国家互联网应急中心

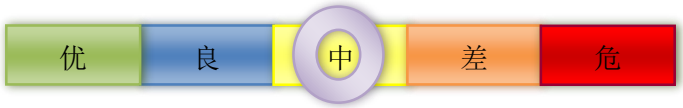
网络安全信息与动态周报

2020 年第 10 期

3 月 2 日-3 月 8 日

CNCERT/CC

本周网络安全基本态势

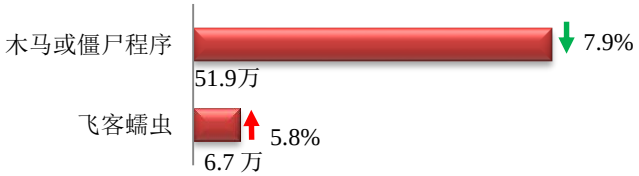


境内感染网络病毒的主机数量	•58.6万	↓ 6.5%
境内被篡改网站总数 其中政府网站数量	•7529 •27	↓ 17.6% ↓ 40.0%
境内被植入后门网站总数 其中政府网站数量	•1578 •3	↑ 2.7% ↑ 200.0%
针对境内网站的仿冒页面数量	•1570	↑ 57.6%
新增信息安全漏洞数量 其中高危漏洞数量	•554 •197	↓ 20.7% ↓ 31.6%

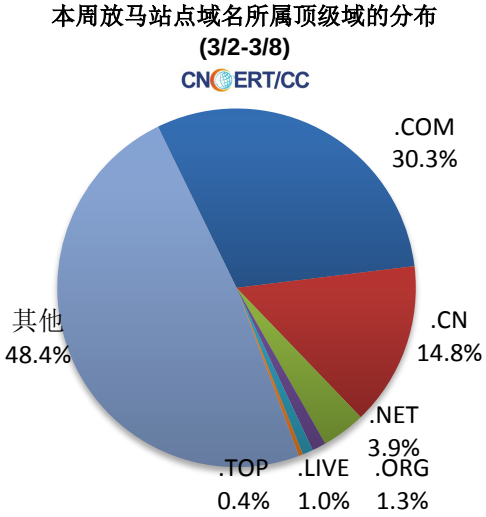
= 表示数量与上周相同　↑ 表示数量较上周环比增加　↓ 表示数量较上周环比减少

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 58.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 51.9 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名 2311 个，涉及 IP 地址 6155 个。在 2311 个域名中，顶级域名为.com 的约占 30.3%。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 338 个 IP。



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。

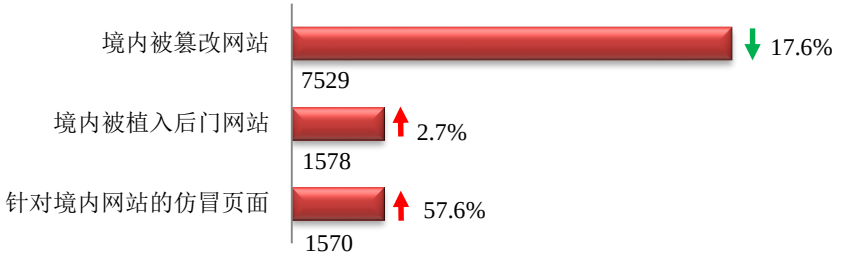
ANVA恶意地址黑名单发布地址

http://www.anva.org.cn/virusAddress/listBlack

中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由中国互联网协会网络与信息安全工作委员会发起、CNCERT 具体组织运作的行业联盟。

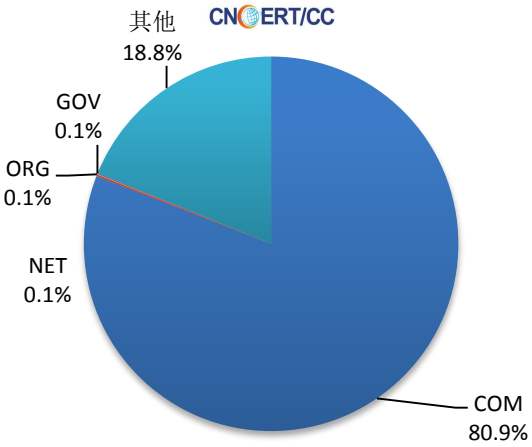
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 7529 个；被植入后门的网站数量为 1578 个；针对境内网站的仿冒页面数量 1570 个。

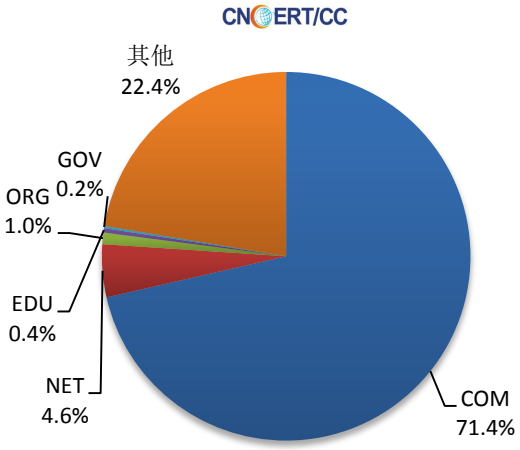


本周境内被篡改政府网站（GOV 类）数量为 27 个（约占境内 0.4%），较上周下降了 40.0%；境内被植入后门的政府网站（GOV 类）数量为 3 个（约占境内 0.2%），较上周上涨了 200.0%。

本周我国境内篡改网站按类型分布
(3/2-3/8)

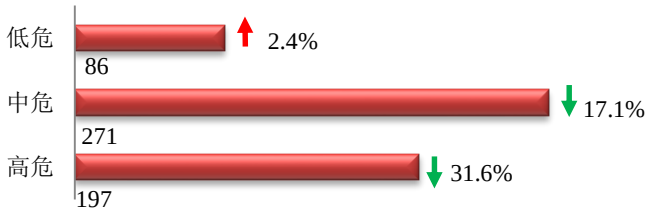


本周我国境内被植入后门网站按类型分布
(3/2-3/8)

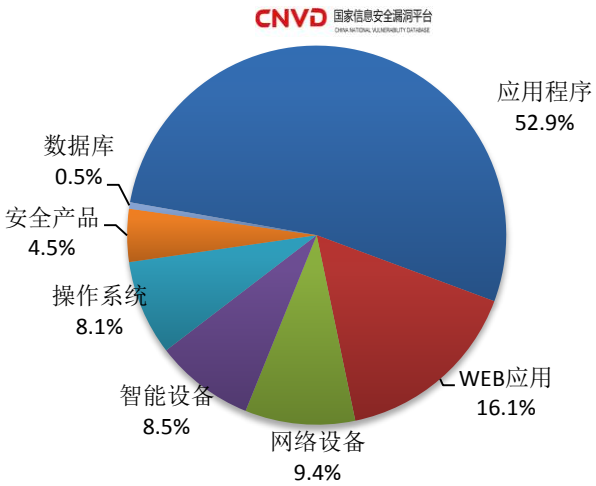


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 554 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
(3/2-3/8)



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 应用和网络设备。

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

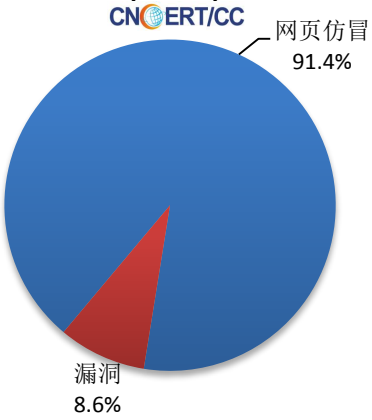
http://www.cnvd.org.cn/webinfo/list?type=4

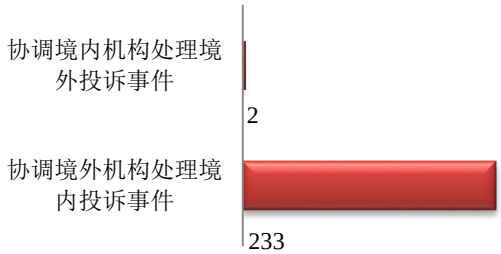
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

本周事件处理情况

本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 525 起，其中跨境网络安全事件 235 起。

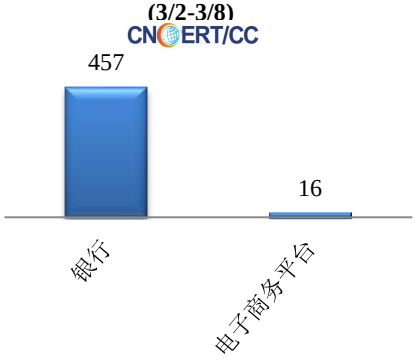
本周CNCERT处理的事件数量按类型分布 (3/2-3/8)



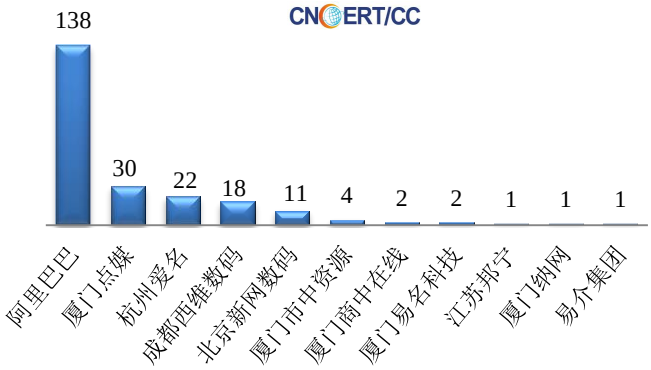


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 480 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包括银行仿冒事件 457 起和电子商务平台 16 起。

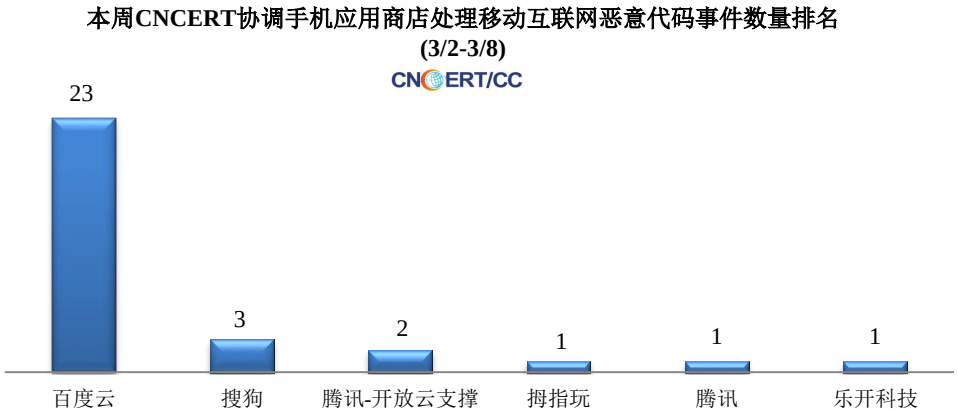
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (3/2-3/8)



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 (3/2-3/8)



本周，CNCERT 协调 6 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 31 个。



业界新闻速递

1、 四部委联合印发《新冠肺炎疫情社区防控工作信息化建设和应用指引（第一版）》

社区是疫情联防联控、群防群控的关键防线。为促进社区防控工作与现代信息技术深度融合，强化外防输入、内防扩散的技术支撑，提高社区防控的信息化、智能化水平，减轻参与城乡社区疫情防控工作人员工作压力，民政部办公厅、中央网信办秘书局、工业和信息化部办公厅、国家卫生健康委办公厅联合印发《新冠肺炎疫情社区防控工作信息化建设和应用指引》（民办发〔2020〕5 号，以下简称《指引》）。

《指引》强调，社区防控工作信息化建设和应用的目标是：按照疫情防控总体部署和社区防控工作要求，坚持适用性、便捷性、安全性和前瞻性相统一，发挥互联网、大数据、人工智能等信息技术优势，依托各类现有信息平台特别是社区信息平台，开发适用于社区防控工作全流程和各环节的功能应用，有效支撑社区疫情监测、信息报送、宣传教育、环境整治、困难帮扶等防控任务，统筹发挥城乡社区组织、社区工作者的动员优势和信息化、智能化手段的技术优势，有效支撑省、市、县、乡四级数据联通，构筑起人防、物防、技防、智防相结合的社区防线，形成立体式社区防控数据链路和闭环，提升城乡社区疫情防控工作成效。

《指引》从疫情监测和重点人群管理、出入管理、信息报送、宣传教育、环境整治、困难帮扶和社区服务等七个方面，提出了社区防控工作信息化建设和应用的基本思路；从部署条件、系统安全、隐私保护、公益原则等四个方面，明确社区防控工作信息化建设和应用的相关支持环境。强调社区防控信息化产品（服务）应遵守《中华人民共和国网络安全法》、《中华人民共和国居民身份证法》和有关法律、行政法规关于个人信息保护的规定，落实中央网信办《关

于做好个人信息保护利用大数据支撑联防联控工作的通知》要求。

根据《指引》有关要求，民政部、中央网信办、工业和信息化部、国家卫生健康委还将指导相关行业协会等社会组织推荐部分社区防控信息化产品（服务），以供各地结合实际自愿选择使用。

2、 工业和信息化部印发《工业数据分类分级指南（试行）》

3 月 4 日，工业和信息化部网站消息，为贯彻《促进大数据发展行动纲要》《大数据产业发展规划（2016-2020 年）》有关要求，更好推动《数据管理能力成熟度评估模型》（GB/T 36073-2018）贯标和《工业控制系统信息安全防护指南》落实，指导企业提升工业数据管理能力，促进工业数据的使用、流动与共享，释放数据潜在价值，赋能制造业高质量发展，工业和信息化部办公厅印发《工业数据分类分级指南（试行）》（以下简称“指南”）。指南指出，工业企业结合生产制造模式、平台企业结合服务运营模式，分析梳理业务流程和系统设备，考虑行业要求、业务规模、数据复杂程度等实际情况，对工业数据进行分类梳理和标识，形成企业工业数据分类清单。工业企业工业数据分类维度包括但不限于研发数据域（研发设计数据、开发测试数据等）、生产数据域（控制信息、工况状态、工艺参数、系统日志等）、运维数据域（物流数据、产品售后服务数据等）、管理数据域（系统设备资产信息、客户与产品信息、产品供应链数据、业务统计数据等）、外部数据域（与其他主体共享的数据等）。平台企业工业数据分类维度包括但不限于平台运营数据域（物联采集数据、知识库模型库数据、研发数据等）和企业管理数据域（客户数据、业务合作数据、人事财务数据等）。指南明确，工业和信息化部负责制定工业数据分类分级制度规范，指导、协调开展工业数据分类分级工作。各地工业和信息化主管部门负责指导和推动辖区内工业数据分类分级工作。有关行业、领域主管部门可参考本指南，指导和推动本行业、本领域工业数据分类分级工作。工业企业、平台企业等企业承担工业数据管理的主体责任，要建立健全相关管理制度，实施工业数据分类分级管理并开展年度复查，并在企业系统、业务等发生重大变更时应及时更新分类分级结果。有条件的企业可结合实际设立数据管理机构，配备专职人员。

3、 澳大利亚修订《电信（拦截和接入）法案》 以推进与美国未来的双边协议

3 月 8 日，“E 安全”网站消息，基于美国《澄清域外合法使用数据法》（《云法案》），澳大利亚联邦政府 3 月 5 日提出修订《电信（拦截和接入）法案》。此次修订将建立一个新的框架，允许协议国出于执法目的，互相跨境访问通信数据。《云法案》是由美国政府在 2019 年颁布，最初旨在解决海外数据访问争议，迫使美国的科技公司交出海外数据。而基于此法案签订的双边协议，旨在改善执法。一旦这些协议生效，每个参与国的执法部门和国家安全机构将能够直接发布命令，要求其他国家管辖范围内的通信和技术

公司提供数据，将大大缩短执法过程中关键通信数据的获取时间。

4、 全球约 10 亿台 Android 设备不再获得更新 将使其面临更大的安全风险

3 月 9 日，“开源中国”网站消息，据统计，40%的 Android 设备不再从谷歌接收到重要的安全更新，这将使它们面临更大的恶意软件或其他安全漏洞风险。根据谷歌 2019 年公布的数据，全球约 40%的 Android 活跃用户使用的是 6.0 或更早版本，而根据《Android 安全公告》中的政策，2019 年未发布针对 7.0 以下版本的 Android 系统的安全补丁。谷歌表示，他们一直在致力于提升 Android 设备的安全性。不过交付操作系统安全更新的时间取决于设备、制造商和移动运营商，智能手机制造商会对 Android 操作系统的某些部分进行定制。重要的是，对于应该为智能设备提供多长时间的更新，一旦不再提供安全更新，客户如何获得其他选择的相关信息等此类问题，应该具有更大的透明度。

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 与 76 个国家和地区的 233 个组织建立了“CNCERT 国际合作伙伴”关系。

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：贾子骁

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315