国家互联网应急中心

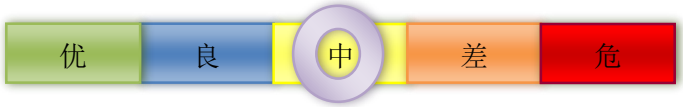
网络安全信息与动态周报

2020 年第 32 期

8 月 3 日-8 月 9 日

CNCERT/CC

本周网络安全基本态势

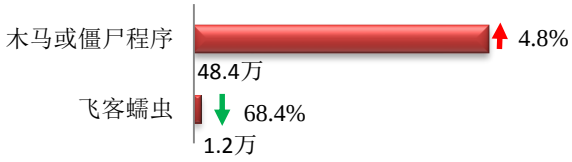


境内感染网络病毒的主机数量	•49.6万	↓ 0.8%
境内被篡改网站总数 其中政府网站数量	•4177 •14	↓ 11.4% ↓ 22.2%
境内被植入后门网站总数 其中政府网站数量	•1325 •7	↑ 2.1% ↑ 133.3%
针对境内网站的仿冒页面数量	•679	↓ 91.4%
新增信息安全漏洞数量 其中高危漏洞数量	•395 •120	↑ 35.3% ↑ 46.3%

= 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

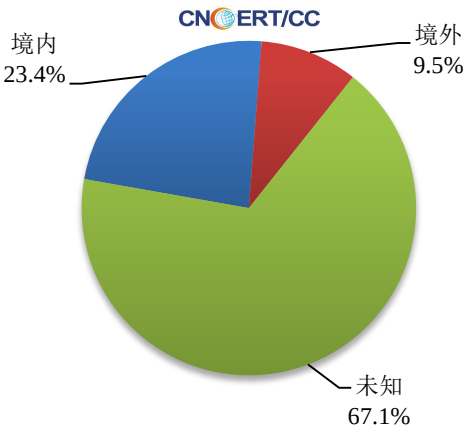
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 49.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 48.4 万以及境内感染飞客（conficker）蠕虫的主机约 1.2 万。

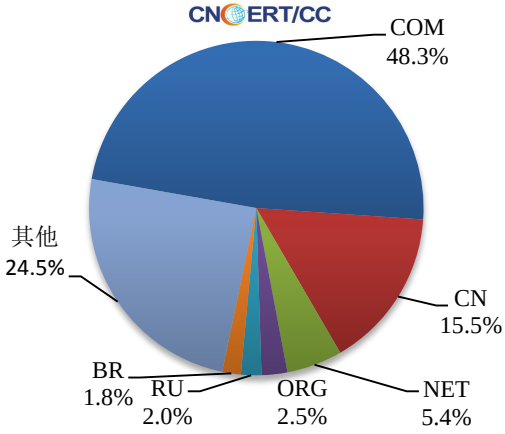


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 3494 个，涉及 IP 地址 7017 个。在 3494 个域名中，有 9.5%为境外注册，且顶级域为.com 的约占 48.3%；在 7017 个 IP 中，有约 67.3%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 442 个 IP。

本周放马站点域名注册所属境内外分布 (8/3-8/9)



本周放马站点域名注册所属顶级域分布 (8/3-8/9)



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。

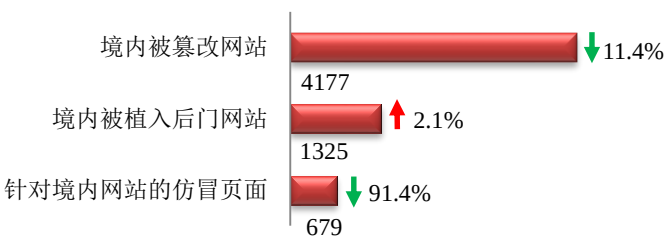
ANVA网络安全威胁信息共享平台

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。

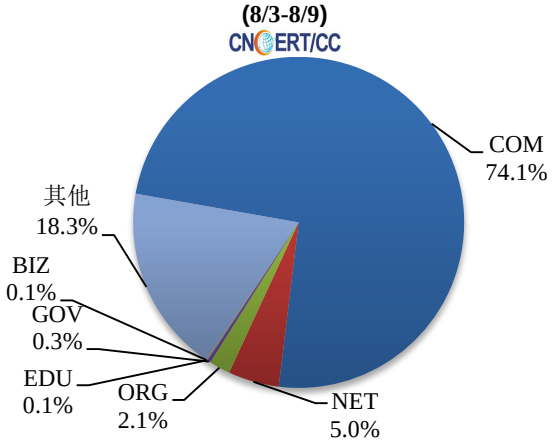
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 4177 个；被植入后门的网站数量为 1325 个；针对境内网站的仿冒页面数量 679 个。

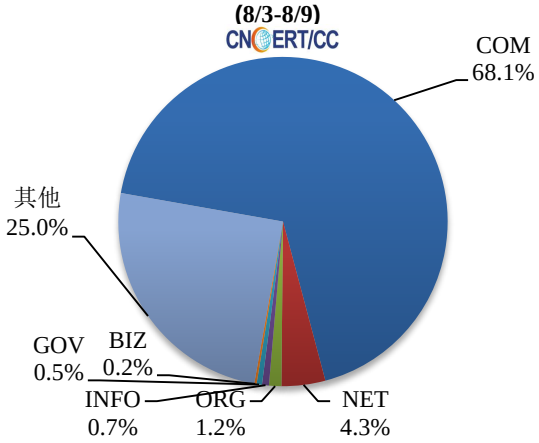


本周境内被篡改政府网站（GOV 类）数量为 14 个（约占境内 0.3%），较上周下降了 22.2%；境内被植入后门的政府网站（GOV 类）数量为 7 个（约占境内 0.5%），较上周上涨了 133.3%。

本周我国境内篡改网站按类型分布
(8/3-8/9)

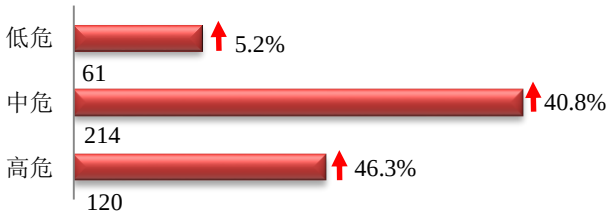


本周我国境内被植入后门网站按类型分布
(8/3-8/9)

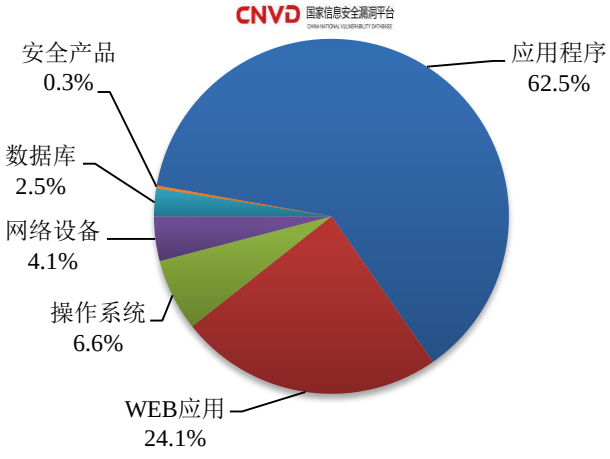


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 395 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
(8/3-8/9)



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。

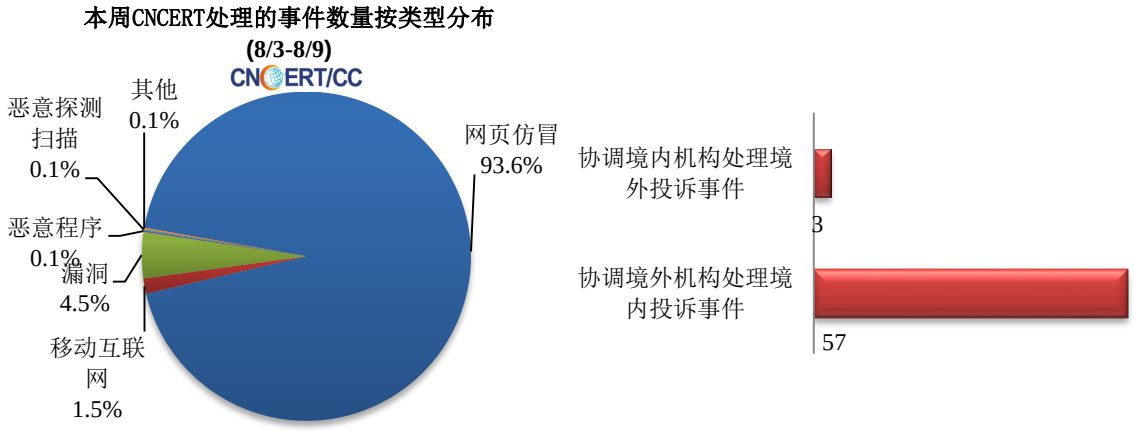
CNVD漏洞周报发布地址

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

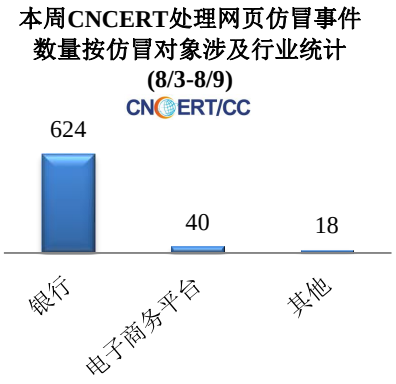
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

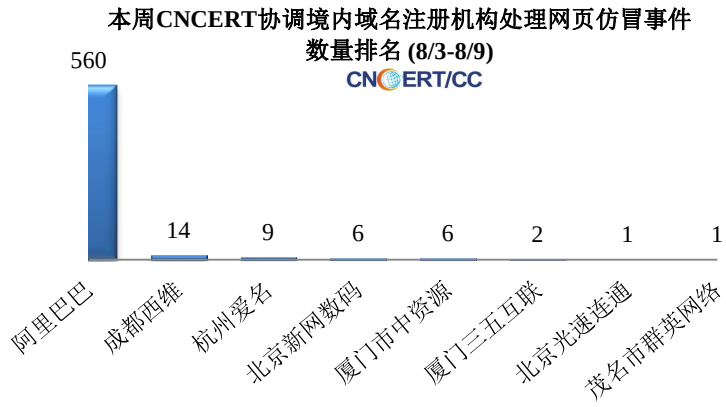
本周事件处理情况

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 699 起，其中跨境网络安全事件 60 起。

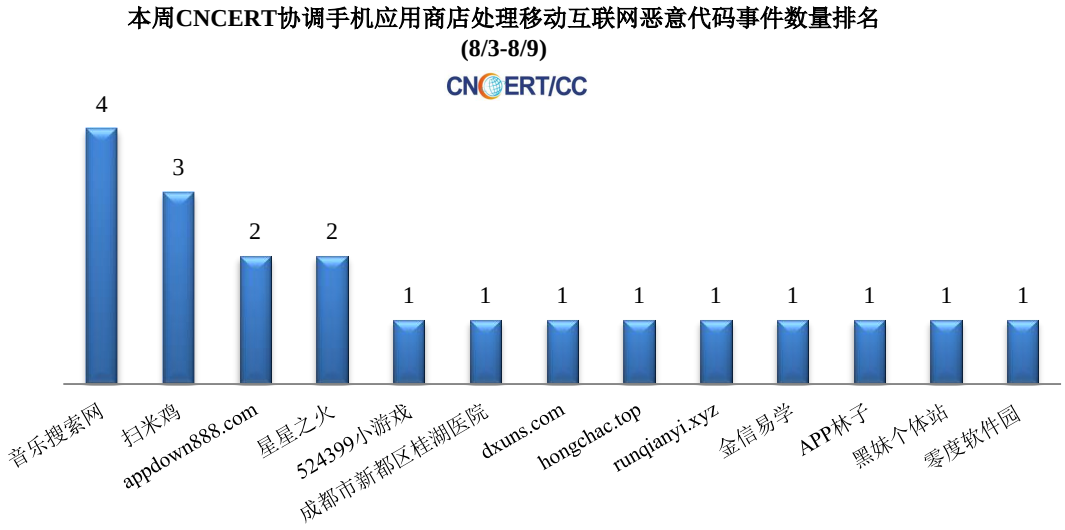


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 682 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 624 起、电子商务平台 40 起、和其他事件 18 起。





本周，CNCERT 协调 13 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 20 个。



业界新闻速递

1、 英特尔 20GB 机密数据泄漏

8 月 8 日，据外媒报道，一名黑客公布了从英特尔窃取的 20GB 芯片机密工程数据。这些数据可能会导致多个平台的用户面临新的零日漏洞威胁。这名黑客在 Telegram 上分享了一条链接，详细介绍了本次泄漏的内容，并在底部附上了一个 Mega 文件。虽然这些内容本身无害，但其中包含了 BIOS 信息和英特尔专有技术的源代码，可用于构建恶意程序。这些曝光的数据称之为“Intel exconfidential Lake”，没有在任何地方公布过，而且大部分信息都处于严格的保密协议（NDA）之下。据称，这些数据是在 2020 年早些时候由一个匿名消息来源入侵英特尔获得的。

2、 295 款 Chrome 恶意扩展程序曝光

近日，广告拦截解决方案公司 AdGuard 发文称，他们于近期发现了 295 个带有恶意的 Chrome 扩展程序，其共同特点是会劫持谷歌和必应的搜索结果，并且会在其中植入广告。在这些被曝光的程序中，大部分没有特别突出的功能，仅能够为 Chrome 的新建标签页应用自定义背景。而在这一事件的技术分析中，AdGuard 方面表示发现了这批恶意扩展程序的共性是都存在有来自 fly-analytics.com 域加载的恶意代码。数据显示，这些扩展程序的下载量已超 8000 万，目前已全部下架。

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：严寒冰

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315