国家互联网应急中心

2021 年第 50 期

12 月 6 日-12 月 12 日

网络安全信息与动态周报

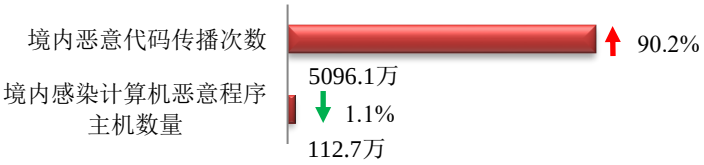
本周网络安全基本态势

境内计算机恶意程序传播次数 境内感染计算机恶意程序主机数量	• 5096.1万 • 112.7万	↑ 90.2% ↓ 1.1%
境内被篡改网站总数 其中政府网站数量	• 2830 • 13	↑ 213.4% ↑ 225.0%
境内被植入后门网站总数 其中政府网站数量	• 439 • 2	↓ 44.5% ↑ 200.0%
针对境内网站的仿冒页面数量	• 247	↓ 32.5%
新增信息安全漏洞数量 其中高危漏洞数量	• 658 • 176	↑ 19.0% ↑ 6.0%

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

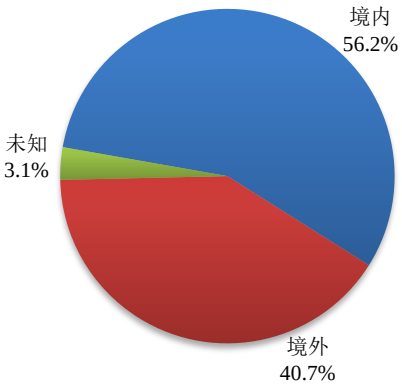
本周网络病毒活动情况

境内计算机恶意程序传播次数约为 5096.1 万次，境内感染计算机恶意程序主机数量约为 112.7 万个。

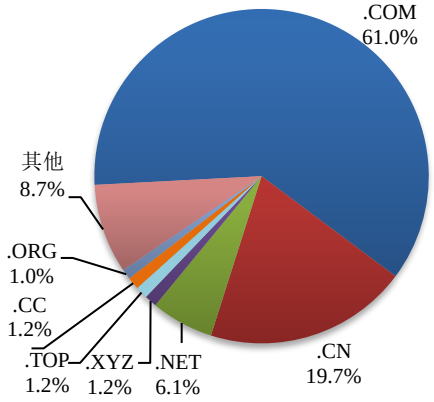


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 924 个，涉及 IP 地址 4574 个。在 924 个域名中，有 40.7%为境外注册，且顶级域为.com 的约占 61.0%；在 4574 个 IP 中，有约 47.8%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 336 个。

本周放马站点域名注册所属境内外分布
(12/6-12/12）



本周放马站点域名注册所属顶级域分布
(12/6-12/12)



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。

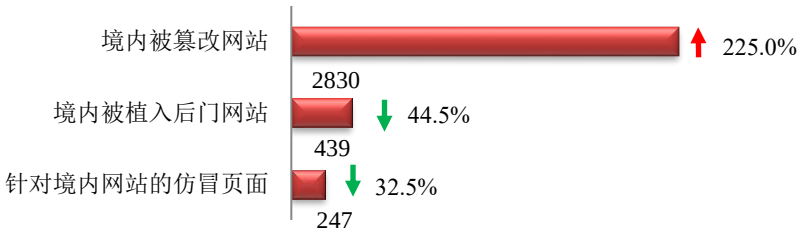
ANVA网络安全威胁信息共享平台

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。

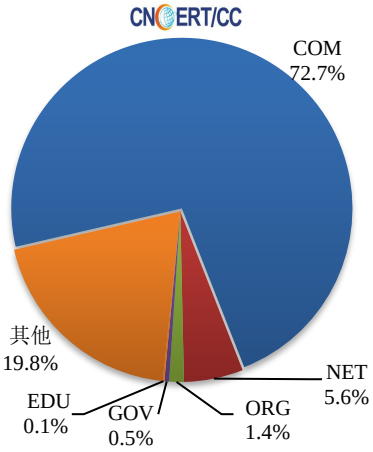
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 2830 个；被植入后门的网站数量为 439 个；针对境内网站的仿冒页面数量为 247 个。

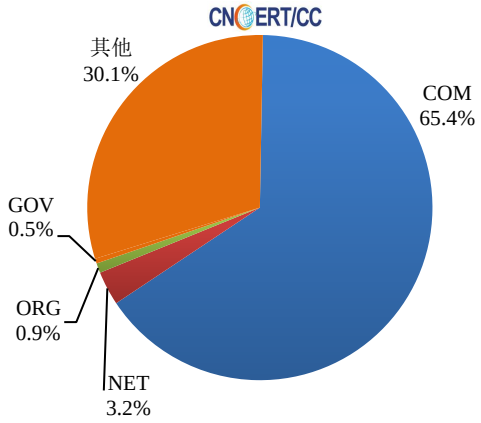


本周境内被篡改政府网站（GOV 类）数量为 13 个（约占境内 0.5%）,与上周相比上升 225.0%；境内被植入后门的政府网站（GOV 类）数量为 2 个（约占境内 0.5%），与上周相比上升 200.0%。

本周我国境内篡改网站按类型分布
(12/6-12/12)

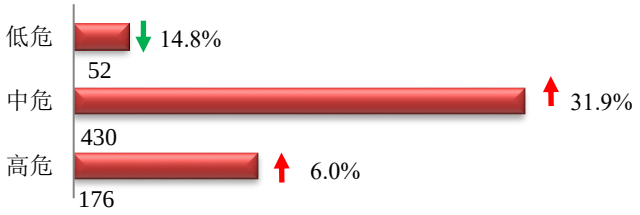


本周我国境内被植入后门网站按类型分布
(12/6-12/12)

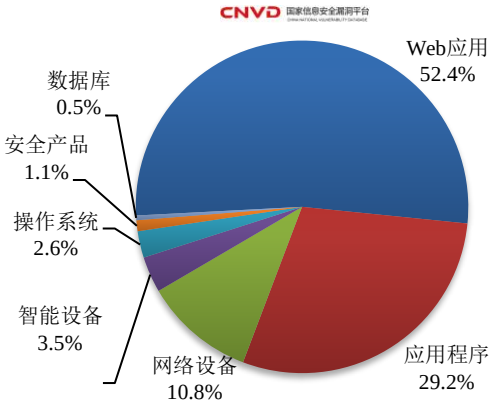


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 658 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
(12/6-12/12）



本周 CNVD 发布的网络安全漏洞中，Web 应用占比最高，其次是应用程序和网络设备。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

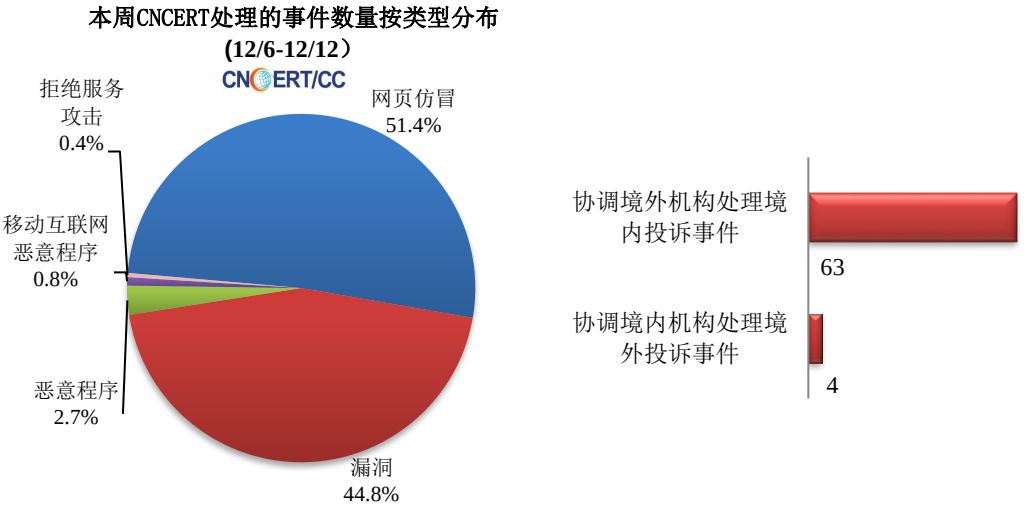
CNVD漏洞周报发布地址

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

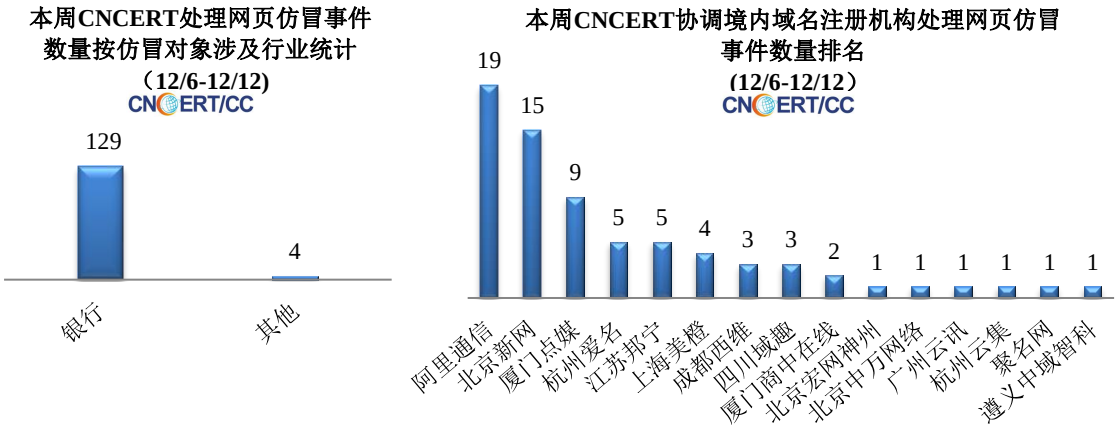
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

本周事件处理情况

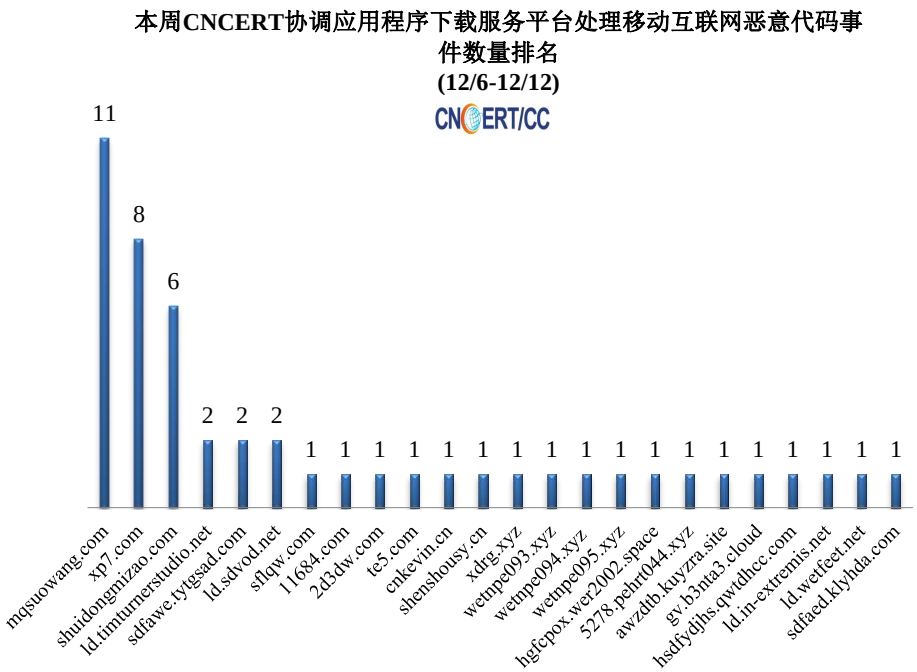
本周，CNCERT 协调云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理网络安全事件 259 起，其中跨境网络安全事件 67 起。



本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理 133 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，银行仿冒事 129 起，其他事件 4 起。



本周，CNCERT 协调 24 个提供恶意移动应用程序下载服务的平台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 49 个。



业界新闻速递

1. 国家计算机网络应急技术处理协调中心（CNCERT）、中国网络空间安全协会发布《App 违法违规收集使用个人信息监测分析报告》

2021 年 12 月 9 日，据 CNCERT 官网消息，近期，CNCERT 会同中国网络空间安全协会对前期专项治理和平台监测发现的 App 违法违规收集使用个人信息问题进行了总结梳理，对问题特点和趋势进行了深入分析，形成了关于 App 收集使用个人信息情况的监测分析报告。报告主要分为两个部分：一是 App 收集使用个人信息总体状况。从 9 个方面进行态势分析和问题阐述，包括依法治理、强制收集、超范围收集、知情同意、隐私政策、明示告知、SDK 收集、账号注销、社会监督等。二是工作建议。从鼓励示范应用、持续专项治理、关键环节把关、强化标准规范、完善投诉举报、加大宣传教育、推进行业自律等方面提出思路建议。此次向社会公开发布该报告，旨在及时反映当前 App 收集使用个人信息整体情况，为行业企业和全社会了解当前 App 个人信息安全形势提供参考。同时，对广大 App 运营者以及应用商店、智能终端等平台积极落实主体责任、提升个人信息保护水平起到参考监督作用，对社会公众提高个人信息安全意识起到宣传促进作用。

2. 关于 Apache Log4j2 存在远程代码执行漏洞的安全公告

2021 年 12 月 10 日，国家信息安全漏洞共享平台（CNVD）收录了 Apache Log4j2 远程代码执行漏洞（CNVD-2021-95914）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。CNVD 对该漏洞的综合评级为“高危”。漏洞影响的产品版本包括：Apache Log4j2 2.0 - 2.15.0-rc1。目前，

漏洞利用细节已公开，Apache 官方已发布新版本完成漏洞修复，CNVD 建议用户尽快进行自查，并及时升级至最新版，同时采取防范性措施避免漏洞攻击威胁。

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 2020 年，已与 78 个国家和地区的 265 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：吕卓航

网址： www.cert.org.cn

Email：cncert_report@cert.org.cn

电话： 010-82990315