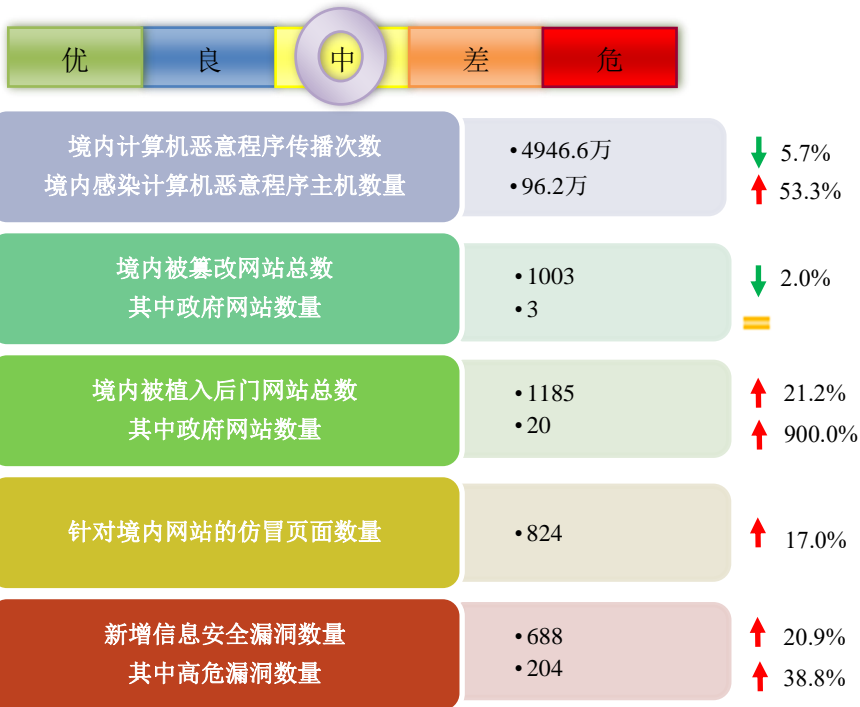


网络安全信息与动态周报

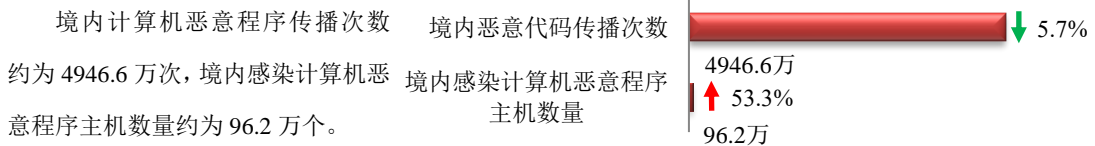


本周网络安全基本态势

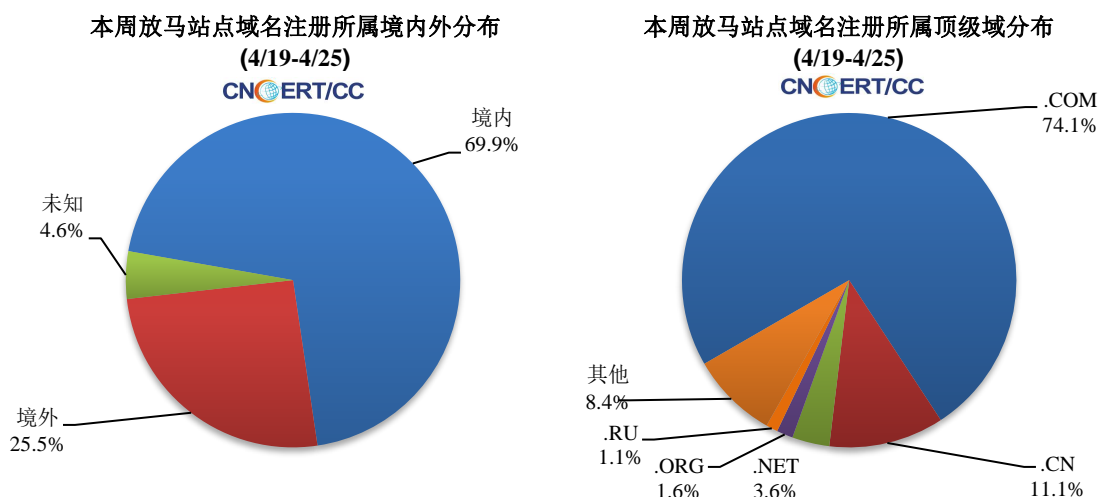


▬ 表示数量与上周相同 ↑ 表示数量较上周环比增加 ↓ 表示数量较上周环比减少

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 13654 个，涉及 IP 地址 14221 个。在 13654 个域名中，有 25.5% 为境外注册，且顶级域为 .com 的约占 74.1%；在 14221 个 IP 中，有约 43.3% 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 818 个。



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。

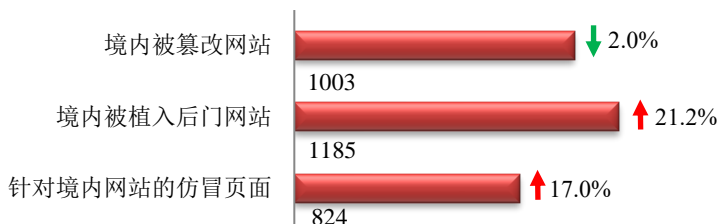
ANVA 网络安全威胁信息共享平台

<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。

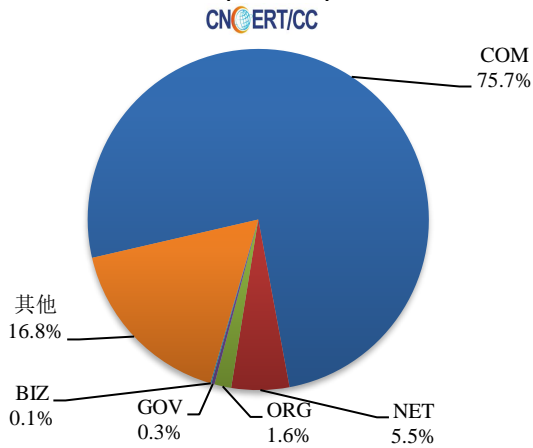
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 1003 个；被植入后门的网站数量为 1185 个；针对境内网站的仿冒页面数量为 824 个。

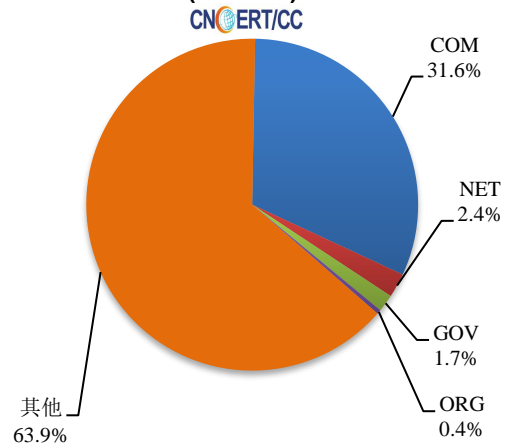


本周境内被篡改政府网站（GOV 类）数量为 3 个（约占境内 0.3%），与上周持平；境内被植入后门的政府网站（GOV 类）数量为 20 个（约占境内 1.7%），与上周相比上升了 900.0%。

本周我国境内篡改网站按类型分布 (4/19-4/25)

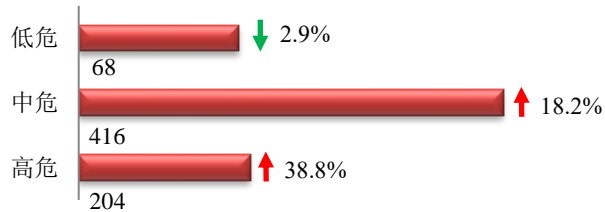


本周我国境内被植入后门网站按类型分布 (4/19-4/25)

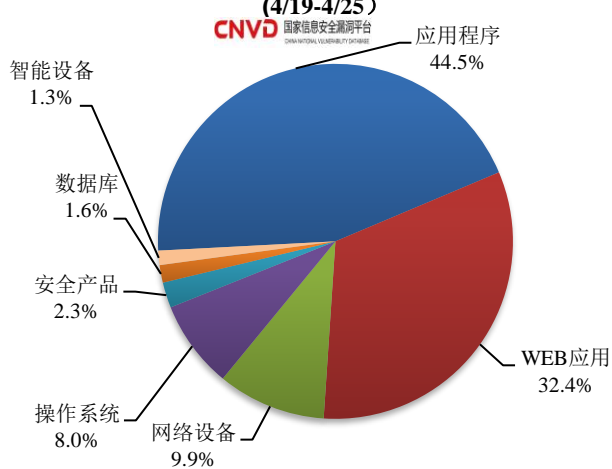


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 688 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 (4/19-4/25)



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

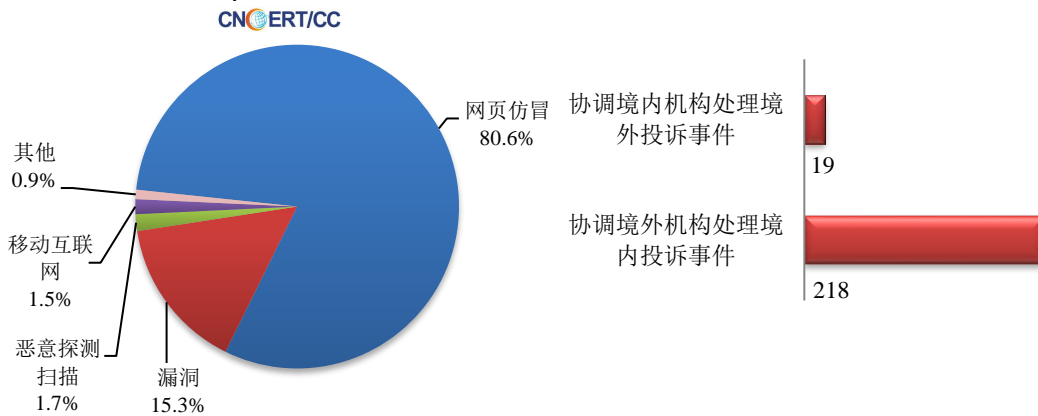
<http://www.cnvd.org.cn/webinfo/list?type=4>

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

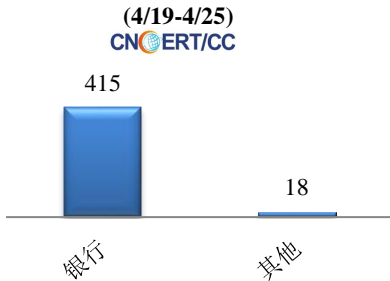
本周，CNCERT 协调云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 537 起，其中跨境网络安全事件 237 起。

本周CNCERT处理的事件数量按类型分布
(4/19-4/25)

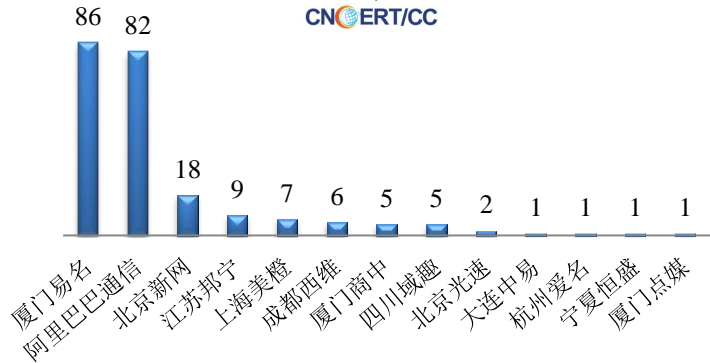


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理 433 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，银行仿冒事件 415 起，其他事件 18 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计
(4/19-4/25)

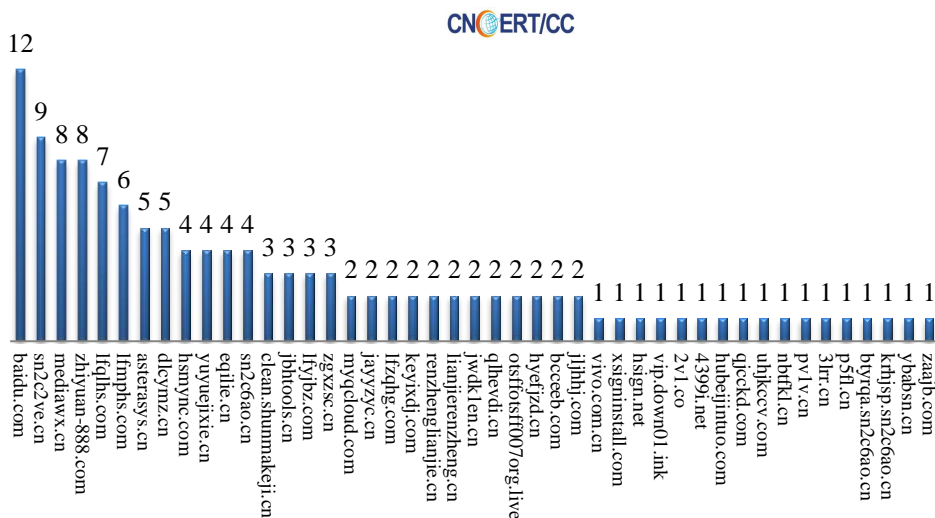


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (4/19-4/25)



本周CNCERT协调手机应用商店处理移动互联网恶意代码事件数量排名
(4/19-4/25)

本周，CNCERT 协调 46 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 129 个。



业界新闻速递

1. Oracle 发布 2021 年 4 月的安全公告

2021 年 4 月 20 日，据国家信息安全漏洞共享平台（CNVD）官网消息，Oracle 发布了 2021 年 4 月份的安全更新，修复了其多款产品存在的 390 个安全漏洞。受影响的产品包括：Oracle Database Server（10 个）、Oracle Global Lifecycle Management（1 个）、OracleNoSQL Database（4 个）、Oracle REST Data Services（1 个）、Oracle Spatial Studio（2 个）、Oracle SQL Developer（1 个）、Oracle Commerce（4 个）、Oracle Communications Applications（13 个）、OracleCommunications（22 个）、Oracle Construction and Engineering（8 个）、OracleE-Business Suite（70 个）、Oracle Enterprise Manager（9 个）、Oracle Financial Services Applications（15 个）、OracleFood and Beverage Applications（2 个）、Oracle Fusion Middleware（45 个）、Oracle Health Sciences Applications（3 个）、OracleHospitality Applications（6 个）、Oracle Hyperion（2 个）、Oracle iLearning（1 个）、Oracle Insurance Applications（1 个）、OracleJava SE（4 个）、Oracle JD Edwards（10 个）、Oracle MySQL（49 个）、Oracle PeopleSoft（18 个）、Oracle Retail Applications（35 个）、Oracle Siebel CRM（8 个）、Oracle Storage Gateway（6 个）、Oracle Supply Chain（5 个）、Oracle Support Tools（1 个）、Oracle Systems（5 个）、Oracle Utilities Applications（5 个）和 OracleVirtualization（24 个）。本次安全更新提供了针对 165 个高危漏洞的补丁，有 221 个漏洞可被远程利用。CNVD 提醒广大 Oracle 用户，请及时下载补丁更新，避免引发漏洞相关的安全事件。

2. 最高检发布检察机关个人信息保护公益诉讼典型案例

2021年4月22日，据最高人民检察院网站消息，最高人民检察院发布检察机关个人信息保护公益诉讼典型案例，包括浙江省杭州市余杭区检察院诉某网络科技有限公司侵害公民个人信息民事公益诉讼案等11件。该发布透露，对未履行个人信息管理和保护义务的互联网企业，检察机关将通过公益诉讼要求其承担公益损害责任，推动落实企业主体责任。在此次发布的余杭区检察院诉某网络科技有限公司侵害公民个人信息民事公益诉讼案中，余杭区检察院发现该公司开发的音乐视频教学类APP存在违法违规收集、储存、使用个人信息等情形，依法向法院提起民事公益诉讼。经调解，该公司自愿对APP进行全面整改，删除违法违规收集、储存的全部用户个人信息，公开赔礼道歉，并承诺不再侵害用户个人信息。对该APP后续整改情况，检察机关引入第三方代表评估，通过合规检测后才允许其重新上架。

3. 工信部通报关于侵害用户权益行为的APP（2021年第4批）

2021年4月23日，据工信部网站消息，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》（工信部信管函〔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，重点督促游戏类、工具类存在问题的企业进行整改。截至目前，尚有93款APP未完成整改。各通信管理局按工业和信息化部APP整治行动部署，积极开展手机应用软件监督检查，广东省通信管理局检查发现仍有45款APP未完成整改。上述APP应在4月29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。

4. 国家七部门联合发布《网络直播营销管理办法（试行）》

2021年4月23日，据中国网信网消息，国家互联网信息办公室、公安部、商务部、文化和旅游部、国家税务总局、国家市场监督管理总局、国家广播电视总局等七部门联合发布《网络直播营销管理办法（试行）》（以下简称《办法》），自2021年5月25日起施行。国家互联网信息办公室有关负责人表示，《办法》旨在规范网络市场秩序，维护人民群众合法权益，促进新业态健康有序发展，营造清朗网络空间。《办法》要求，直播营销平台应当建立健全账号及直播营销功能注册注销、信息安全管理、营销行为规范、未成年人保护、消费者权益保护、个人信息保护、网络和数据安全管理等机制、措施。同时，《办法》还对直播营销平台相关安全评估、备案许可、技术保障、平台规则、身份认证和动态核验、高风险和违法违规行为识别处置、新技术和跳转服务风险防范、构成商业广告的付费导流服务等作出详细规定。《办法》将从事直播营销活动的直播发布者细分为直播间运营者和直播营销人员，明确年龄限制和行为红线，对直播间运营者和直播营销人员相关广告活动、线上线下直播场所、商品服务信息核验、虚拟形象使用、与直播营销人员服务机构开展商业合作等方面提出具体要求。《办法》强调，直播营销平台应当积极协助消费者维护合法权益，提供必要的证据等支持。直播间运营者、直播营销人员应当依法依规履行消费者权益保护责任和义务，

不得故意拖延或者无正当理由拒绝消费者提出的合法合理要求。《办法》提出，国家七部门建立健全线索移交、信息共享、会商研判、教育培训等工作机制，依据各自职责做好网络直播营销相关监督管理工作。各地各部门要加强监督检查，加强对行业协会商会的指导，查处违法违规行为，对严重违法违反法律法规的直播营销市场主体依法开展联合惩戒。

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：郭禹

网址：www.cert.org.cn

Email: cncert_report@cert.org.cn

电话：010-82990315