

网络安全信息与动态周报

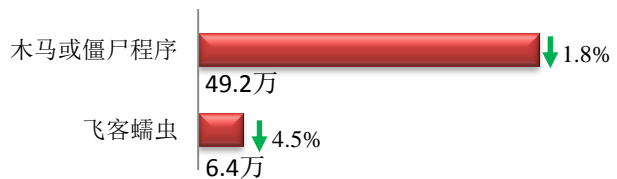
本周网络安全基本态势



—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

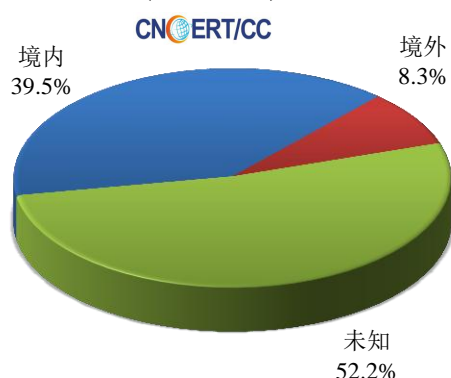
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 55.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 49.2 万以及境内感染飞客（conficker）蠕虫的主机约 6.4 万。

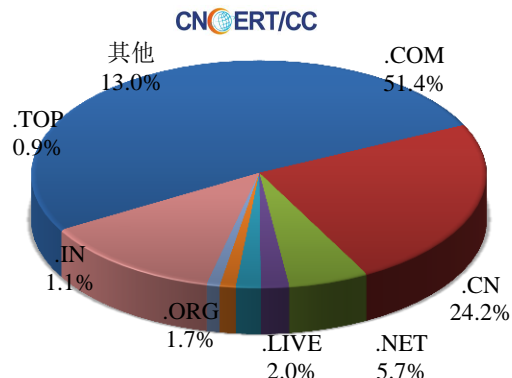


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 1604 个，涉及 IP 地址 2581 个。在 1604 个域名中，有 8.3% 为境外注册，且顶级域为 .com 的约占 51.4%；在 2581 个 IP 中，有约 11.4% 位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 298 个 IP。

本周放马站点域名注册所属境内外分布
(12/02-12/08)



本周放马站点域名所属顶级域的分布
(12/02-12/08)



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。

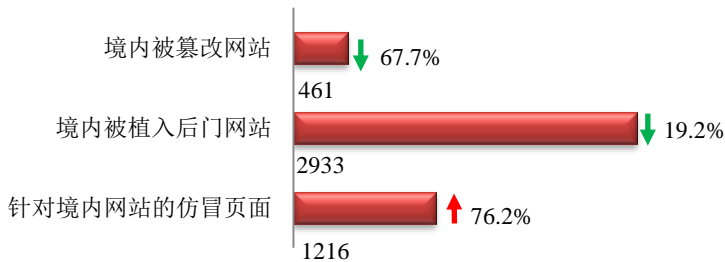
ANVA 恶意地址黑名单发布地址

<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。

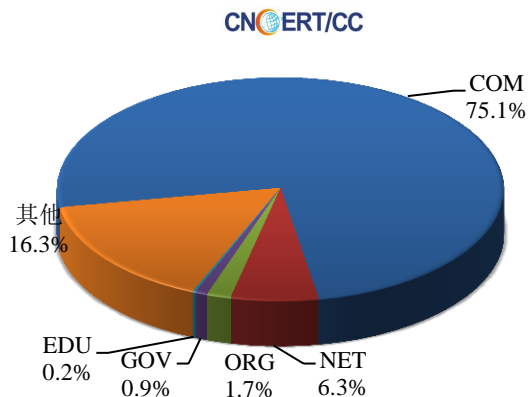
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 461 个；被植入后门的网站数量为 2933 个；针对境内网站的仿冒页面数量 1216 个。

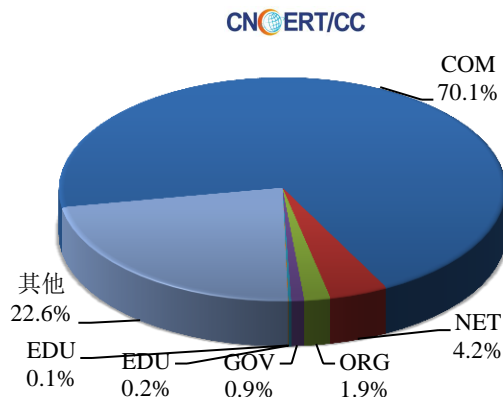


本周境内被篡改政府网站（GOV类）数量为4个（约占境内0.9%），较上周环比下降了20.0%；境内被植入后门的政府网站（GOV类）数量为27个（约占境内0.9%），较上周环比下降了27.0%。

本周我国境内篡改网站按类型分布
(12/02-12/08)



本周我国境内被植入后门网站按类型分布
(12/02-12/08)

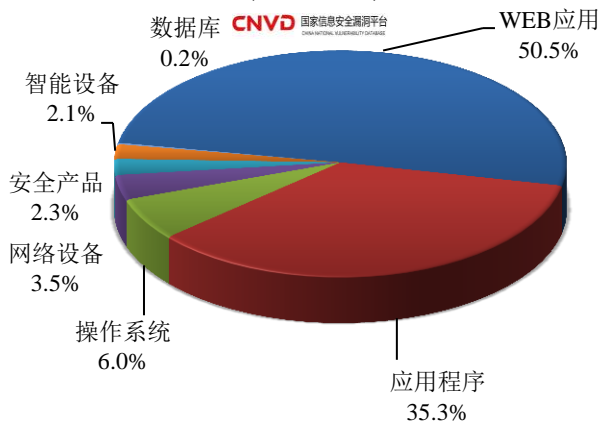


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞481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
(12/02-12/08)



本周CNVD发布的网络安全漏洞中，应用程序漏洞占比最高，其次是应用程序和操作系统。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

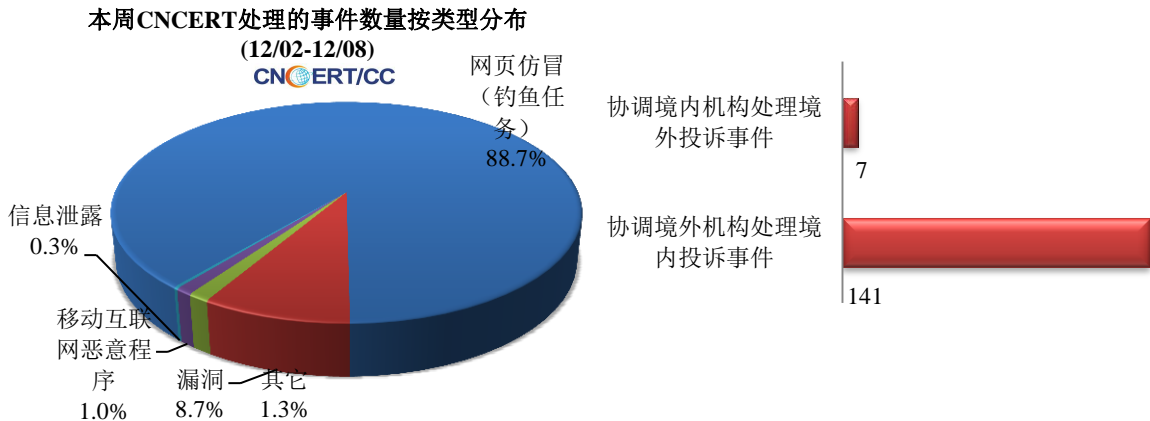
CNVD漏洞周报发布地址

<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。

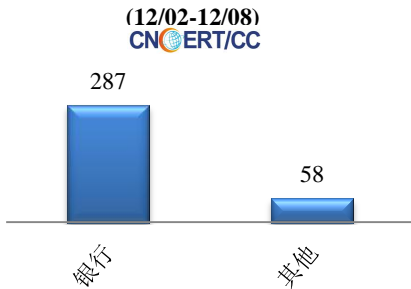
本周事件处理情况

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 389 起，其中跨境网络安全事件 148 起。

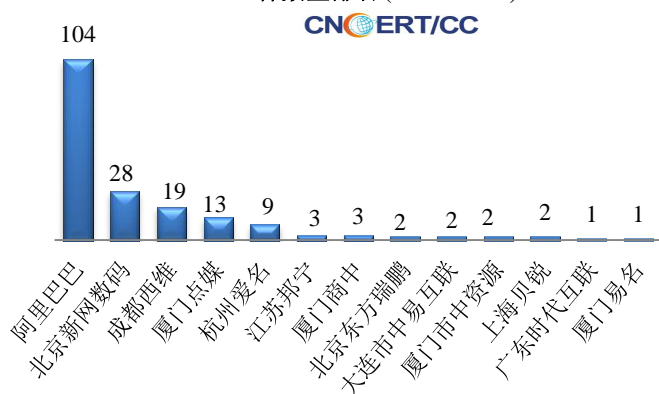


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 345 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包括银行仿冒事件 287 起和其他事件 58 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计

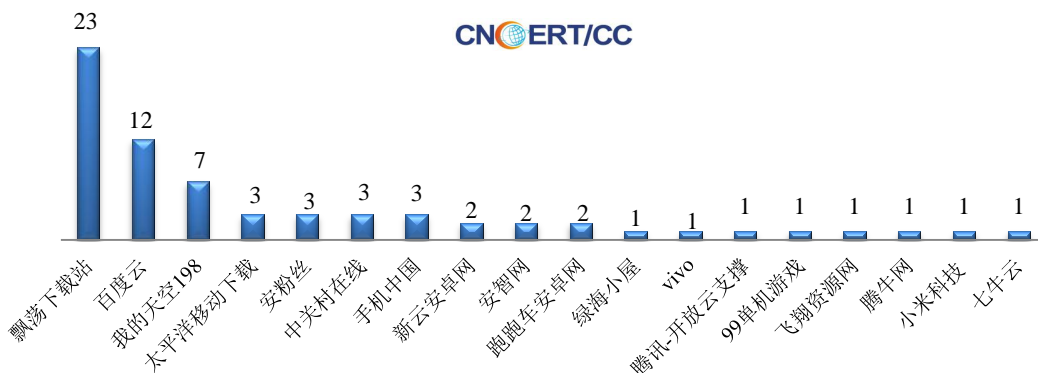


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (12/02-12/08)



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
(12/02-12/08)

本周，CNCERT 协调 18 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 68 个。



业界新闻速递

1、俄罗斯总统普京签署法案：在智能设备上强制安装俄应用程序

12月2日，据路透社报道，俄罗斯总统普京签署了一项法案，要求所有在俄罗斯销售的智能手机、电脑和智能电视都必须预装俄罗斯软件。据报道称，该法案将于2020年7月1日生效，主要用来帮助俄罗斯的信息技术公司与外国公司竞争，让消费者在购买新设备时不必下载软件。普京签署的这项法案规定，政府将列出需要安装在不同设备上的俄罗斯应用程序清单。

2、北约举行大规模网络军演

12月2日，据俄罗斯卫星网报道，爱沙尼亚国防部新闻部门发布消息称，北约大规模网络军演“网络联盟（Cyber Coalition）”于12月2日至6日在爱沙尼亚的“国防军事学院”基地举行，由北约协同网络防御卓越中心（CCDCOE）筹划实施。该报道援引爱军方消息称：“‘网络联盟’演习由29个北约国家中的27个成员、欧盟以及包括日本、阿尔及利亚、奥地利、芬兰、爱尔兰和瑞典在内的6个北约伙伴国参加。参演国家将派出约700名相关人员，其中包括网络安全专家、技术人员、军队、政府官员以及企业代表。”

3、印度内阁批准《个人数据保护法案》

12月5日，综合《印度时报》和《今日印度》网站消息，在12月4日印度总理莫迪主持的内阁会议上，印度内阁通过了《个人数据保护法案》。内阁批准后，该法案将提交议会进行审议。该法案主要涉及公共和私人实体处理个人数据的框架，包含有关个人数据适用范围，处罚和赔偿，行为守则和执行模式等要素。据悉，该法案由印度政府根据欧盟2018年推出的《一般数据保护条例》（GDPR）而制定，以规范政府和私营公司对个人数据的使用，由前最高法院法官 BN Srikrishna 领导的高级专家小组编写。

4、德国建立欧洲最大应用型网络安全研究中心

12月5日，新华社消息，德国弗劳恩霍夫协会4日发布新闻公报，网络安全是数字化成功的前提，也是在国际竞争中保持领先的重要条件。为此，该协会联手德国高校，建立了欧洲最大的应用型网络安全研究中心——国家应用型网络安全研究中心 ATHENE。据公报介绍，新研究中心由弗劳恩霍夫安全信息技术研究所、图像数据处理研究所，以及达姆施塔特工业大学、达姆施塔特应用科学大学联合建立。新研究中心官网显示，该中心将开展尖端研究，并采取灵活高效的运作模式，可在短时间内应对新挑战。

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 2018 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：姚力

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315