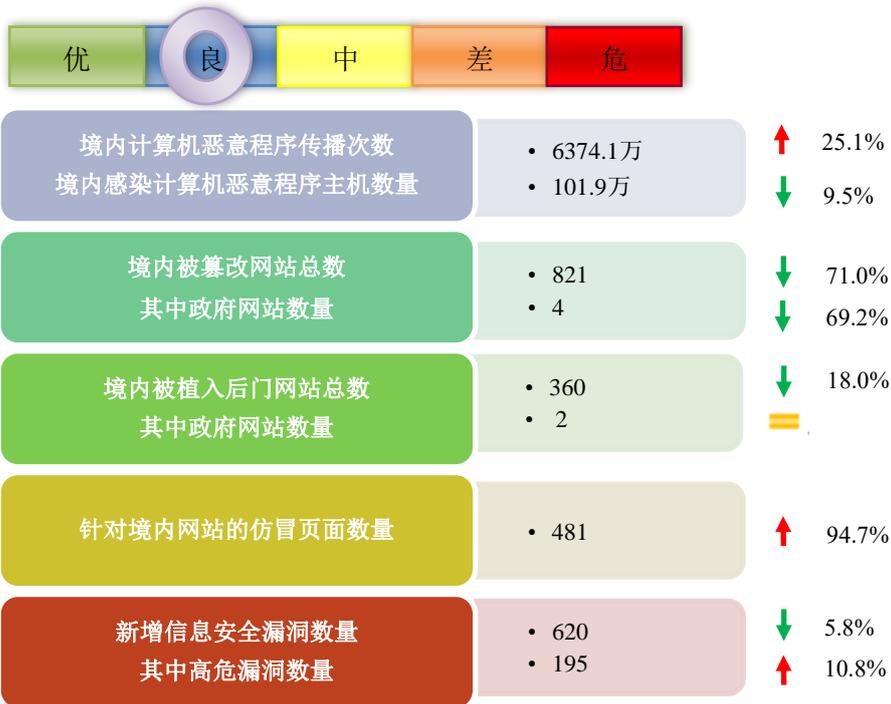
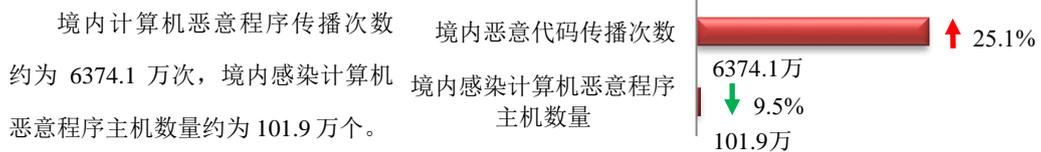


本周网络安全基本态势



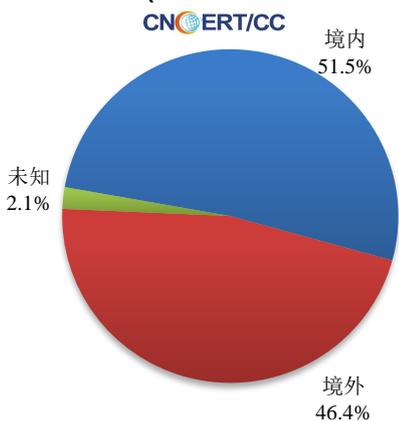
■ 表示数量与上周相同
 ↑ 表示数量较上周环比增加
 ↓ 表示数量较上周环比减少

本周网络病毒活动情况

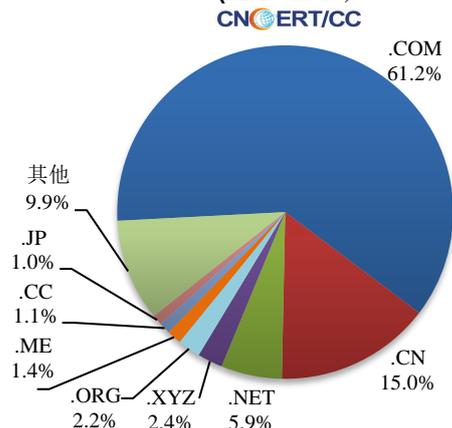


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 6809 个，涉及 IP 地址 36362 个。在 6809 个域名中，有 46.4% 为境外注册，且顶级域为 .com 的约占 61.2%；在 36362 个 IP 中，有约 87.2% 位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 688 个。

本周放马站点域名注册所属境内外分布
(12/13-12/19)



本周放马站点域名注册所属顶级域分布
(12/13-12/19)



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。

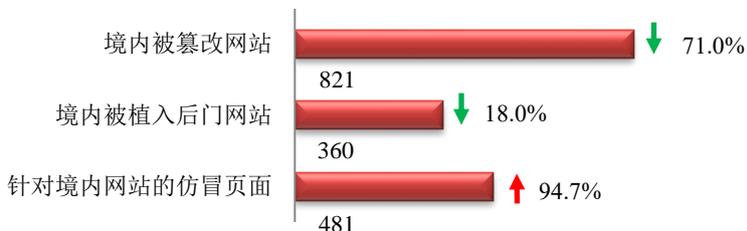
ANVA 网络安全威胁信息共享平台

<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。

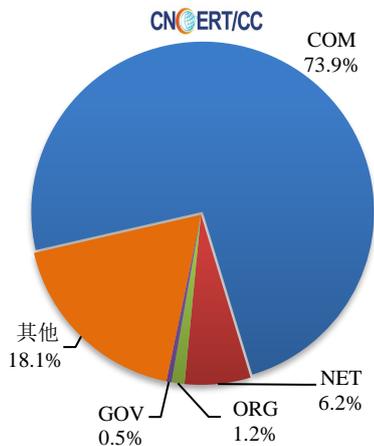
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 821 个；被植入后门的网站数量为 360 个；针对境内网站的仿冒页面数量 481 个。

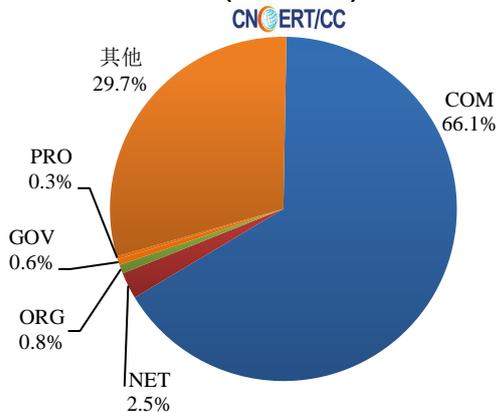


本周境内被篡改政府网站（GOV类）数量为4个（约占境内0.5%），与上周相比下降69.2%；境内被植入后门的政府网站（GOV类）数量为2个（约占境内0.6%），与上周相比持平。

本周我国境内篡改网站按类型分布
(12/13-12/19)

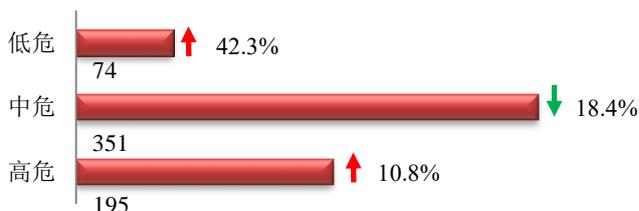


本周我国境内被植入后门网站按类型分布
(12/13-12/19)

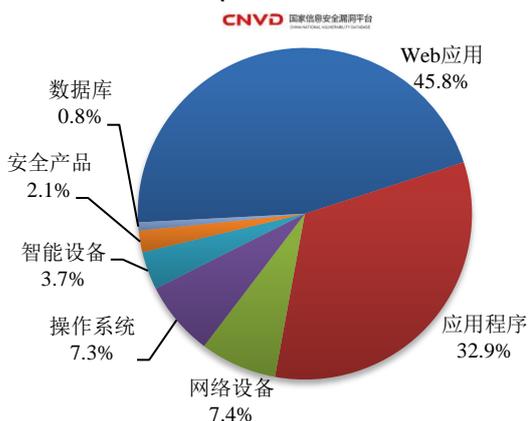


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞620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
(12/13-12/19)



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>

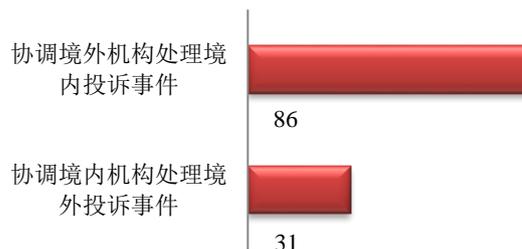
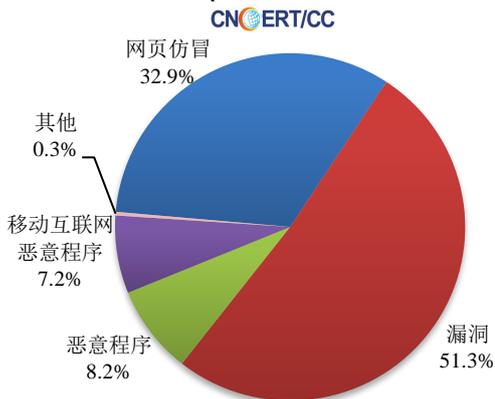
国家信息安全漏洞共享平台(缩写CNVD)是CNCERT联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。



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 304 起，其中跨境网络安全事件 117 起。

本周CNCERT处理的事件数量按类型分布
(12/13-12/19)

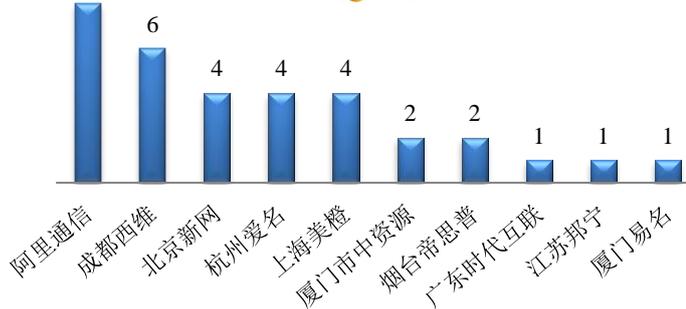


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理 100 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，银行仿冒事件 58 起，其他事件 42 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计
(12/13-12/19)

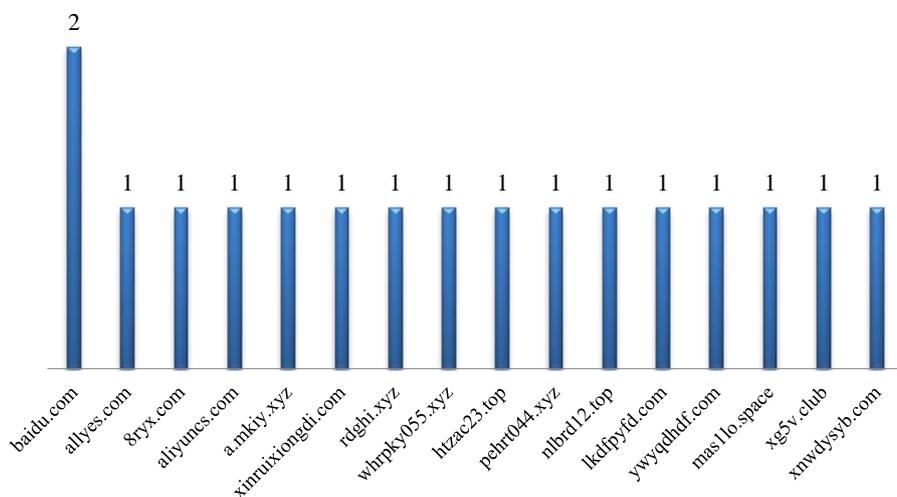


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名
(12/13-12/19)



本周，CNCERT 协调 16 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 17 个。

本周CNCERT协调应用程序下载服务平台处理移动互联网恶意代码事件数量排名
(12/13-12/19)
CNCERT/CC



业界新闻速递

1. CNCERT 发布《Apache Log4j2 远程代码执行漏洞排查及修复手册》

近期，Apache Log4j2 远程代码执行漏洞（CNVD-2021-95914）曝光，引发社会广泛关注。攻击者利用该漏洞，可在未授权的情况下远程执行代码，获得服务器控制权限。经 CNCERT 综合技术分析研判，该漏洞具有危害程度高、利用难度低、影响范围大的特点。为正确处置突发漏洞风险，降低漏洞带来的损失，12 月 15 日，CNCERT 整理并发布了《Apache Log4j2 远程代码执行漏洞排查及修复手册》，以供相关单位、企业及个人参考。详情请参见 CNCERT 官网。

2. 微软发布 2021 年 12 月安全更新

12 月 16 日，据国家信息安全漏洞共享平台（CNVD）消息，12 月 14 日，微软发布了 2021 年 12 月份的月度例行安全公告，修复了多款产品存在的 64 个安全漏洞。受影响的产品包括：Windows 11（29 个）、Windows Server 2022（29 个）、Windows 10 21H1（30 个）、Windows 10 20H2 & Windows Server v20H2（30 个）、Windows 10 2004 & Windows Server v2004（30 个）、Windows 8.1 & Server 2012 R2（21 个）、Windows Server 2012（21 个）、Windows RT 8.1（21 个）和 Microsoft Office-related software（6 个）。利用上述漏洞，攻击者可以绕过安全功能限制，获取敏感信息，提升权限，执行远程代码，或发起拒绝服务攻击等。CNVD 提醒广大 Microsoft 用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

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：楼书逸

网址：www.cert.org.cn

Email：cncert_report@cert.org.cn

电话：010-82990315