国家互联网应急中心

2020 年第 49 期

11 月 30 日-12 月 6 日

网络安全信息与动态周报

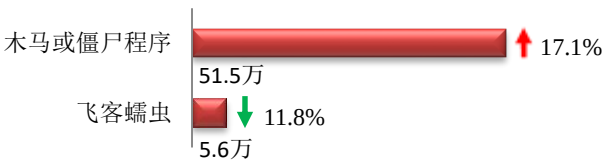
本周网络安全基本态势

境内感染网络病毒的主机数量	•57.1万	↑ 13.5%
境内被篡改网站总数 其中政府网站数量	•4704 •29	↓ 3.9% ↑ 20.8%
境内被植入后门网站总数 其中政府网站数量	•556 •0	↓ 20.5%
针对境内网站的仿冒页面数量	•18114	↑ 2.2%
新增信息安全漏洞数量 其中高危漏洞数量	•266 •81	↓ 26.1% ↓ 9.0%

= 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

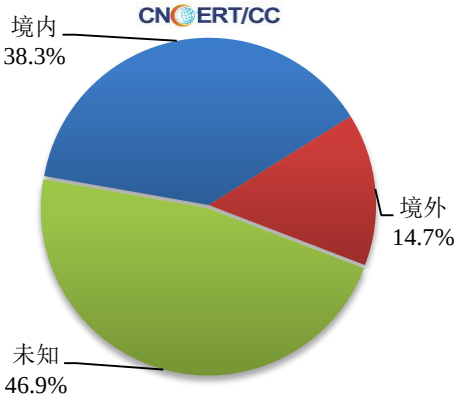
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 57.1 万个，其中包括境内被木马或被僵尸程序控制的主机约 51.5 万以及境内感染飞客（conficker）蠕虫的主机约 5.6 万。

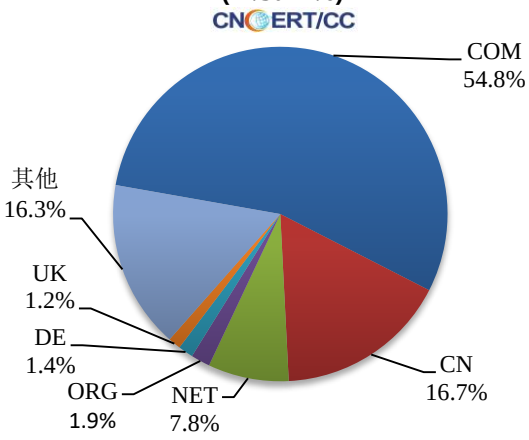


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1242 个，涉及 IP 地址 9805 个。在 1242 个域名中，有 14.7%为境外注册，且顶级域为.com 的约占 54.8%；在 9805 个 IP 中，有约 17.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 8435 个 IP。

本周放马站点域名注册所属境内外分布
(11/30-12/6)



本周放马站点域名注册所属顶级域分布
(11/30-12/6)



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。

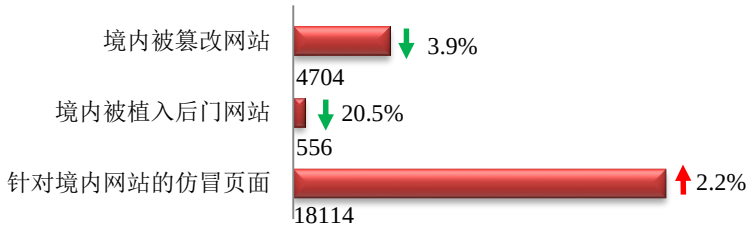
ANVA网络安全威胁信息共享平台

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。

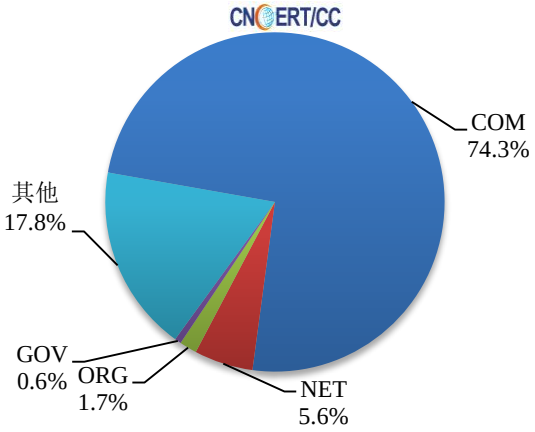
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 4704 个；被植入后门的网站数量为 556 个；针对境内网站的仿冒页面数量为 18114 个。

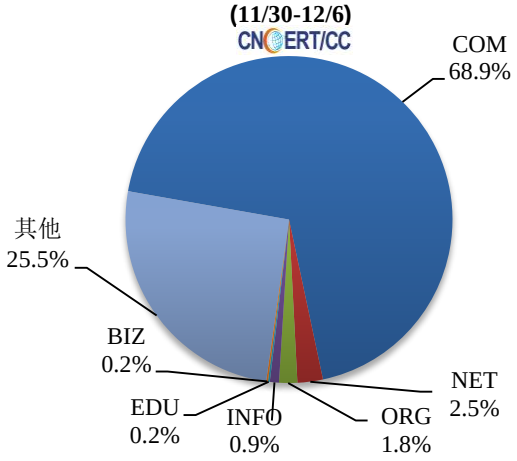


本周境内被篡改政府网站（GOV 类）数量为 29 个（约占境内 0.6%），较上周上涨了 20.8%；境内被植入后门的政府网站（GOV 类）数量为 0 个。

本周我国境内篡改网站按类型分布
(11/30-12/6)

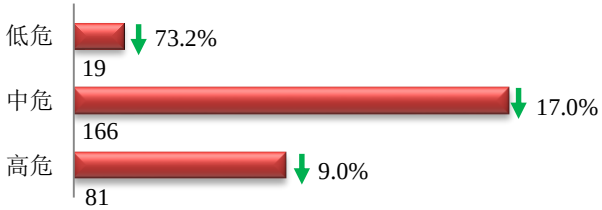


本周我国境内被植入后门网站按类型分布
(11/30-12/6)

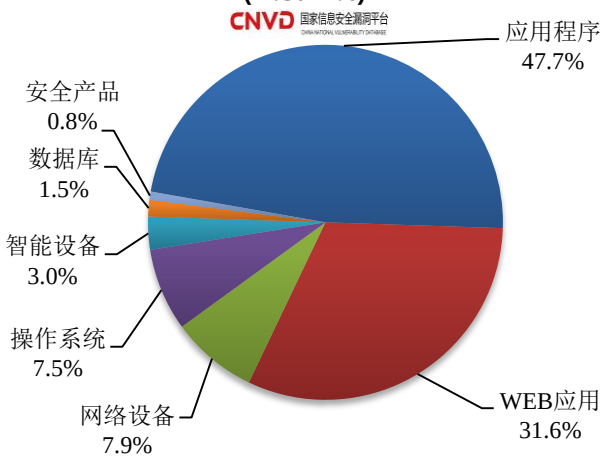


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 266 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
(11/30-12/6)



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

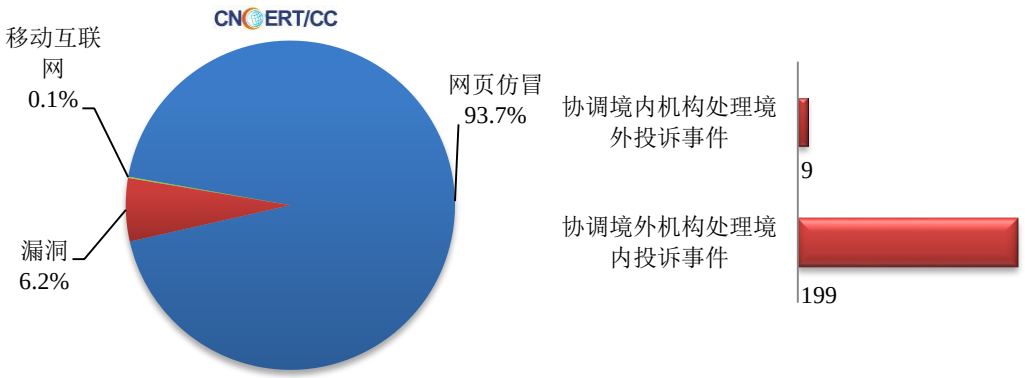
http://www.cnvd.org.cn/webinfo/list?type=4

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

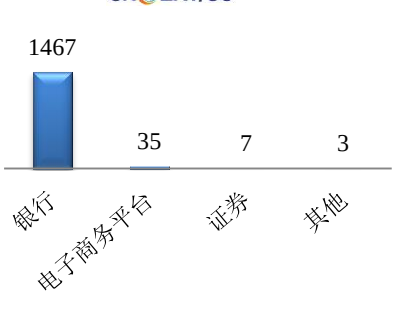
本周，CNCERT 协调基础电信企业、云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 1614 起，其中跨境网络安全事件 208 起。

本周CNCERT处理的事件数量按类型分布
(11/30-12/6)

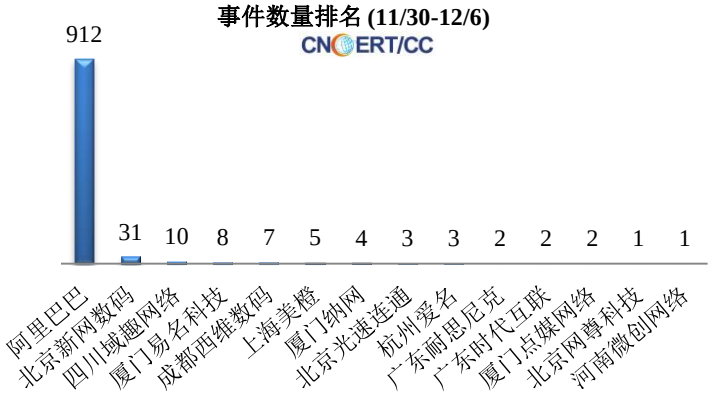


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1512 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 1467 起、电子商务平台 35 起、证券 7 起以及其他事件 3 起。

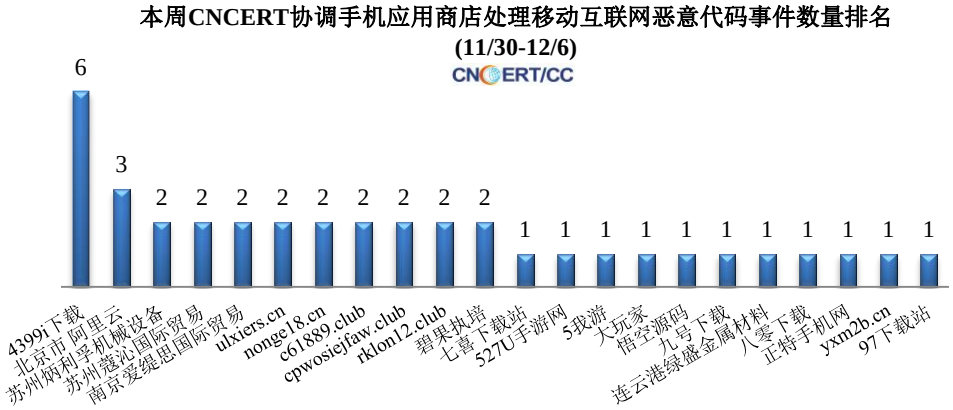
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计
(11/30-12/6)



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 (11/30-12/6)



本周，CNCERT 协调 22 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 38 个。



业界新闻速递

1. 国家互联网信息办公室就《常见类型移动互联网应用程序（App）必要个人信息范围》公开征求意见

近年来，移动互联网应用程序（App）得到广泛应用，在促进经济社会发展、服务民生等方面发挥了重要作用。同时，App 超范围收集、强制收集用户个人信息普遍存在，用户拒绝同意就无法安装使用。为落实《中华人民共和国网络安全法》关于个人信息收集合法、正当、必要的原则，规范 App 个人信息收集行为，保障公民个人信息安全，国家互联网信息办公室研究起草了《常见类型移动互联网应用程序（App）必要个人信息范围（征求意见稿）》，现向社会公开征求意见。该文件规定了地图导航、网络约车、即时通信等 38 类常见类型 App 必要个人信息范围。必要个人信息是指保障 App 基本功能正常运行所必须的个人信息，缺少该信息 App 无法提供基本功能服务。只要用户同意收集必要个人信息，App 不得拒绝用户安装使用。

2. 工信部通报 60 家侵害用户权益行为 APP

依据《网络安全法》《电信条例》《电信和互联网用户个人信息保护规定》等法律法规，按照《关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》（工信部信管〔2020〕164 号）工作部署，工业和信息化部近期组织第三方检测机构对手机应用软件进行检查，督促存在问题的企业进行整改。截至目前，尚有 60 款 APP 未完成整改，上述 APP 应在 12 月 10 日前完成整改落实工作。逾期不整改的，工业和信息化部将依法依规组织开展相关处置工作。

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：王适文

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315