国家互联网应急中心

网络安全信息与动态周报

2017 年第 46 期

11 月 6 日-11 月 12 日

CNCERT/CC

本周网络安全基本态势

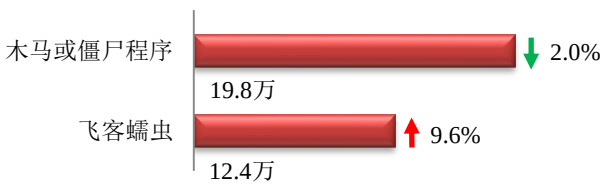
境内感染网络病毒的主机数量	• 32.2万	↑ 2.2%
境内被篡改网站总数 其中政府网站数量	• 1665 • 53	↑ 34.7% ↑ 32.5%
境内被植入后门网站总数 其中政府网站数量	• 785 • 29	↑ 8.0% ↓ 9.4%
针对境内网站的仿冒页面数量	• 347	↑ 11.2%
新增信息安全漏洞数量 其中高危漏洞数量	• 534 • 153	↑ 17.4% ↑ 57.7%

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

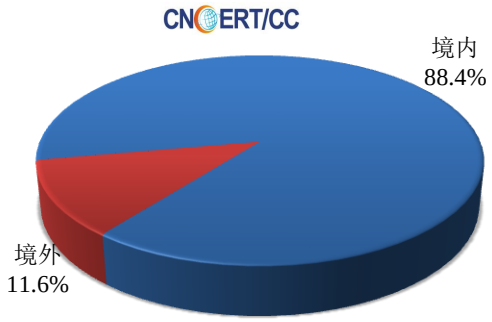
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 32.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 19.8 万以及境内感染飞客（conficker）蠕虫的主机约 12.4 万。

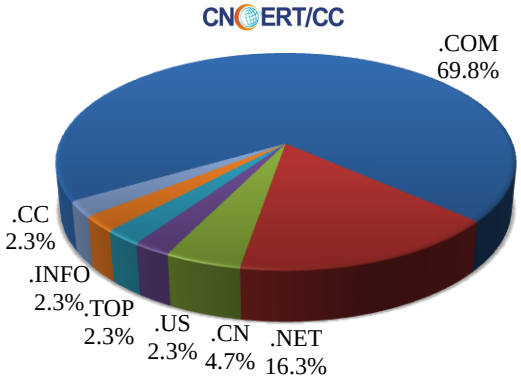


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 43 个，涉及 IP 地址 261 个。在 43 个域名中，有 11.6%为境外注册，且顶级域为.com 的约占 69.8%；在 261 个 IP 中，有约 33.3%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 3 个 IP。

本周放马站点域名注册所属境内外分布
(11/6-11/12)



本周放马站点域名所属顶级域的分布
(11/6-11/12)



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。

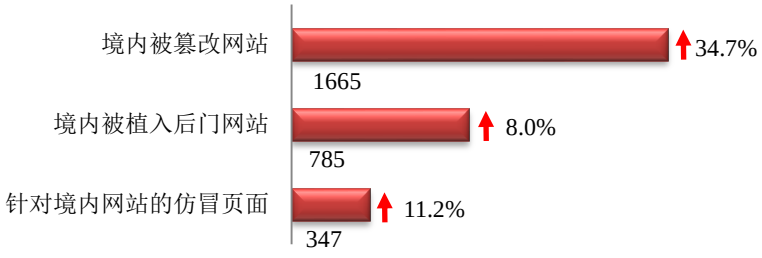
ANVA恶意地址黑名单发布地址

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。

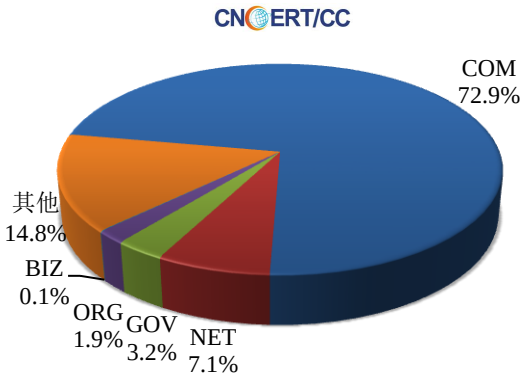
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1665 个；境内被植入后门的网站数量为 785 个；针对境内网站的仿冒页面数量为 347。

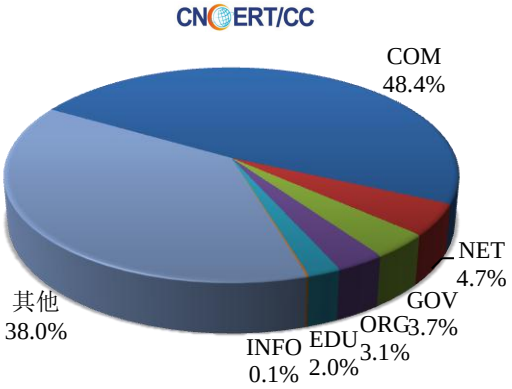


本周境内被篡改政府网站（GOV 类）数量为 53 个（约占境内 3.2%），较上周环比上升了 32.5%；境内被植入后门的政府网站（GOV 类）数量为 29 个（约占境内 3.7%），较上周环比下降了 9.4%；针对境内网站的仿冒页面涉及域名 280 个，IP 地址 124 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被篡改网站按类型分布
(11/6-11/12)

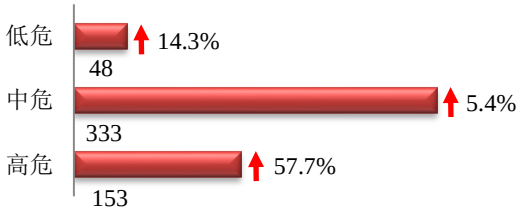


本周我国境内被植入后门网站按类型分布
(11/6-11/12)

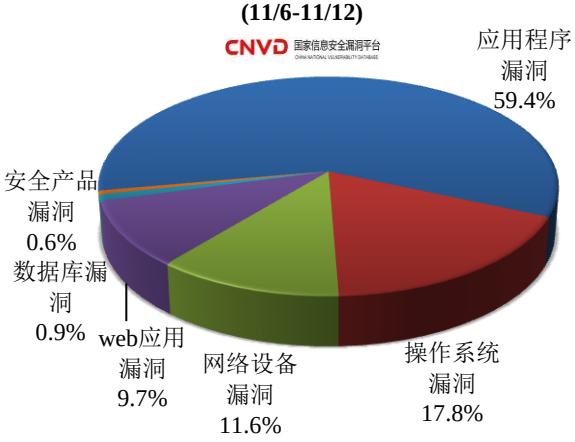


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 534 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
(11/6-11/12)



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。

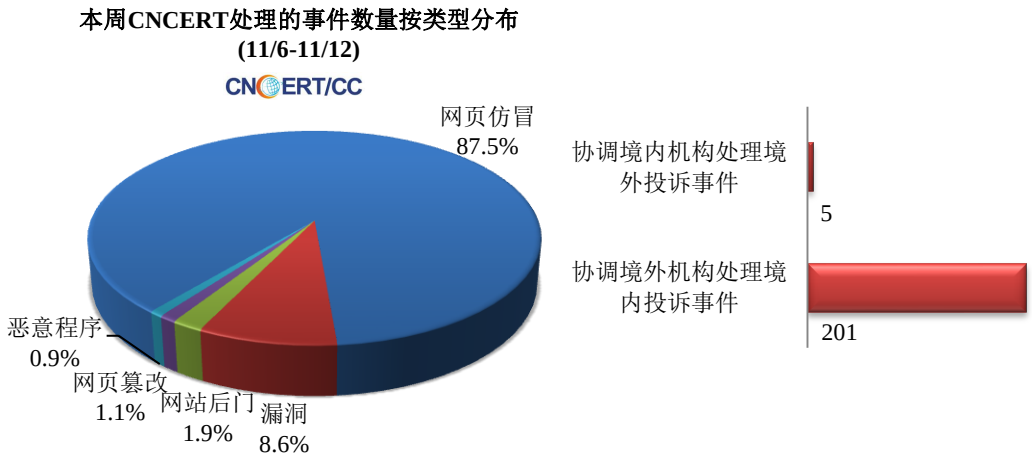
CNVD漏洞周报发布地址

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。

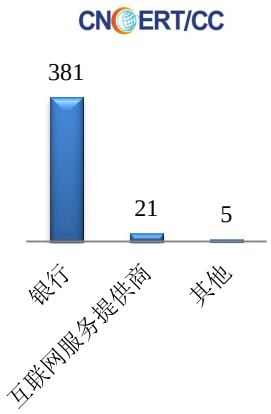
本周事件处理情况

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 465 起，其中跨境网络安全事件 206 起。

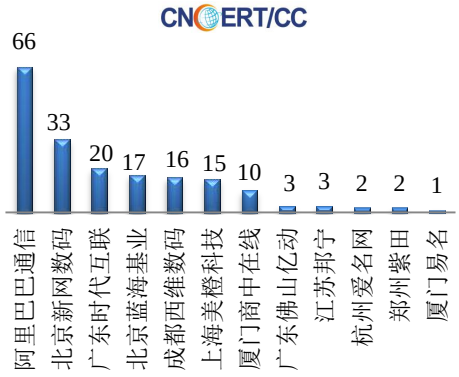


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 407 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 381 起和互联网服务提供商仿冒事件 21 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(11/6-11/12)

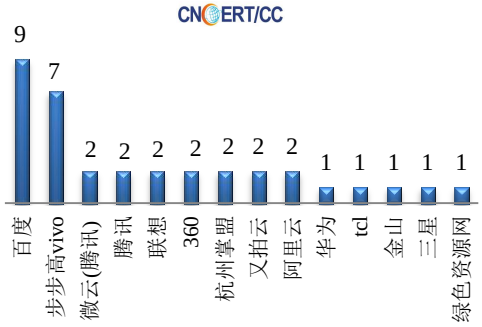


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (11/6-11/12)



本周，CNCERT 协调 14 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 35 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 (11/6-11/12)



业界新闻速递

1、新加坡立法严格限制企业使用国民身份证权限，以防个人信息盗窃、欺诈等非法活动

HackerNews.cc11 月 10 日消息 新加坡个人数据保护委员会（PDPC）于近期正在修订国家“个人数据保护法案”（PDPA）指导方针，意在严格限制企业使用国民身份证（NRIC）权限，以防各组织或个人信息被用于盗窃、欺诈等非法活动。与此同时，该国还提出一项新安全法案，希望能够削减官僚作风、缓解各政府公共部门的数据共享问题。个人数据保护法案（PDPA）的指导方针是专门为收集、使用和披露国家公民身份证号码的企业提供规范式管理。PDPC 表示，部分常见的商业惯例将在法案修订后不得不进行更改。不过，使用 NRIC 号码仍然是验证个人身份的必要手段。目前，由于企业获取公民身份证号码的服务种类繁多，因此 PDPC 有必要审查涉及其应用的指导方针。

2、“五眼联盟”顶级黑客检验美军网络防御力

人民网 11 月 10 日消息 前不久，美军邀请“五眼联盟”的数百名顶级黑客，开展了为期数周的“黑进”美国国防部、空军和陆军网络挑战大赛，以检验美军真实的网络防御能力。“五眼联盟”是美国主导的包括英国、加拿大、澳大利亚和新西兰在内的监听组织“UKUSA”，他们共享网络漏洞等情报，是网络空间行动的盟友。美军称此次行动取得了不错的效果，“黑进五角大楼”发现了 138 个漏洞，“黑进空军”发现了 207 个漏洞，“黑进陆军”发现了 118 个漏洞。这些网络漏洞的发现，帮助美军消除了网络空间安全的潜在威胁，修复了美军网络的脆弱性。

3、北约拟增设两个司令部重视网络安全防御

E 安全 11 月 10 日消息 北大西洋公约组织（NATO，简称北约）11 月 8 日在布鲁塞尔总部召开防长会，计划增设两个司令部，这是北约自“冷战”结束以来首次改革指挥架构，并在与俄罗斯地缘政治关系紧张之际，加大对网络防御的重视。北约防长同意增设两个司令部，从原来的七个增加到九个。其中一个新设指挥中心将重点关注大西洋的海事安全，另一个将负责欧洲的军力调动。新设司令部的选址将会在明年敲定。在本周三在布鲁塞尔举行的会议上，北约防长还决定将网络纳入北约所有行动中，与传统的海、陆、空领域并重。北约秘书长 Jens Stoltenberg（延斯·斯托尔腾贝格）指出，改革指挥架构的目的在于提升北约的网络领域实力至可与海、陆、空威慑力相当的水平。

4、英国协助卡塔尔制定金融行业网络安全标准

E 安全 11 月 7 日消息 英国网络安全大使 Conrad Prince（康拉德·普林斯）表示，英国已向卡塔尔提供专业知识，帮助对方制定并实施适当的网络安全标准。Prince 强调英格兰银行（BoE）推出的新框架“CBest”，其旨在帮助识别金融行业哪些方面易遭遇复杂的网络攻击。该框架利用政府和商业提供商的情报识别针对特定金融机构的潜在攻击者。Prince 在卡塔尔央行组织的第四届年度信息安全会议上表示，英国政府、英格兰银行和 Crest 致力于与卡塔尔合作，支持制定并实施类似的标准，以改进金融行业的信息安全。英格兰银行已与道德安全测试员理事会（Crest）和网络情报公司 Digital Shadows 合作制定新的认证标准。Prince 补充称，这是英国和卡塔尔共同努力改善在金融服务行业网络安全方面互相保护的方式。他对英国与卡塔尔在关键和重要的网络安全方面的合作持乐观态度。

5、尼泊尔 NIC 亚洲银行 SWIFT 遭入侵

搜狐网 11 月 8 日消息 11 月 5 日消息，尼泊尔 NIC 亚洲银行（NIC Asia Bank）的安全专家近期发现 SWIFT 服务器遭到黑客入侵，被盗资金高达 4.6 亿卢比（约合 4700 万 RMB ），随后仅追回 1.1 亿卢比。该机构已向尼泊尔中央调查局请求支持，以便追查那些入侵 SWIFT 服务器的犯罪踪迹。据悉，NIC 亚洲银行在印度毕马威会计师事务所的支持下申请了法庭调查，并将其结果提交至尼泊尔中央银行与中央调查局进行后续审查。尼泊尔副检察长兼刑事情报科（CIB）负责人 Pushkar Karki 证实，NIC 亚洲银行支付系统确实遭到黑客攻击，当前 CIB 已经开始展开调查，之后安全专家将根据结果针对银行采取适当保护措施。NIC 亚洲银行在通知监管机构之后，中央银行立即进行了一项单独的调查。其结果显示，由于操控 NIC 亚洲银行 SWIFT 系统的工作人员使用了一台专门运营 SWIFT 的设备处理其他事务，因此导致黑客有机可图。

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：张艳茹

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158