国家互联网应急中心

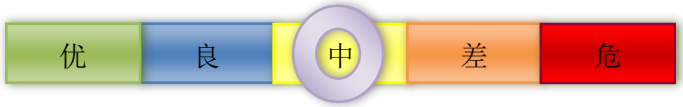
网络安全信息与动态周报

2020 年第 36 期

8 月 31 日-9 月 6 日

CNCERT/CC

本周网络安全基本态势

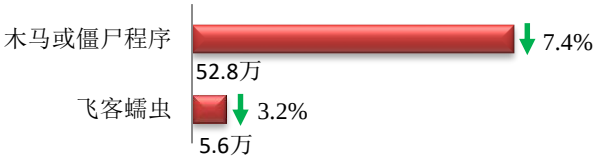


境内感染网络病毒的主机数量	•58.4万	↓ 7.0%
境内被篡改网站总数 其中政府网站数量	•2707 •11	↓ 0.1% ↑ 83.3%
境内被植入后门网站总数 其中政府网站数量	•1158 •4	↓ 1.3% =
针对境内网站的仿冒页面数量	•17546	↑ 81.3%
新增信息安全漏洞数量 其中高危漏洞数量	•465 •131	↓ 30.9% ↓ 54.7%

= 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

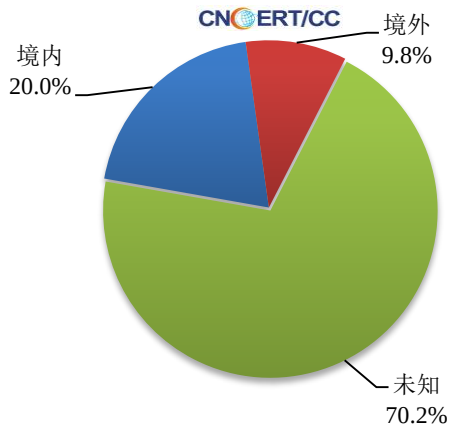
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 58.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 52.8 万以及境内感染飞客（conficker）蠕虫的主机约 5.6 万。

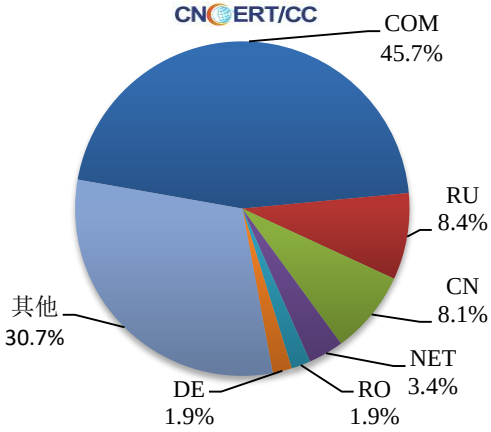


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 645 个，涉及 IP 地址 2226 个。在 645 个域名中，有 9.8%为境外注册，且顶级域为.com 的约占 45.7%；在 2226 个 IP 中，有约 56.2%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 98 个 IP。

本周放马站点域名注册所属境内外分布
(8/31-9/6)



本周放马站点域名注册所属顶级域分布
(8/31-9/6)



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。

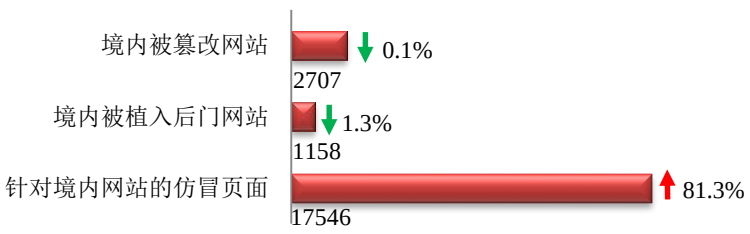
ANVA网络安全威胁信息共享平台

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。

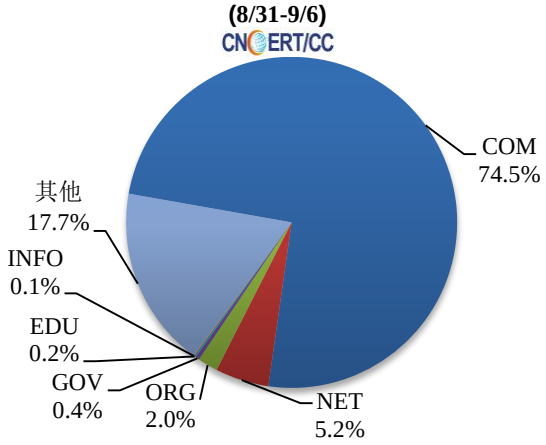
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 2707 个；被植入后门的网站数量为 1158 个；针对境内网站的仿冒页面数量 17546 个，主要是互联网上出现了大量“ETC 在线认证”的仿冒页面。

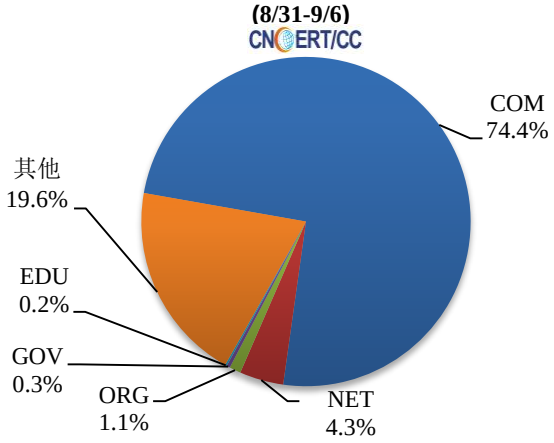


本周境内被篡改政府网站（GOV 类）数量为 11 个（约占境内 0.4%），较上周上涨了 83.3%；境内被植入后门的政府网站（GOV 类）数量为 4 个（约占境内 0.3%），与上周持平。

本周我国境内篡改网站按类型分布
(8/31-9/6)

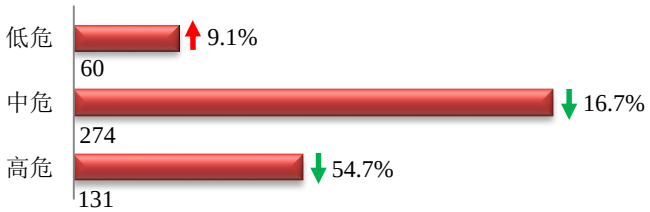


本周我国境内被植入后门网站按类型分布
(8/31-9/6)

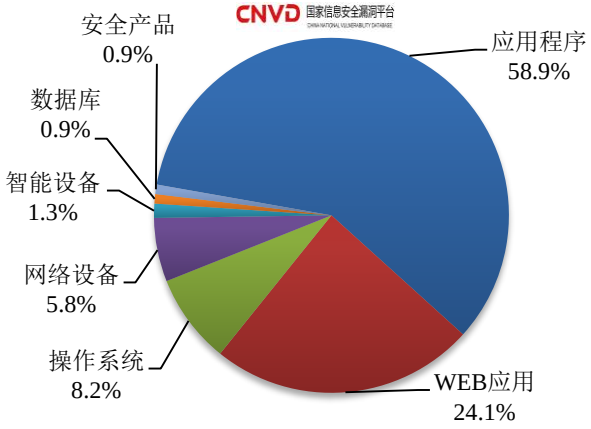


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 465 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
(8/31-9/6)



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。

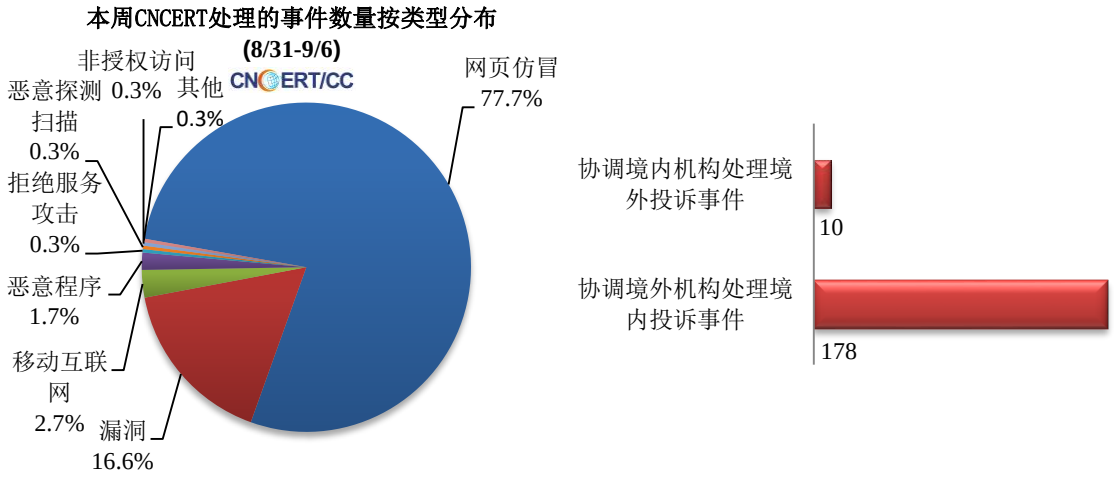
CNVD漏洞周报发布地址

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

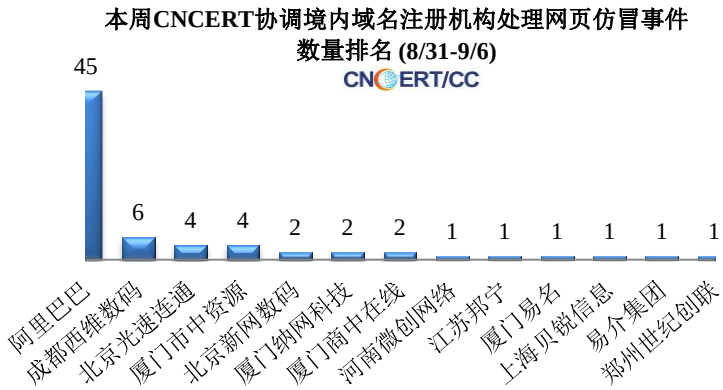
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

本周事件处理情况

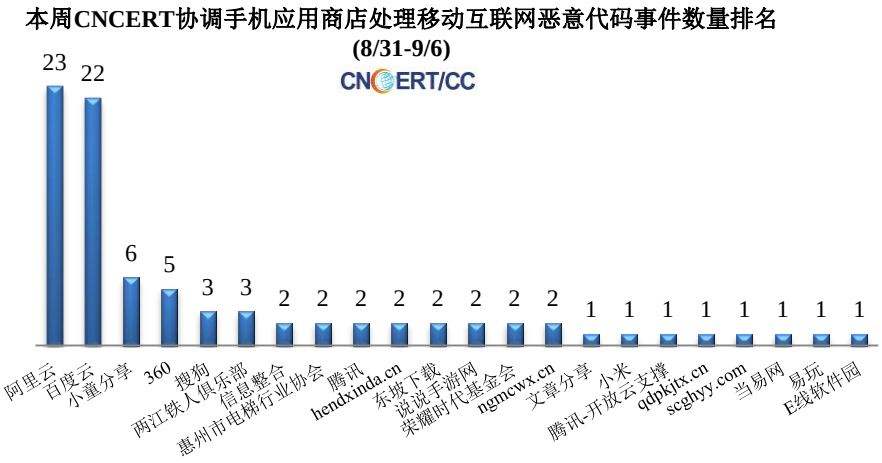
本周，CNCERT 协调基础电信企业、云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 296 起，其中跨境网络安全事件 188 起。



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 229 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 203 起、电子商务平台 22 起和其他事件 4 起。



本周，CNCERT 协调 22 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 86 个。



业界新闻速递

1、 工信部通报 101 款侵害用户权益行为 APP

8 月 31 日，工信部通报了 101 款侵害用户权益行为 APP。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，督促存在问题的企业进行整改。截至目前，尚有 101 款 APP 未完成整改。上述 APP 应在 9 月 7 日前完成整改落实工作，逾期不整改的，工信部将依法依规组织开展相关处置工作。

公告显示，此次检测中，应用宝、豌豆荚、小米应用商店等部分移动应用分发平台管理主体责任缺位，对上架 APP 审核把关不严，检测发现问题较多，未严格落实《移动智能终端应用软件预置和分发管理暂行规定》要求，后续工信部将对问题突出、有令不行、整改不彻底的企业依法严厉处置。

2、 第八届中日韩互联网应急年会顺利召开

2020 年 8 月 24 日至 25 日，中国国家计算机网络应急技术处理协调中心（CNCERT/CC）、日本计算机应急响应协调中心（JPCERT/CC）和韩国计算机应急响应协调中心（KrCERT/CC）操作层面代表在线召开了第八届中日韩互联网应急年会，会议由 KrCERT/CC 主办。该年会是根据三方于 2011 年签订的“国家级计算机安全事件响应小组联合合作备忘录”召开。由于疫情原因，此次会议在线上召开。

本届中日韩互联网应急年会的主要成果包括：共同回顾了三方合作活动尤其是事件协调活动；从各自角度分享了网络安全趋势、政策更新情况和技术发展；分享重大跨境事件处置案例和合作建议；分享调查问卷情况以加强对彼此能力的了解；了解彼此新冠疫情下的网络安全事件态势以及处置措施。下届年会将由 JPCERT/CC 于 2021 年负责主办。

3、 以色列芯片巨头 TowerJazz 被黑，制造部门暂停运转

9 月 6 日，路透社报道，以色列芯片巨头 TowerJazz 突然遭受网络攻击，部分系统服务器和制造部门暂停运转。根据集邦咨询等半导体行业研究机构统计，TowerJazz 公司是全球排名前十的芯片代工企业，在模拟芯片代工行业处于领军地位，其在射频和高性能模拟电路领域的技术可支持众多消费类、工业设施级和汽车电子应用的高速、低功耗产品，市场领先性较强。该公司随即发表了一份官方声明：“TowerJazz 已经通知相关部门，迅速组建了一只全球领先的技术团队，并且与执法部门紧密合作，在保险服务商的协调下，力求尽快恢复遭受网络攻击的系统。公司已经采取进一步措施防止事态扩大。目前，我们尚未具体评估此次攻击到底对公司造成的实质性影响。”

4、 最新的 WordPress 插件存在漏洞，大量的网站正在被探测和攻击

9 月 6 日，ZDNet 网站消息，广泛使用的 WordPress 插件中存在一个漏洞，被利用引发大量网站被探测和攻击。据报道，攻击突然激增是在黑客发现并利用了“文件管理器”中的零日漏洞之后发生的，该“文件管理器”是 WordPress 的一个插件，在约 70 万个站点上使用。黑客首先对互联网上的网站进行探测，如果探测成功，则攻击者将利用该漏洞在网站上植入后门。开发人员团队在获悉攻击的同一天，发布了一个补丁用于修复该漏洞。

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：常霞

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315