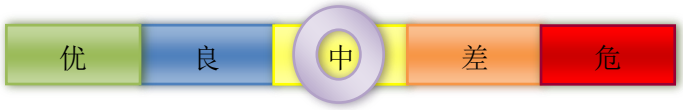
国家互联网应急中心

网络安全信息与动态周报

2020 年第 7 期
2 月 10 日-2 月 16 日

CNCERT/CC

本周网络安全基本态势

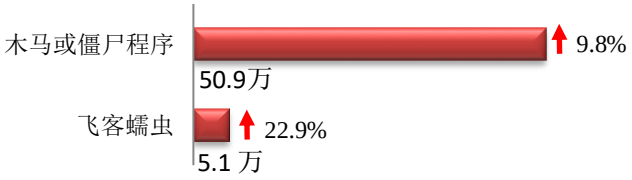


境内感染网络病毒的主机数量	•56.0万	↑ 10.9%
境内被篡改网站总数 其中政府网站数量	•3363 •11	↑ 158.9% ↑ 175.0%
境内被植入后门网站总数 其中政府网站数量	•1591 •4	↑ 14.1% =
针对境内网站的仿冒页面数量	•720	↓ 40.2%
新增信息安全漏洞数量 其中高危漏洞数量	•609 •247	↑ 6.3% ↑ 17.1%

= 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 56.0 万个，其中包括境内被木马或被僵尸程序控制的主机约 50.9 万以及境内感染飞客（conficker）蠕虫的主机约 5.1 万。



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。

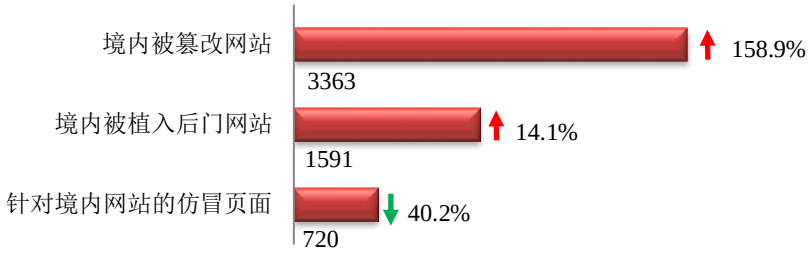
ANVA恶意地址黑名单发布地址

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。

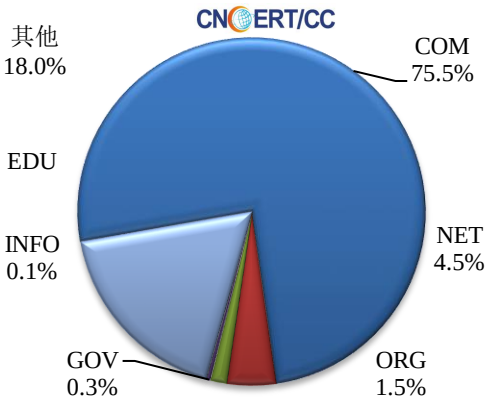
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 3363 个；被植入后门的网站数量为 1591 个；针对境内网站的仿冒页面数量 720 个。

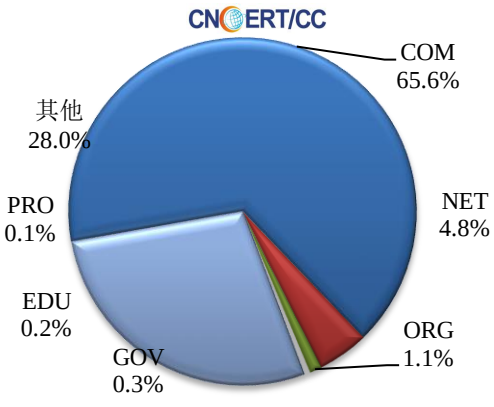


本周境内被篡改政府网站（GOV 类）数量为 11 个（约占境内 0.3%），较上周上涨了 175.0%；境内被植入后门的政府网站（GOV 类）数量为 4 个（约占境内 0.3%），与上周持平。

本周我国境内篡改网站按类型分布
(2/10-2/16)

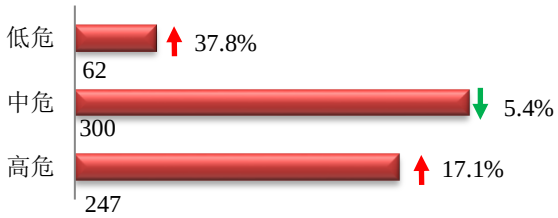


本周我国境内被植入后门网站按类型分布
(2/10-2/16)

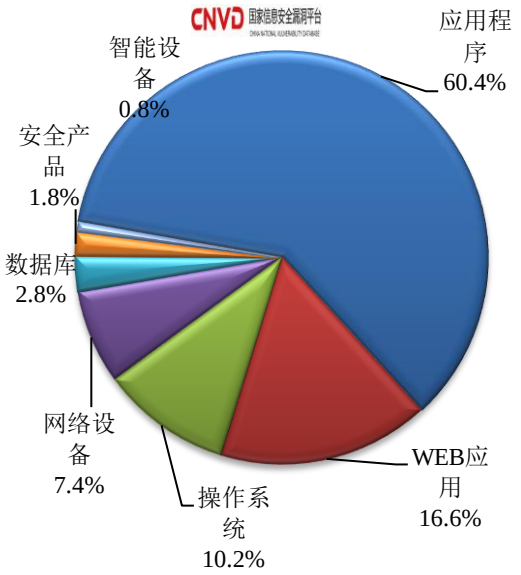


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 609 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
(2/10-2/16)



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。

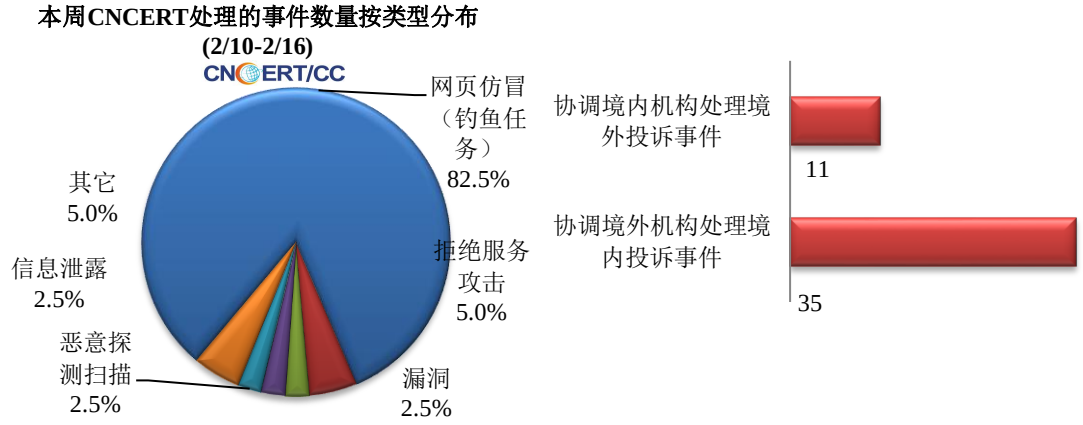
CNVD漏洞周报发布地址

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

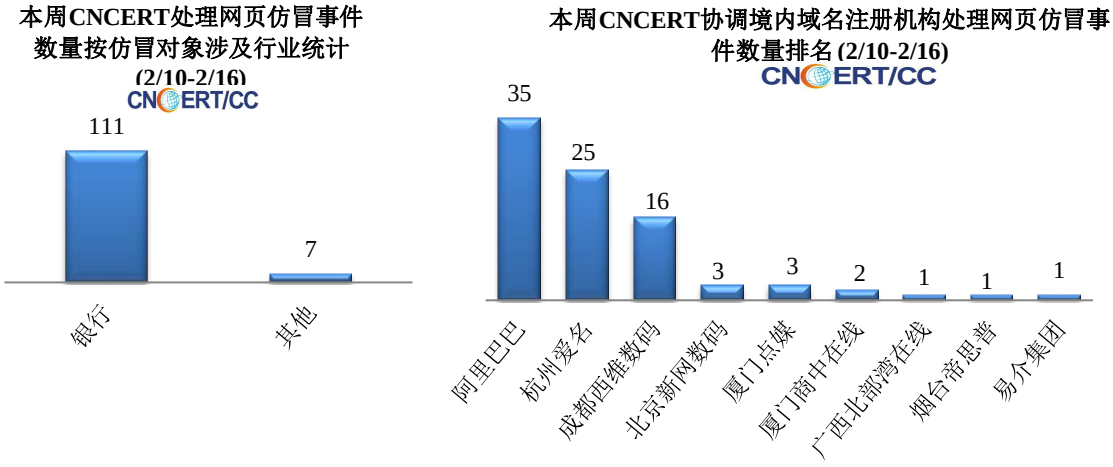
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 173 起，其中跨境网络安全事件 46 起。

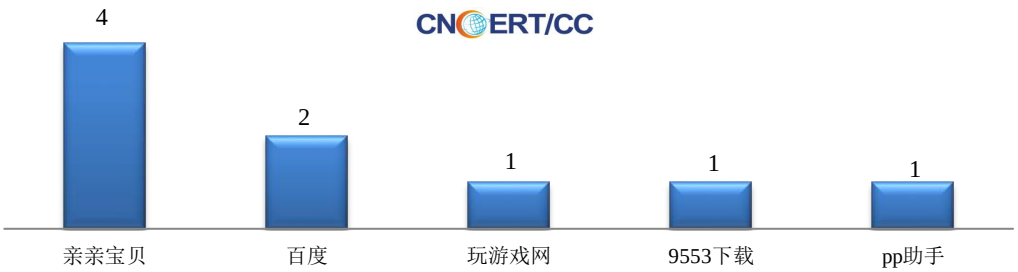


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 118 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包括银行仿冒事件 111 起和其他事件 7 起。



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 9 个。

本周CNCERT协调手机应用商店处理移动互联网恶意代码事件数量排名
(2/10-2/16)



业界新闻速递

1、 国务院办公厅印发《国家政务信息化项目建设管理办法》

近日，国务院办公厅印发《国家政务信息化项目建设管理办法》（以下简称《办法》），对国家政务信息系统的规划、审批、建设、共享和监管作出规定。

《办法》指出，要规范国家政务信息化建设管理，推动政务信息系统跨部门跨层级互联互通、信息共享和业务协同，强化系统应用绩效考核。国家政务信息系统主要包括：国务院有关部门和单位负责实施的国家统一电子政务网络平台、国家重点业务信息系统、国家信息资源库、国家信息安全基础设施、国家电子政务基础设施（数据中心、机房等）、国家电子政务标准化体系以及相关支撑体系等符合《政务信息系统定义和范围》规定的系统。

《办法》提出，加强国家政务信息化项目建设投资和运行维护经费协同联动，对于未按要求共享数据资源、未纳入国家政务信息系统总目录、不符合密码应用和网络安全要求等情况的政务信息系统，不安排运行维护经费。有关部门要建立国家政务信息化建设管理的协商机制，做好统筹协调，开展督促检查和评估评价，推广经验成果，形成工作合力。

2、 奥运会、国际奥委会推特账号被黑 账号已被暂时锁定

2 月 15 日，推特公司称，奥运会官方推特账号和国际奥委会（IOC）媒体事务的推特账号被黑客入侵，目前已被暂时锁定。推特公司的发言人在一封电子邮件声明中说，这些账号是通过第三方平台被黑的。针对此事，国际奥委会发言人表示正在调查此违规行为。此外，推特公司还提到，西班牙足球俱乐部巴塞罗那俱乐部的账号也面临类似的情况。“巴塞罗那足球俱乐部将进行网络安全审核，并将审查所有协议以及与第三方工具的链接，以避免再次发生此类事件。”在遭黑客攻击后，巴塞罗那俱乐部在一条推文中说道。

3、 640 万以色列选民数据遭泄露 政府选举应用中发现严重漏洞

2 月 10 日，据外媒报道，由以色列总理内塔尼亚胡领导的利库德集团(Likud)开发的选举应用程序 Elector 配置中的错误可能潜在地暴露并损害了近 650 万以色列公民的个人资料。该数据库包含 64.5 万余名以色列公民的个人详细资料，包括姓名、电话号码、身份证号码、家庭住址、性别、年龄和政治偏好，这些人都有资格在即将举行的选举中投票。据悉，该应用程序的开发人员暴露了 API 端点，同时由于没有使用两因素身份验证机制保护管理员帐户造成了此次泄露。目前，Electoral 应用程序的官方网站已被关闭，并已从 Google 和 Bing 等搜索引擎的缓存中删除，以防止进一步访问该网站的源代码和 admin API 端点。

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：王适文

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315