国家互联网应急中心

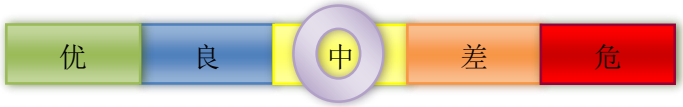
网络安全信息与动态周报

2020 年第 8 期

2 月 17 日-2 月 23 日

CNCERT/CC

本周网络安全基本态势

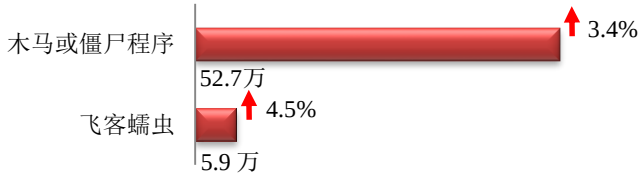


境内感染网络病毒的主机数量	•58.6万	↑ 4.5%
境内被篡改网站总数 其中政府网站数量	•9636 •46	↑ 186.5% ↑ 318.2%
境内被植入后门网站总数 其中政府网站数量	•1746 •7	↑ 9.7% ↑ 75.0%
针对境内网站的仿冒页面数量	•740	↑ 2.8%
新增信息安全漏洞数量 其中高危漏洞数量	•514 •200	↓ 15.6% ↓ 19.0%

= 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 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 52.7 万以及境内感染飞客（conficker）蠕虫的主机约 5.9 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。

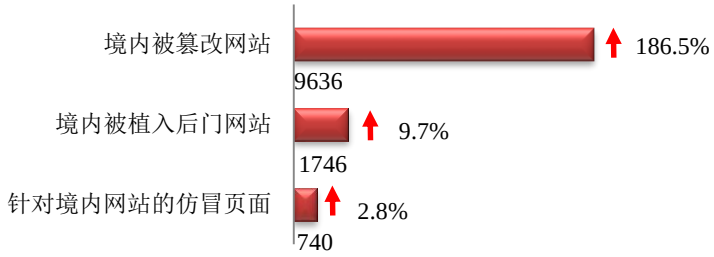
ANVA恶意地址黑名单发布地址

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。

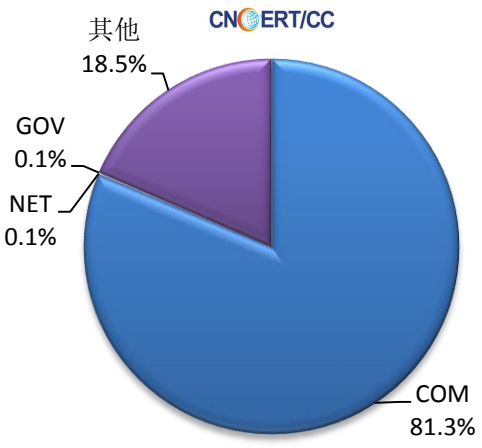
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 9636 个；被植入后门的网站数量为 1746 个；针对境内网站的仿冒页面数量 740 个。

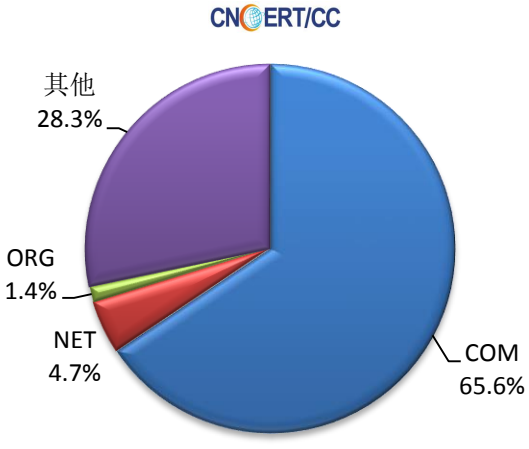


本周境内被篡改政府网站（GOV 类）数量为 46 个（约占境内 0.3%），较上周上涨了 175.0%；境内被植入后门的政府网站（GOV 类）数量为 7 个（约占境内 0.3%），较上周上涨了 75.0%。

本周我国境内篡改网站按类型分布
(2/17-2/23)

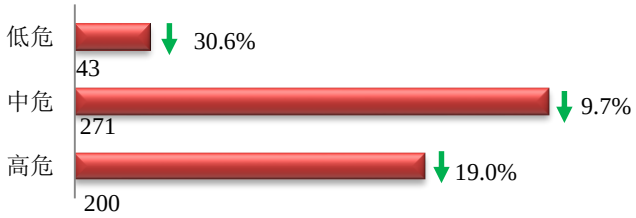


本周我国境内被植入后门网站按类型分布
(2/17-2/23)

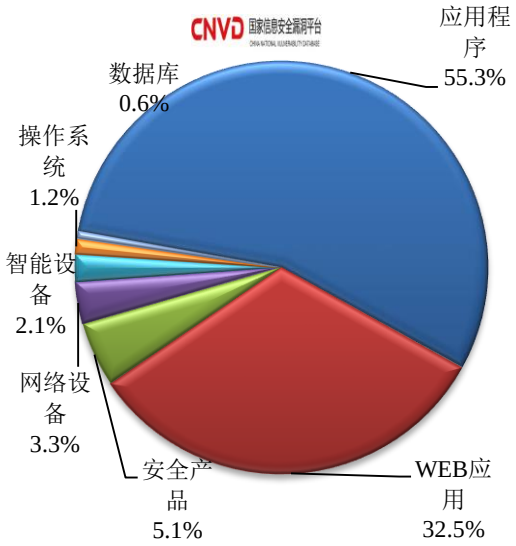


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 514 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
(2/17-2/23)



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 应用和安全产品。

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

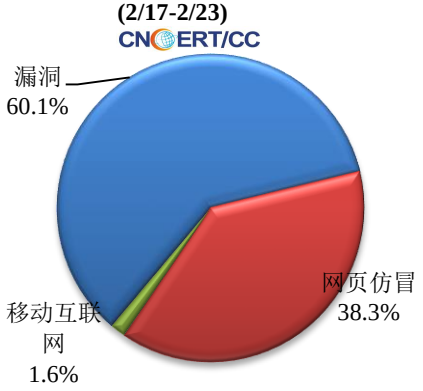
http://www.cnvd.org.cn/webinfo/list?type=4

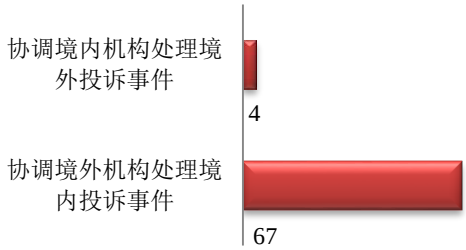
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 381 起，其中跨境网络安全事件 71 起。

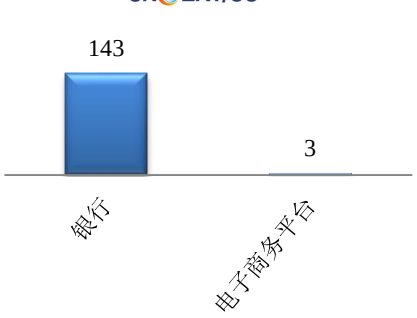
本周CNCERT处理的事件数量按类型分布
(2/17-2/23)



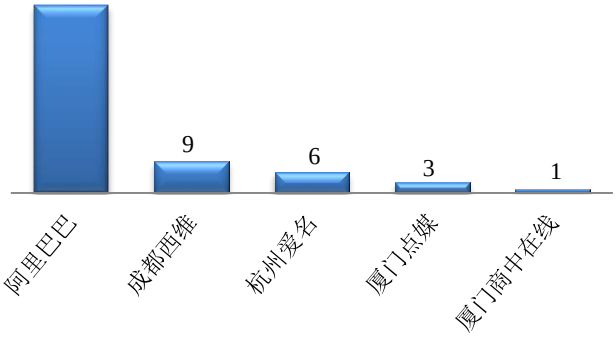


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 146 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包括银行仿冒事件 143 起和其他事件 3 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计
(2/17-2/23)

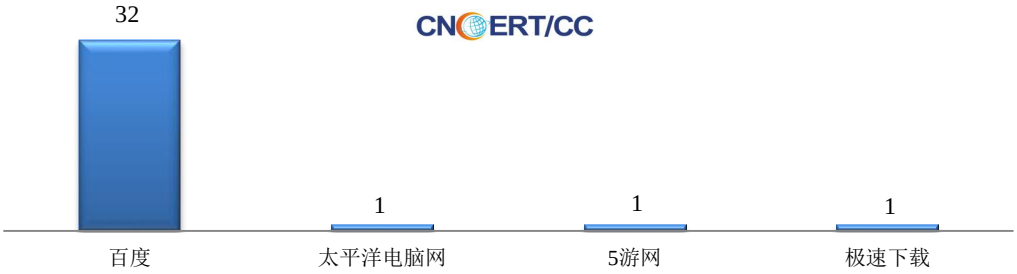


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (2/17-2/23)



本周，CNCERT 协调 4 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 35 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
(2/17-2/23)



业界新闻速递

1、 中国人民银行发布 2020 版《网上银行系统信息安全通用规范》

近日，2020 年 2 月，中国人民银行下发《关于<网上银行系统信息安全通用规范>行业标准的通知》（银发[2020]35 号），对新版《网上银行系统信息安全通用规范》(JR/T 0068-2020)（以下简称“新版规范”）进行了正式发布。新版规范是 2012 版的《网上银行系统信息安全通用规范》(JR/T 0068-2012)的替换修订版本。

新版规范有三个重点修订内容：即针对新技术出现和应用提出了新的安全要求、就新的业务和监管要求进行了补充和明确以及重新梳理并提升关于业务连续性与灾难恢复、安全事件与应急响应的安全要求。在新版规范中，业务连续性与灾难恢复、安全事件与应急响分别单独成节，作为安全管理规范的一部分，提升了相关安全要求，对网上银行业务影响分析、制定备份策略、建立备份恢复程序、实施应用级备份等规定进行了详细的梳理和规定。

2、 WordPress 主题插件严重漏洞修复 影响将近 20 万个网站

2 月 18 日，“FREEBUF”网站消息，WordPress 的 ThemeGrill Demo Importer 程序用于轻松导入 ThemeGrill 主题演示内容、小工具和设置，使他们更轻松地快速自定义主题，最近爆出存在漏洞。该漏洞存在于 ThemeGrill Demo Importer 插件从 1.3.4 到 1.6.1

的版本中，攻击者利用该漏洞可以管理员身份登录，并将网站的整个数据库还原为默认状态，从而完全控制这些网站。目前，程序开发人员已更新了该插件，删除该严重漏洞。根据官方 WordPress 插件存储库的统计数据，最流行的版本是 1.4 到 1.6，占当前安装的 98%以上。该插件目前安装在近 200000 个 WordPress 网站上，而最流行的版本最容易受到攻击。WordPress 安全公司 WebARX 的研究人员提醒，快速自动登录的管理员账户也有一个前提条件，目标数据库有用户“admin”的存在。

3、 欧盟发布《欧洲数据战略》

2 月 19 日，美国“National Law Review”网站报道，欧盟委员会发布《欧洲数据战略》，希望通过立法、技术标准和公私合作等举措，创建更加宽松的数据经济发展环境，让欧盟成为数据领域未来的领导者。欧盟委员会（EC）希望制定共同的欧洲规则，以确保数据可以在欧盟内部实现跨部门流动；欧洲的规则和价值观得到充分尊重，尤其是在个人数据保护、消费者保护立法和竞争法中；数据访问和使用的规则公平、实用、明确，数据治理机制清晰可信；基于欧洲的价值观，对国际数据流采取开放而自信的处理方式。EC 的目标是创建一个真正的单一数据市场，对来自世界各地的数据开放，“企业可以轻松访问几乎无限量的高质量工业数据”。

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：饶毓

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315