国家互联网应急中心

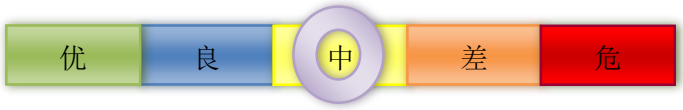
网络安全信息与动态周报

2020 年第 17 期

4 月 20 日-4 月 26 日

CNCERT/CC

本周网络安全基本态势

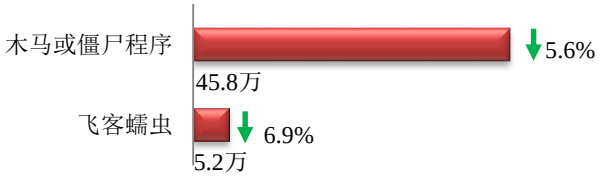


境内感染网络病毒的主机数量	•51.0万	↓ 17.1%
境内被篡改网站总数 其中政府网站数量	•4265 •23	↓ 44.7% ↓ 20.7%
境内被植入后门网站总数 其中政府网站数量	•1138 •1	↓ 22.4% ↓ 88.9%
针对境内网站的仿冒页面数量	•227	↑ 15.2%
新增信息安全漏洞数量 其中高危漏洞数量	•533 •253	↑ 27.2% ↑ 24.0%

= 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

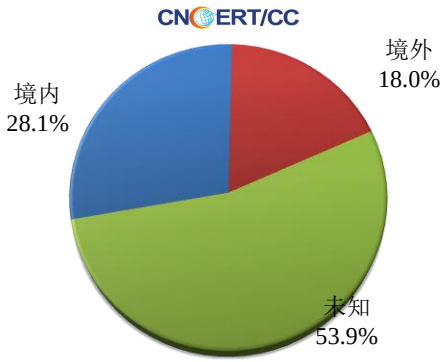
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 51.0 万个，其中包括境内被木马或被僵尸程序控制的主机约 45.8 万以及境内感染飞客（conficker）蠕虫的主机约 5.2 万。

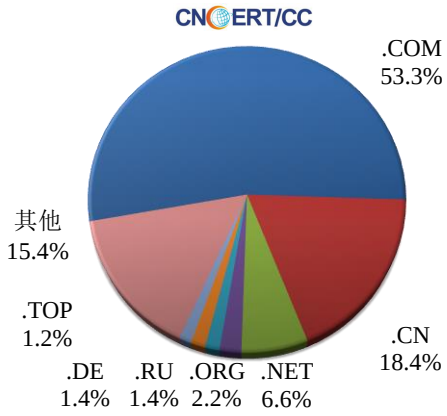


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 835 个，涉及 IP 地址 3931 个。在 835 个域名中，有 18.0%为境外注册，且顶级域为.com 的约占 53.3%；在 3931 个 IP 中，有约 57.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 272 个 IP。

本周放马站点域名注册所属境内外分布
(4/20-4/26)



本周放马站点域名所属顶级域的分布
(4/20-4/26)



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。

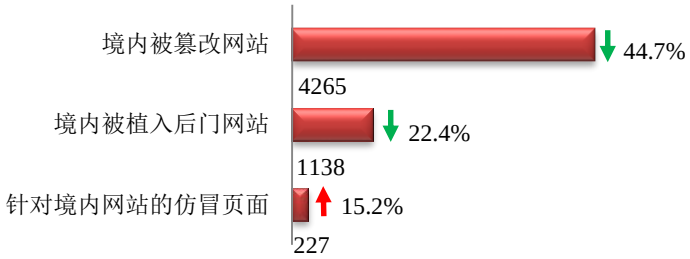
ANVA恶意地址黑名单发布地址

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。

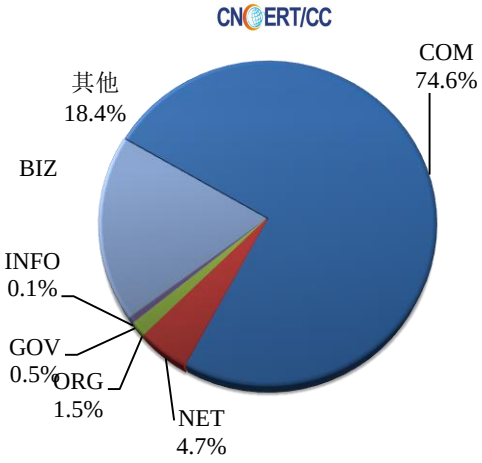
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 4265 个；被植入后门的网站数量为 1138 个；针对境内网站的仿冒页面数量 227 个。

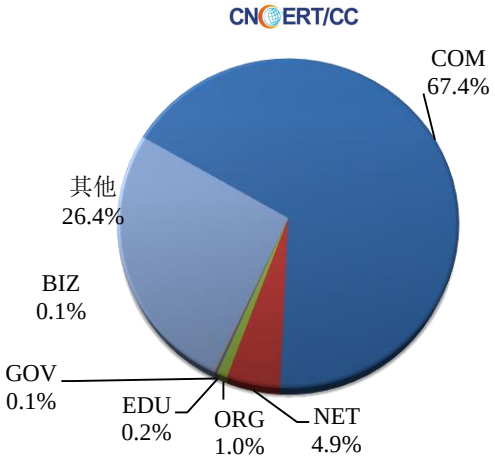


本周境内被篡改政府网站（GOV 类）数量为 23 个（约占境内 0.5%），较上周下降了 20.7%；境内被植入后门的政府网站（GOV 类）数量为 1 个（约占境内 0.1%），较上周下降了 88.9%。

本周我国境内篡改网站按类型分布
(4/20-4/26)

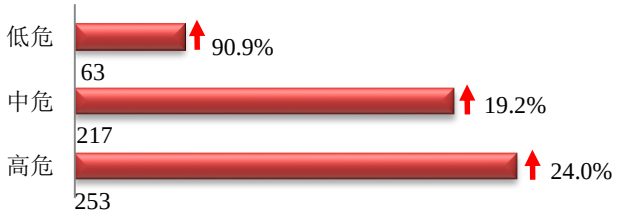


本周我国境内被植入后门网站按类型分类
(4/20-4/26)

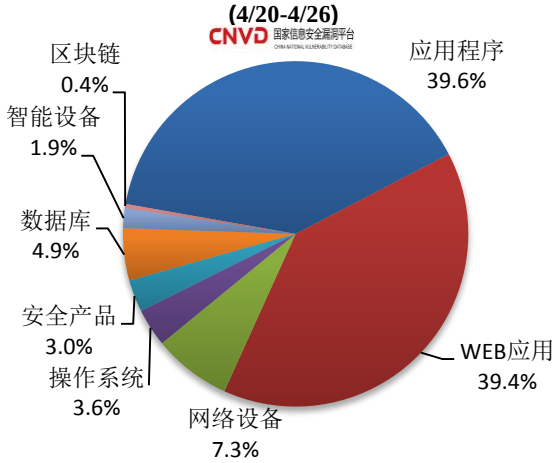


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 533 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
(4/20-4/26)



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

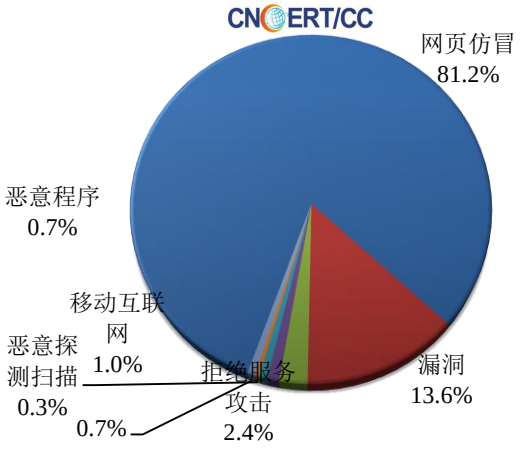
http://www.cnvd.org.cn/webinfo/list?type=4

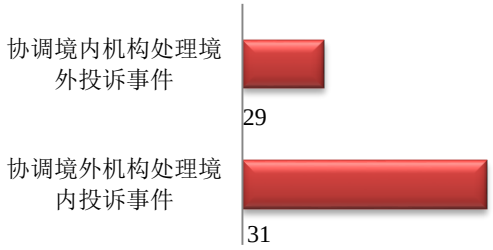
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 287 起，其中跨境网络安全事件 60 起。

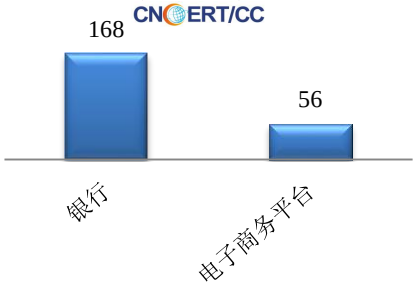
本周CNCERT 处理的事件数量按类型分布 (4/20-4/26)



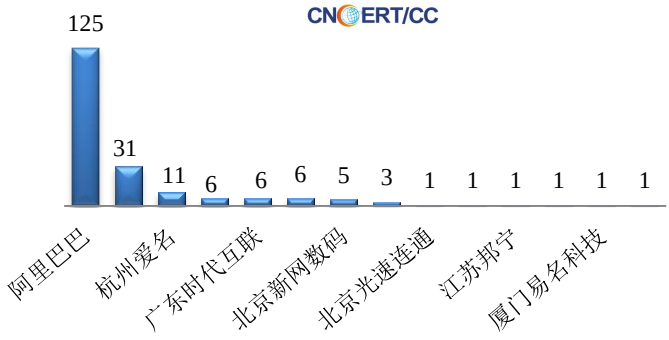


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 231 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包括银行仿冒事件 168 起和电子商务平台 56 起。

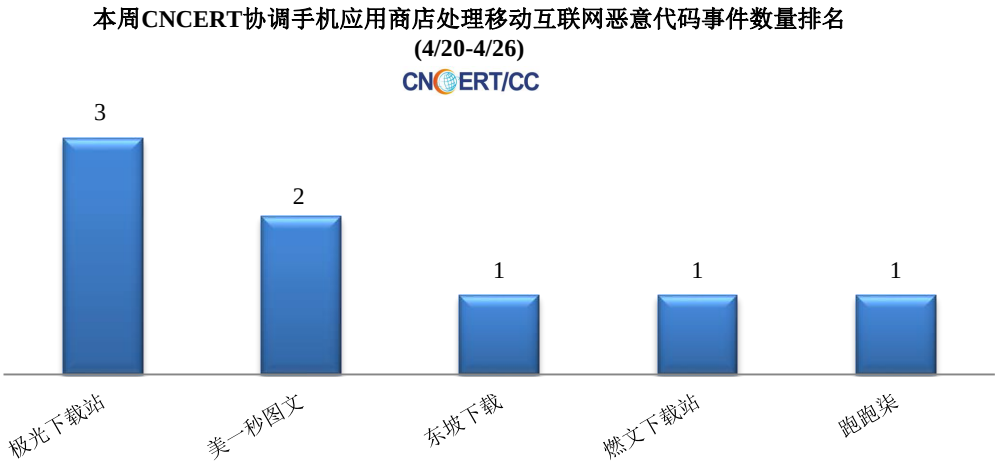
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (4/20-4/26)



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 (4/20-4/26)



本周，CNCERT 协调 5 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 8 个。



业界新闻速递

1、 国家互联网信息办公室关于发布第三批境内区块链信息服务备案编号的公告

2019 年 2 月 15 日《区块链信息服务管理规定》（以下简称《管理规定》）正式实施以来，国家互联网信息办公室依法依规组织开展备案审核工作，已发布 2 批次共 506 个境内区块链信息服务名称及备案编号，现发布第三批共 224 个境内区块链信息服务名称及备案编号。根据《管理规定》要求，区块链信息服务提供者应当在其对外提供服务的互联网站、应用程序等显著位置标明其备案编号。备案仅是对主体区块链信息服务相关情况的登记，不代表对其机构、产品和服务的认可，任何机构和个人不得用于任何商业目的。网信部门后续将会同各有关部门，依据《管理规定》对备案主体进行监督检查，并督促未备案主体尽快履行备案义务。

2、 CNCERT 发布《2019 年我国互联网网络安全态势综述》报告

4 月 20 日，国家互联网应急中心（CNCERT）编写的《2019 年我国互联网网络安全态势综述》报告（以下简称“2019 年态势报告”）正式发布。为全面反映当前我国网络安全的整体态势，CNCERT 自 2010 年以来，每年及时发布前一年度网络安全态势情况综述，至今已连续发布 11 年，对我国党政机关、行业企业及全社会了解我国网络安全形势，提高网络安全意识，做好网络安全工作提供了有力参考。

2019 年态势报告立足于 CNCERT 网络安全宏观监测数据与工作实践，报告涉及 2019 年典型网络安全事件、网络安全新趋势及日常网络安全事件应急处置实践等内容。报告

主要分为四个部分：一是总结 2019 年我国互联网网络安全状况，二是预测 2020 年网络安全热点，三是结合网络安全态势分析提出对策建议，四是梳理网络安全监测数据。

3、 脸谱网与美国联邦贸易委员会就剑桥分析事件和解 认罚 50 亿美元创记录

4 月 24 日，综合多家网站消息，脸谱网（Facebook）4 月 23 日发文称，其与美国联邦贸易委员会（FTC）于 2019 年 7 月就剑桥分析事件达成的和解协议获得了联邦法院的批准。按照该协议，脸谱网将向 FTC 缴纳 50 亿美元（约合人民币 354 亿元）的罚款，刷新了单个公司因侵犯消费者隐私而被处罚款的最高金额纪录，并且比之前的纪录高出近 20 倍。FTC 主席乔伊•西蒙斯透露，法院要求脸谱网在其运营的每个阶段都要考虑到隐私问题，并为其高管和隐私权相关的决定提供更多的透明度和问责制。

4、 WHO 称近期网络诈骗急剧增加并呼吁保持警惕

4 月 23 日，“世界卫生组织（WHO）官网”消息，WHO 发现，新型冠状病毒肺炎（COVID-19）大流行以来，针对其员工的网络攻击和针对公众的电子邮件诈骗急剧增加。目前的网络攻击数量是去年同期针对该组织的攻击数量的 5 倍多。本周，大约 450 封 WHO 电子邮件地址和密码被泄露到网上，同时泄露的还有数千名参与 COVID-19 应对工作人员的信息。WHO 称，这次攻击影响了一个旧的外部系统，该系统由现役和退休人员以及合作伙伴使用。据悉，在电子邮件中冒充 WHO 的骗子越来越多地将目标对准了公众，以诱骗公众捐款到其虚拟基金。WHO 正在将受影响的系统迁移到更安全的身份验证系统。同时，WHO 与私营部门合作，以建立更健全的内部系统并加强安全措施，并就网络安全风险对工作人员进行教育。WHO 要求公众对欺诈性电子邮件保持警惕，并建议使用可靠来源获取关于 COVID-19 和其他健康问题的真实信息。

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：周彧

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315