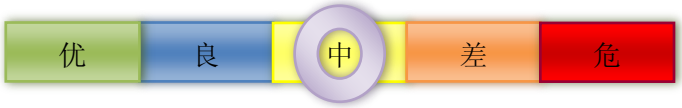
2016 年 5 月 16 日-5 月 22 日网络安全基本态势

（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

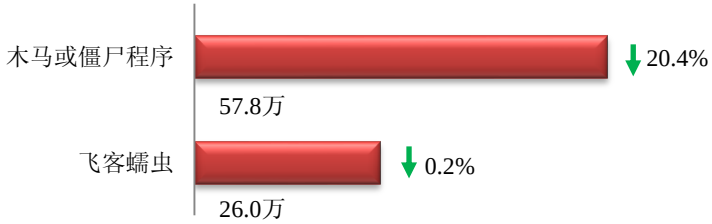


境内感染网络病毒的主机数量	•83.8万	↓15.0%
境内被篡改网站总数 其中政府网站数量	•3143 •76	↓6.0% ↓10.6%
境内被植入后门网站总数 其中政府网站数量	•8823 •230	↓37.3% ↓44.6%
针对境内网站的仿冒页面数量	•4861	↑75.9%
新增信息安全漏洞数量 其中高危漏洞数量	•219 •83	↓21.2% ↓25.9%

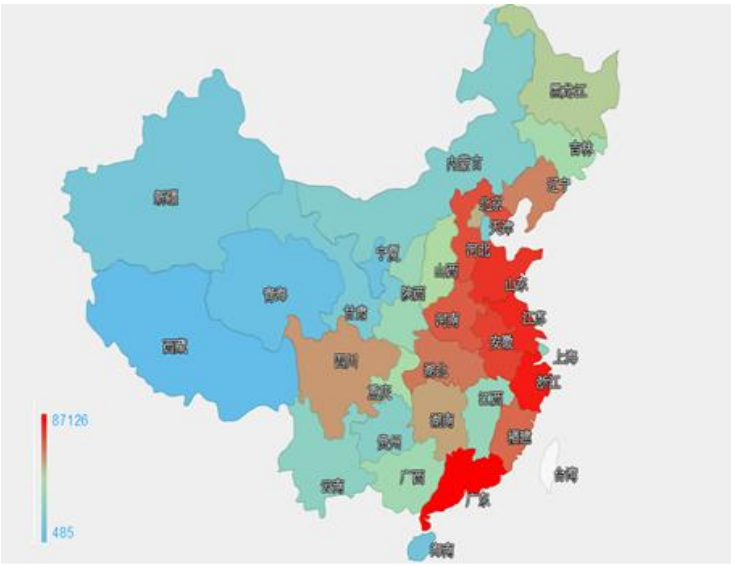
═表示数量与上周相同　↑表示数量较上周环比增加　↓表示数量较上周环比减少

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 83.8 万个，其中包括境内被木马或被僵尸程序控制的主机约 57.8 万以及境内感染飞客（conficker）蠕虫的主机约 26.0 万。

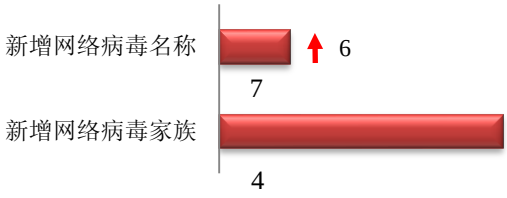


木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、浙江省和江苏省。



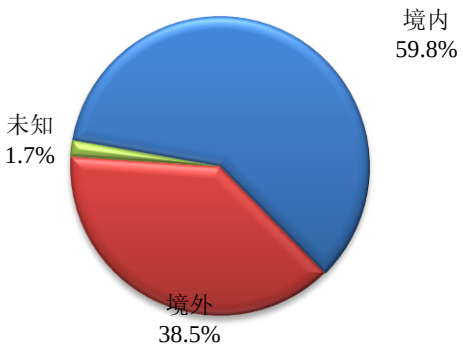
广东省	•约8.7万个（约占中国大陆总感染量的15.1%）
浙江省	•约8.4万个（约占中国大陆总感染量的14.6%）
江苏省	•约4.4万个（约占中国大陆总感染量的7.6%）

本周 CNCERT 捕获的新增网络病毒文件，按网络病毒名称统计新增 7 个，按网络病毒家族统计新增 4 个。

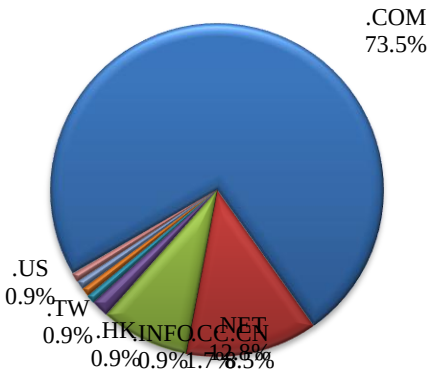


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 117 个，涉及 IP 地址 363 个。在 117 个域名中，有 38.5%为境外注册，且顶级域为.com 的约占 73.5%；在 363 个 IP 中，有约 94.2%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 26 个 IP。

本周放马站点域名注册所属境内外分布
(5/16-5/22)



本周放马站点域名所属顶级域的分布
(5/16-5/22)



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。

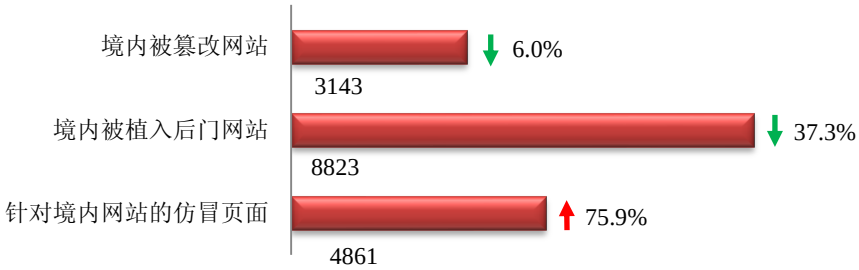
ANVA恶意地址黑名单发布地址

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。

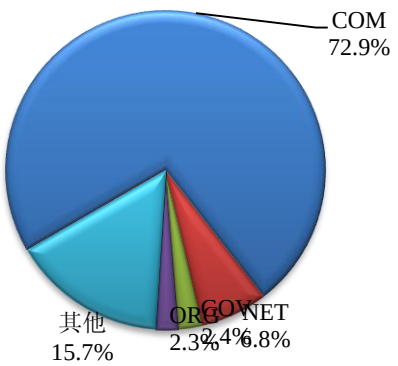
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 3143 个；境内被植入后门的网站数量为 8823 个；针对境内网站的仿冒页面数量为 4861。

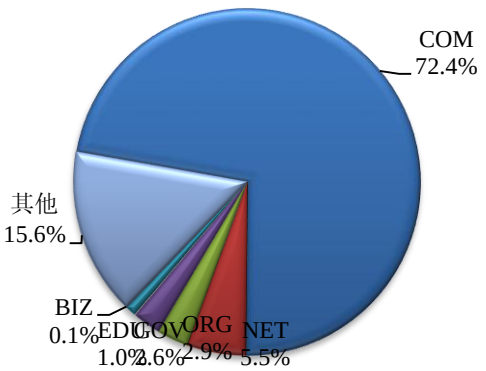


本周境内被篡改政府网站（GOV 类）数量为 76 个（约占境内 2.4%），较上周环比下降了 10.6%；境内被植入后门的政府网站（GOV 类）数量为 230 个（约占境内 2.6%），较上周环比下降了 44.6%；针对境内网站的仿冒页面涉及域名 1967 个，IP 地址 1289 个，平均每个 IP 地址承载了约 4 个仿冒页面。

本周我国境内被篡改网站按类型分布
(5/16-5/22)

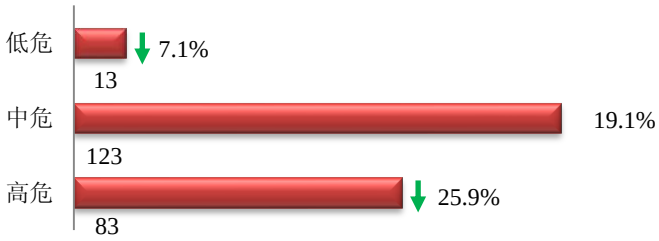


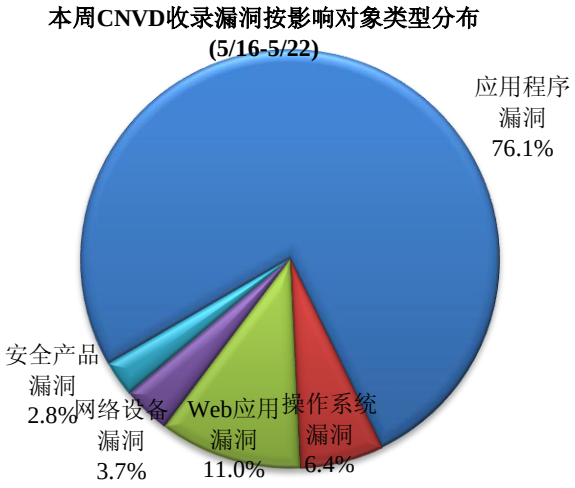
本周我国境内被植入后门网站按类型分布
(5/16-5/22)



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 219 个，信息安全漏洞威胁整体评价级别为中。





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 Web 应用漏洞。

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

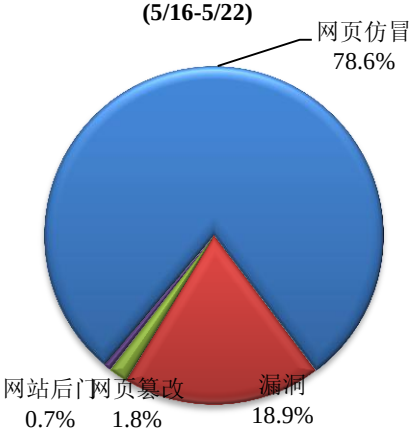
http://www.cnvd.org.cn/webinfo/list?type=4

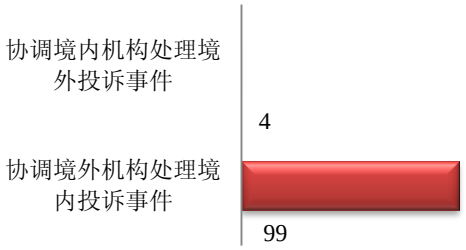
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 760 起，其中跨境网络安全事件 183 起。

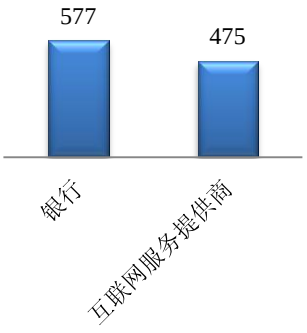
本周CNCERT处理的事件数量按类型分布
(5/16-5/22)



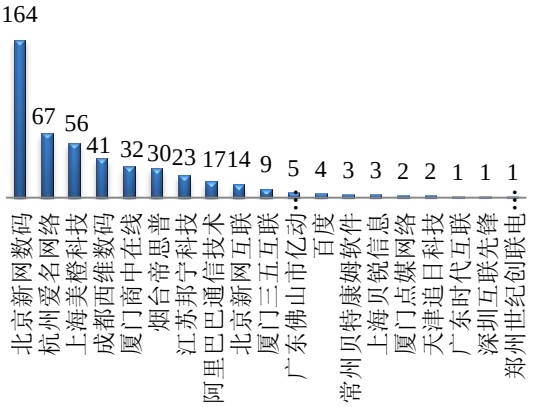


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1052 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事 577 起和互联网服务提供商仿冒事件 475 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(5/16-5/22)



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 (5/16-5/22)



本周，CNCERT 协调 21 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 155 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 (5/16-5/22)