国家互联网应急中心

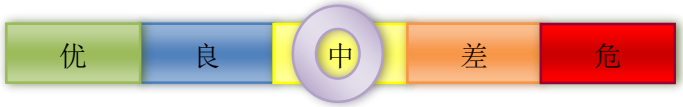
网络安全信息与动态周报

2020 年第 27 期

6 月 29 日-7 月 5 日

CNCERT/CC

本周网络安全基本态势

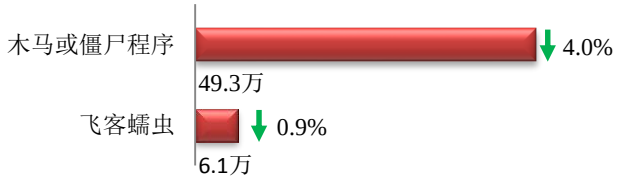


境内感染网络病毒的主机数量	•55.4万	3.6%
境内被篡改网站总数 其中政府网站数量	•6668 •26	7.9% 23.8%
境内被植入后门网站总数 其中政府网站数量	•1360 •2	7.1% 100.0%
针对境内网站的仿冒页面数量	•1028	43.0%
新增信息安全漏洞数量 其中高危漏洞数量	•400 •83	54.4% 20.2%

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*

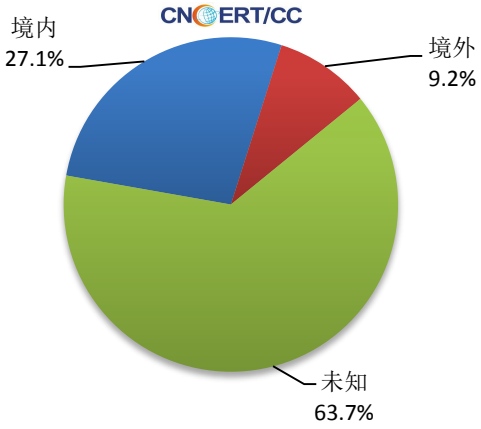
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 55.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 49.3 万以及境内感染飞客（conficker）蠕虫的主机约 6.1 万。

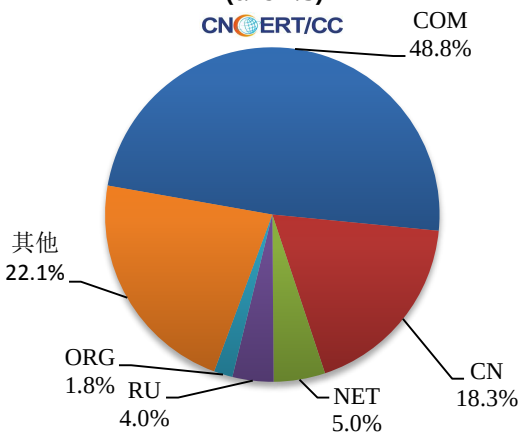


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 3096 个，涉及 IP 地址 7677 个。在 3096 个域名中，有 9.2%为境外注册，且顶级域为.com 的约占 48.8%；在 7677 个 IP 中，有约 59.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 751 个 IP。

本周放马站点域名注册所属境内外分布
(6/29-7/5)



本周放马站点域名注册所属顶级域分布
(6/29-7/5)



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。

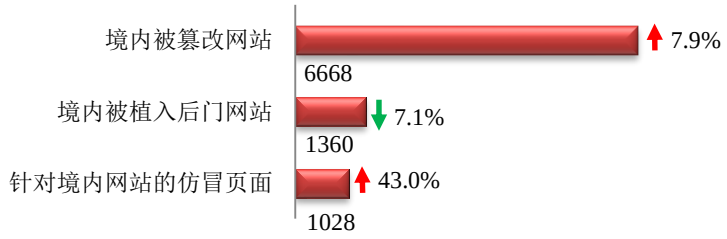
ANVA网络安全威胁信息共享平台

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

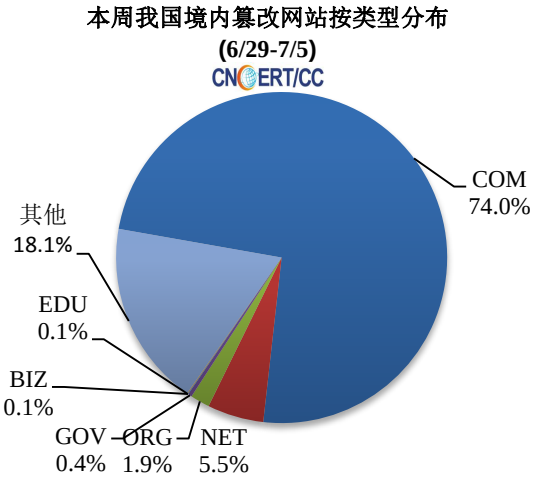
中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由 CNCERT 发起并组织运作的行业联盟。

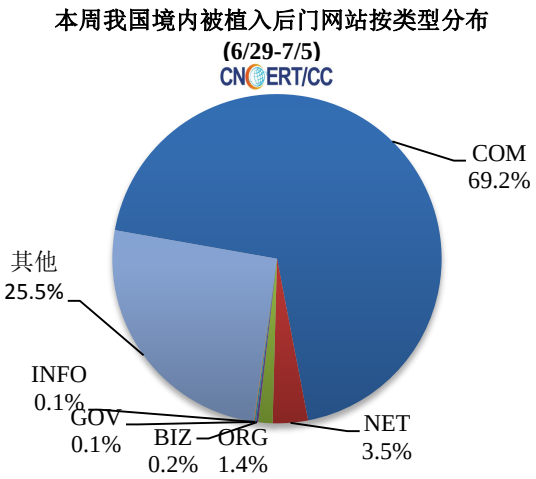
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 6668 个；被植入后门的网站数量为 1360 个；针对境内网站的仿冒页面数量 1028 个。



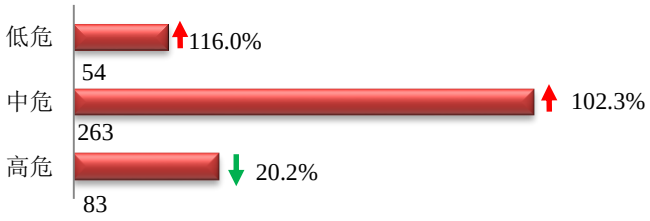
本周境内被篡改政府网站（GOV 类）数量为 26 个（约占境内 0.4%），较上周上涨了 23.8%；境内被植入后门的政府网站（GOV 类）数量为 2 个（约占境内 0.1%），较上周下降了 100.0%。

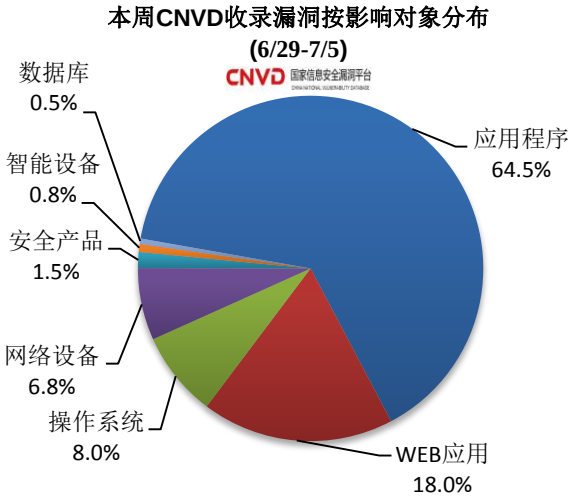




本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 400 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

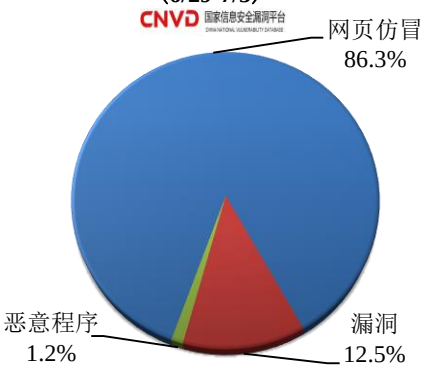
http://www.cnvd.org.cn/webinfo/list?type=4

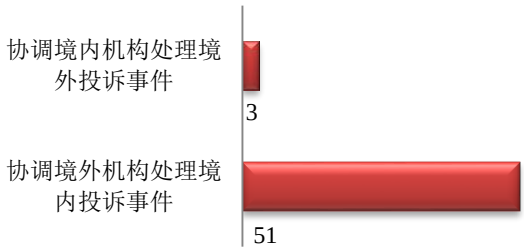
国家信息安全漏洞共享平台(缩写CNVD)是CNCERT联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 248 起，其中跨境网络安全事件 54 起。

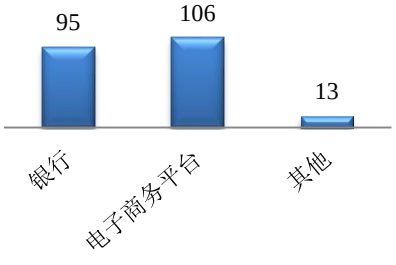
本周CNCERT处理的事件数量按类型分布
（6/29-7/5）



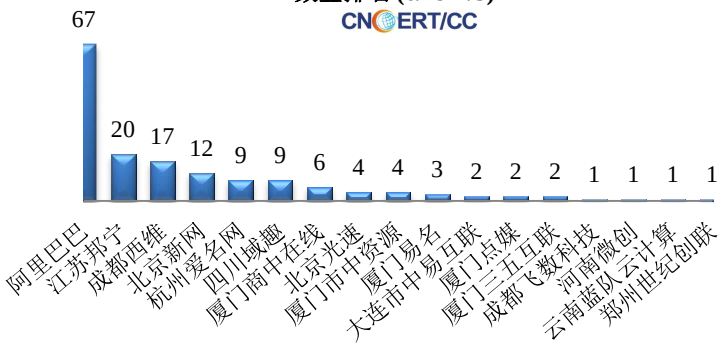


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 214 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 95 起、电子商务平台 106 起和其他事件 13 起。

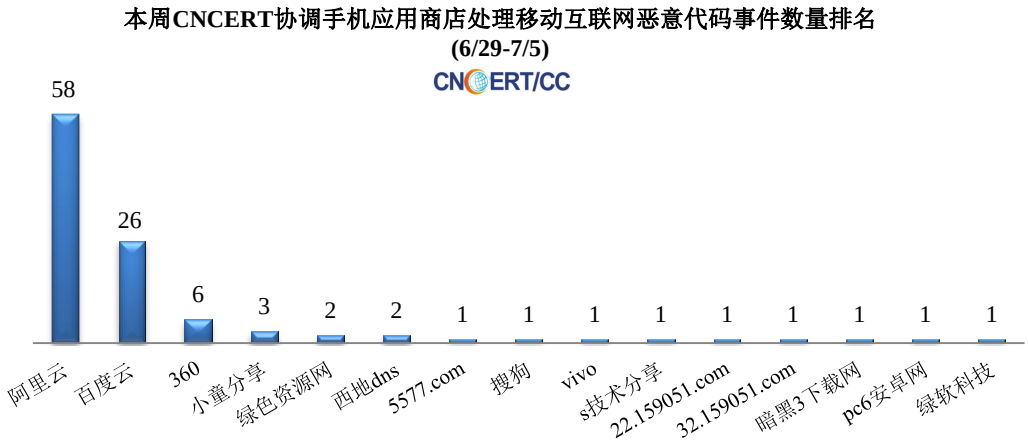
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计
(6/29-7/5)



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 (6/29-7/5)



本周，CNCERT 协调 15 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 106 个。



业界新闻速递

1、 国家卫生健康委办公厅关于做好信息化支撑常态化疫情防控工作的通知

6 月 29 日，为充分发挥信息化在支撑疫情监测分析、创新诊疗模式、提升服务效率、促进人员安全有序流动等方面的作用，国家卫生健康委办公厅印发《关于做好信息化支撑常态化疫情防控工作的通知》（以下简称《通知》），指导各地利用信息化手段支撑常态化疫情防控工作。

《通知》从六个方面提出了相关要求。一是强化疫情监测预警，支撑疫情防控工作。加强区域统筹，完善中国疾病预防控制信息系统，强化疫情信息监测预警。完善预警指挥系统。二是完善健康通行码政策标准，推动人员安全有序流动。优化防疫健康服务，完善健康通行码“一码通行”，推进多“码”融合。三是推广疫情期间线上服务经验，大力发展“互联网+医疗健康”。鼓励“互联网+医疗健康”规范有序发展，发挥平台作用，强化数据共享，完善标准规范，扩大创新试点。四是拓展“互联网+政务”服务，推动政务信息共享和“一网通办”。推进“互联网+政务”服务，统筹推进医疗机构、医师、护士电子证照建设应用，积极推广“出生一件事”，推动政务信息系统整合。五是推进信息化新型基础设施建设，加快建立应急指挥系统。持续完善平台功能，建立基础数据库，建立应急指挥系统，开展大数据综合分析。六是强化网络安全工作，切实保障个人信息和网络安全。落实网络安全责任，加大网络安全投入，加强网络安全防护和保障能力，组织网络安全宣传教育和培训。

2、 工信部通报 2020 年第二批侵害用户权益行为 APP

7 月 3 日，工信部官网消息，工信部信息通信管理局发布《关于侵害用户权益行为的 APP 通报（2020 年第二批）》。依据《网络安全法》《电信条例》《电信和互联网用户个人信息保护规定》等法律法规，工信部近期组织第三方检测机构对手机应用软件进行检查，对发现存在问题的企业进行督促整改。截至目前，尚有 15 款 APP 未完成整改，应在 7 月 14 日前完成整改落实工作，逾期不整改的，将依法依规组织开展相关处置工作。

3、 日本通信公司 NTT 称服务器遭攻击致使 892 家企业信息泄露

7 月 2 日，央视网消息，日本 NTT 通信公司就公司内部服务器遭受网络攻击问题称，追加调查中新发现可能有 271 家企业的施工信息等外露。另悉，日本自卫队和海上保安厅的相关信息也可能泄露。出于保密原因，NTT 表示不公布具体的公司名。目前确定，271 家企业中有 83 家已查明经由海外服务器非法访问，而发生信息泄露。据称，此外还新发现 188 家企业可能因为员工私人终端途径的非法访问，导致了信息外露。另据共同社消息，5 月底，NTT 公布有 621 家企业可能发生信息外露，加上此次新发现的情况，因 NTT 通信服务漏洞而导致信息泄露的企业总数达 892 家。

4、 罕见 ThiefQuest 恶意软件泛滥！ 为攻击 Mac 用户量身定制

7 月 3 日，E 安全消息，据外媒报道，K7 实验室的恶意软件研究人员发表了有关 Mac 勒索软件新示例，命名为“ThiefQuest”。除勒索软件的基本功能外，ThiefQuest 还具有其他整套间谍软件的功能，可使其从受感染的计算机中窃取文件，在系统中搜索密码和加密货币钱包数据，以及运行功能强大的键盘记录程序以获取密码，信用卡号或其他用户信息。同时，ThiefQuest 的间谍软件组件还长期潜伏在受感染的设备上作为后门使用，这意味着它甚至会在电脑重启后仍然存在，并可能被用作额外攻击的发射台，以此进行“第二阶段”的攻击。而且，该恶意软件显示的索要赎金信息只列出了一个静态的比特币地址，受害者只能往固定地址汇款。鉴于比特币的匿名特性，在收到付款后攻击者无法知道是哪位用户已经付款，哪位没有付款。

5、 Docker 服务器遭极罕见 DDoS 恶意软件感染

6 月 29 日，E 安全消息，据外媒报道，安全研究人员发现，针对 Docker 服务器第一批有组织的持久性攻击正在发生，这些攻击是利用 DDoS 恶意软件感染来配置错误的群集。据悉，这两个僵尸网络都运行 XORDDoS 和 Kaiji 恶意软件毒株版本。而且，两种恶意软件操作都有悠久且有据可查的历史，尤其是 XORDDoS 已被发现使用了很多年。但是，这两个 DDoS 僵尸网络通常以路由器和智能设备为目标，此前从来没有针对过复杂的云设置，例如 Docker 集群。研究人员表示，黑客经常使用 Docker 来管理自己的攻击基础架构。

因为 Docker 黑客最常见的来源是使管理接口（API）处于在线状态而无需身份验证或受到防火墙的保护，所以对于希望保护其服务器安全的用户而言，检查 API 接口是第一件事。研究人员同时建议 Docker 服务器管理员通过遵循一系列基本步骤来保护其 Docker 部署。

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：顾笑南

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315