国家互联网应急中心

网络安全信息与动态周报

2017 年第 42 期

10 月 9 日-10 月 15 日

CNCERT/CC

本周网络安全基本态势

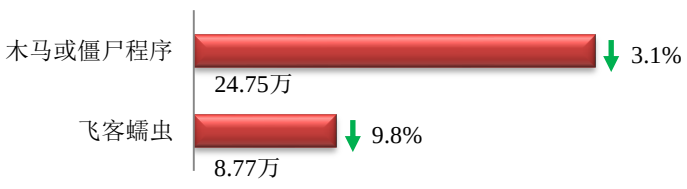
境内感染网络病毒的主机数量	•33.52万	↓ 4.9%
境内被篡改网站总数 其中政府网站数量	•2758 •64	↑ 0.2% ↑ 45.5%
境内被植入后门网站总数 其中政府网站数量	•853 •42	↑ 11.5% ↑ 23.5%
针对境内网站的仿冒页面数量	•333	↑ 32.7%
新增信息安全漏洞数量 其中高危漏洞数量	•219 •88	↓ 33.2% ↓ 26.1%

v

═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

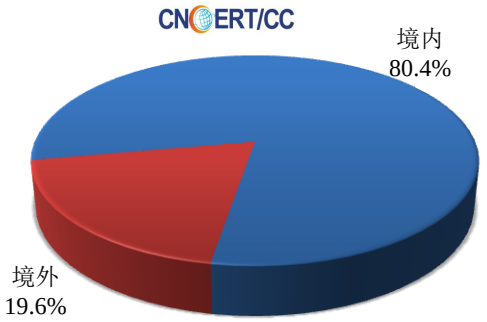
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 33.52 万个，其中包括境内被木马或被僵尸程序控制的主机约 24.75 万以及境内感染飞客（conficker）蠕虫的主机约 8.77 万。

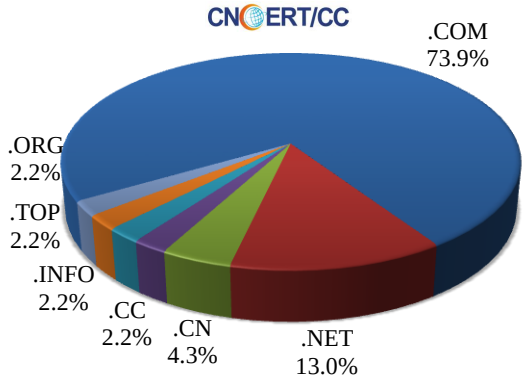


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 46 个，涉及 IP 地址 348 个。在 46 个域名中，有 19.6%为境外注册，且顶级域为.com 的约占 73.9%；在 348 个 IP 中，有约 6.9%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 2 个 IP。

本周放马站点域名注册所属境内外分布
(10/9-10/15)



本周放马站点域名所属顶级域的分布
(10/9-10/15)



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。

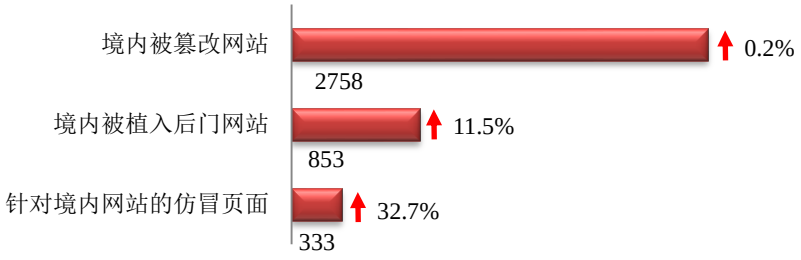
ANVA恶意地址黑名单发布地址

http://www.anva.org.cn/virusAddress/listBlack

中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由中国互联网协会网络与信息安全工作委员会发起、CNCERT 具体组织运作的行业联盟。

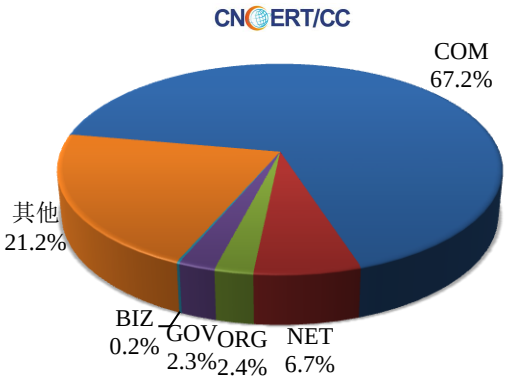
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2758 个；境内被植入后门的网站数量为 853 个；针对境内网站的仿冒页面数量为 333。

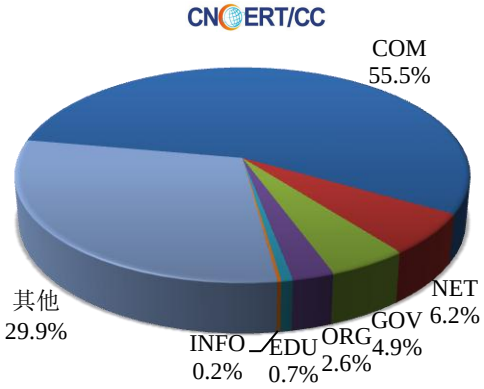


本周境内被篡改政府网站（GOV 类）数量为 64 个（约占境内 2.3%），较上周环比上升了 45.5%；境内被植入后门的政府网站（GOV 类）数量为 42 个（约占境内 4.9%），较上周环比上升了 23.5%；针对境内网站的仿冒页面涉及域名 287 个，IP 地址 136 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被篡改网站按类型分布
(10/9-10/15)

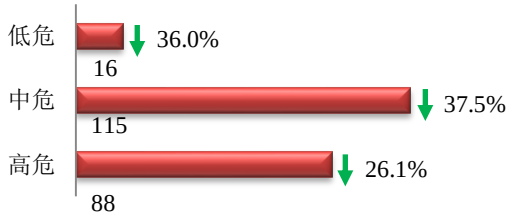


本周我国境内被植入后门网站按类型分布
(10/9-10/15)

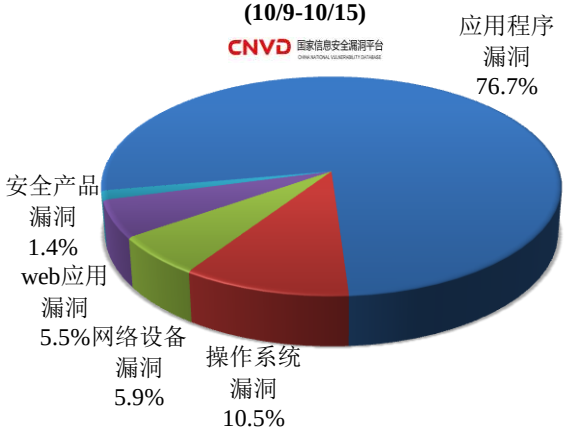


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 219 个，信息安全漏洞威胁整体评价级别为高。



本周CNVD收录漏洞按影响对象类型分布
(10/9-10/15)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是操作系统漏洞和网络设备漏洞。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

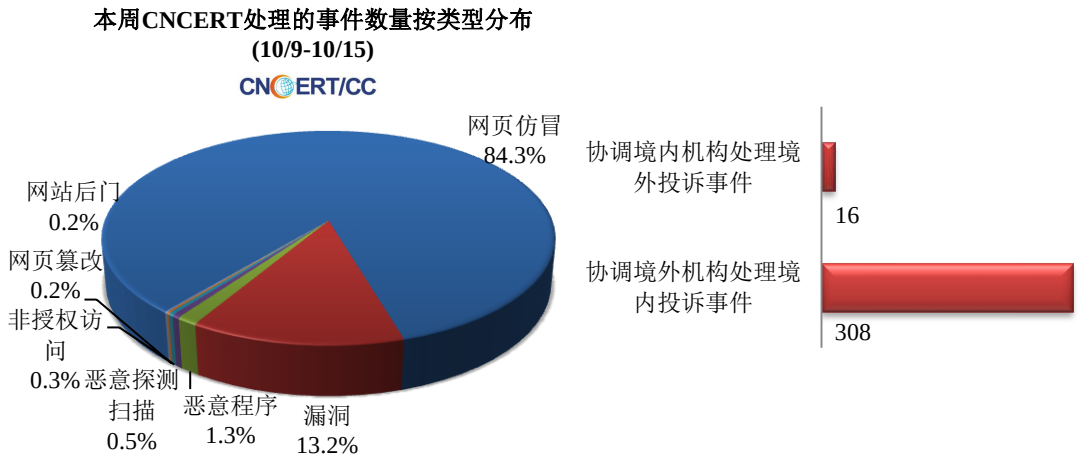
CNVD漏洞周报发布地址

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、基础电信运营商、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。

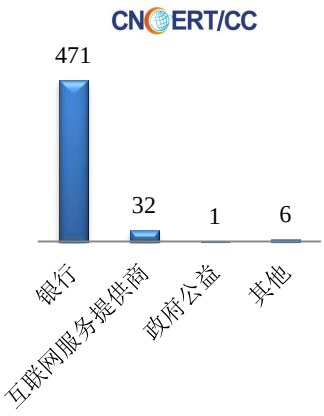
本周事件处理情况

本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 605 起，其中跨境网络安全事件 324 起。

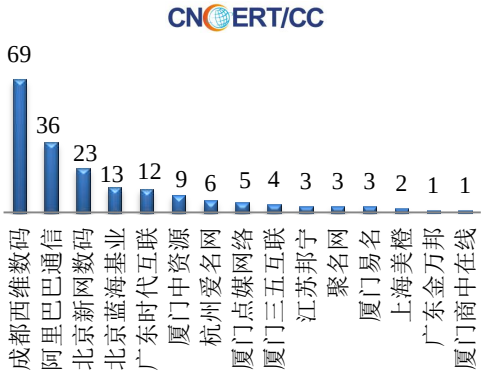


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 510 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 471 起和互联网服务提供商仿冒事件 32 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(10/9-10/15)

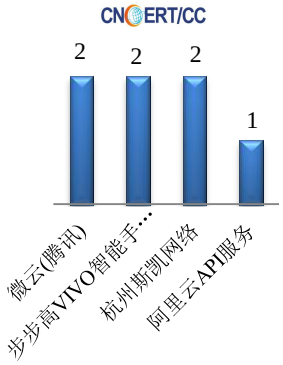


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (10/9-10/15)



本周，CNCERT 协调 4 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 7 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 (10/9-10/15)



业界新闻速递

1、全球网络安全合作计划（Epic）正式启动

E 安全 10 月 14 日消息 世界各地网络安全生态系统已经启动，旨在加强各区域生态系统间的协作关系。来自 14 个创始网络安全生态系统中多数区域的代表已经在本届于克拉科夫召开的 CyberSec 欧洲网络安全论坛上签署一份意向书，计划建立新的全球性安全协作组织。这一创新与网络安全生态系统平台全球生态系统（简称全球 Epic）将着眼于共同建立全球生态系统，同时采用足以改变世界的各类解决方案以应对高影响网络安全挑战。结合各方的知识、经验与专业技能，全球 Epic 将共同开发出创新型解决方案，推动知识共享，执行趋势分析，同时研究、影响并设立全球层面安全标准。各创始生态系统来自跨越三大洲的共十个国家，这亦反映出该平台的全球性特征。目前的 14 大创始生态系统分别为：Cyberspark（以色列）、安全信息技术中心（英国）、The Hague Security Delta（荷兰）、全球网络安全资源——卡尔顿大学（加拿大）、新不伦瑞克大学（加拿大）、CyberTech Network（美国）、科西斯科学院（波兰）、托里诺政治理事会（意大利）、La Fundación Incyde（西班牙）、Cyber

Wales（英国）、bwtech@UMBC（美国）、Procomer（哥斯达黎加）、Innovation Boulevard Surrey、BC（加拿大）、CSA（新加坡）。

2、澳大利亚发布《关键基础设施安全法案》草案公开征询意见

E 安全 10 月 12 日消息 澳大利亚总检察长乔治·布兰迪斯发布《关键基础设施安全法案》公开草案。法案旨在管理外国对澳大利亚关键基础设施带来的破坏、间谍和胁迫性国家安全风险。澳大利亚政府发布草案，公开征询意见，书面意见提交截止时间为 2017 年 11 月 10 日。法案将创建关键基础设施相关的国家安全风险管理框架，包括保存关键基础设施资产的资产登记信息，并启动部长级“终极权力”。该法案的重要部分在于确定关键基础设施的所有者和运营者。注释备忘录指出，澳大利亚政府并不知道关键基础设施资产的所有者，政府认为难以获取信息以保护这类资产。针对这一问题，法案将创建登记信息，登记关键基础设施资产的所有者、运营者或有权访问这些资产的各方。法案还提出“终极权力”，当政府别无它法时，让总检察长办公室出马缓解关键基础设施中发现的重大国家安全风险。

3、凯悦酒店集团支付系统再遭黑客入侵，旗下 41 家酒店客户信息在线泄露

HackerNews.cc10 月 15 日消息 凯悦酒店集团近期证实，旗下 41 家酒店的支付系统已遭黑客入侵，其中美国、中国、墨西哥等 11 个国家的客户数据在线泄露。然而，中国受影响情况最为严重，因为近一半受影响酒店位于中国境内。调查显示，受影响客户信息包括持卡人姓名、卡号、到期时间以及内部验证码。目前，凯悦酒店正与第三方安全专家、信用卡公司以及权威机构展开全面调查。据悉，安全研究人员在凯悦酒店的支付系统中发现未经授权的访问记录，其受访时间从今年 3 月 18 日至 7 月 2 日。此外，根据调查，他们了解到，这种未经授权的数据访问由第三方将恶意软件代码植入酒店 IT 系统造成。知情人士透露，凯悦开始向所有受害客户提供相关咨询，以便了解他们是否因此遭受黑客攻击以及其他可疑活动。目前，公司尚未透露多少客户在此次违规中可能受到影响。

4、银行窃贼运用新的透支技术盗取东欧银行 4000 多万美元

凤凰网 10 月 14 日消息 Trustwave SpiderLabs 10 月 10 日发布的报告显示，网络犯罪团伙使新招窃取东欧银行逾 4000 万美元（约合人民币 2 亿 6335 万元）。这帮黑客游刃有余地并用几大招数发起攻击：入侵银行网络+操纵透支额度+禁用欺诈提醒+从 ATM 机大笔提现。这类盗窃是目前为止最复杂的银行盗窃，与去年 SWIFT（全球金融电讯协会）惊天银行大劫案相当。这份报告显示，这一系列攻击今年 3 月开始爆发。SpiderLabs 网络威胁检测及响应副总裁 Brian Hussey（布莱恩·赫西）表示，发起这些攻击的黑客不是“独行侠”，而是组织严密的国际犯罪团伙所为。Hussey 称，所在公司调查了后苏联国家五家银行遭遇的盗窃案。攻击者从每家银行窃取了 300 万美元至 1000 万美元，已知黑客组织共盗取 4000 多万美元，但可能还存在其它受害银行。

5、47GB 医疗数据库泄露 含 15 万患者姓名和检查结果

cnBeta.COM10 月 11 日消息 近日据网络安全机构 Kromtech Security 的信息专家披露，一份包含 47GB 医疗数据文件的 Amazon S3 云存储对象提供公开访问，包含多达 315,363 份 PDF 档案，疑似为来自医疗设备公司 Patient Home Monitoring 的医疗数据存储纪录遭破解泄露，涉及近 15 万患者的姓名、地址、医生和病例纪录以

及周常血液检查结果等隐私信息。又是一起大规模的涉及公众隐私信息的泄露事件。Kromtech Security 公司指出该公司网站上的隐私相关页面，该公司保障患者拥有权利知晓谁访问了与其相关的医疗健康保密信息，以及以和目的访问。而这起大规模各种泄露事件无疑违反了这项隐私条例，也违背了美国 HIPAA 法案（健康保险携带和责任法案）。Kromtech 方面称它们在 9 月 29 日发现了该公司的相关文件被泄露，随后在 10 月 5 日以邮件形式通知了该公司的相关问题。但在 10 月 6 日，这份泄露数据库已经开启了公众访问，目前尚未消息披露谁破解并泄露了这份文件。

关于国家互联网应急中心（CNCERT）

国家互联网应急中心是国家计算机网络应急技术处理协调中心的简称（英文简称为 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，是一个非政府非盈利的网络安全技术协调组织，主要任务是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展中国互联网上网络安全事件的预防、发现、预警和协调处置等工作，以维护中国公共互联网环境的安全、保障基础信息网络和网上重要信息系统的安全运行。目前，CNCERT 在我国大陆 31 个省、自治区、直辖市设有分中心。

同时，CNCERT 积极开展国际合作，是中国处理网络安全事件的对外窗口。CNCERT 是国际著名网络安全合作组织 FIRST 正式成员，也是 APCERT 的发起人之一，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。截止 2016 年，CNCERT 与 69 个国家和地区的 185 个组织建立了“CNCERT 国际合作伙伴”关系。

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：高川

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158