

网络安全信息与动态周报

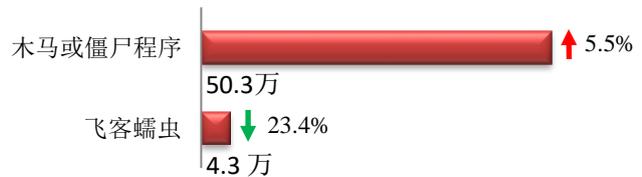
本周网络安全基本态势



= 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 54.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 50.3 万以及境内感染飞客（conficker）蠕虫的主机约 4.3 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。

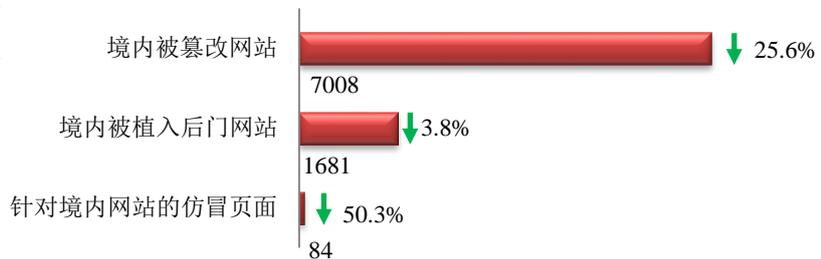
ANVA 恶意地址黑名单发布地址

<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。

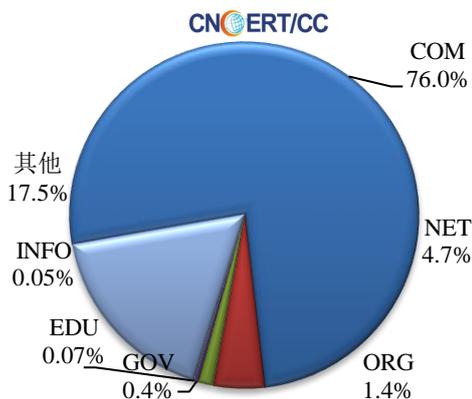
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 7008 个；被植入后门的网站数量为 1681 个；针对境内网站的仿冒页面数量 84 个。

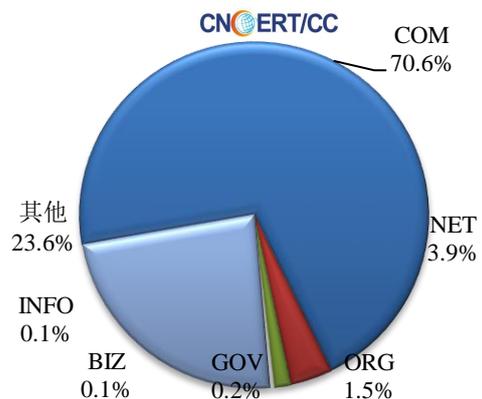


本周境内被篡改政府网站 (GOV 类) 数量为 28 个 (约占境内 0.4%)，较上周上涨了 16.7%；境内被植入后门的政府网站 (GOV 类) 数量为 4 个 (约占境内 0.2%)，较上周上涨了 300.0%。

本周我国境内篡改网站按类型分布 (1/27-2/2)

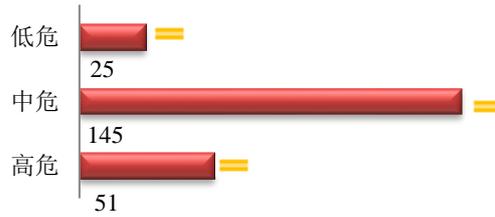


本周我国境内被植入后门网站按类型分布 (1/27-2/2)

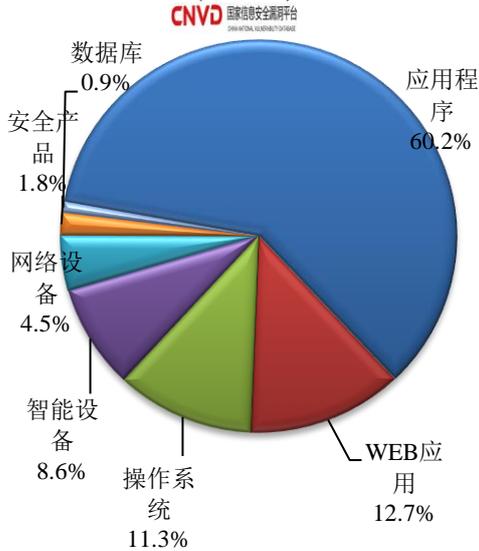


本周重要漏洞情况

本周,国家信息安全漏洞共享平台(CNVD)新收录网络安全漏洞 221 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类型分布
(1/27-2/2)



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。

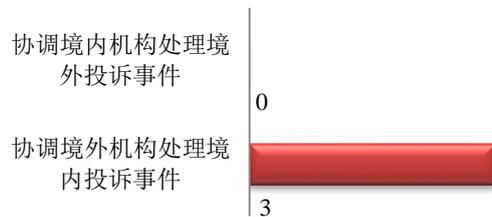
CNVD漏洞周报发布地址

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

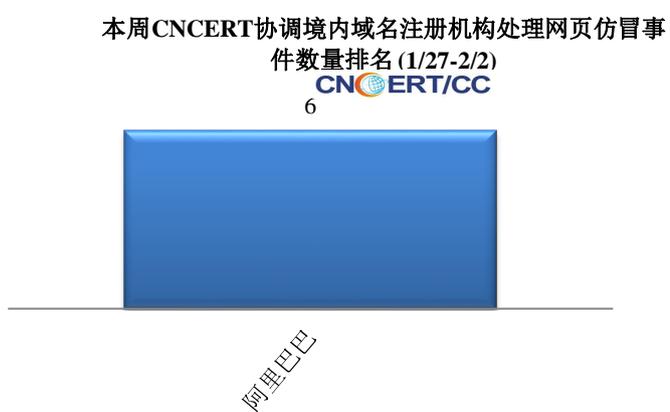
国家信息安全漏洞共享平台(缩写CNVD)是CNCERT联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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10起,其中跨境网络安全事件3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 10 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，均为银行仿冒事件。



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：何能强

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315