

网络安全信息与动态周报

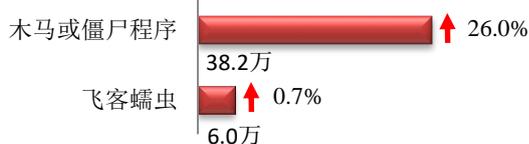
本周网络安全基本态势



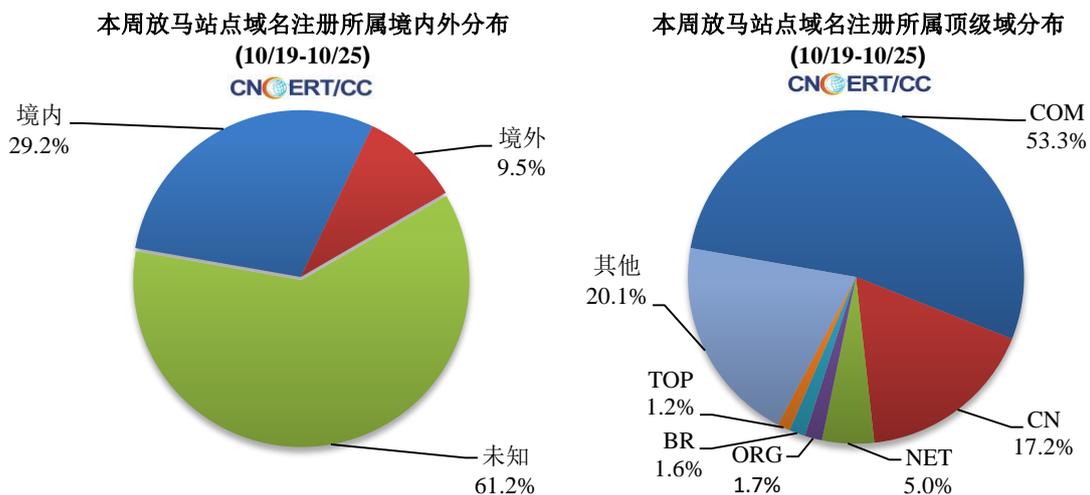
= 表示数量与上周相同 ↑ 表示数量较上周环比增加 ↓ 表示数量较上周环比减少

本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 44.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 38.2 万以及境内感染飞客（conficker）蠕虫的主机约 6.0 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 1802 个，涉及 IP 地址 11581 个。在 1802 个域名中，有 9.5% 为境外注册，且顶级域为 .com 的约占 53.3%；在 11581 个 IP 中，有约 24.4% 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 591 个 IP。



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>

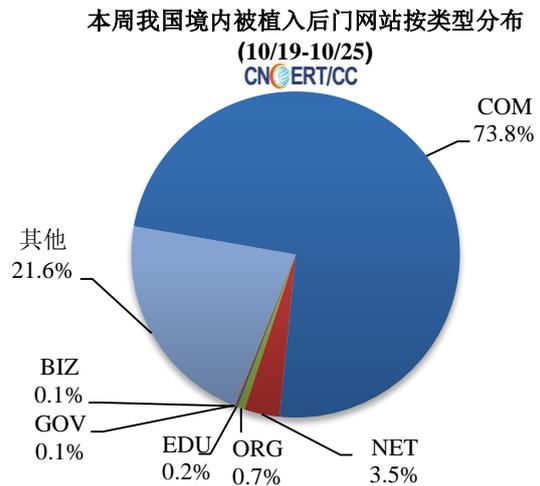
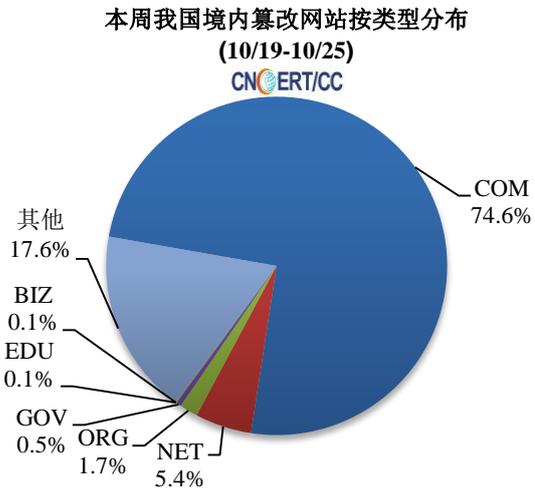
中国反网络病毒联盟 (Anti Network-Virus Alliance of China, 缩写 ANVA) 是由 CNCERT 发起并组织运作的行业联盟。

本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 5933 个；被植入后门的网站数量为 862 个；针对境内网站的仿冒页面数量 1500 个的仿冒页面。

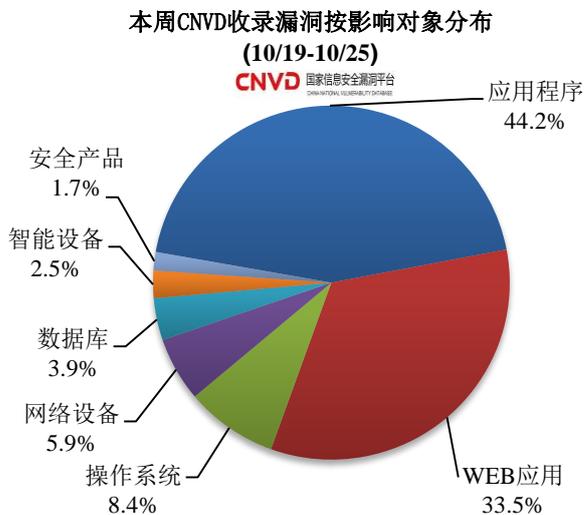
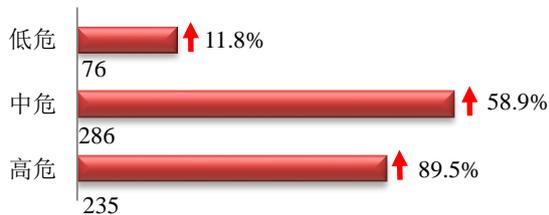


本周境内被篡改政府网站（GOV 类）数量为 28 个（约占境内 0.5%），较上周下降了 12.5%；境内被植入后门的政府网站（GOV 类）数量为 1 个（约占境内 0.1%），与上周持平。



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 597 个，信息安全漏洞威胁整体评价级别为中。



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 应用和操作系统。

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

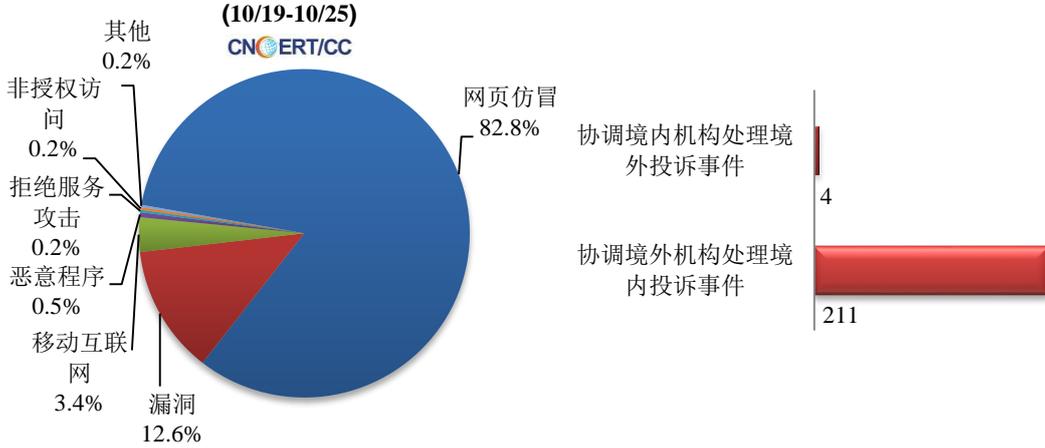
<http://www.cnvd.org.cn/webinfo/list?type=4>

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 412 起，其中跨境网络安全事件 215 起。

本周CNCERT处理的事件数量按类型分布

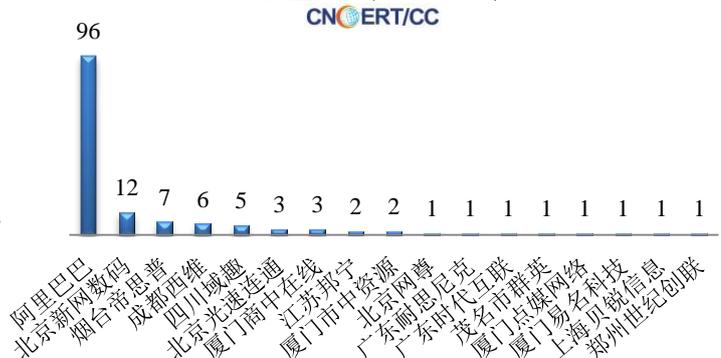


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 341 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 275 起、电子商务平台 64 起、证券 1 起以及其他事件 1 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计

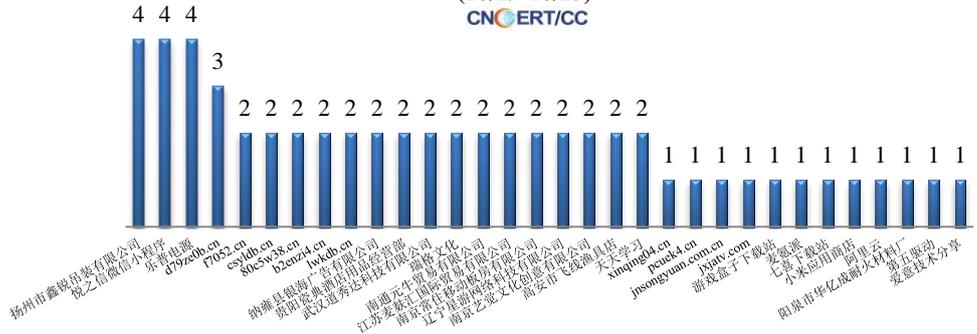


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (10/19-10/25)



本周，CNCERT 协调 32 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 59 个。

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
(10/19-10/25)



业界新闻速递

1. 个人信息保护法（草案）征求意见

10月29日，中国人大网消息，第十三届全国人大常委会第二十二次会议对《中华人民共和国个人信息保护法（草案）》进行了审议。现将《中华人民共和国个人信息保护法（草案）》在中国人大网公布，社会公众可以直接登录中国人大网（www.npc.gov.cn）提出意见，也可以将意见寄送全国人大常委会法制工作委员会（北京市西城区前门西大街1号，邮编：100805。信封上请注明个人信息保护法草案征求意见）。征求意见截止日期：2020年11月19日。

2. 工信部发布 2020 年第五批关于侵害用户权益行为的 APP 通报

10月27日，工信部官网消息，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〔2020〕164号）工作部署，工信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。通报表示，截至目前，尚有131款APP未完成整改，并要求APP应在11月2日前完成整改落实工作。此次检测中，输入法类、旅游出行类、电商类、音视频类等APP检测发现问题较多，部分应用商店及移动应用分发平台管理主体责任缺位，SDK企业存在违规收集用户个人信息的行为。后续工信部将对问题突出、有令不行、整改不彻底的相关企业，采取全面下架、停止接入、行政处罚以及纳入电信业务经营不良名单或失信名单等措施，依法严厉处置。

3. 芬兰心理治疗公司 Vastaamo 遭数据泄露

10月21日，Newsnowfinland网站消息，芬兰心理治疗公司 Vastaamo 表示遭遇数据泄露，黑客利用其客户的个人信息进行勒索。黑客与该公司患者联系称他们已获得客户详细信息。该公司目前通知了

芬兰网络安全应急中心，并与独立的安全专家合作对该事件进行调查。该公司表示，目前尚不清楚黑客窃取了患者病历数量以及入侵数据系统的时间。

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 and 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：胡俊

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315