国家互联网应急中心

网络安全信息与动态周报

2020 年第 50 期

12 月 7 日-12 月 13 日

CNCERT/CC

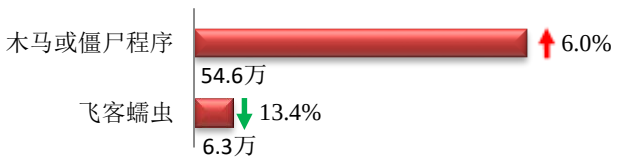
本周网络安全基本态势

境内感染网络病毒的主机数量	•60.9万	↑ 6.8%
境内被篡改网站总数 其中政府网站数量	•4078 •19	↓ 13.3% ↓ 34.5%
境内被植入后门网站总数 其中政府网站数量	•580 •2	↑ 4.3%
针对境内网站的仿冒页面数量	•13861	↓ 23.5%
新增信息安全漏洞数量 其中高危漏洞数量	•293 •142	↑ 10.2% ↑ 75.3%

= 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

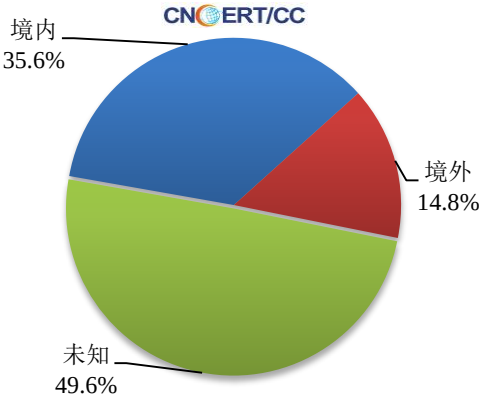
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 60.9 万个，其中包括境内被木马或被僵尸程序控制的主机约 54.6 万以及境内感染飞客（conficker）蠕虫的主机约 6.3 万。

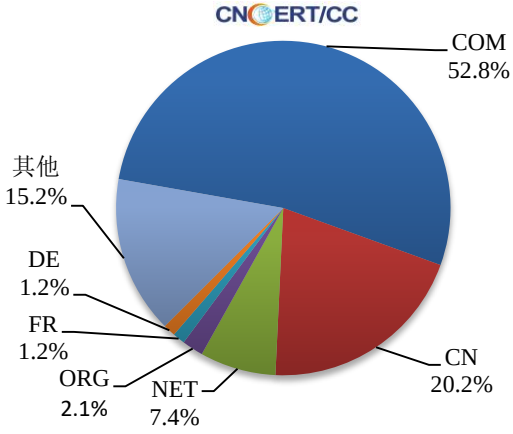


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 925 个，涉及 IP 地址 4588 个。在 925 个域名中，有 14.8%为境外注册，且顶级域为.com 的约占 52.8%；在 4588 个 IP 中，有约 27.9%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 462 个 IP。

本周放马站点域名注册所属境内外分布
(12/7-12/13)



本周放马站点域名注册所属顶级域分布
(12/7-12/13)



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。

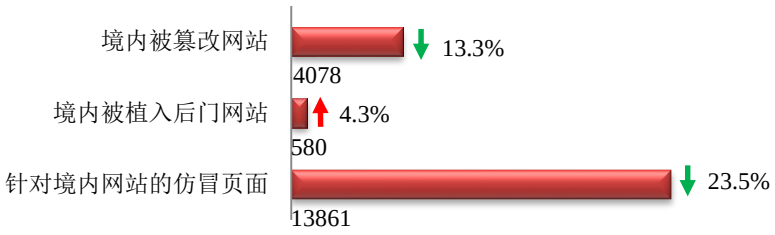
ANVA网络安全威胁信息共享平台

https://share.anva.org.cn/web/publicity/listurl

中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由 CNCERT 发起并组织运作的行业联盟。

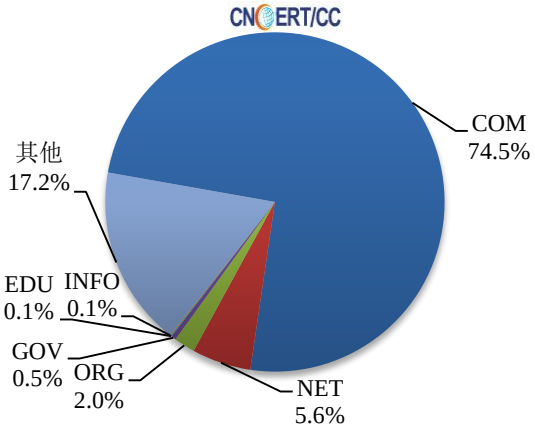
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 4078 个；被植入后门的网站数量为 580 个；针对境内网站的仿冒页面数量为 13861 个。

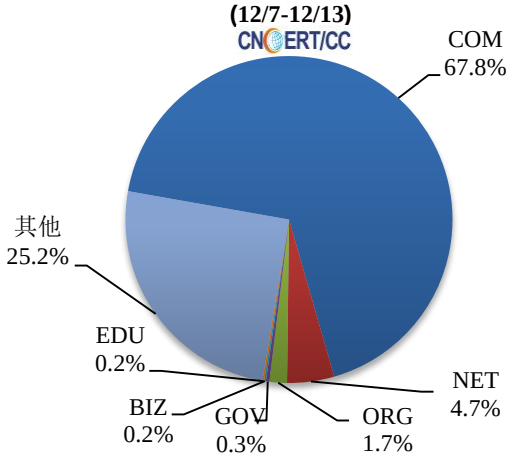


本周境内被篡改政府网站（GOV 类）数量为 19 个（约占境内 0.5%），较上周下降了 34.5%；境内被植入后门的政府网站（GOV 类）数量为 2 个（约占境内 0.3%）。

本周我国境内篡改网站按类型分布
(12/7-12/13)



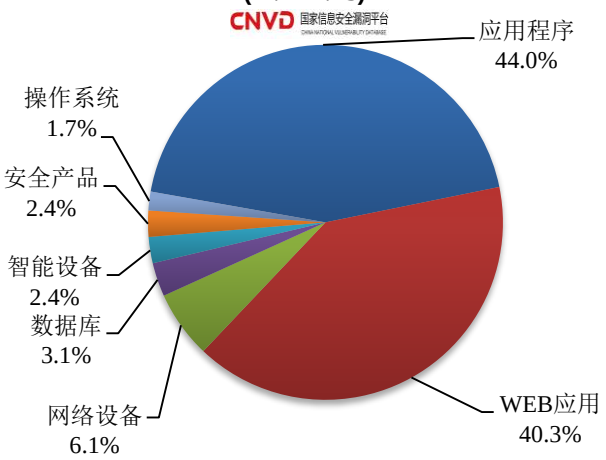
本周我国境内被植入后门网站按类型分布
(12/7-12/13)



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 293 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
(12/7-12/13)



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 应用和网络设备。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

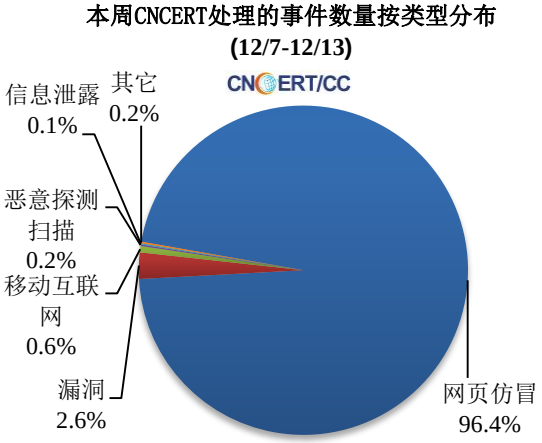
CNVD漏洞周报发布地址

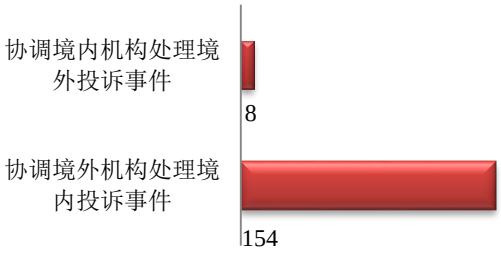
http://www.cnvd.org.cn/webinfo/list?type=4

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、基础电信企业、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。

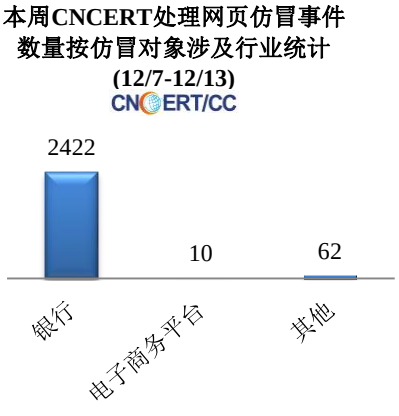
本周事件处理情况

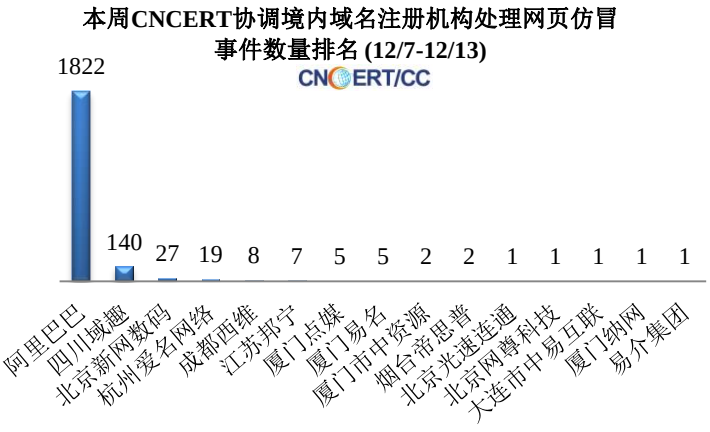
本周，CNCERT 协调基础电信企业、云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 2588 起，其中跨境网络安全事件 162 起。



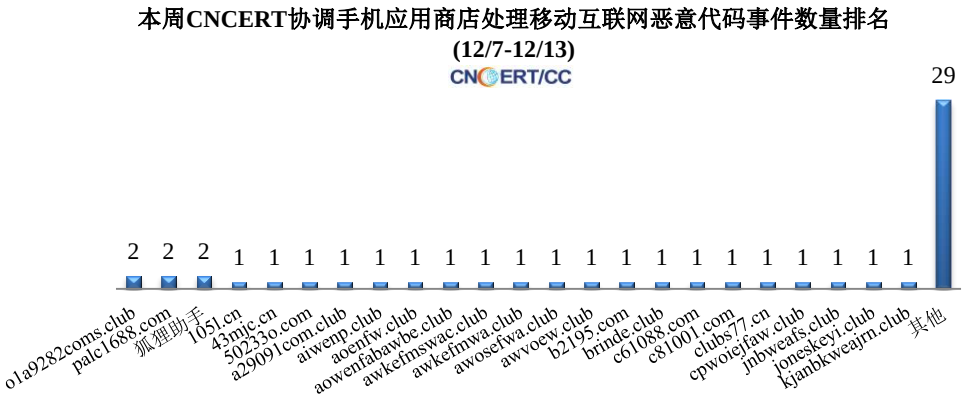


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 2494 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 2422 起、电子商务平台 10 起以及其他事件 62 起。





本周，CNCERT 协调 52 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 55 个。



业界新闻速递

1. 关于发布第八届 CNCERT 网络安全应急服务支撑单位考核结果的通知

2020 年 8 月至 9 月期间，CNCERT 组织开展了第八届 CNCERT 网络安全应急服务支撑单位（以下简称“支撑单位”）考核工作。

本次考核对象为第八届支撑单位全体，考核内容是 2019 年 7 月 1 日至 2020 年 6 月 30 日期间支撑工作情况。大部分支撑单位都能够按照要求在日常或特定任务期间，较好地支撑国家中心及分中心各项业务工作，但也有少数支撑单位与国家中心或分中心联系不够密切，支撑不力。在国家级支撑单位中，有 3 家考评等级为优，5 家为良，3 家为中。在省级支撑单位中，有 17 家考评等级为优，23 家为良，24 家为中，5 家为差。在工业控制领域支撑单位中，有 5 家考评等级为优，5 家为良，8 家为中。在反网络诈骗领域支撑单位中，有 1 家考评等级为良，4 家为中。

各单位考核结果将以邮件形式向 CNCERT 各分中心及所有支撑单位公布，针对部分支撑不力的支撑单位，CNCERT 将要求其加以改进，视其后续支撑情况再作处理。

2. 关于 6 家单位增选为第八届 CNCERT 网络安全应急服务支撑单位的公告

2020 年 8 月至 9 月期间，在第八届 CNCERT 网络安全应急服务支撑单位（以下简称“支撑单位”）考核期间，CNCERT 组织各分中心开展了支撑单位增改选工作。本次增改选工作由 CNCERT 国家中心和分中心提名、国家中心审议确定，旨在根据实际工作需求，针对本地支撑力量十分薄弱的省份予以补充，以满足网络安全工作实际需要，促进地方网络安全工作，进一步完善网络安全应急体系。

经提名推荐、筛选和审议，CNCERT 决定增选“中移物联网有限公司”、“江苏君立华域信息安全技术股份有限公司”、“沈阳汉林科技有限公司”、“湖南省金盾信息安全等级保护评估中心有限公司”和“西安讯蜂科技有限公司”5 家单位为第八届省级支撑单位，增选“恒安嘉新(北京)科技股份公司”为第八届工业控制领域支撑单位，有效期从 2020 年 7 月 1 日起，至 2021 年 6 月 30 日止。同时取消“智宇科技股份有限公司”、“北京锐安科技有限公司”、“杭州智御网络科技有限公司”省级支撑单位称号。

CNCERT 将与上述企业联系处理发放证书、签署合作协议等事宜，并在网站“应急体系——应急服务支撑单位”栏目更新相关信息，敬请留意。

关于国家互联网应急中心（CNCERT）

国家计算机网络应急技术处理协调中心（英文简称 CNCERT/CC），成立于 2001 年 8 月，为非政府非盈利的网络安全技术中心，是中国计算机网络应急处理体系中的牵头单位。作为国家级应急中心，CNCERT/CC 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，运行和管理国家信息安全漏洞共享平台（CNVD），维护公共互联网安全，保障关键信息基础设施的安全运行。

CNCERT/CC 在中国大陆 31 个省、自治区、直辖市设有分支机构，并通过组织网络安全企业、学校、社会组织和研究机构，协调骨干网络运营单位、域名服务机构和其他应急组织等，构建中国互联网安全应急体系，共同处理各类互联网重大网络安全事件。CNCERT/CC 积极发挥行业联动合力，发起成立了中国反网络病毒联盟（ANVA）和中国互联网网络安全威胁治理联盟（CCTGA）。

同时，CNCERT/CC 积极开展网络安全国际合作，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，已与 78 个国家和地区的 260 个组织建立了“CNCERT/CC 国际合作伙伴”关系。CNCERT/CC 是国际应急响应与安全组织 FIRST 的正式成员，以及亚太计算机应急组织 APCERT 的发起者之一，还积极参加亚太经合组织、国际电联、上合组织、东盟、金砖等政府层面国际和区域组织的网络安全相关工作。

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