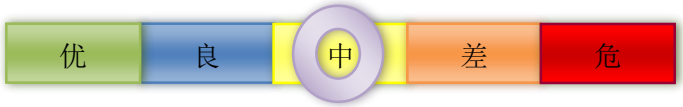
国家互联网应急中心

2020 年第 33 期
8 月 10 日-8 月 16 日

网络安全信息与动态周报

本周网络安全基本态势

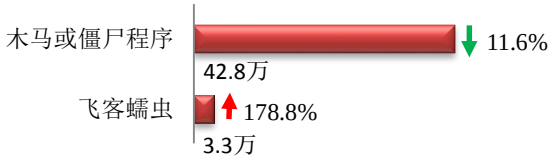


境内感染网络病毒的主机数量	•46.1万	7.0%
境内被篡改网站总数 其中政府网站数量	•3967 •18	5.0% 28.6%
境内被植入后门网站总数 其中政府网站数量	•1461 •6	10.3% 14.3%
针对境内网站的仿冒页面数量	•17805	2522.2%
新增信息安全漏洞数量 其中高危漏洞数量	•301 •124	23.8% 3.3%

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

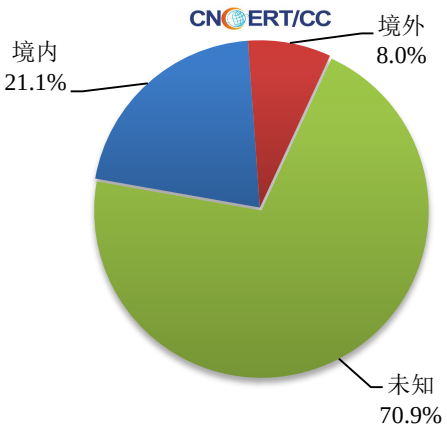
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 46.1 万个，其中包括境内被木马或被僵尸程序控制的主机约 42.8 万以及境内感染飞客（conficker）蠕虫的主机约 3.3 万。

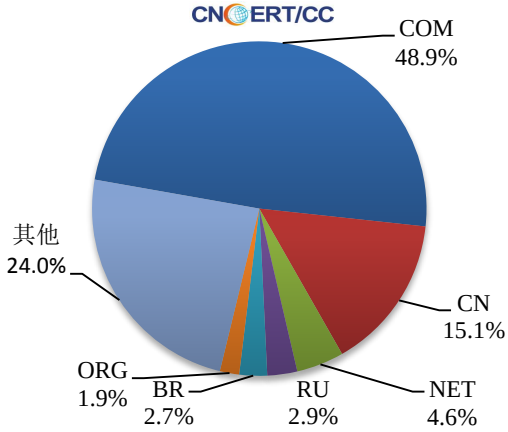


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 3315 个，涉及 IP 地址 6737 个。在 3315 个域名中，有 8.0%为境外注册，且顶级域为.com 的约占 48.9%；在 6737 个 IP 中，有约 68.3%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 398 个 IP。

本周放马站点域名注册所属境内外分布
(8/10-8/16)



本周放马站点域名注册所属顶级域分布
(8/10-8/16)



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。

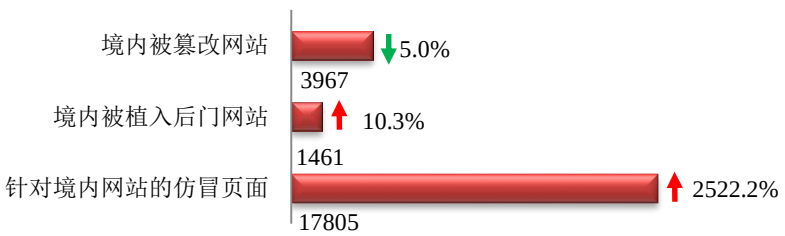
ANVA网络安全威胁信息共享平台

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。

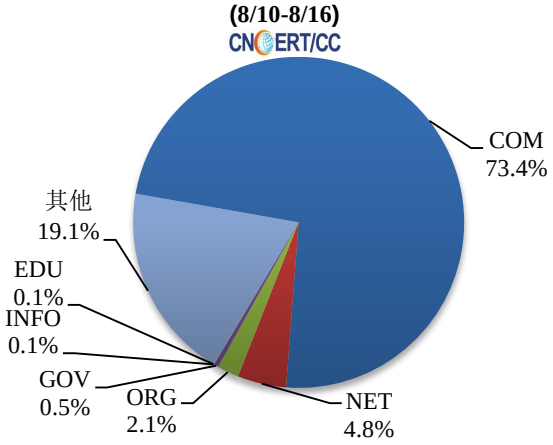
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 3967 个；被植入后门的网站数量为 1461 个；针对境内网站的仿冒页面数量 17805 个，主要是互联网上出现了大量“ETC 在线认证”的仿冒页面。

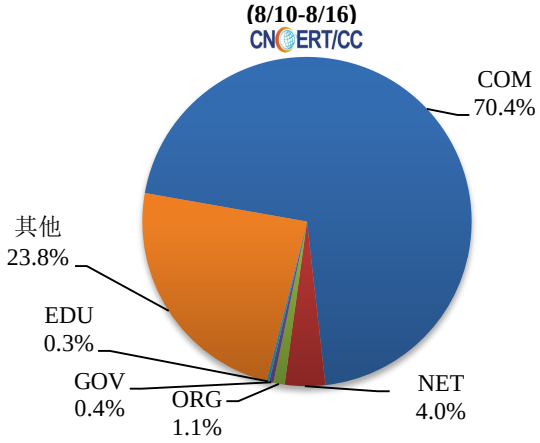


本周境内被篡改政府网站（GOV 类）数量为 18 个（约占境内 0.5%），较上周上涨了 28.6%；境内被植入后门的政府网站（GOV 类）数量为 6 个（约占境内 0.4%），较上周下降了 14.3%。

本周我国境内篡改网站按类型分布
(8/10-8/16)

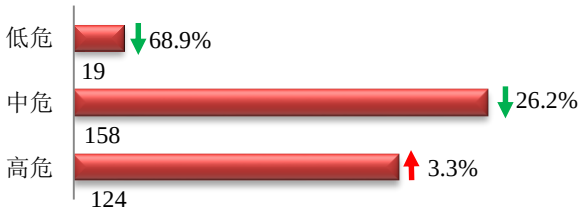


本周我国境内被植入后门网站按类型分布
(8/10-8/16)

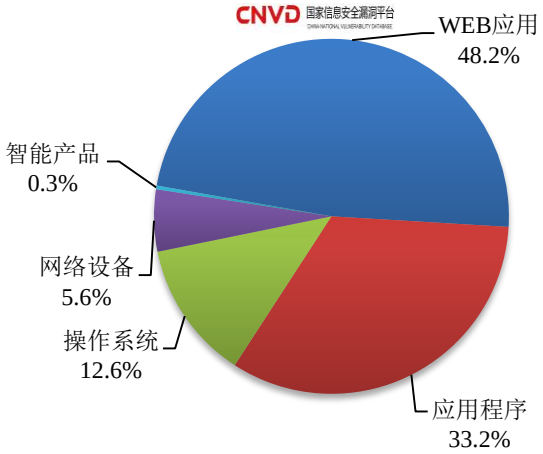


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 301 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
(8/10-8/16)



本周 CNVD 发布的网络安全漏洞中，WEB 应用漏洞占比最高，其次是应用程序和操作系统。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

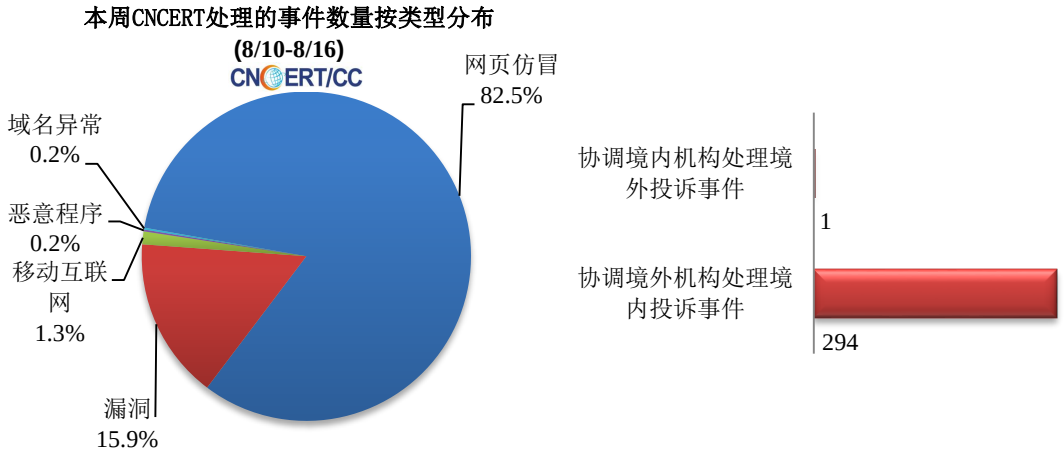
CNVD漏洞周报发布地址

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

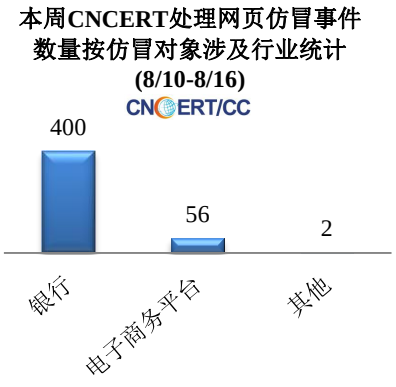
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

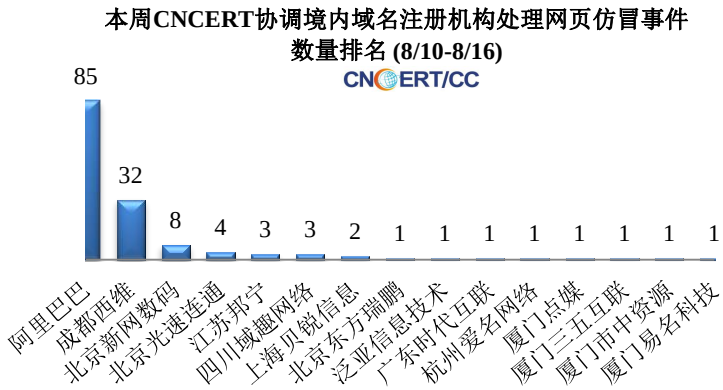
本周事件处理情况

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 555 起，其中跨境网络安全事件 295 起。

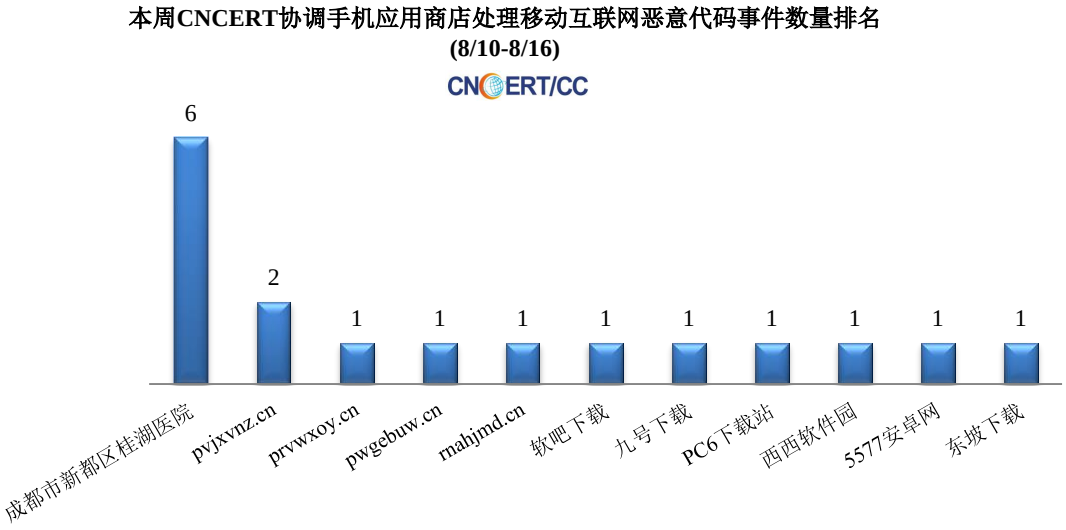


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 458 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 400 起、电子商务平台 56 起、和其他事件 2 起。





本周，CNCERT 协调 11 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 17 个。



业界新闻速递

1、 2020 中国网络安全年会在网上成功召开

8 月 12 日，以“并肩应对威胁挑战”为主题的 2020 中国网络安全年会在网上成功召开。本届中国网络安全年会由国家互联网信息办公室指导，国家计算机网络应急技术处理协调中心（CNCERT/CC）主办，天融信、启明星辰、长安通信、恒安嘉新、安天、阿里云、奇安信、深信服、安恒、亚信安全联合主办，中国通信学会通信安全技术委员会协办。中央网络安全和信息化委员会办公室副总工程师、国家计算机网络应急技术处理协调中心主任李湘宁致欢迎辞。中国工程院院士邬贺铨、邬江兴、张平作主旨报告，工业和信息化部网络安全管理局副局长张新，公安部十一局巡视员、副局长、总工程师郭启全致辞。此外，奇安信集团董事长齐向东，安天科技集团股份有限公司董事长、首席架构师肖新光，杭州安恒信息技术股份有限公司董事长、总裁范渊，天融信科技集团首席执行官李雪莹，亚信安全总裁陆光明，长安通信科技有限责任公司常务副总裁陈训逊，恒安嘉新（北京）科技股份公司首席执行官陈晓光，阿里巴巴副总裁刘松，启明星辰集团合伙人、高级副总裁、网御星云公司总裁胡晓峰，深信服科技股份有限公司副总裁、核心战略负责人马程也围绕网络安全热点问题分享了精彩观点。

今年，2020 中国网络安全年会首次以网上方式举办，大会还设置了“5G 时代的万物互联与安全挑战”“新基建—工业互联网安全”“网络安全态势感知”“5G 的数字能力与安全”“新基建新安全”“5G 安全论坛”等共 6 个主题分论坛。经过 16 年的发展，一年一度的“中国网络安全年会”已成为国内网络安全领域的重要会议，得到政府有关部

门、互联网企业、重要信息系统单位和广大互联网用户的广泛关注，是国内网络安全“产、学、研、用”各界进行技术业务交流的重要桥梁和纽带，对于推动我国网络安全工作、提高社会网络安全意识起到了积极作用。

2、 《2019 年中国互联网网络安全报告》发布

8 月 11 日，CNCERT 编写的《2019 年中国互联网网络安全报告》正式发布。自 2008 年起，CNCERT 持续编写发布中国互联网网络安全年度报告，依托 CNCERT 多年来从事网络安全监测、预警和应急处置等工作的实际情况，对我国互联网网络安全状况进行总体判断和趋势分析，具有重要的参考价值。该系列报告为政府部门提供监管支撑，为互联网企业提供运行管理技术支持，向社会公众普及互联网网络安全知识，对提高全社会、全民的网络安全意识发挥积极作用。《2019 年中国互联网网络安全报告》汇总分析了 CNCERT 自有网络安全监测数据和 CNCERT 网络安全应急服务支撑单位报送的数据，具有重要的参考价值，内容涵盖我国互联网网络安全态势分析、网络安全监测数据分析、网络安全事件案例详解、网络安全政策和技术动态等多个方面。其中，报告对计算机恶意程序传播和活动、移动互联网恶意程序传播和活动、网站安全监测、DDoS 攻击监测、安全漏洞预警与处置、网络安全事件接收与处理等情况进行深入细致的分析，并对 2019 年的典型网络安全事件进行专题介绍。此外，报告对国内网络安全组织发展情况和 CNCERT 举办的国内外重要活动等进行了总结。最后，报告对 2020 年网络安全热点问题进行预测。

3、 关于防范黑客通过仿冒“ETC 在线认证”网站实施网络诈骗的风险提示

近期，CNCERT 监测发现互联网上出现大量仿冒“ETC 在线认证”网站的钓鱼页面。诈骗分子通过此类钓鱼网站，诱骗获取用户的真实姓名、银行卡账号、身份证号、银行预留手机号、取款密码等个人隐私信息，从而盗取资金。请广大网民强化风险意识，加强安全防范，避免不必要的经济损失，主要建议包括：（1）要仔细核对网址，如北京市 ETC 的官方网站为 https://www.bjetc.cn/；（2）不要轻易打开来历不明的网址链接；（3）据悉 ETC 官方近期没有在线验证要求，如有业务办理方面的疑惑，可及时联系当地 ETC 网点进行咨询；（4）不轻易提供自己的银行卡号、取款密码、身份证号等重要隐私信息。

4、 Apache Struts 披露了一个远程代码执行漏洞

8 月 13 日，Apache Struts 官方发布安全公告，披露 S2-059 Struts 远程代码执行漏洞（CVE-2019-0230、CNVD-2020-46202）。公告指出在使用某些 tag 等情况下可能存在 OGNL 表达式注入漏洞，从而造成远程代码执行，风险极大，CNVD 认定该漏洞危害等级

为“高危”。Apache Struts 官方提醒 ApacheStruts 用户尽快升级到 2.5.22 或以上版本，避免遭遇黑客攻击。

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：丁丽

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315