国家互联网应急中心

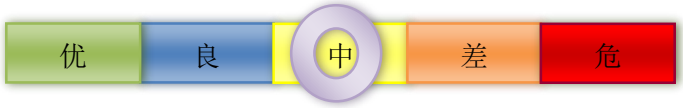
网络安全信息与动态周报

2020 年第 24 期

6 月 8 日-6 月 14 日

CNCERT/CC

本周网络安全基本态势

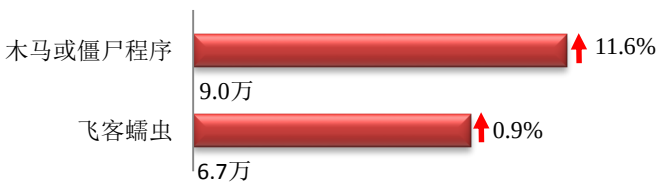


境内感染网络病毒的主机数量	•15.7万	↑ 6.7%
境内被篡改网站总数 其中政府网站数量	•9606 •37	↑ 28.5% ↑ 2.8%
境内被植入后门网站总数 其中政府网站数量	•1287 •4	↓ 4.7% ↓ 50.0%
针对境内网站的仿冒页面数量	•769	↑ 12.1%
新增信息安全漏洞数量 其中高危漏洞数量	•563 •211	↑ 21.1% ↑ 40.7%

= 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

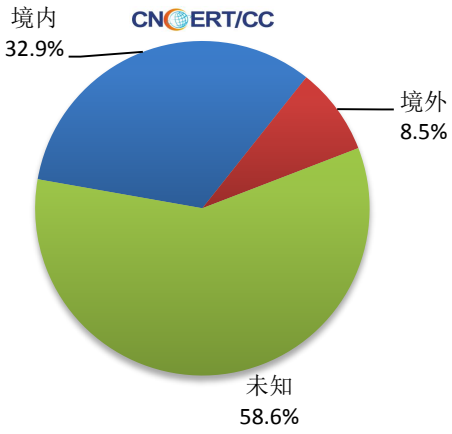
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 15.7 万个，其中包括境内被木马或被僵尸程序控制的主机约 9.0 万以及境内感染飞客（conficker）蠕虫的主机约 6.7 万。

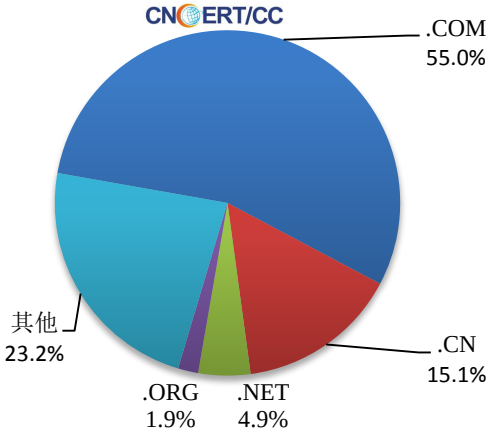


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 1477 个，涉及 IP 地址 3560 个。在 1477 个域名中，有 8.5%为境外注册，且顶级域为.com 的约占 55.0%；在 3560 个 IP 中，有约 61.1%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 482 个 IP。

本周放马站点域名注册所属境内外分布
(6/8-6/14)



本周放马站点域名所属顶级域的分布
(6/8-6/14)



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。

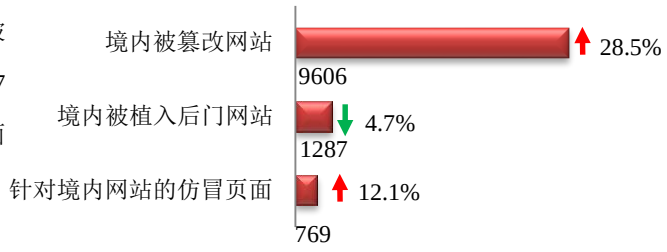
ANVA网络安全威胁信息共享平台

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。

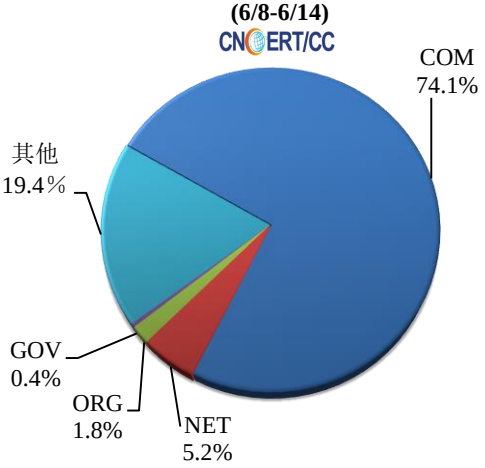
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 9606 个；被植入后门的网站数量为 1287 个；针对境内网站的仿冒页面数量 769 个。

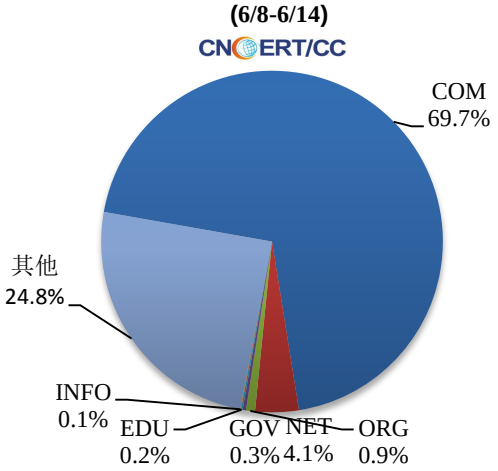


本周境内被篡改政府网站（GOV 类）数量为 37 个（约占境内 0.4%），较上周上涨了 2.8%；境内被植入后门的政府网站（GOV 类）数量为 4 个（约占境内 0.3%），较上周下降了 50.0%。

本周我国境内篡改网站按类型分布
(6/8-6/14)

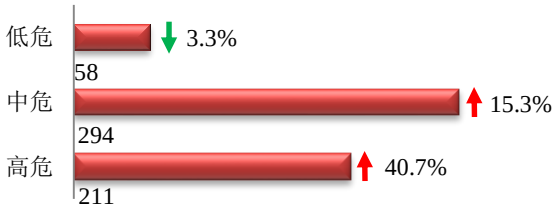


本周我国境内被植入后门网站按类型分类
(6/8-6/14)

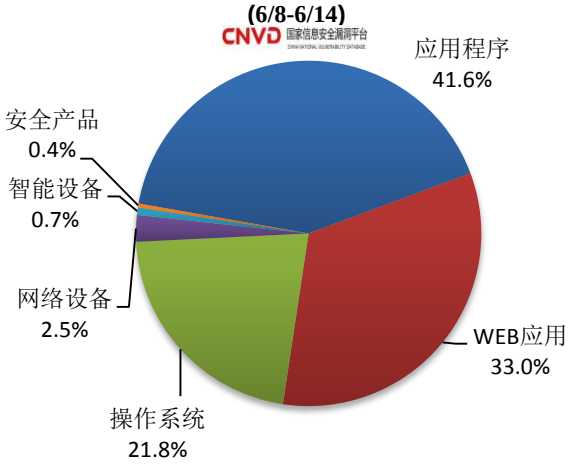


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 563 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
(6/8-6/14)



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。

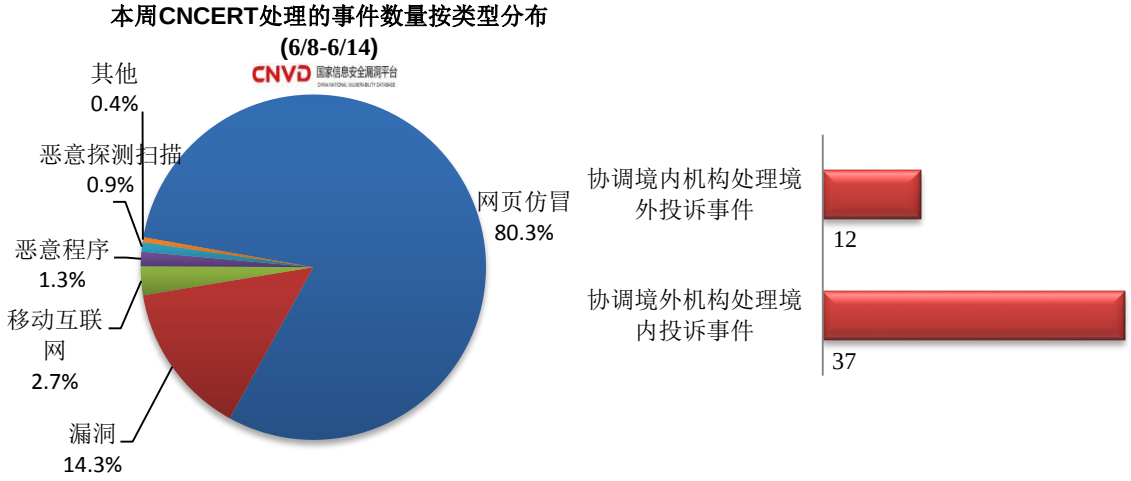
更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

CNVD漏洞周报发布地址

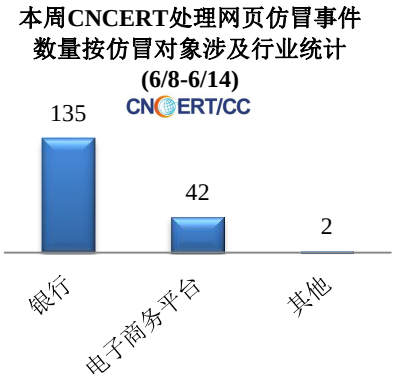
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

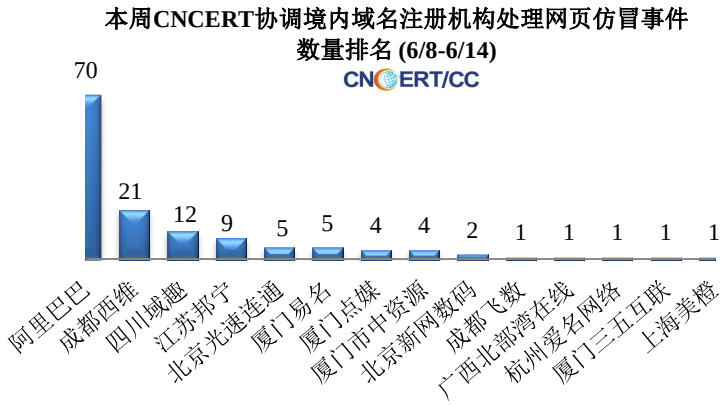
本周事件处理情况

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 223 起，其中跨境网络安全事件 49 起。

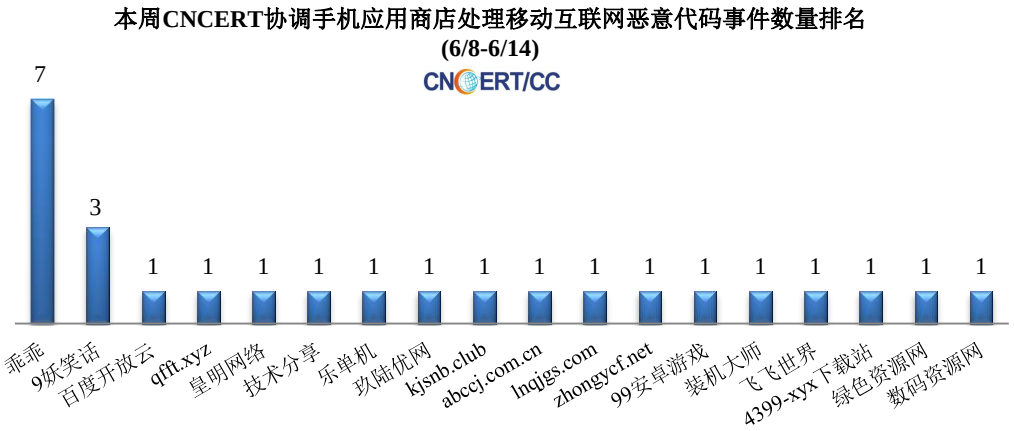


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 179 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 135 起、电子商务平台 42 起和其他事件 2 起。





本周，CNCERT 协调 18 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 26 个。



业界新闻速递

1、 工信部就媒体报道 App 侵害用户权益问题开展问询约谈

6 月 12 日消息，据工信部官网发布的消息，6 月 10 日，针对近期央视新闻曝光手机 APP 侵害用户权益的问题，工信部依据《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，组织第三方检测机构对手机应用软件进行检查，并对发现存在问题的企业进行了集中约谈，要求相关企业于 6 月 17 日前完成整改。

2、 西门子的可编程逻辑控制器存在严重漏洞

6 月 12 日，据外媒报道，德国工业巨头西门子的可编程逻辑控制器（PLC）出现严重的安全漏洞，黑客可以远程利用漏洞发起拒绝服务（DoS）攻击并修改设备的配置参数。据西门子方面称，漏洞影响了其所有用于基本控制任务的“LOGO！8 BM”设备的所有版本，用于极端条件的 SIPLUS 版本也会受到影响。西门子还表示，未经身份验证的攻击者，获取具有对 TCP 端口 135 的网络访问权限，无需用户干预的情况下就可以利用这些漏洞来读取和修改设备的配置并获取有关文件。据思科的 Talos 威胁情报和研究小组发现三个身份验证漏洞对应 CVE 标识符都是 CVE-2020-7589（TALOS-2020-1024/CVE-2020-7589、TALOS-2020-1025/CVE-2020-7589、TALOS-2020-1026/CVE-2020-7589）。根据 Talos 发布的公告，三个漏洞均与 LOGO！的 TDE 文本显示功能有关。黑客将特制数据包发送到目标系统即可利用漏洞。Talos 威胁情报和研究小组表示，其中两个缺陷使攻击者可以删除设备上的信息，第三个漏洞可能被利用来上传或覆盖 SD 卡上的文件，这可能会影响设备的完整性和可用性。

3、 印度视频点播服务巨头 ZEE5 遭到黑客入侵

6 月 9 日，E 安全消息，据外媒报道，印度视频点播巨头 ZEE5 遭黑客入侵，同时，攻击者扬言要在网络犯罪地下市场上出售所窃取的数据库信息。据报道，一个名为约翰·威克（John Wick）”的黑客声称，已经入侵了印度视频点播巨头 ZEE5，并威胁要在网络犯罪市场上出售该数据库。这名黑客声称从 Zee5.com 窃取了超过 150GB 的实时数据，攻击者还发布了来自受损数据库的部分数据，以及源代码中存在的密钥。大量的数据包括最近的交易，密码，电子邮件，手机号码，电子邮件地址，消息等。

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：贺铮

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315