国家互联网应急中心

2017 年第 53 期

12 月 25 日-12 月 31 日

网络安全信息与动态周报

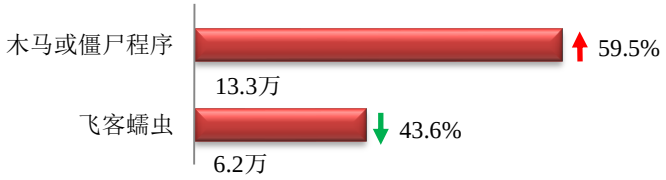
本周网络安全基本态势

境内感染网络病毒的主机数量	• 19.5万	↑ 0.7%
境内被篡改网站总数 其中政府网站数量	• 2382 • 42	↑ 15.6% ↓ 6.7%
境内被植入后门网站总数 其中政府网站数量	• 858 • 26	↓ 4.8% ↑ 100.0%
针对境内网站的仿冒页面数量	• 372	↑ 5.4%
新增信息安全漏洞数量 其中高危漏洞数量	• 294 • 91	↓ 33.2% ↓ 53.1%

= 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

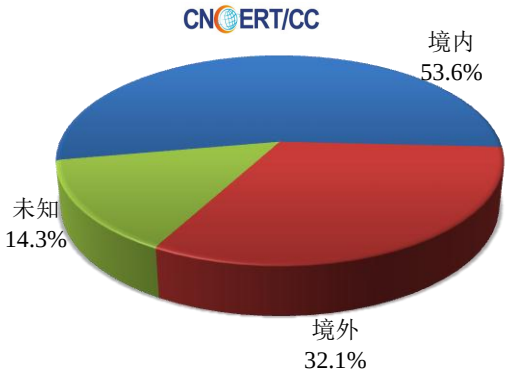
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 19.5 万个，其中包括境内被木马或被僵尸程序控制的主机约 13.3 万以及境内感染飞客（conficker）蠕虫的主机约 6.2 万。

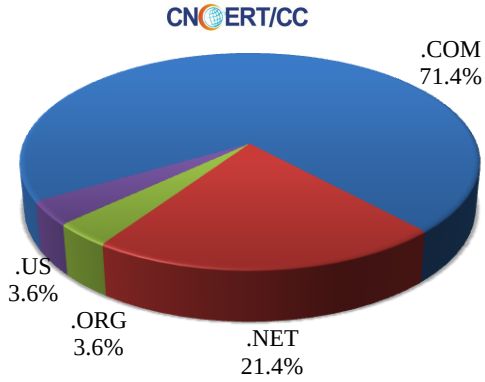


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 28 个，涉及 IP 地址 206 个。在 28 个域名中，有 32.1%为境外注册，且顶级域为.com 的约占 71.4%；在 206 个 IP 中，有约 25.7%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 1 个 IP。

本周放马站点域名注册所属境内外分布
(12/25-12/31)



本周放马站点域名所属顶级域的分布
(12/25-12/31)



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。

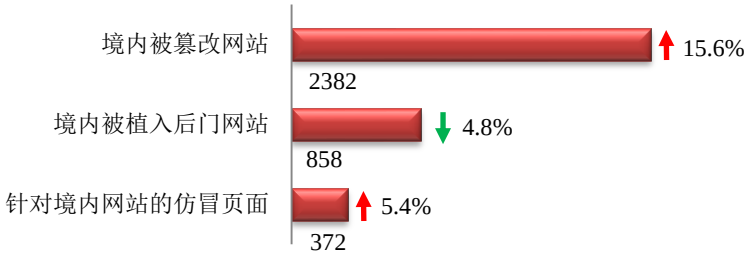
ANVA恶意地址黑名单发布地址

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。

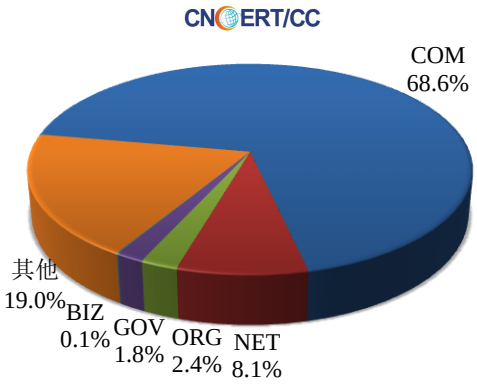
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2382 个；境内被植入后门的网站数量为 858 个；针对境内网站的仿冒页面数量为 372。

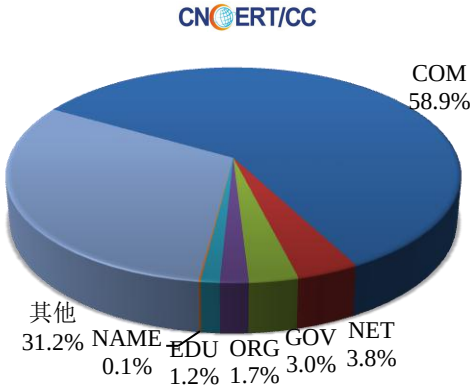


本周境内被篡改政府网站（GOV 类）数量为 42 个（约占境内 1.8%），较上周环比下降了 6.7%；境内被植入后门的政府网站（GOV 类）数量为 26 个（约占境内 3.0%），较上周环比上升了 100.0%；针对境内网站的仿冒页面涉及域名 294 个，IP 地址 140 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被篡改网站按类型分布
(12/25-12/31)

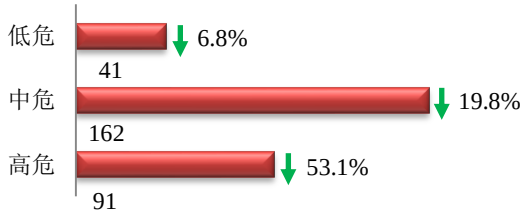


本周我国境内被植入后门网站按类型分布
(12/25-12/31)

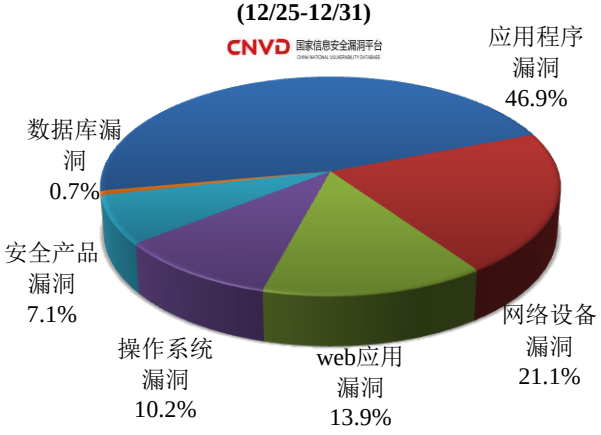


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 294 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
(12/25-12/31)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是网络设备漏洞和 web 应用漏洞。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

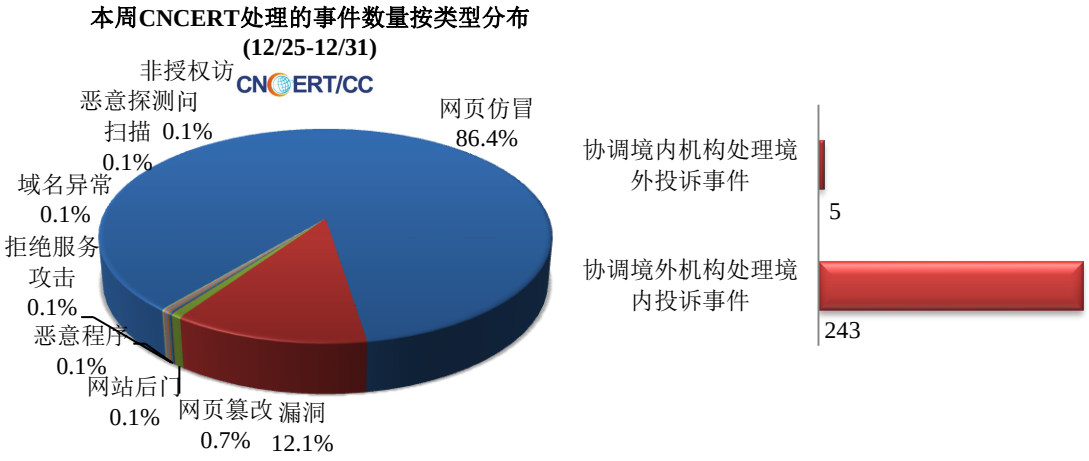
CNVD漏洞周报发布地址

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。

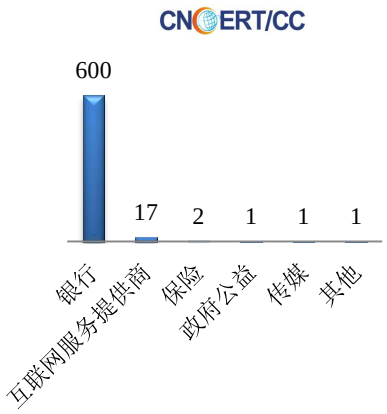
本周事件处理情况

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 720 起，其中跨境网络安全事件 248 起。

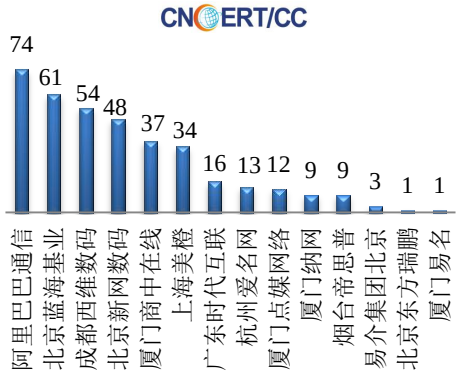


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 622 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 600 起和互联网服务提供商仿冒事件 17 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(12/25-12/31)

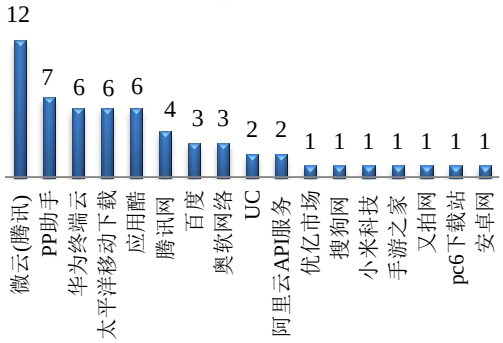


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (12/25-12/31)



本周，CNCERT 协调 17 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 58 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 (12/25-12/31)



业界新闻速递

1、工信部印发工业控制系统信息安全行动计划

新浪网 12 月 29 日消息 工信部印发《工业控制系统信息安全行动计划（2018-2020 年）》。行动计划提出，到 2020 年，全系统工控安全管理工作体系基本建立，全社会工控安全意识明显增强。建成全国在线监测网络，应急资源库，仿真测试、信息共享、信息通报平台（即一网一库三平台）。培育一批影响力大、竞争力强的龙头骨干企业，创建 3-5 个国家新型工业化产业示范基地（工业信息安全），产业创新发展能力大幅提高。

2、美国军方计划将网络士兵派上战场

E 安全 12 月 25 日消息 本月初美国官员表示，美国陆军很快会将网络战士派上战场，美国军希望对敌方的计算机系统发动攻势的企图昭然若揭。美国夏威夷作战部队指挥官罗伯特-赖安上校表示，美国陆军的任务通常是“攻击和摧毁”，但网络部队的目标略有差异，并非一切都要摧毁。例如可以通过非机动手段施以影响、制造

混乱并取得控制权。美国陆军网络司令部威廉-哈特曼上校表示，网络士兵已整合到步兵部队长达半年，今后将会根据指挥官的需求展开行动。过去三年，美国陆军已在加利福尼亚州南部针对此类行动展开训练。哈特曼未详述网络部队具备的网络能力，只表示网络战士会挖掘信息或拦截计划性的攻击。

3、越南政府组建“Force 47”网络战部队

HackerNews.cc12 月 30 日消息 据 IBTimes 英文网报道，越南人民军总政治部副主任 Nguyen Trong Nghia 于 12 月 25 日宣称越南已建立“Force 47”网络战部队，旨在打击互联网上传播的“错误观点”。Nguyen Trong Nghia 表示越南应毫不犹豫向世界展示“Force 47”，并且必须每时每刻都做好主动打击敌人的准备。目前该部队可能已经开始在某些地区运作。知情人士透露，越南政府对混乱和不能遏制容忍的言论自由产生了巨大的担忧。随着互联网发展愈加迅速，越南中央军事委员会有志于建立一支常备部队打击错误观点。目前越南军方与越南的政府部门已合作建立了一个装备精良的网络战部门“Force 47”。对此网络安全公司 FireEye Inc 发出警告称，越南在防御能力相对较弱的地区构建了强大的网络间谍能力。网络间谍活动对国家的吸引力越来越大，部分原因是它可以通过适度的投资、似是而非的“推诿”和有限的风险提供大量的信息。

4、Forever 21 承认支付系统遭到黑客攻击

cnBeta.COM12 月 30 日消息 据外媒报道，当地时间周四，Forever 21 证实其消费者支付银行卡信息被暴露给了黑客。不过这家公司并未公布受影响的客户数量，仅表示曾在今年 4 月 3 日至 11 月 18 日之间发生的交易受在影响范围内。黑客们收集走了信用卡号码、卡片可使用截止日期、验证码甚至持卡人的姓名。据这家公司透露，黑客通过在一些门店的销售终端安装恶意软件以达到网络攻击的目的。这是网络犯罪分子针对大型零售店发起网络攻击的又一个例子。快餐连锁店 Chipotle 和视频游戏零售店 GameStop 今年也曾都遭到过类似的攻击。Forever 21 表示，他们现在已经对这起网络改攻击展开了调查。

5、以德交易所 DNS 遭黑客劫持 已损失超过 26.6 万美元

搜狐网 12 月 29 日消息 以德（EtherDelta）是用于以太坊（Ethereum）与 ERC20 兼容代币（已经部署在 Ethereum 区块链上的代币）之间进行交易的加密货币交易所。它并不需要登录，并且可以在全世界任何地区都能安全使用。因其分布式、去中心化以及加密签名交易的特性，而深受加密货币交易者的欢迎。在上周三，这个加密货币交易所遭遇了黑客攻击，许多用户在不知情的情况下将其代币发送给了黑客，而不是用于交换。据调查统计，至少有 308 个以太币（约价值 266,789 美元）以及其他潜在价值超过数十万美元的代币被盗。显然，支配 EtherDelta 行为的智能合约在攻击中并没有受到损害。相反，攻击者成功地劫持了 EtherDelta 的 DNS 服务器，并为交易者提供了一个虚假版本。虚假网站模仿了真实网站的域名，这比常见的网络钓鱼攻击更为危险。EtherDelta 官方在 Twitter 上确认了这一攻击事件，并建议所有用户暂时不要使用该网站。

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：严寒冰

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158