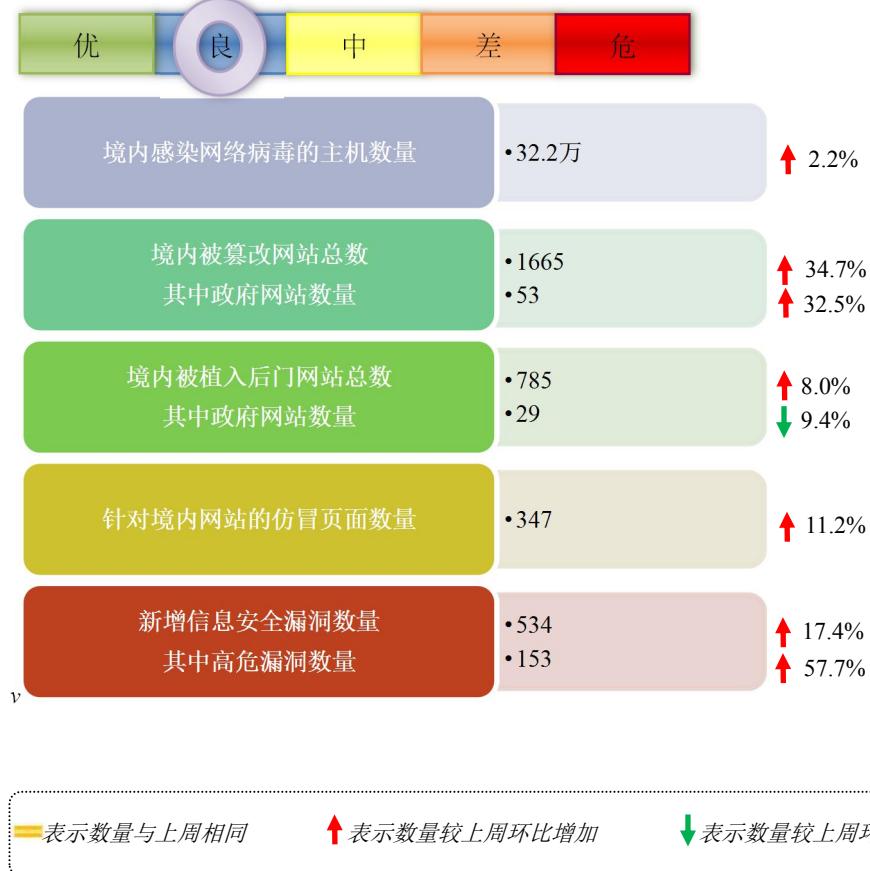


11月6日-11月12日网络安全基本态势

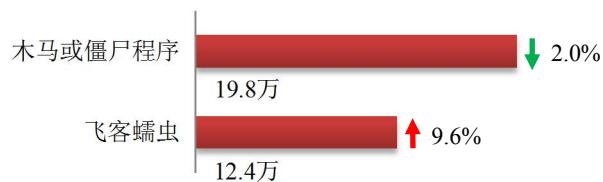
(信息来源：国家计算机网络应急技术处理协调中心)

本周网络安全基本态势



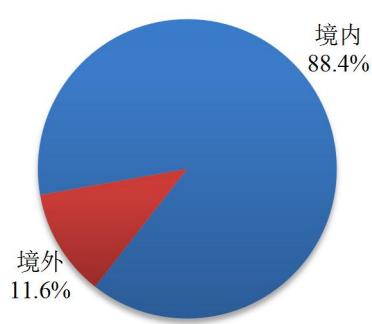
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 32.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 19.8 万以及境内感染飞客（conficker）蠕虫的主机约 12.4 万。

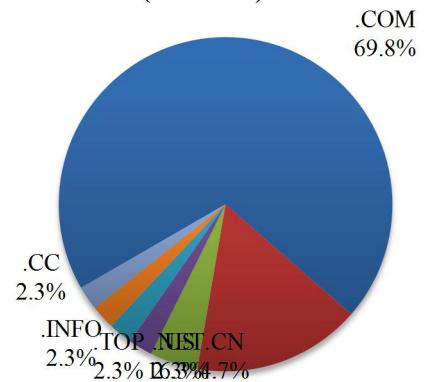


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 43 个，涉及 IP 地址 261 个。在 43 个域名中，有 11.6% 为境外注册，且顶级域为.com 的约占 69.8%；在 261 个 IP 中，有约 33.3% 位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 3 个 IP。

本周放马站点域名注册所属境内外分布
(11/6-11/12)



本周放马站点域名所属顶级域的分布
(11/6-11/12)



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。

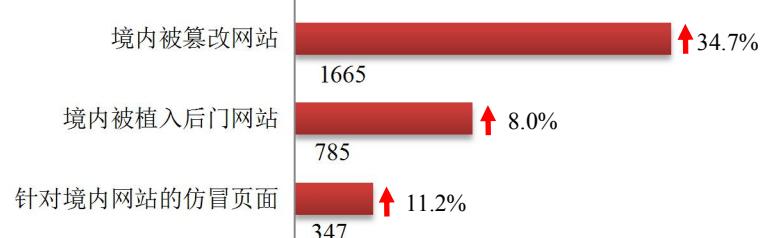
ANVA 恶意地址黑名单发布地址

<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。

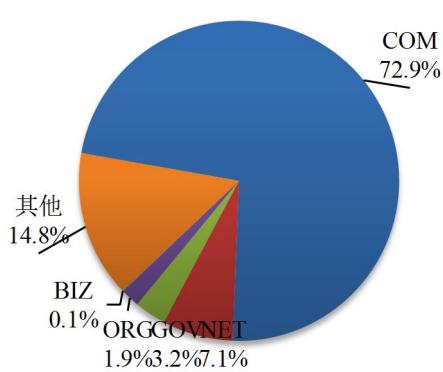
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1665 个；境内被植入后门的网站数量为 785 个；针对境内网站的仿冒页面数量为 347。

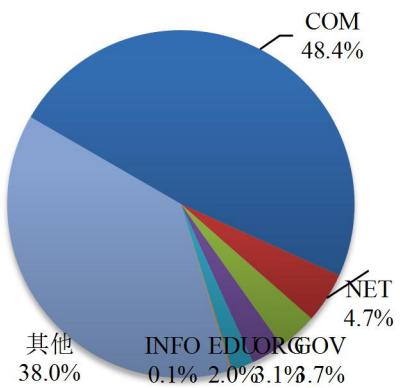


本周境内被篡改政府网站 (GOV 类) 数量为 53 个 (约占境内 3.2%)，较上周环比上升了 32.5%；境内被植入后门的政府网站 (GOV 类) 数量为 29 个 (约占境内 3.7%)，较上周环比下降了 9.4%；针对境内网站的仿冒页面涉及域名 280 个，IP 地址 124 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被篡改网站按类型分布
(11/6-11/12)

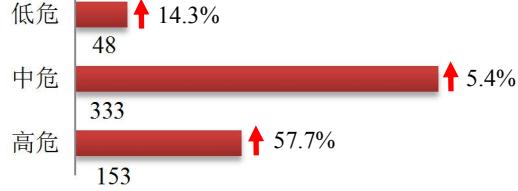


本周我国境内被植入后门网站按类型分布
(11/6-11/12)

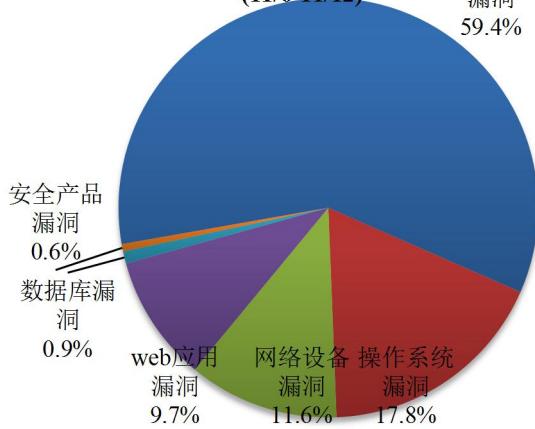


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 534 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
(11/6-11/12)



本周 CNVD 发布的网络安全漏洞中，
应用程序漏洞占比最高，其次是操作系统
漏洞和网络设备漏洞。

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

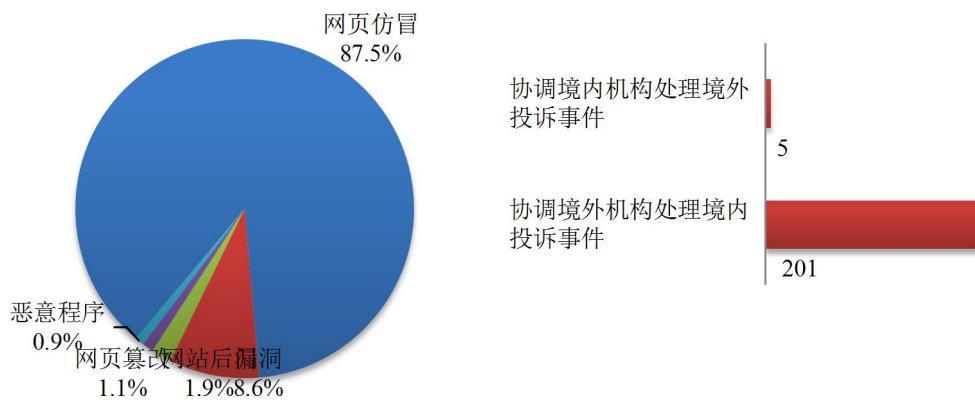
<http://www.cnvd.org.cn/webinfo/list?type=4>

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

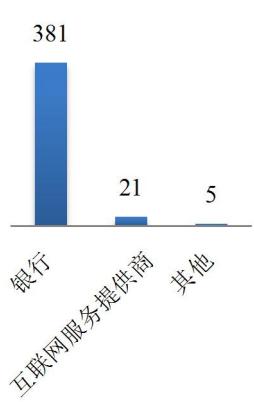
本周，CNCERT协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 465 起，其中跨境网络安全事件 206 起。

本周CNCERT处理的事件数量按类型分布
(11/6-11/12)

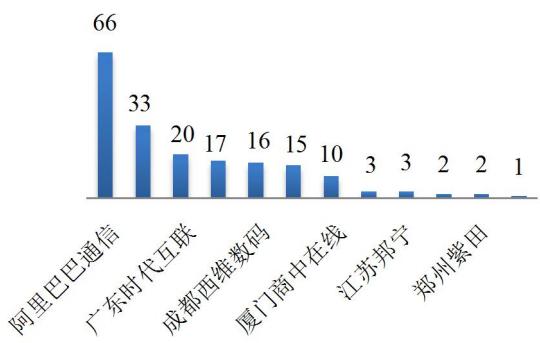


本周，CNCERT协调境内外域名注册机构、境外CERT等机构重点处理了407起网页假冒投诉事件。根据假冒对象涉及行业划分，主要包含银行假冒事件381起和互联网服务提供商假冒事件21起。

本周CNCERT处理网页仿冒事件数量
按仿冒对象涉及行业统计(11/6-11/12)



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 (11/6-11/12)



本周, CNCERT 协调 14 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
(11/6-11/12)

