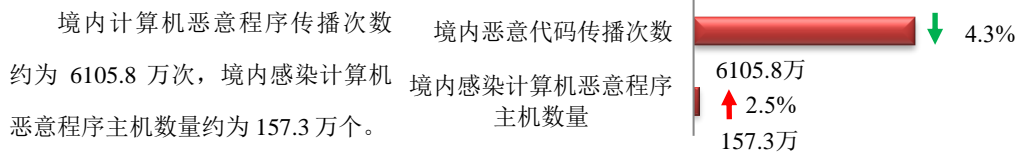


## 本周网络安全基本态势



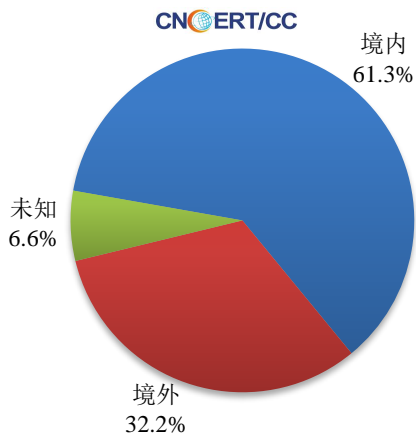
■ 表示数量与上周相同    ↑ 表示数量较上周环比增加    ↓ 表示数量较上周环比减少

## 本周网络病毒活动情况

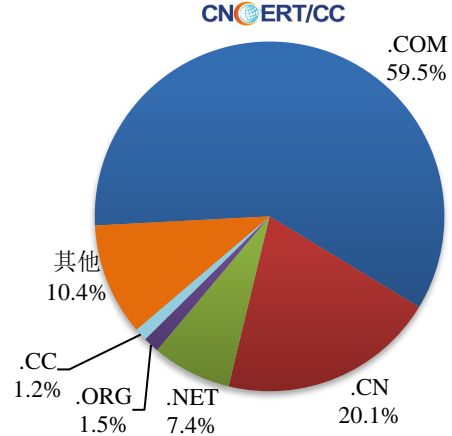


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1020 个，涉及 IP 地址 4177 个。在 1020 个域名中，有 32.2% 为境外注册，且顶级域为 .com 的约占 59.5%；在 4177 个 IP 中，有约 61.1% 位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 243 个。

本周放马站点域名注册所属境内外分布  
(4/11-4/17)



本周放马站点域名注册所属顶级域分布  
(4/11-4/17)



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。

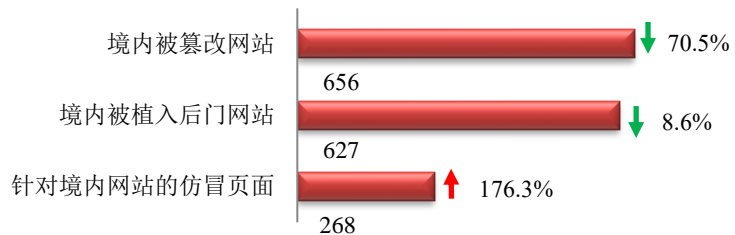
ANVA 网络安全威胁信息共享平台

<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。

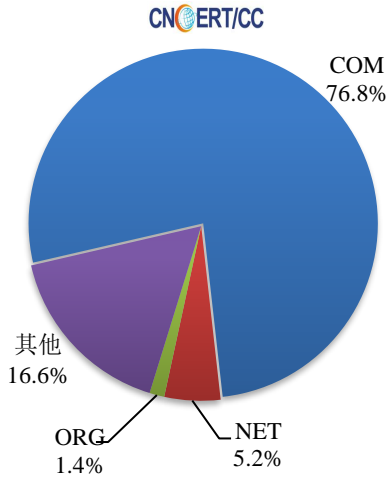
## 本周网站安全情况

本周 CNCERT 监测发现境内境内被篡改网站数量 656 个；被植入后门的网站数量为 627 个；针对境内网站的仿冒页面数量 268 个。

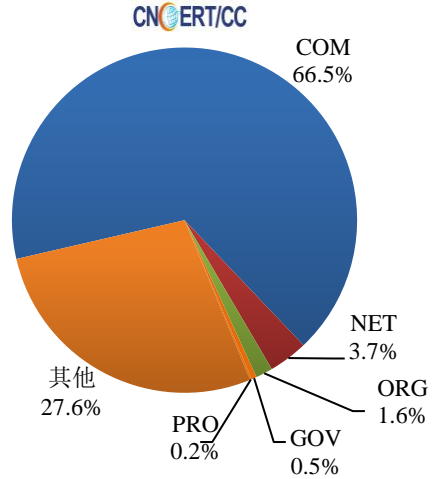


本周境内被篡改政府网站（GOV类）数量为0个；境内被植入后门的政府网站（GOV类）数量为3个（约占境内0.5%），与上周相比下降82.4%。

本周我国境内篡改网站按类型分布  
(4/11-4/17)

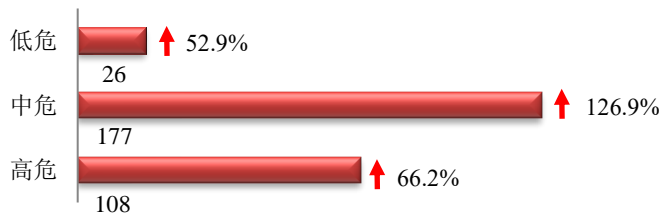


本周我国境内被植入后门网站按类型分布  
(4/11-4/17)

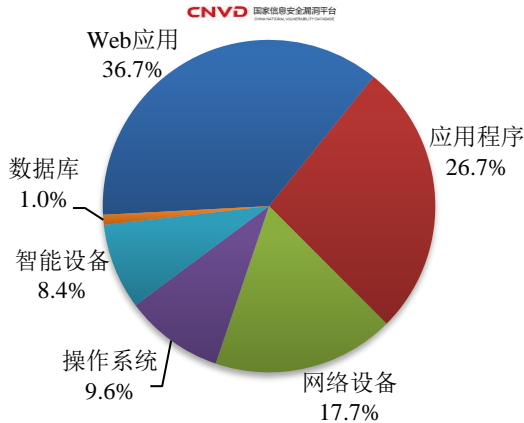


### 本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 311 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  
(4/11-4/17)



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

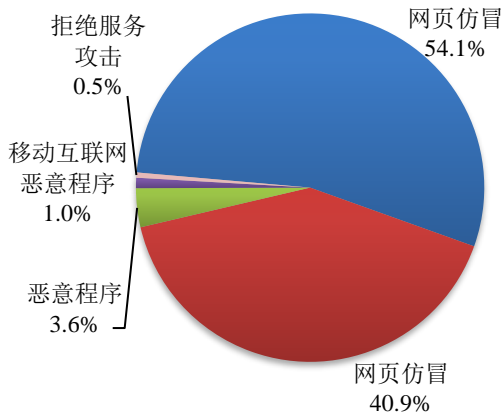
<http://www.cnvd.org.cn/webinfo/list?type=4>

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。

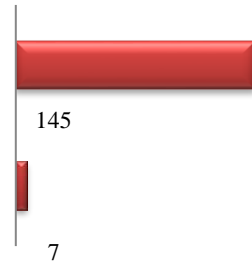
## 本周事件处理情况

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416起，其中跨境网络安全事件152起。

本周CNCERT处理的事件数量按类型分布  
(4/11-4/17)  
CNCERT/CC

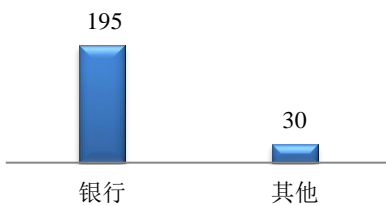


协调境外机构处理境内投诉事件  
协调境内机构处理境外投诉事件

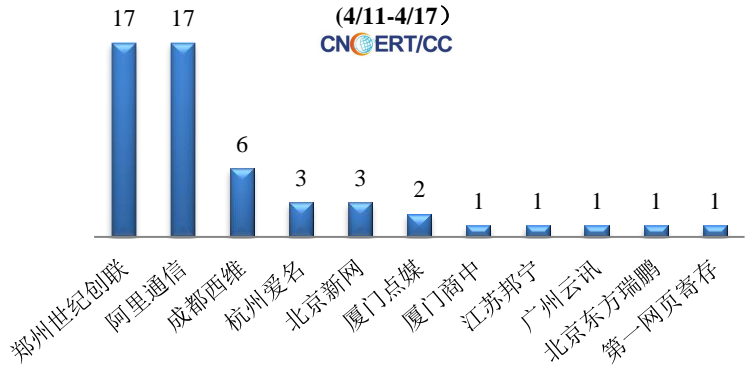


本周，CNCERT协调境内外域名注册机构、境外CERT等机构重点处理225页仿冒投诉事件。根据仿冒对象涉及行业划分，银行仿冒事件195起，其他事件30起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计  
(4/11-4/17)  
CNCERT/CC

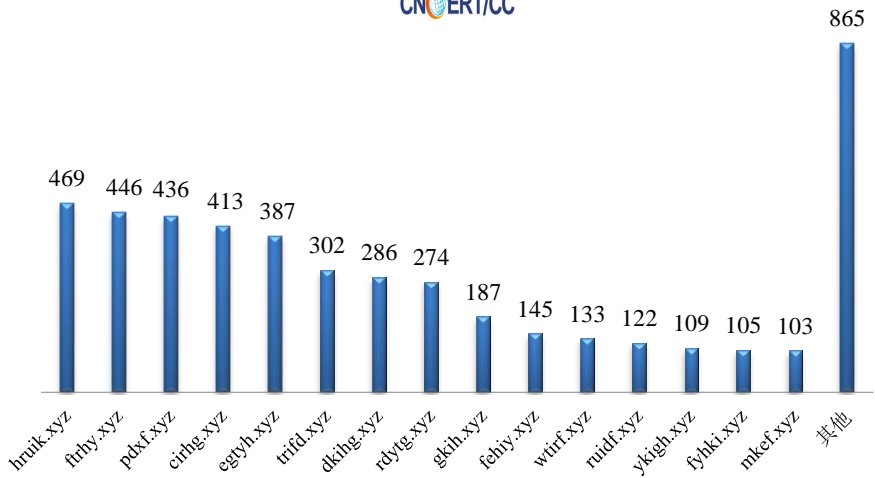


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名  
(4/11-4/17)  
CNCERT/CC



本周，CNCERT 协调 102 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 4782 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 (4/11-4/17)  
CNCERT/CC



## 业界新闻速递

### 1. 关于 Fodcha 僵尸网络大规模传播的风险提示

4月13日，据CNCERT官网消息，近期，国家互联网应急中心（CNCERT）与三六零数字安全科技集团有限公司共同监测发现一个新的且在互联网上快速传播的DDoS僵尸网络，通过跟踪监测发现其每日上线境内肉鸡数（以IP数计算）已超过1万、且每日会针对超过100个攻击目标发起攻击，给网络空间带来较大威胁。由于该僵尸网络最初使用的C2域名folded.in，以及使用chacha算法来加密网络流量，将其命名为Fodcha。请广大网民强化风险意识，加强安全防范，避免不必要的经济损失，及时修复相关系统漏洞，不使用弱密码或默认密码，定期更换密码。当发现主机感染僵尸木马程序后，立即核实主机受控情况和入侵途径，并对受害主机进行清理。

### 2. 微软发布2022年4月安全更新

4月13日，据国家信息安全漏洞共享平台CNVD消息，4月12日，微软发布了2022年4月份的月度例行安全公告，修复了多款产品存在的103个安全漏洞。受影响的产品包括：Windows 11（69个）、Windows Server 2022（98个）、Windows 10 21H2（72个）、Windows 10 21H1（72个）、Windows 10 20H2 & Windows Server v20H2（97个）、Windows 8.1 & Server 2012 R2（63个）、Windows Server 2012（57个）、Windows RT 8.1（47个）和Microsoft Office-related software（4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 2021 年，已与 81 个国家和地区的 274 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：朱天

网址：[www.cert.org.cn](http://www.cert.org.cn)

Email：[cncert\\_report@cert.org.cn](mailto:cncert_report@cert.org.cn)

电话：010-82990315