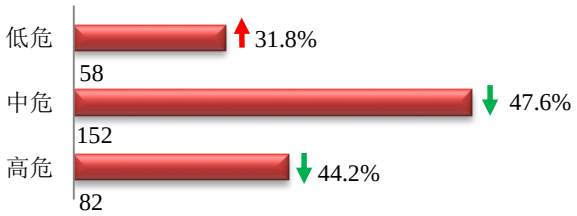


本周我国境内被植入后门网站按类型分布
(7/27-8/2)

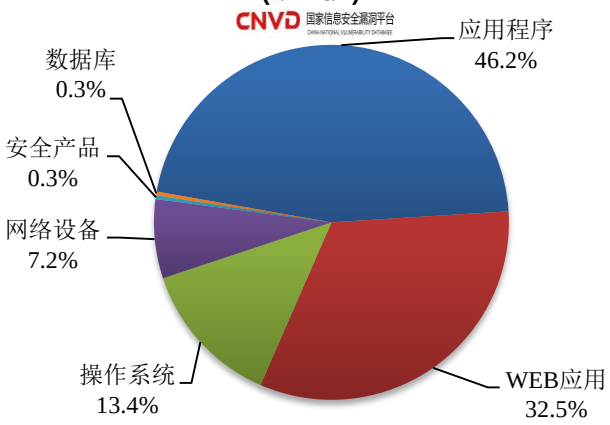


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 292 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
(7/27-8/2)



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。

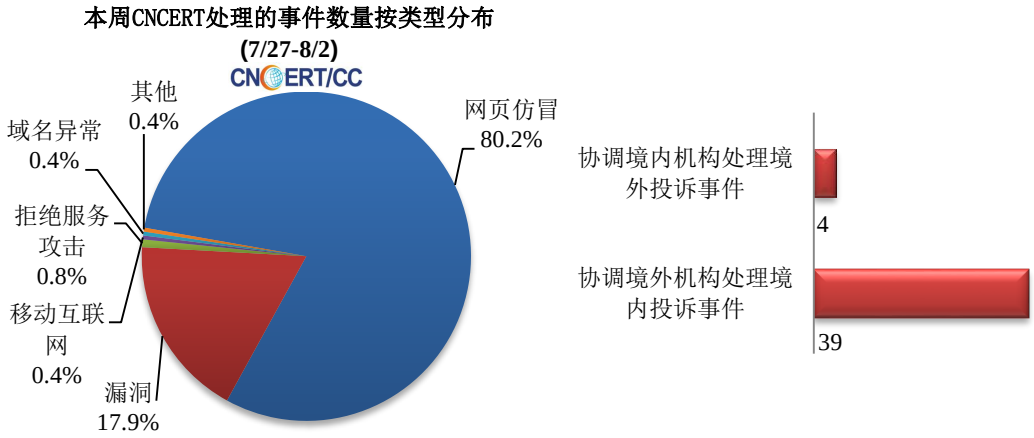
CNVD漏洞周报发布地址

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

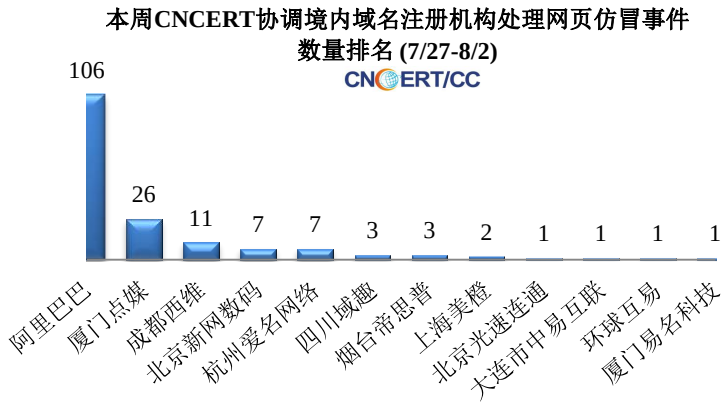
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

本周事件处理情况

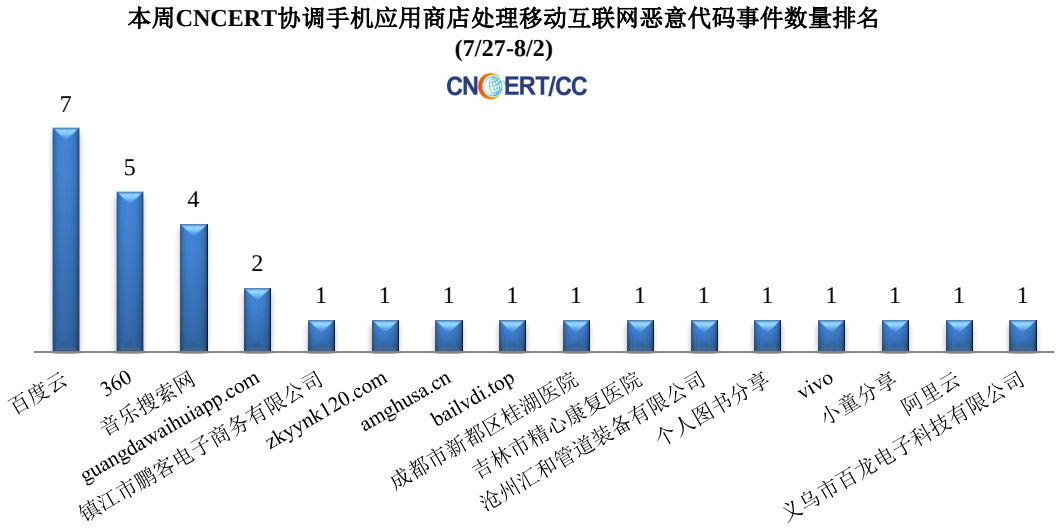
本周，CNCERT 协调基础电信企业、云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 263 起，其中跨境网络安全事件 43 起。



本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 211 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 194 起、电子商务平台 8 起、证券 2 起和其他事件 7 起。



本周，CNCERT 协调 16 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 30 个。



业界新闻速递

1、 公安部集中打击治理电信网络诈骗犯罪取得阶段性成效

7 月 28 日，公安部网站消息，公安部 7 月 28 日在京召开新闻发布会，通报今年以来公安机关打击治理电信网络诈骗犯罪工作有关情况。公安部刑事侦查局通报，今年以来，在党中央的坚强领导下，公安部深入贯彻落实全国打击治理电信网络新型违法犯罪工作电视电话会议精神，组织开展“云剑—2020”、“长城 2 号”、“510”等专项打击行动，坚持立足境内，集中打击高发类案，全力铲除诈骗窝点，重拳整治黑灰产业，全面加强预警防范，取得阶段性成效。上半年，全国共破获电信网络诈骗案件 10.1 万起，抓获犯罪嫌疑人 9.2 万名，同比分别上升 73.7%、78.4%。从严从重从快打击涉疫情诈骗犯罪，共破案 1.6 万起，抓获犯罪嫌疑人 7506 名，有力服务全国疫情防控大局；集中打击网络贷款、网络刷单、杀猪盘、冒充客服等 4 类电信网络诈骗高发类犯罪，共捣毁窝点 2460 个，抓获嫌疑人 1.9 万名，破获案件 2.3 万起，高发类案得到有效遏制，网络贷款类案件占比由年初的 40%下降至 20%，网络刷单诈骗日均发案下降 30%，杀猪盘案件造成的损失数环比下降 25%，冒充客服类案件连续两个月发案环比下降；严厉打击为电信网络诈骗提供服务的黑灰产犯罪，共捣毁黑灰产犯罪窝点 7200 余个，查处黑灰产犯罪嫌疑人 3.2 万名，斩断犯罪链条，堵塞监管漏洞；对诈骗窝点集中、黑灰产泛滥、行业问题突出的重点地域实施红黄牌警告和挂牌整治制度，压实地方主体责任，铲除犯罪土壤，重点地域面貌大为改观；强化技术反制和资金拦截，累计拦截诈骗电话 1.2 亿个、封堵诈骗域名网址 21 万个，为群众直接避免经济损失 666 亿元；全力落实预警劝阻措施，开通 96110

反诈预警专号，进一步提高预警劝阻效率和成功率，累计防止 561 万名群众被骗；全面加强宣传防范，在全国公安机关“百万民警进千万家”活动中专题部署反诈宣传工作，将宣传的触角延伸至居委会、村委会，切实提升群众的识骗防骗能力。

下一步，公安机关将始终保持严打高压态势，全力以赴铲窝点、抓金主、追赃款、摧灰产、堵漏洞，坚决将犯罪分子的嚣张气焰打下去，切实维护人民群众合法权益和社会治安大局稳定。同时，充分发挥国务院部际联席会议机制优势，坚持打防并举、齐抓共管、源头治理，打一场反诈人民战争，坚决遏制案件高发多发态势。公安机关正告诈骗分子，立即停止一切违法犯罪活动，主动投案自首，争取宽大处理。公安机关提醒广大群众，要切实提高警惕，增强防范意识，避免上当受骗遭受财产损失和不法侵害。

2、 工信部部署纵深推进 APP 侵犯用户权益专项整治行动

为切实加强用户个人信息保护，按照2020年信息通信行业行风建设暨纠风工作安排，工业和信息化部 7 月 29 日下午在京召开会议，部署开展纵深推进 APP 侵害用户权益专项整治行动。会上，工业和信息化部信息通信管理局对《关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》（工信部信管函〔2020〕164 号）进行宣贯，重点介绍了此次专项行动中整治目标、三类整治对象、四方面重点任务以及 10 类突出问题。会议强调，全行业要以此次整治工作为契机，努力为人民群众提供更安全、更健康、更干净的信息环境。一是提高政治站位，坚决把群众利益放在首位；二是不折不扣，严格落实企业主体责任；三是守土有责、尽责，进一步加大监督惩处力度；四是加强技管结合，持续提升 APP 技术检测能力；五是加强协同治理，推动社会共治。

3、 化妆品巨头雅芳泄漏 1900 万条数据记录

7 月 28 日，外媒 Infosecurity 报道，近日，全球化妆品品牌雅芳(Avon)因云服务器配置不当，泄漏了 1,900 万份记录，其中包括个人信息和技术日志。研究人员发现雅芳在 Azure 服务器上的 Elasticsearch 数据库公开暴露，且没有密码保护或加密。该漏洞意味着，任何拥有该服务器 IP 地址的人都可以访问该公司的开放数据库。暴露的数据库包含有关客户和员工的个人身份信息（PII），包括全名、电话号码、生日、电子邮件和家庭住址以及 GPS 坐标。此外包括 40,000 多个安全令牌、OAuth 令牌、内部日志、账户设置和技术服务器信息。目前，雅芳正在继续调查，以确定事件的严重程度，包括可能泄漏的个人数据。

4、 黑客利用电子银行 Dave 漏洞窃取 750 万用户数据

7 月 30 日，据外媒报道，近日，一位攻击者在某黑客论坛上免费发布了包含 7,516,691 个 Dave 用户记录的数据库，包括真实姓名、电话号码、电子邮件、出生日期、家庭住址以及 bcrypt 加密的密码，某些信息中还包括银行卡信息和社会安全号码。电子银行 Dave 承认其应用存在安全漏洞，并被黑客利用导致用户信息泄露。Dave 表示，该漏洞源于其工程团队之前使用的分析平台 Waydev。目前，Dave 公司已修复了黑客利用的漏洞，并将此事件通知用户，Dave 应用的密码也将被重置。

5、 GRUB2 引导加载程序高风险漏洞影响数十亿设备

有网络安全研究人员披露了一个存在 GRUB2 引导加载程序中的高风险漏洞，其影响全球数十亿设备，几乎包括运行任何 Linux 发行版或 Windows 系统的服务器和工作站、笔记本电脑、台式机和 IoT 系统。安全引导是统一可扩展固件接口(UEFI)的一个安全特性，它使用引导加载程序加载关键组件、外围设备和操作系统，同时确保在引导过程中只执行经过加密签名的代码。该漏洞被称为 BootHole，CVE 收录编号为 CVE-2020-10713，如果被利用，可能允许攻击者绕过安全引导特性，获得对目标系统的高特权持久和秘密访问。

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：李金凝

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315