国家互联网应急中心

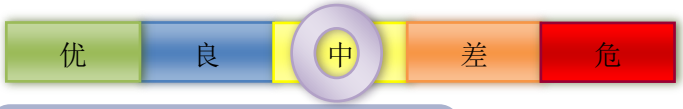
网络安全信息与动态周报

2019 年第 43 期

10 月 21 日-10 月 27 日

CNCERT/CC

本周网络安全基本态势

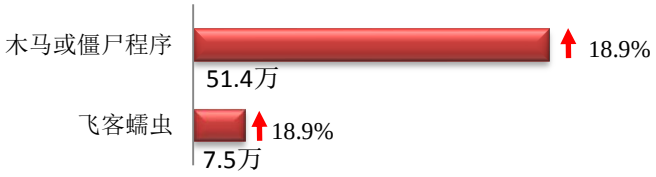


境内感染网络病毒的主机数量	•58.9 万	↑18.9%
境内被植入后门网站总数 其中政府网站数量	•3119 •32	↑59.2% ↑77.8%
针对境内网站的仿冒页面数量	•572	↓0.3%
新增信息安全漏洞数量 其中高危漏洞数量	•479 •125	↑18.0% ↑25.0%

═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

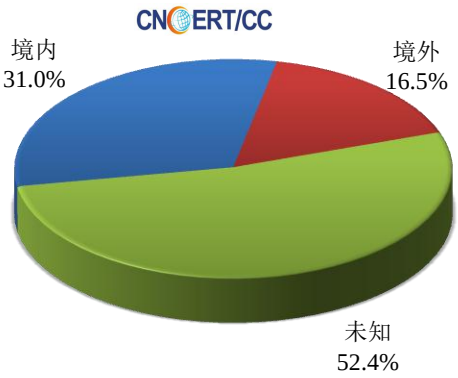
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 58.9 万个，其中包括境内被木马或被僵尸程序控制的主机约 51.4 万以及境内感染飞客（conficker）蠕虫的主机约 7.5 万。

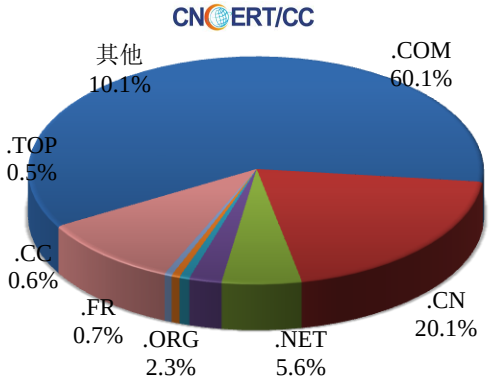


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 1695 个，涉及 IP 地 2805 个。在 1695 个域名中，有 16.5%为境外注册，且顶级域为.com 的约占 60.1%；在 2805 个 IP 中，有约 40.6%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 367 个 IP。

本周放马站点域名注册所属境内外分布
(10/21-10/27)



本周放马站点域名所属顶级域的分布
(10/21-10/27)



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。

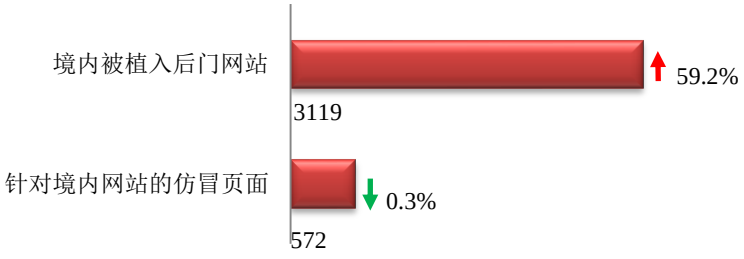
ANVA恶意地址黑名单发布地址

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。

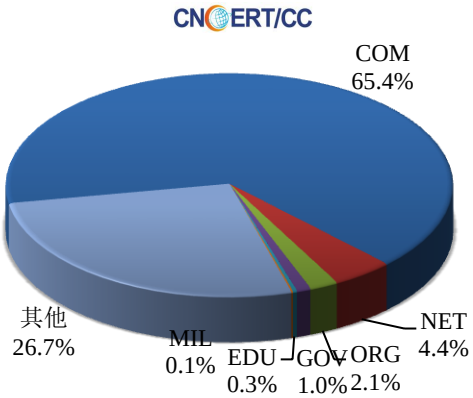
本周网站安全情况

本周 CNCERT 监测发现境内被植入后门的网站数量为 3119 个；针对境内网站的仿冒页面数量 572 个。



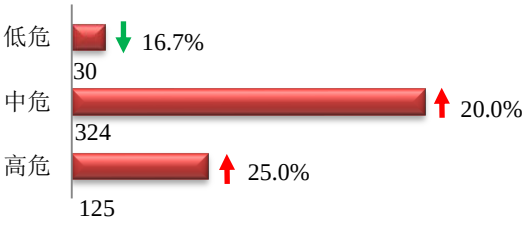
本周境内境内被植入后门的政府网站（GOV 类）数量为 32 个（约占境内 1.0%），较上周环比上涨 77.8%；针对境内网站的仿冒页面涉及域名 368 个，IP 地址 195 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被植入后门网站按类型分布
(10/21-10/27)

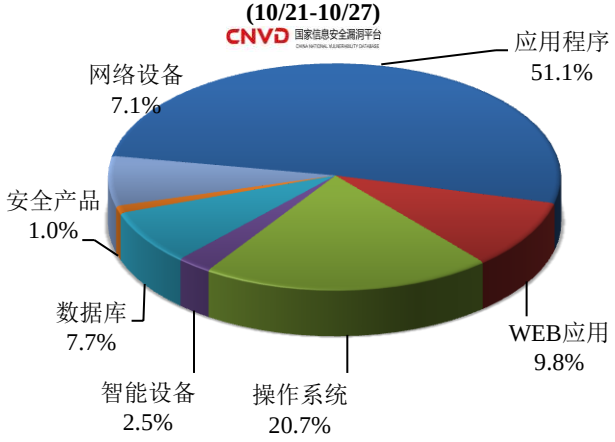


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 479 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类型分布
(10/21-10/27)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是操作系统和 WEB 应用漏洞。

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

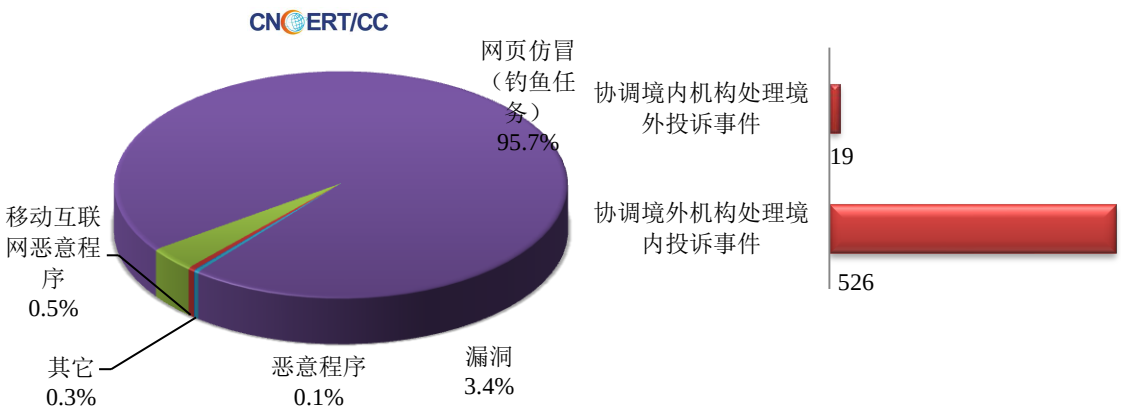
http://www.cnvd.org.cn/webinfo/list?type=4

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

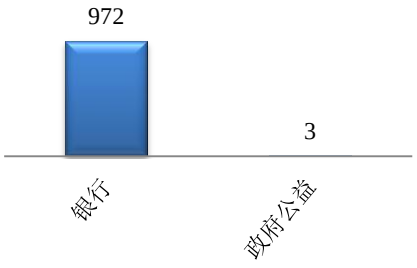
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 1049 起，其中跨境网络安全事件 545 起。

本周CNCERT处理的事件数量按类型分布
(10/21-10/27)

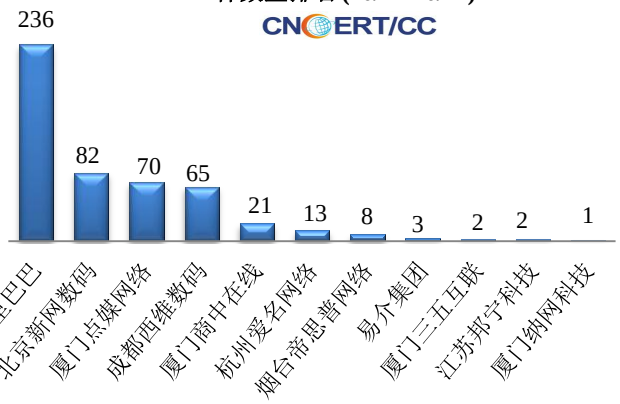


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 975 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 972 起和其他仿冒事件 3 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (10/21-10/27)

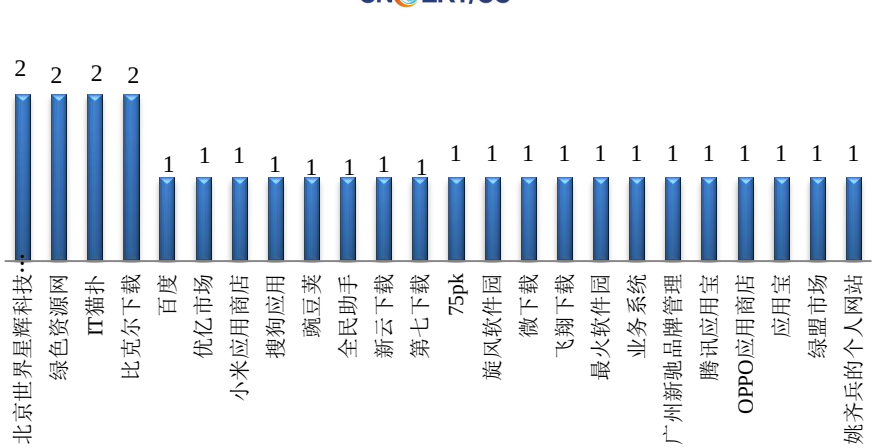


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (10/21-10/27)



本周，CNCERT 协调 24 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 28 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 (10/21-10/27)



业界新闻速递

1、 第六届世界互联网大会：网络安全技术发展和国际合作论坛 21 日在乌镇举行

10 月 23 日中国网信网消息，21 日上午，第六届世界互联网大会网络安全技术发展和国际合作论坛在浙江

乌镇举行。此次论坛由国家计算机网络应急技术处理协调中心主办，中国网络空间安全协会协办。论坛以“携手前行”为主题，围绕网络安全技术发展、网络安全国际合作两个领域展开交流对话，通过主旨发言与专家对话等形式，分享网络安全领域最新技术情况与最佳实践经验。

中央网络安全和信息化委员会办公室副主任、国家互联网信息办公室副主任盛荣华，全国政协委员、中国网络空间安全协会理事长王秀军出席论坛并致辞，柬埔寨电信管理局主席莫阿·查克利亚，中国工程院院士、清华大学计算机科学与技术系主任吴建平，中国工程院院士、浙江大学信息学部主任陈纯，国家计算机网络应急技术处理协调中心主任李湘宁等共 27 名国内外政府官员、国际组织代表、顶级专家学者、相关企业行业代表在论坛上围绕网络安全与国际合作展开深入交流。

2、 我国首部《密码法》表决通过，2020 年 1 月 1 日正式实施

10 月 26 日新华社消息，十三届全国人大常委会第十四次会议 26 日表决通过密码法，将自 2020 年 1 月 1 日起施行。密码法旨在规范密码应用和管理，促进密码事业发展，保障网络与信息安全，提升密码管理科学化、规范化、法治化水平，是我国密码领域的综合性、基础性法律。

该密码法共五章四十四条，分为总则部分、核心密码与普通密码部分、商用密码部分、法律责任部分以及附则部分，规定了国家密码管理部门的规章制定权，此外，为突显人才培养对于密码事业的重要性，密码法规定国家加强密码人才培养和队伍建设，对在密码工作中作出突出贡献的组织和个人，按照国家有关规定给予表彰和奖励。

3、 美智库发布深度伪造技术政策报告

10 月 23 日美国国际战略研究中心（CSIS）官网消息，美国国际战略研究中心发布《深度伪造技术政策简报》报告。“深度伪造”（Deepfake）是“深度学习”和“伪造”的混合词，即利用深度学习算法，实现音频和视频的模拟和伪造。报告分析了该技术对个人生活和民主国家的影响，指出出于政治目的伪造信息正在通过互联网迅速传播，破坏美国及其盟国的民主进程。同时，报告指出该技术存在有益用途，可应用于电影制作和医学成像等领域，建议政府应制定相关规则与法律，并提高辨别真伪的技术能力。

4、 美国防部将大规模研究 5G 技术的各种应用

10 月 23 日美国“Nextgov”网站消息，美国国防部当日宣布，在未来几个月内，它将开始“大规模”研究 5G 技术的各种应用。该项目最初将在四个尚未命名的国内军事设施中进行，并集中在三个领域：使用 5G 来扩大 VR 和 AR 系统在培训和任务规划中的使用；开发智能仓库以改善物流；探索共享不同类型频谱的新策略。据悉，国防部已经就这一计划征询了电信行业的意见，并利用他们的意见为该计划的初始设计提供了信息。

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。截至 2017 年，CNCERT 与 72 个国家和地区的 211 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：丁丽

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315