国家互联网应急中心

网络安全信息与动态周报

2017 年第 44 期

10 月 23 日-10 月 29 日

CNCERT/CC

本周网络安全基本态势

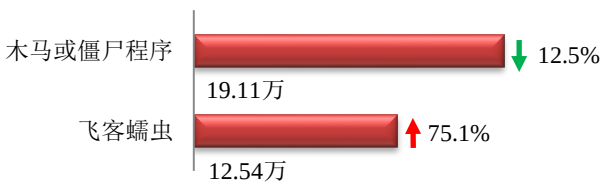
境内感染网络病毒的主机数量	•31.65万	9.2%
境内被篡改网站总数 其中政府网站数量	•1115 •31	30.6% 29.5%
境内被植入后门网站总数 其中政府网站数量	•305 •11	45.7% 65.6%
针对境内网站的仿冒页面数量	•273	16.0%
新增信息安全漏洞数量 其中高危漏洞数量	•482 •127	19.3% 11.4%

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

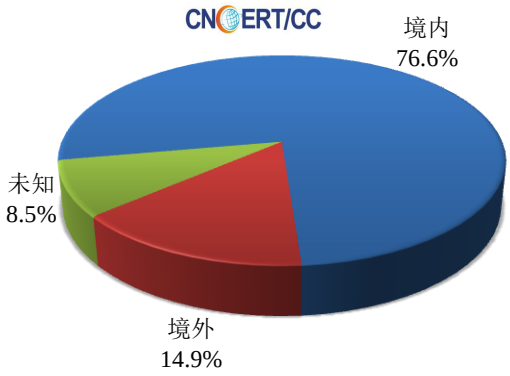
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 31.65 万个，其中包括境内被木马或被僵尸程序控制的主机约 19.11 万以及境内感染飞客（conficker）蠕虫的主机约 12.54 万。

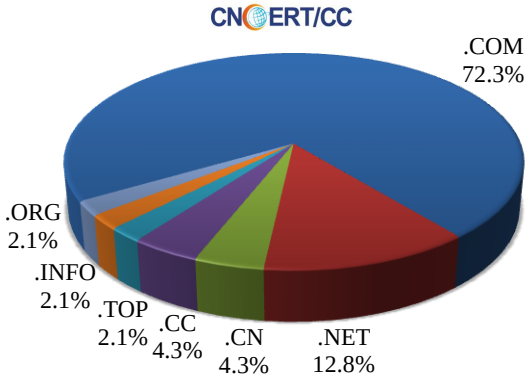


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 47 个，涉及 IP 地址 296 个。在 47 个域名中，有 14.9%为境外注册，且顶级域为.com 的约占 72.3%；在 296 个 IP 中，有约 32.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 4 个 IP。

本周放马站点域名注册所属境内外分布
(10/23-10/29)



本周放马站点域名所属顶级域的分布
(10/23-10/29)



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。

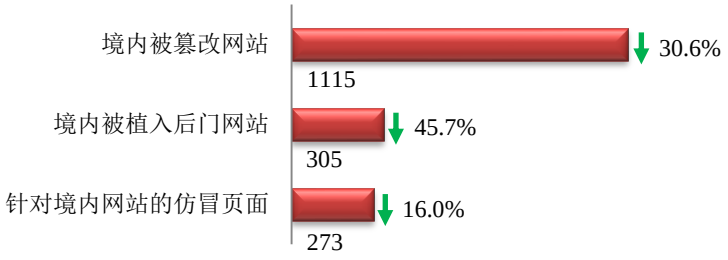
ANVA恶意地址黑名单发布地址

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。

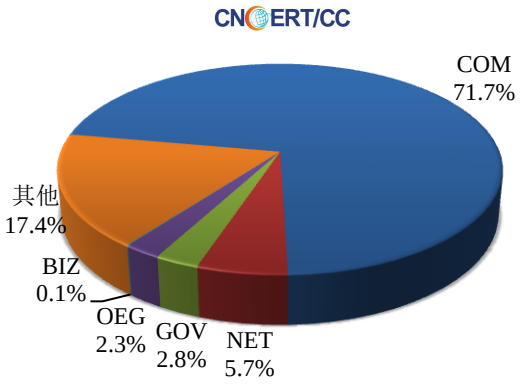
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1115 个；境内被植入后门的网站数量为 305 个；针对境内网站的仿冒页面数量为 273。

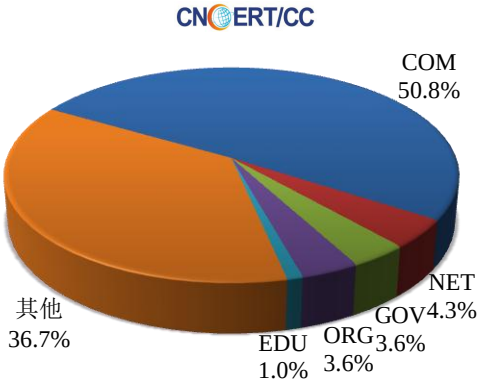


本周境内被篡改政府网站（GOV 类）数量为 31 个（约占境内 2.8%），较上周环比下降了 29.5%；境内被植入后门的政府网站（GOV 类）数量为 11 个（约占境内 3.6%），较上周环比下降了 65.6%；针对境内网站的仿冒页面涉及域名 238 个，IP 地址 96 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被篡改网站按类型分布
(10/23-10/29)

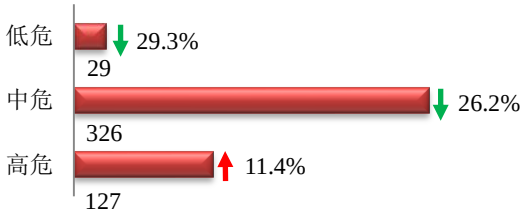


本周我国境内被植入后门网站按类型分布
(10/23-10/29)

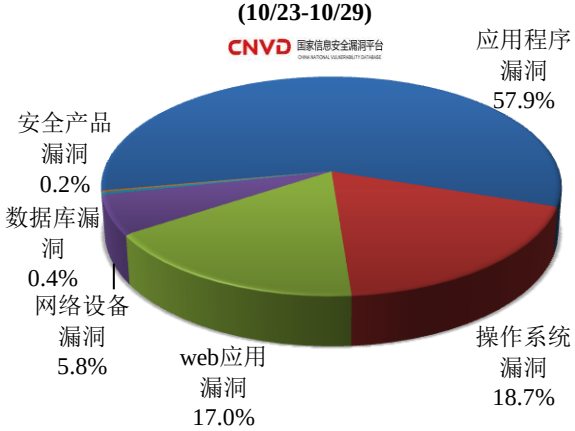


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 482 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
(10/23-10/29)



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。

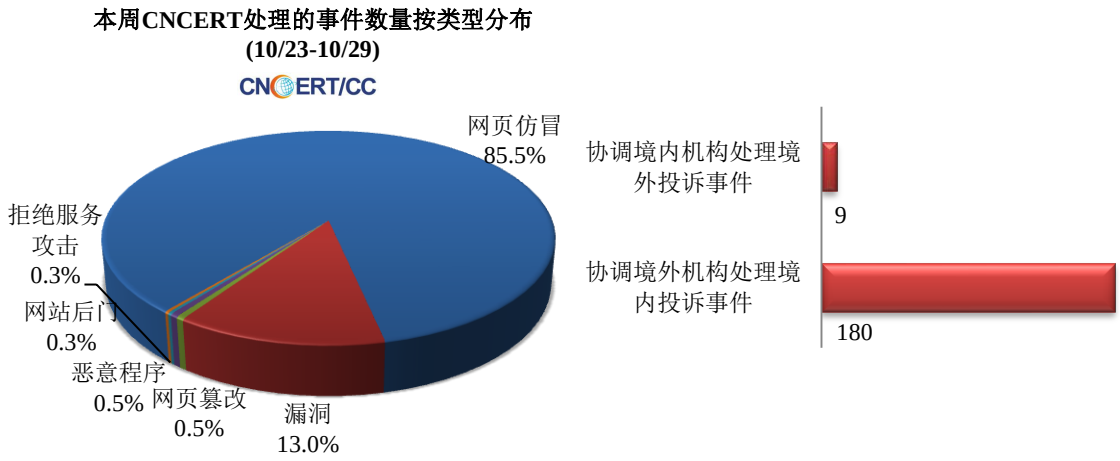
CNVD漏洞周报发布地址

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。

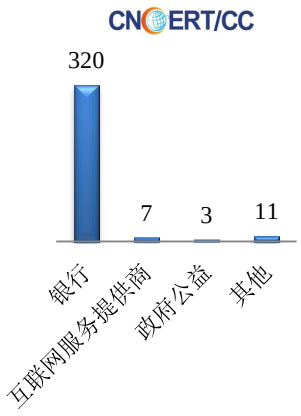
本周事件处理情况

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 399 起，其中跨境网络安全事件 189 起。

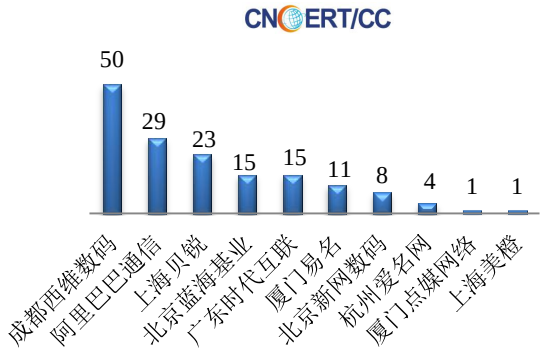


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 341 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 320 起和互联网服务提供商仿冒事件 7 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(10/23-10/29)

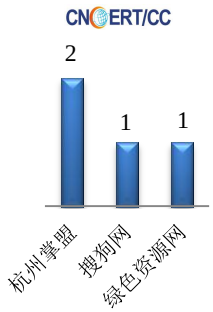


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (10/23-10/29)



本周，CNCERT 协调 3 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 4 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 (10/23-10/29)



业界新闻速递

1、美参议院情报委员会通过新的《外国情报监视法》

中新网 10 月 25 日消息 当地时间 10 月 24 日，美国参议院情报委员会以 12 票赞成、3 票反对，通过了更新的《外国情报监视法》（FISA）。据报道，FISA 的第 702 条允许政府对美国境内的外籍人士实施监控，以获取情报，用于打击国际恐怖主义和网络威胁。该法案的目前版本将于 2017 年底失效，参议员们提议修改并延长该法案有效期至 2025 年。美国参议院情报委员会主席理查德•伯尔说：“这项议案再次授权给我们国家最有价值的情报搜集机构，确保情报委员会和执法部门的每一个人都有所需的工具和权力，来保障我们的安全。”据报道，更新的法案加入了参议员马克•沃纳的提案。该提案规定，若联邦调查局（FBI）在调查中需要查看和使用美国人的信息，需要在一个工作日内向外国情报监视法庭提交申请，后者则有两个工作日来裁决。而分析指出，任何基于国外情报和执法要求的申请都是合法的，也就意味着基本上所有的申请都会得到批准。美国中央情报局、国家安全局前雇员爱德华 • 斯诺登对此前公众未知的监听项目进行披露后，美对法案进行了修正，该法案以第

702 条法规而闻名。

2、英国新法案引争议：黑客攻击受害者将获精神赔偿

环球网 10 月 23 日消息 今年夏季，英国政府推出最新版《数据保护法案》，首次将“精神损失”纳入索赔范畴，但却引发不小的争议。英国《每日邮报》22 日报道称，根据英国现行法律，黑客攻击受害者只有在经济利益受到侵害，如银行账户被“洗劫”时方可提出索赔。但最新法案明确提出，受害者只要蒙受“精神或心理伤害”便可提出经济赔偿，赔偿数额视遭入侵数据的“敏感度”而定，最高可达 6000 英镑（约合人民币 5.2 万元）。不仅如此，当局对存在网络安全疏漏的公司也将提高罚款力度。最新版《数据保护法案》预计将于明年同欧盟组织的《数据保护通用条例》同步实施。然而另一方面，新法案也引发不小的忧虑。有法律专家指出，类似的规定对企业经营者冲击巨大，法案生效前留给他们适应新规、做出调整的时间也非常有限。此外，新法案还可能导致企业故意延缓、甚至隐瞒网络安全事故。另一方面，新的诈骗行业也很有可能应运而生——行骗者有可能通过伪造“被黑”的假象，向公司企业或机构“碰瓷”并骗赔。

3、欧洲爆发新勒索病毒 已扩散至多国

搜狐网 10 月 25 日消息 据外媒 10 月 25 日消息，周二一款名为“坏兔子”的勒索软件发动攻击，致使欧洲数国电脑系统遭冻结，并已经开始向美国扩散。这次的软件名为“坏兔子”（Bad Rabbit），是勒索软件的一种；勒索软件将受害电脑的文件加密，让电脑无法使用，从而要求支付赎金。这次的勒索软件要求支付 0.05 枚比特币（合 275 美元），不过支付赎金之后是否可以解密电脑文件尚不清楚。捷克反病毒公司 Avast Software s.r.o.说，到周二晚间，该软件已经开始向美国传播。同样在周二，美国国土安全部的计算机紧急事态应变团队发布了一项警讯，称已接获多个感染报告。安全研究人士称，该勒索软件伪装成奥多比系统公司的 Flash 多媒体产品更新，一经下载就会试图在受害电脑所处的网络传播。安全研究人士说，到周二晚间，攻击已经蔓延到俄罗斯、乌克兰、保加利亚、土耳其和德国。Nikitin 说，受害者包括俄罗斯的国际文传电讯社（Interfax）、乌克兰基辅的地铁系统、乌克兰敖德萨的国际机场以及乌克兰的基础设施部。

4、黑客正通过新型技术分发银行木马 Ursnif 感染日本金融行业

HackerNews.cc10 月 29 日消息 网络安全公司 IBM 研究团队 X-Force 近期发现黑客正通过新型技术肆意分发银行木马 Ursnif，旨在感染日本金融行业、窃取目标用户敏感信息。据称，黑客主要通过网页注入攻击和页面重定向等操作展开网络钓鱼活动。银行木马 Ursnif（又名：Gozi）首次于 2007 年在英国的一起网络银行诈骗中发现。随后，该恶意软件源代码于 2010 年意外泄露，并被其他黑客重新利用、创建木马，比如 Vawtrak 和 Neverquest。据悉，除北美、澳大利亚和日本之外，黑客此前还一直瞄准西班牙、波兰、保加利亚和捷克共和国的银行开展网络攻击活动。知情人士透露，为了能在日本大规模分发 Ursnif 有效负载，其黑客以日本金融服务与信用卡支付通知为主题伪造电子邮件，从而分发恶意软件感染目标企业。研究人员表示，该邮件中包含一份 JavaScript 文件（.zip）。一旦用户点击打开，其系统将重定向至另一恶意页面，从而启动 PowerShell 脚本后从远程服务器上获取有效负载，并与 Ursnif 一起感染用户。值得注意的是，黑客似乎已经将攻击活动的范围扩展到用户本地网络邮件、云存储、加密货币交易平台和电子商务网站等。

5、亚太网络信息中心托管的 Whois 数据库哈希密码在线泄露，或致相关域名遭黑客劫持

HackerNews.cc10 月 25 日消息 据外媒报道，eBay 员工 Chris Barcellos 于 10 月 12 日在亚太网络信息中心（APNIC）托管的 Whois 数据库中发现哈希密码在线泄露，或可导致相关域名遭黑客劫持，从而允许攻击者访问与修改域名的所有权限。随后，研究人员立即上报 APNIC 进行处理。据悉，公司于本周一证实，APNIC 在该问题被曝光的第二天已妥善解决。APNIC 副总监表示：“虽然密码的详细信息是散列分布的，但如果黑客使用正确的工具进行破解，那么他们极有可能从哈希表中排出正确密码后在域名维护程序中植入自己的详细信息，从而有效接管合法网站。调查显示，在线暴露的密码主要用于保护 Whois 数据库管理员和 IRT 目标对象的访问记录。APNIC 表示，此次事件的发生是因为技术人员在 APNIC Whois 数据库升级期间无意将哈希密码存储在 2017 年 6 月的可下载列表中。不过，公司现已经将所有管理人员和 IRT 目标对象的密码进行了安全转移。好在，尚未发现任何滥用迹象。目前，研究人员正进行事后审查，以确保此类事件不再发生。

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：王英

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158