国家互联网应急中心

网络安全信息与动态周报

2017 年第 45 期

10 月 30 日-11 月 5 日

CNCERT/CC

本周网络安全基本态势

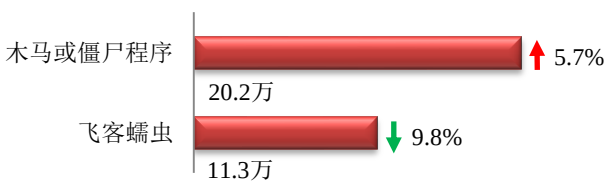
境内感染网络病毒的主机数量	•31.5万	0.4%
境内被篡改网站总数 其中政府网站数量	•1236 •40	10.9% 29.0%
境内被植入后门网站总数 其中政府网站数量	•727 •32	138.4% 190.9%
针对境内网站的仿冒页面数量	•312	14.3%
新增信息安全漏洞数量 其中高危漏洞数量	•455 •97	5.6% 23.6%

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

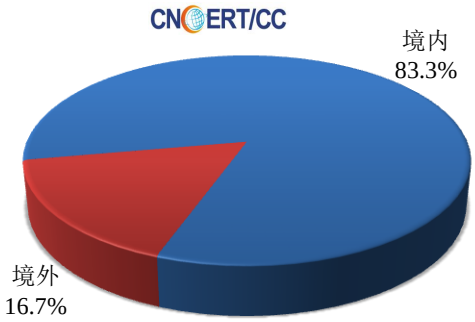
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 31.5 万个，其中包括境内被木马或被僵尸程序控制的主机约 20.2 万以及境内感染飞客（conficker）蠕虫的主机约 11.3 万。

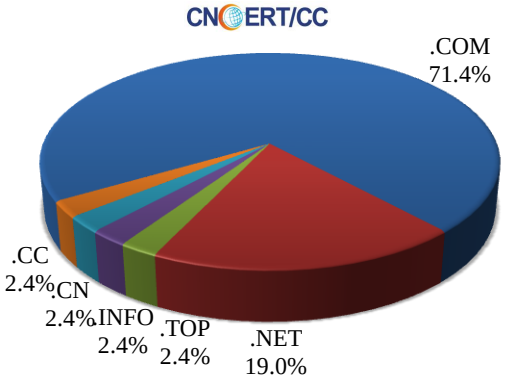


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 42 个，涉及 IP 地址 295 个。在 42 个域名中，有 16.7%为境外注册，且顶级域为.com 的约占 71.4%；在 295 个 IP 中，有约 30.2%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 1 个 IP。

本周放马站点域名注册所属境内外分布
(10/30-11/5)



本周放马站点域名所属顶级域的分布
(10/30-11/5)



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。

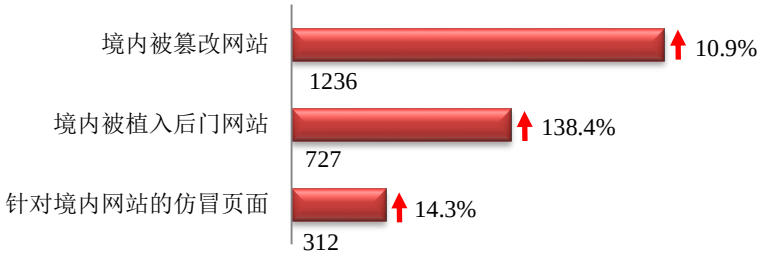
ANVA恶意地址黑名单发布地址

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。

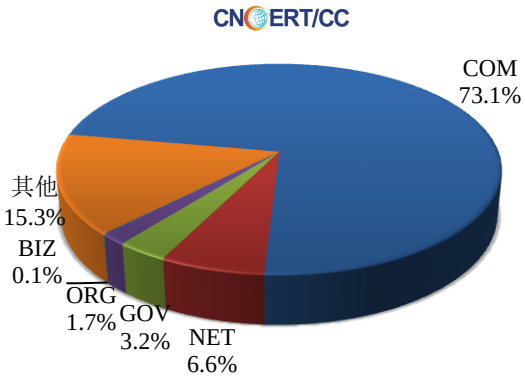
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1236 个；境内被植入后门的网站数量为 727 个；针对境内网站的仿冒页面数量为 312。

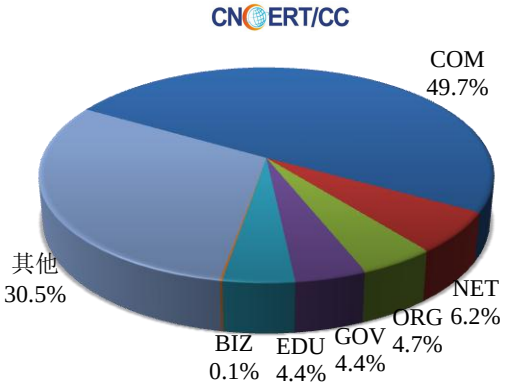


本周境内被篡改政府网站（GOV 类）数量为 40 个（约占境内 3.2%），较上周环比上升了 29.0%；境内被植入后门的政府网站（GOV 类）数量为 32 个（约占境内 4.4%），较上周环比上升了 190.9%；针对境内网站的仿冒页面涉及域名 276 个，IP 地址 115 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被篡改网站按类型分布
(10/30-11/5)

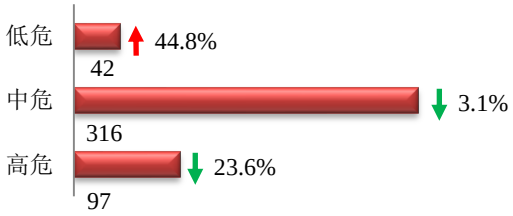


本周我国境内被植入后门网站按类型分布
(10/30-11/5)

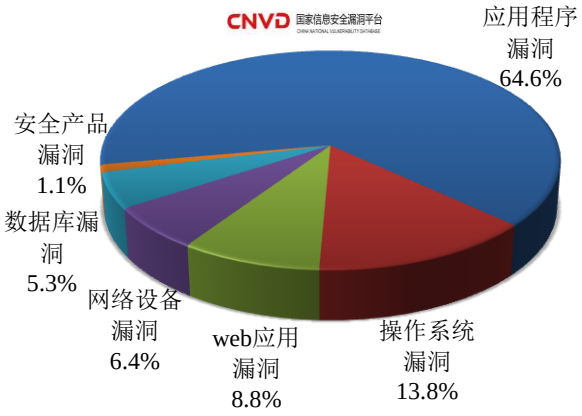


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 455 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
(10/30-11/5)



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 web 应用漏洞。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

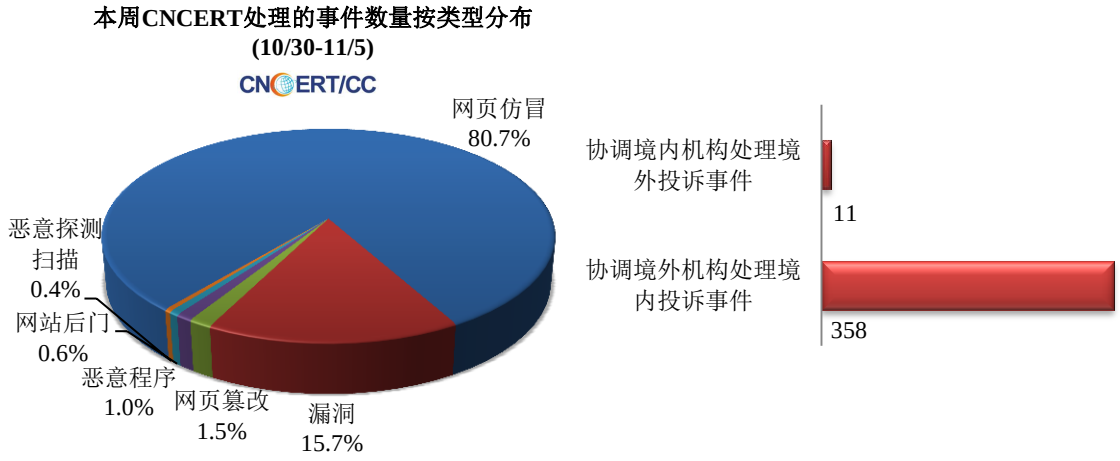
CNVD漏洞周报发布地址

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。

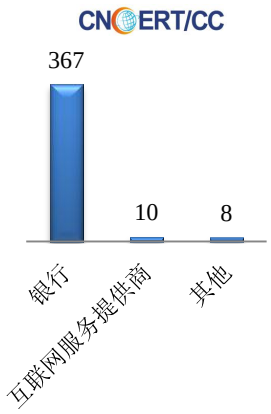
本周事件处理情况

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 477 起，其中跨境网络安全事件 369 起。

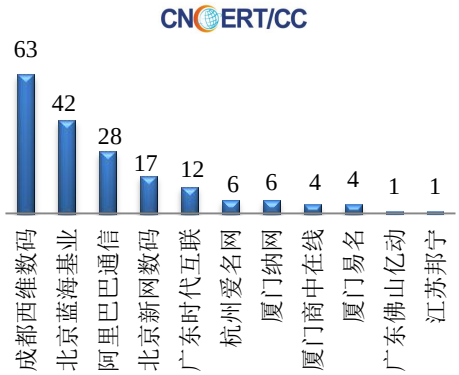


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 385 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 367 起和互联网服务提供商仿冒事件 10 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(10/30-11/5)

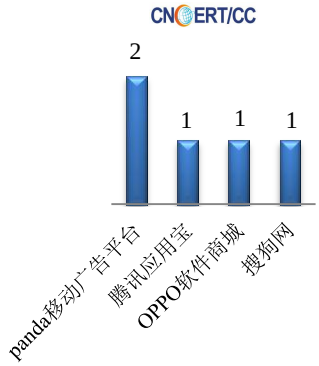


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (10/30-11/5)



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 5 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 (10/30-11/5)



业界新闻速递

1、俄副总理：中俄将探讨建造防范网络攻击的电信设备

环球网 10 月 30 日消息 据俄罗斯卫星网 10 月 30 日报道，俄罗斯副总理德米特里·罗戈津 10 月 30 日在俄中政府首脑会议筹备工作政府间委员会会议后向记者表示，两国商定就建造防范网络攻击的电信设备进行讨论。罗戈津表示：“双方约定，将在近期的俄中合作平台讨论建造信托电信设备的问题，以防止可能的网络攻击。”罗戈津强调，俄方与中方分享了有关针对中俄网络攻击事件数量的信息。俄认为在金砖合作机制的框架下，有充分的理由提出这一议题，并打造关键基础设施保护体系。

2、特朗普政府计划制定新的“网络安全战略”

E 安全 11 月 3 日消息 特朗普当局计划制定新的网络安全战略，该战略将以今年 5 月发布的总统行政令主要内容作为基础。白宫国土安全顾问 Tom Bossert（汤姆·博塞特）在本周二表示，主要考虑到奥巴马时代的网

络计划与战略正在新的历史背景下迅速过时，特朗普政府正在计划建立一项新的网络安全战略，该战略将遵循特朗普于今年 5 月发布的网络安全总统行政令大纲，但具体启动时间尚未确定。Bossert 在参加当天由 Palo Alto Networks 公司主办的华盛顿网络安全会议时指出，一旦完成这项有利于政府及国家的战略方案的筹备工作，会第一时间进行公布。他表示与此前的总统行政令一样，这项网络安全战略也很可能分为三大主要组成部分：提升联邦政府计算机网络安全性；利用政府资源更好地保护诸如医院、银行与金融企业等关键信息基础设施；在网络空间建立良好行为规范，同时惩治不良行为。

3、德以启动首个网络安全领域创新与合作“加速器”

新华网 11 月 3 日消息 德国与以色列的首个网络安全领域创新和研发合作项目“加速器”，11 月 2 日在位于耶路撒冷的希伯来大学正式启动。这一名为“黑森以色列网络安全合作加速器”的机构，由德国夫琅禾费安全信息技术研究所和希伯来大学网络安全研究中心共同建立。据悉，这一“加速器”将吸引来自德国和以色列的网络领域高端人才，共同致力于网络技术、互联网基础设施和软件安全等网络安全领域项目的创新与研发，并为高科技领域的初创企业提供更多进入市场的成功机会。据介绍，首批来自以色列和德国的 16 名参与者首先将接受为期两周的培训，然后开展为期两个月的、有针对性的创新技术研发和开发，成果将于明年 1 月在德国达姆施塔特市进行评定。

4、荷兰政府推出新法案，当局可拦截与分析互联网流量

E 安全 11 月 1 日消息 荷兰政府近期推出一项新法律法规——信息和安全服务法案（Wet op de inlichtingen-en veiligheidsdiensten），旨在赋予当局拦截与分析互联网流量的权限。尽管其他国家也有类似的法律，但该法律的特殊之处在于当局有权通过“伪造密钥”技术进行秘密攻击，从而获取网络犯罪分子加密通信数据。据悉，该法案将于 2018 年 1 月生效。然而，Mozilla 工程师担心荷兰当局会在该法案生效后通过当地政府运营的认证机构（CA）签发不信任证书，允许他们创建 SSL 代理并在网络监视行动中，对所有用户实施“中间人”（MitM）攻击。研究人员 Chris van Pelt 表示，如果政府继续在国家主要互联网传输节点上运行 CA 签发的证书，那么未来将会对所有 Mozilla 用户的安全造成损害。对此，Mozilla 与荷兰其他主要的浏览器厂商将逐步取消 HTTPS 提供商的支持，尽管这个过渡阶段极其缓慢。

5、印度成立道德黑客部队“卡其帽”，保护政府关键基础设施免受侵害

E 安全 11 月 1 日消息 印度警方高级官员表示，印度国家警方将创建一个由经认证的道德黑客组成的专门力量，用于保护喀拉拉邦的关键信息基础设施免受全球网络安全威胁的迅速变化。被称为“卡其帽（KH，Khaki Hats）”的部队将仅由选定的警务人员组成，他们能够熟练使用最新的渗透软件评估计算机网络的安全性。印度国家警方亟需拥有一直专门的黑客力量。理想情况下，警方希望 KH 能够成为网络犯罪调查国际合作安排的一部分。印度警方高级官员 Loknath Behera 和 Manoj Abraham 正在负责执行该计划。

6、伦敦希思罗机场大量安保信息遭泄露 或遭致命性打击

环球网 10 月 30 日消息 “伦敦希思罗机场大量安保信息遭泄露。”据英国《星期日镜报》10 月 28 日报道，泄露信息包括英国女王及各国政要进出希思罗机场的路径、安保措施等机密信息。事件被曝光后，机场和英国

安全部门高度紧张，机场表示正在对内部人员进行“紧急调查”。报道称，一名伦敦市民近日在一处道路上捡到一个 U 盘，后来发现该 U 盘中有 76 个文件夹，共有 170 多个文件，包括地图、文字资料和视频等。这些内容有 2.5G，没有进行加密，U 盘也没有登录密码。 拾到 U 盘的居民将其交给《星期日镜报》，而该报则将相关信息通知机场和英国安保部门。希思罗机场表示正在对事件展开彻查，而不愿透露身份的英国安全部门人士认为，这次事件表明，该机场的安全存在很大的漏洞。英国警方担心，这些信息可能已经被一些人复制，并在“暗网”上出售。如果这些信息落入恐怖分子之手，那对于希思罗机场乃至英国政要的安全，都是致命性的打击。

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：刘立伟

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158