国家互联网应急中心

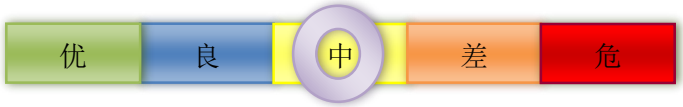
网络安全信息与动态周报

2020 年第 29 期

7 月 13 日-7 月 19 日

CNCERT/CC

本周网络安全基本态势

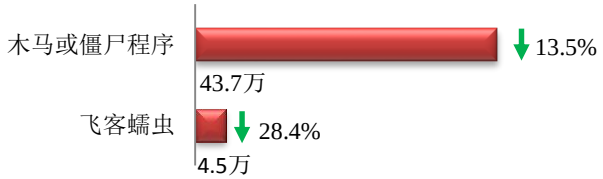


境内感染网络病毒的主机数量	•48.2万	↓ 15.2%
境内被篡改网站总数 其中政府网站数量	•5384 •19	↑ 15.4% ↓ 13.6%
境内被植入后门网站总数 其中政府网站数量	•1367 •3	↑ 15.1%
针对境内网站的仿冒页面数量	•792	↓ 28.0%
新增信息安全漏洞数量 其中高危漏洞数量	•336 •133	↑ 33.3% ↑ 137.5%

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

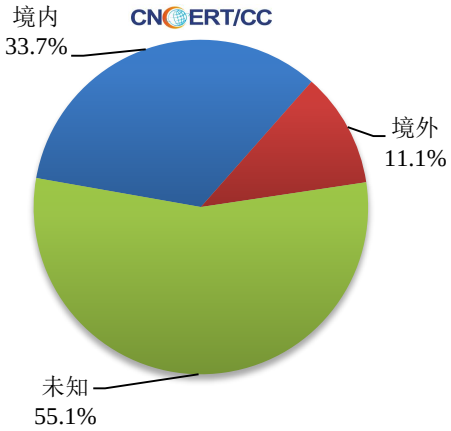
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 48.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 43.7 万以及境内感染飞客（conficker）蠕虫的主机约 4.5 万。

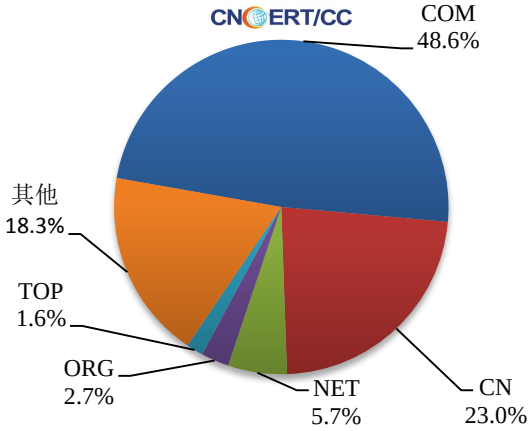


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 738 个，涉及 IP 地址 2712 个。在 738 个域名中，有 11.1%为境外注册，且顶级域为.com 的约占 48.6%；在 2712 个 IP 中，有约 73.6%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 208 个 IP。

本周放马站点域名注册所属境内外分布
(7/13-7/19)



本周放马站点域名注册所属顶级域分布
(7/13-7/19)



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。

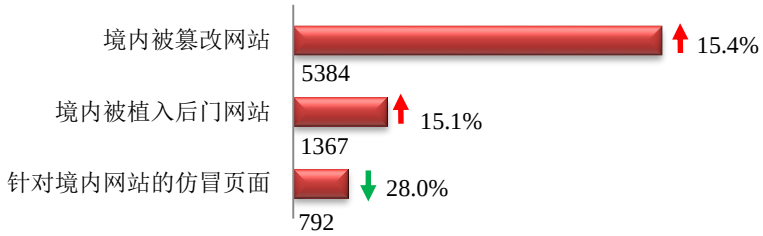
ANVA网络安全威胁信息共享平台

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。

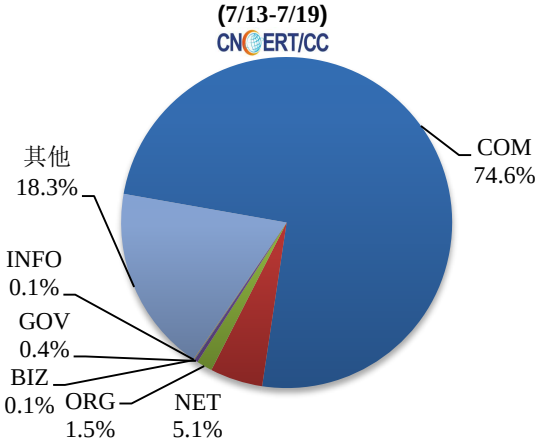
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 5384 个；被植入后门的网站数量为 1367 个；针对境内网站的仿冒页面数量 792 个。

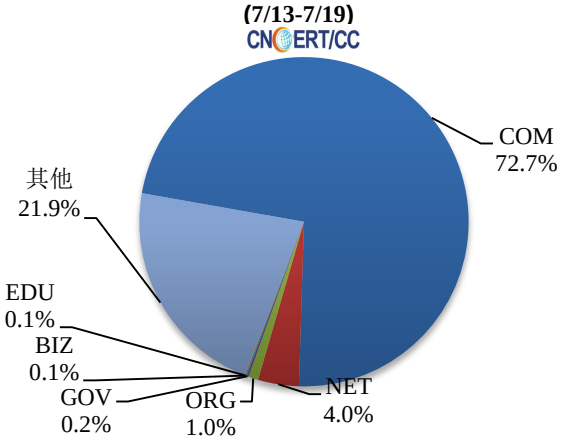


本周境内被篡改政府网站（GOV 类）数量为 19 个（约占境内 0.4%），较上周下降了 13.6%；境内被植入后门的政府网站（GOV 类）数量为 3 个（约占境内 0.2%）。

本周我国境内篡改网站按类型分布
(7/13-7/19)

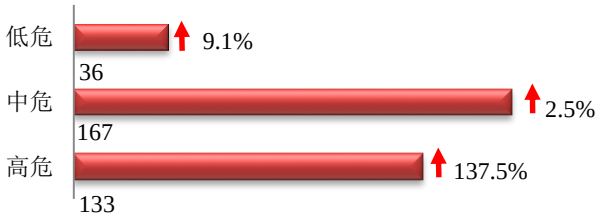


本周我国境内被植入后门网站按类型分布
(7/13-7/19)

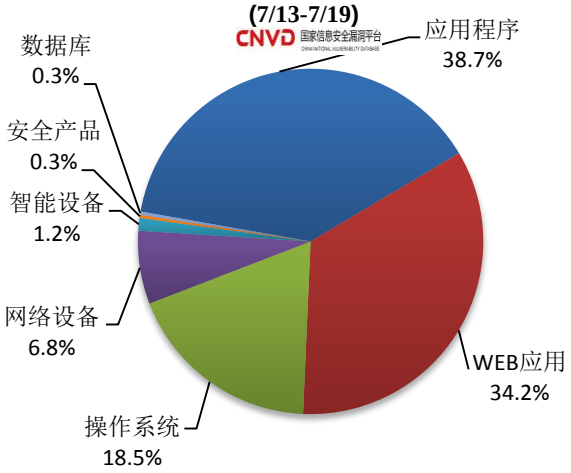


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 336 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
(7/13-7/19)



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

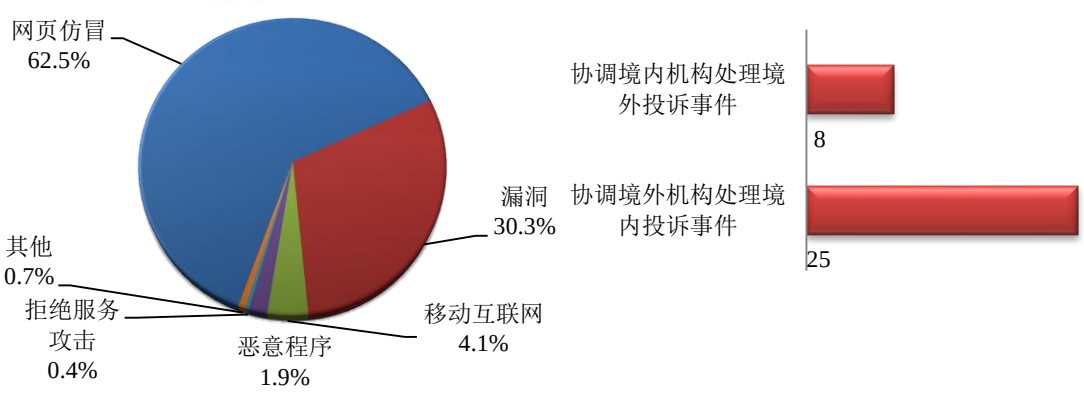
http://www.cnvd.org.cn/webinfo/list?type=4

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

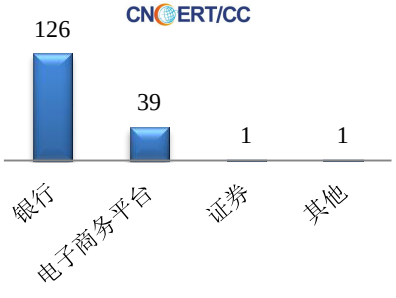
本周，CNCERT 协调基础电信企业、云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 267 起，其中跨境网络安全事件 33 起。

本周CNCERT处理的事件数量按类型分布
(7/13-7/19)

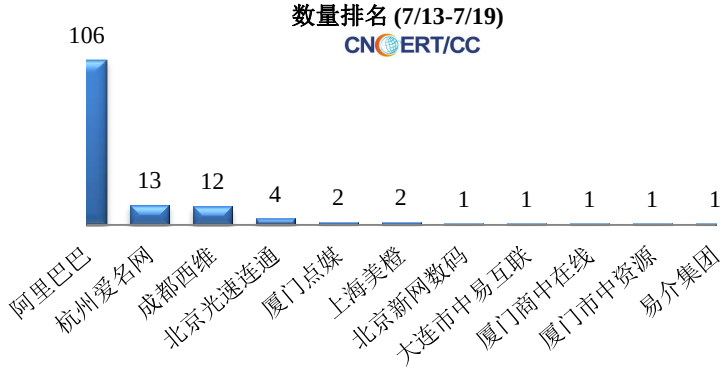


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 167 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 126 起、电子商务平台 39 起、证券 1 起和其他事件 1 起。

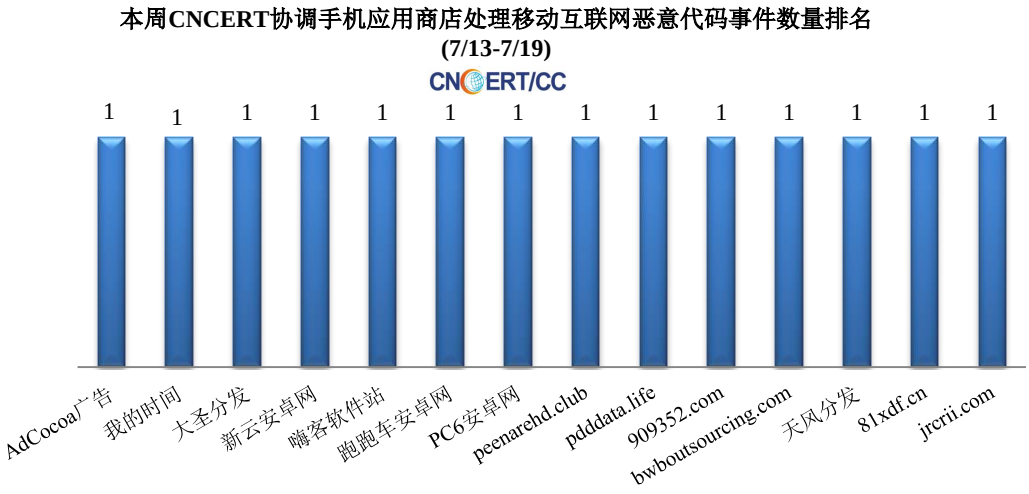
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计
(7/13-7/19)



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 (7/13-7/19)



本周，CNCERT 协调 14 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 14 个。



业界新闻速递

1、 工业和信息化部要求严厉查处“3·15”晚会曝光的信息通信领域违规行为

7 月 20 日，据工信部官网消息，针对 7 月 16 日央视播出“3·15”晚会报道的 SDK 违规收集用户个人信息的问题，工信部第一时间组织相关单位进行认真核查，依法依规严厉查处涉事企业。一是立即组织北京、上海通信管理局对涉事两家 SDK 企业，北京招彩旺旺信息技术有限公司和上海氪信信息技术有限公司进行核查处理。二是立即组织第三方检测机构对曝光使用上述两家 SDK 的 50 余款 APP 进行技术检测，对存在问题的 APP 第一时间启动下架程序。三是立即启动应用商店联动处置机制，责成阿里、腾讯、百度、华为、小米、OPPO、vivo、360 等国内主要应用商店，第一时间对类似问题进行“地毯式”排查，对发现问题一律第一时间予以下架，同时要求应用商店及时通知 APP 运营开发者自查自纠，及时发现、处理违规收集用户个人信息的 SDK。

下一步，工信部将采取常态化监管措施，加强移动互联网应用程序 APP 综合治理。集聚产业力量，推动技术手段建设，大幅提升技术检测水平。加强监督检查，加大对各类违规行为的处置和曝光力度，对未经用户同意收集使用用户个人信息等违规行为，依法予以查处，切实维护用户合法权益。

2、 Twitter 遭受重大安全漏洞 美国大批名人推特账户被黑

7 月 15 日，据纽约时报消息，美国大批知名人士和公司的推特账户被黑客攻陷，包括比尔·盖茨、埃隆·马斯克、乔·拜登、巴拉克·奥巴马、苹果公司等。据悉，黑客成功劫持盖茨和苹果等知名帐号后，通过这些账户发布推文以推广加密货币骗局，欺骗

这些名人的粉丝将钱寄到区块链地址以换取更大的回报。据统计在 Twitter 中提到的比特币地址，已经通过数百笔交易累计达到了 10 多万美元的交易额。对于此次事件，Twitter 在其官方博客公布了其遭遇严重安全事件的细节及整改措施。同时， Twitter 已阻止那些已经沦陷的帐户发布推文，以防止该骗局的进一步发酵。目前，大多数被黑帐户已恢复为所有者所有，并且删除了欺诈帖子。

3、 超过 1.42 亿美高梅酒店客人详细资料在暗网上出售

7 月 15 日，据外媒报道，暗网上出现了一则广告，出售 1.4 亿余名美高梅酒店客人的详细资料。据称，这些信息包括名人和政府雇员的数据，包括姓名、地址、电子邮件、电话号码和出生日期。发布广告的人声称，这些数据实际上来自于数据泄露监测服务 DataViper 最近的一次攻击。此次事件来自于去年该酒店的一次数据泄露，一名黑客未经授权访问了一个云端服务器，其中包含了以往客人的信息。实际受影响的客人数量可能会更多，俄罗斯黑客论坛上的帖子称，名单上有 2 亿人的详细信息。

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：郭禹

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315