国家互联网应急中心

网络安全信息与动态周报

2019 年第 1 期

12 月 31 日-1 月 6 日

CNCERT/CC

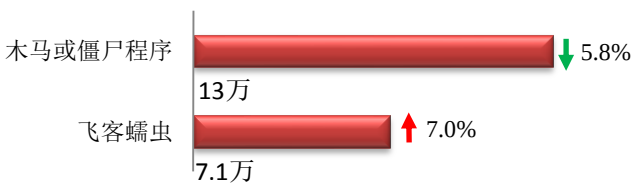
本周网络安全基本态势

境内感染网络病毒的主机数量	•20.1万	↓1.6%
境内被篡改网站总数 其中政府网站数量	•669 •52	↓9.1% ↓3.7%
境内被植入后门网站总数 其中政府网站数量	•553 •10	↓16.1% ↑100.0%
针对境内网站的仿冒页面数量	•2940	↑82.4%
新增信息安全漏洞数量 其中高危漏洞数量	•138 •44	↓66.7% ↓73.5%

=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

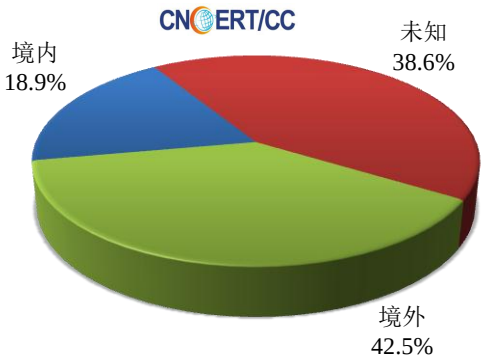
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 20.1 万个，其中包括境内被木马或被僵尸程序控制的主机约 13.0 万以及境内感染飞客（conficker）蠕虫的主机约 7.1 万。

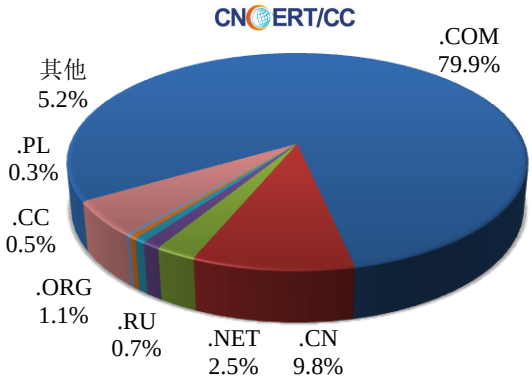


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 6864 个，涉及 IP 地址 5281 个。在 6864 个域名中，有 18.9%为境外注册，且顶级域为.com 的约占 79.9%；在 5281 个 IP 中，有约 54.3%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 614 个 IP。

本周放马站点域名注册所属境内外分布
(12/31-1/6)



本周放马站点域名所属顶级域的分布
(12/31-1/6)



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。

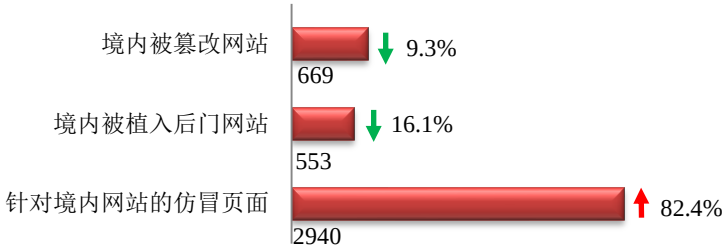
ANVA恶意地址黑名单发布地址

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。

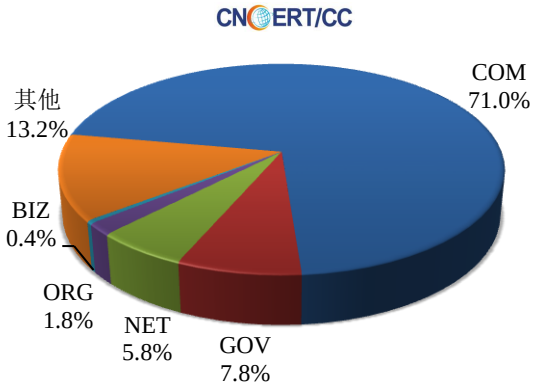
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 669 个；境内被植入后门的网站数量为 553 个；针对境内网站的仿冒页面数量 2940 个。

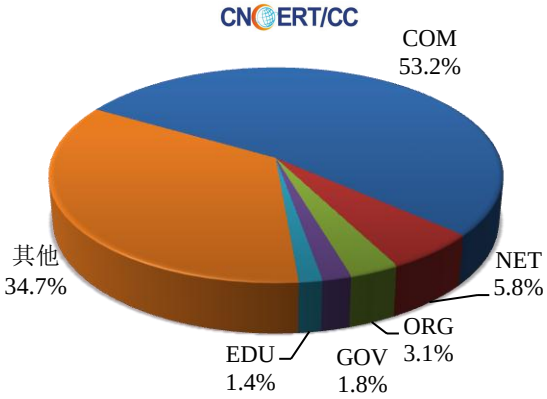


本周境内被篡改政府网站（GOV 类）数量为 52 个（约占境内 7.8%），较上周环比下降了 3.7%；境内被植入后门的政府网站（GOV 类）数量为 10 个（约占境内 1.8%），较上周环上升了 100.0%；针对境内网站的仿冒页面涉及域名 810 个，IP 地址 301 个，平均每个 IP 地址承载了约 11 个仿冒页面。

本周我国境内被篡改网站按类型分布
(12/31-1/6)

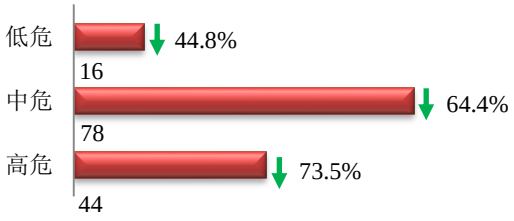


本周我国境内被植入后门网站按类型分布
(12/31-1/6)

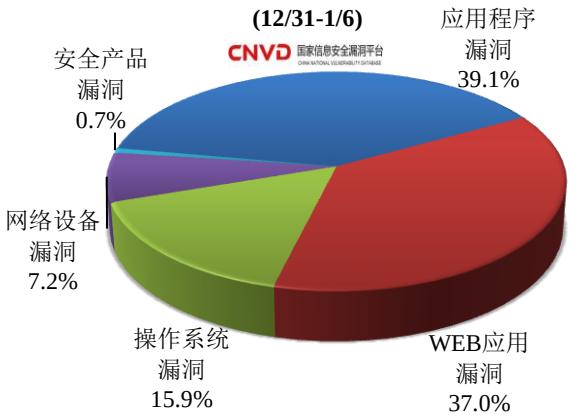


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 138 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
(12/31-1/6)



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 WEB 应用程序漏洞和操作系统漏洞。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

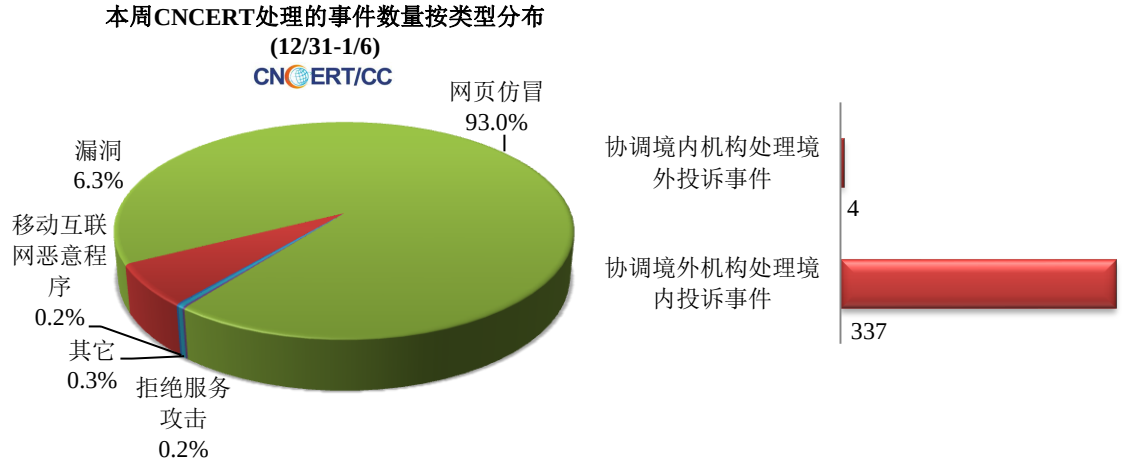
CNVD漏洞周报发布地址

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

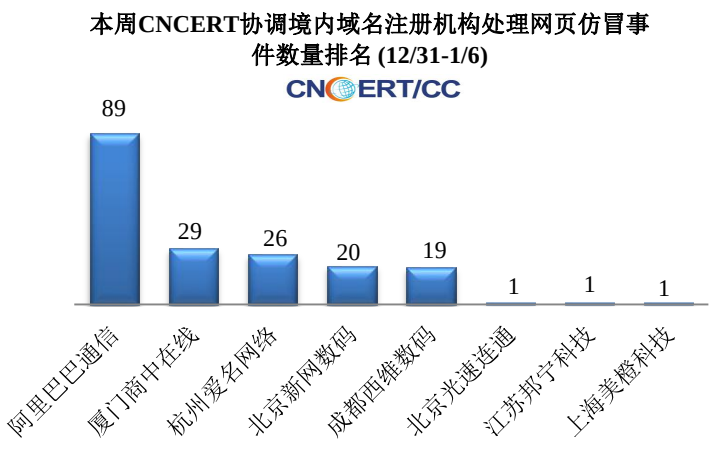
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

本周事件处理情况

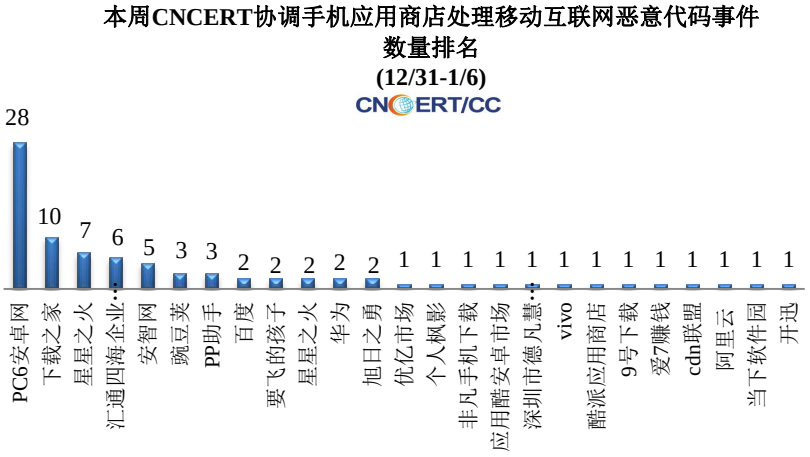
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 585 起，其中跨境网络安全事件 341 起。



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 554 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 531 起和互联网服务提供商事件 9 起。



本周，CNCERT 协调 25 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 85 个。



业界新闻速递

1、网信办启动网络生态治理专项行动

中国日报 1 月 3 日消息 据《中国日报》报道，日前，国家网信办积极回应民众关切要点，决定启动网络生态治理专项行动，针对网络生态有害信息屡禁不止等频发问题重拳出击，予以坚决制止。据介绍，此次专项行动于 2019 年 1 月正式启动，将持续开展 6 个月，分为“启动部署”、“全面整治”、“督导检查”、“总结评估”四个阶段，对各类网站、移动客户端、论坛贴吧、即时通信工具、直播平台等重点环节中的淫秽色情、低俗庸俗、暴力血腥、恐怖惊悚、赌博诈骗、网络谣言、封建迷信、谩骂恶搞、威胁恐吓、标题党、仇恨煽动、传播不良生活方式和不良流行文化等 12 类负面有害信息进行整治，集中解决网络生态重点环节突出问题，充分运用现有行政执法手段，严厉查处关闭一批违法违规网站和账号，有效遏制有害信息反弹、反复势头，促进网络生态空间更加清朗。

2、英国成首个发布自动驾驶网络安全标准国家

新京报 1 月 3 日消息 英国成为第一个发布自动驾驶网络安全标准的国家，该标准将保护自动驾驶车辆免受网络攻击。据英国政府估计，2035 年英国网联车和自动驾驶车辆市值将达 520 亿英镑。据悉，该标准由英国标准协会发布，捷豹路虎、福特、宾利以及英国国家网络安全中心的学者和专家共同研发，由英国运输部提供资金支持。该标准发布后，将帮助汽车生命周期及生态系统内的各方更好地了解如何提升并保持车辆的安全性及智能交通系统的安全性。

3、巴西政府将成立国家个人数据保护局

E 安全 1 月 1 日消息 巴西前总统米歇尔·特梅尔（Michel Temer）12 月 28 公布一项“临时措施”，提出

成立“国家个人数据保护局”（简称 ANPD），并延长巴西新数据隐私法（基于欧盟 GDPR 制定）的生效日期，将其从 18 个月延长到 24 个月，这就意味着企业须在 2020 年 8 月 16 日前满足合规，而非 2020 年 2 月。特梅尔最初在 2018 年 8 月签署的新数据隐私法中否决了成立 ANPD 的提案，否决的主要原因在于该机构的自治模式。然而由于巴西当局认为该机构对实施新规则至关重要，因此巴西政府被迫解决该问题。 12 月 28 日公布的这项“临时措施”提出，ANPD 的职责包括制定信息处理框架，指导组织机构遵守规则，以及负责监督并对违规组织机构进行处罚。新机构将包括 5 名董事会成员和由 23 名成员组成的咨询委员会，董事会成员由总统亲自选定。23 名咨询委员会成员将包括来自公共、私营和第三部门的代表。

4、印度当局要求社交网络利用微软 PhotoDNA 扫描所有照片

E 安全 1 月 1 日消息 指纹工具微软 PhotoDNA 可通过预先扫描用户上传的内容，帮助线上服务清除虐待儿童的图片。 印度当局要求社交网络利用微软 PhotoDNA 扫描所有照片-E 安全 PhotoDNA 为图片创建了独特的数字签名（即“哈希”），并将该签名与其他图片的签名（哈希）做对比，以识别相似的图像。当所匹配的数据库包含之前识别过的非法图像的哈希值时，工具 PhotoDNA 刚好有助于删除、销毁并报道虐待儿童材料的分布。该技术在印度引发舆论哗然，此前，印度中央调查局曾报道要求社交网络开始使用该工具扫描用户相册。然而，印度中央调查局似乎还要求社交网络寻找用户相册中的特定照片，这些照片与虐待无关，亦在该工具的设计初衷之外。

5、德国数百名政界人士机密信息被泄露：包含默克尔等人

cnBeta.COM1 月 4 日消息 在过去的数周，黑客们陆续泄露了有关德国总理默克尔（Angela Merkel）和其他数百名政界人士的机密数据，这是迄今为止德国发生的最大规模的政治家信息泄露事件。据一项初步评估结果显示，这些被泄露的信息包括电子邮件地址、手机号码、身份证照片和个人聊天记录等。这些信息是在过去数周通过一个自称“G0d”的 Twitter 账户泄露的，账户信息显示，该用户位于汉堡，并使用“安全研究”、“艺术家”和“讽刺与反讽”等词来描述自己。 目前，德国联邦安全机构“德国联邦信息安全局”（BSI）正在调查此事。BSI 一发言人今日在接受电话采访时并未透露更详细的信息，而德国其他相关部门也尚未对此发表评论。

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：李志辉

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158