国家互联网应急中心

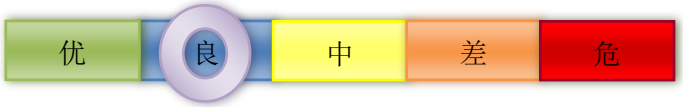
# 网络安全信息与动态周报

**2017 年第 50 期**

**12 月 4 日-12 月 10 日**

CNCERT/CC

## 本周网络安全基本态势

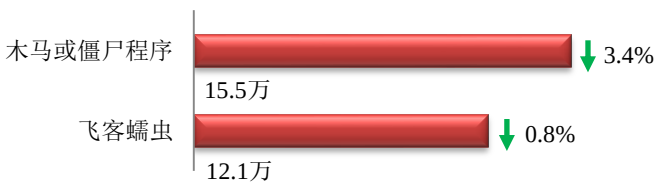



| | | |
|---|---|---|
| 境内感染网络病毒的主机数量 | •27.6万 | 2.3% |
| 境内被篡改网站总数<br>其中政府网站数量 | •1761<br>•44 | 32.1%<br>8.3% |
| 境内被植入后门网站总数<br>其中政府网站数量 | •927<br>•20 | 5.6%<br>31.0% |
| 针对境内网站的仿冒页面数量 | •340 | 7.9% |
| 新增信息安全漏洞数量<br>其中高危漏洞数量 | •480<br>•158 | 1.5%<br>9.2% |

*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*

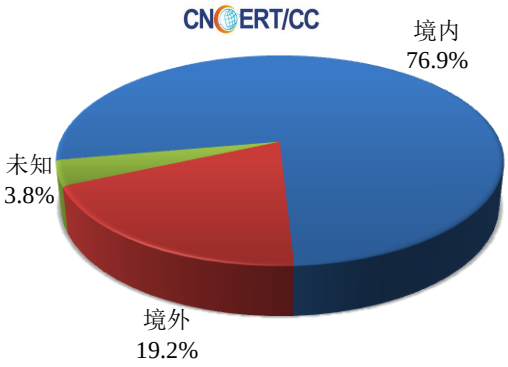
## 本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 27.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 15.5 万以及境内感染飞客（conficker）蠕虫的主机约 12.1 万。

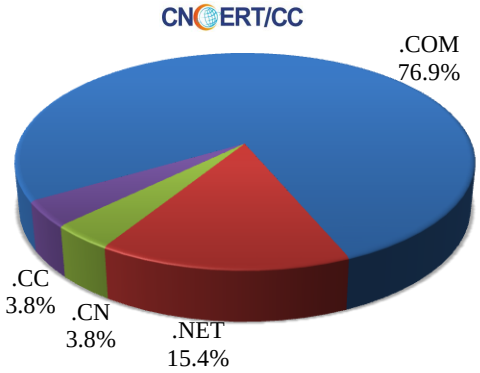


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 26 个，涉及 IP 地址 183 个。在 26 个域名中，有 19.2%为境外注册，且顶级域为.com 的约占 76.9%；在 183 个 IP 中，有约 28.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 2 个 IP。

**本周放马站点域名注册所属境内外分布**
**(12/4-12/10)**




**本周放马站点域名所属顶级域的分布**
**(12/4-12/10)**




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。

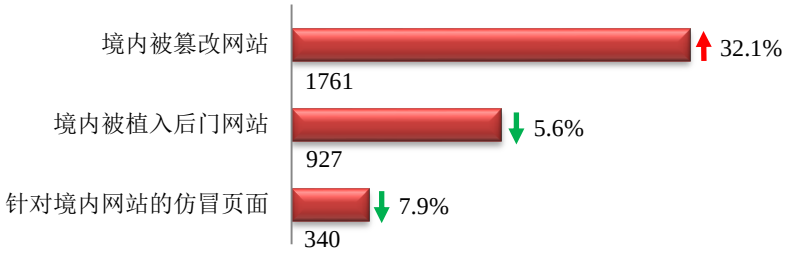
**ANVA恶意地址黑名单发布地址**

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。*

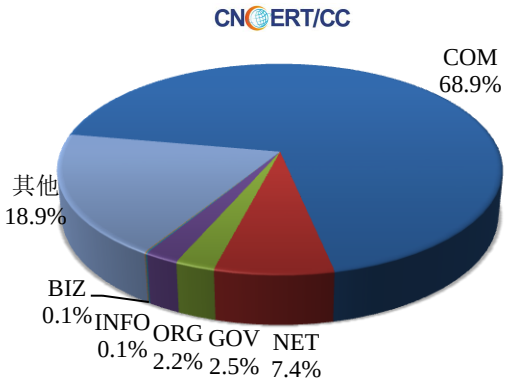
## 本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1761 个；境内被植入后门的网站数量为 927 个；针对境内网站的仿冒页面数量为 340。

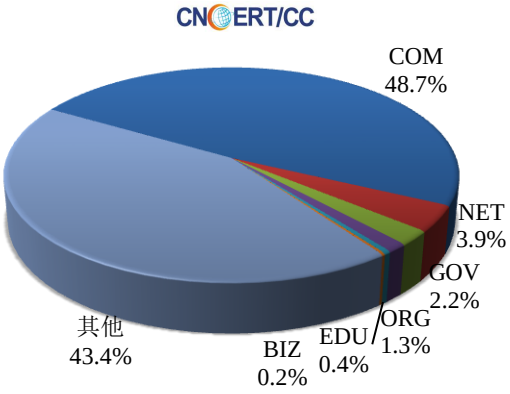


本周境内被篡改政府网站（GOV 类）数量为 44 个（约占境内 2.5%），较上周环比下降了 8.3%；境内被植入后门的政府网站（GOV 类）数量为 20 个（约占境内 2.2%），较上周环比下降了 31.0%；针对境内网站的仿冒页面涉及域名 297 个，IP 地址 139 个，平均每个 IP 地址承载了约 2 个仿冒页面。

**本周我国境内被篡改网站按类型分布**
**(12/4-12/10)**

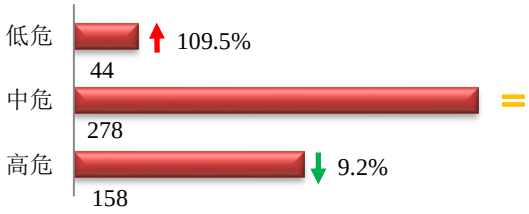



**本周我国境内被植入后门网站按类型分布**
**(12/4-12/10)**

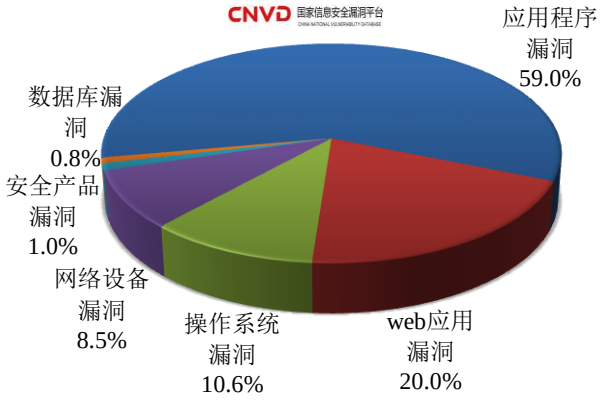



## 本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 480 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**
**(12/4-12/10)**




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。

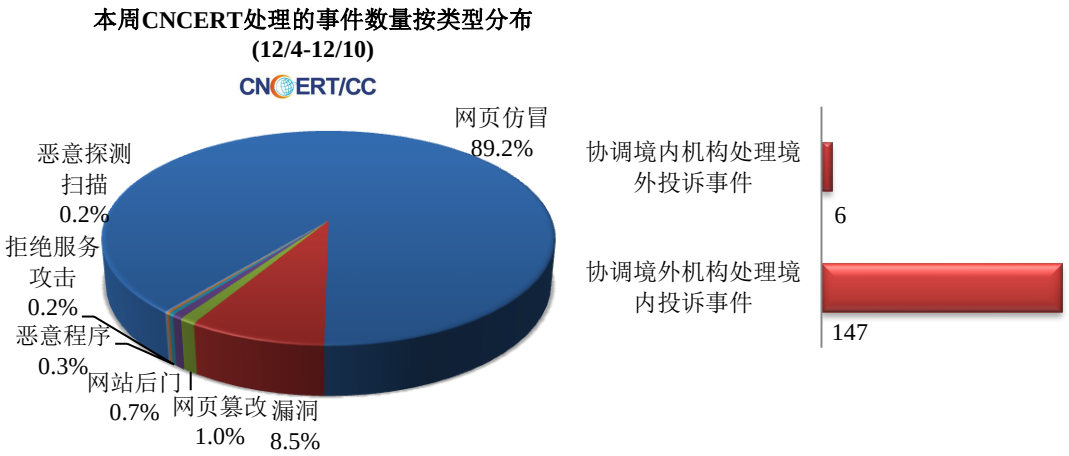
**CNVD漏洞周报发布地址**

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。*

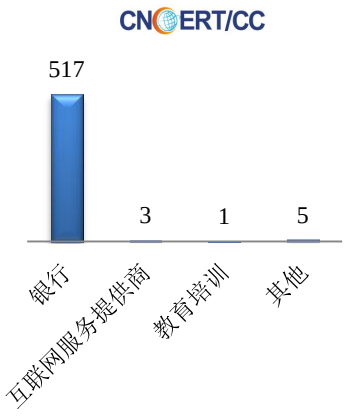
## 本周事件处理情况

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 590 起，其中跨境网络安全事件 153 起。

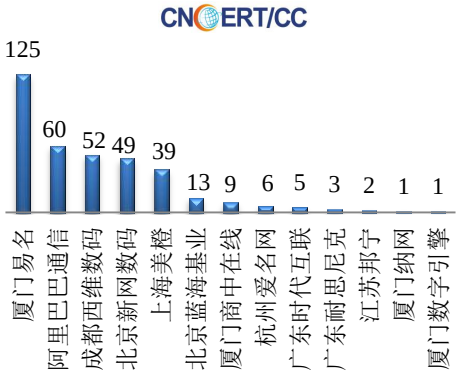



本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 526 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 517 起和互联网服务提供商仿冒事件 3 起。

**本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(12/4-12/10)**

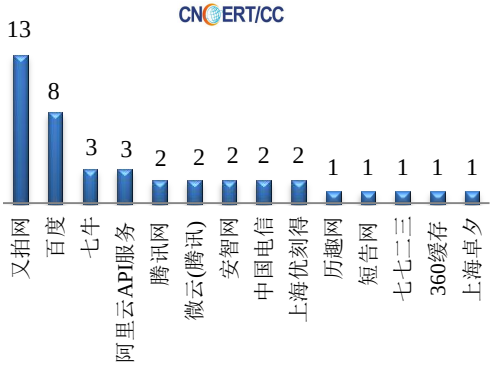



**本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (12/4-12/10)**




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 42 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 (12/4-12/10)**




## 业界新闻速递

### 1、国家域名服务平台浙江节点正式启用

中国日报网 12 月 4 日消息 12 月 2 日，“国家域名服务平台——浙江节点”在浙江乌镇互联网国际会展中心举行启用仪式。该节点部署上线后，将纳入国家域名顶级节点服务平台并对外服务。国家互联网信息办公室信息化发展局副局长兼中国互联网络信息中心（CNNIC）副主任曾宇、浙江省经济和信息化委员会副主任吴君青等出席仪式。作为国家网络基础资源的注册服务管理机构，CNNIC 积极探索开放合作的发展模式，集中优势力量构建坚实的互联网基础设施。自 2015 年，CNNIC 携手浙江经信委签署战略合作协议，双方共同推动国家域名顶级节点在浙江的建设、部署和上线，进一步完善国家域名服务平台生态区域分布。曾宇副局长在致辞中介绍，“作为互联网的重要基础设施，域名资源的运行服务安全直接关系整个互联网的安全。尤其是作为我国在全球互联网上身份标识的“.CN”、“.中国”国家顶级域名的安全稳定运行，对我国乃至全球互联网的正常运转起着举足轻重的作用。”

## 2、美银行建防御系统：备份数据应对网络攻击影响

中新网 12 月 4 日消息 据外媒 12 月 4 日报道，美国银行业推出了一个应对末日网络攻击的计划，希望在一家银行遭到严重网络攻击时，避免整个金融系统受到波及。据报道，目前参与进来的银行和信用联盟总共拥有约 4 亿账户，参与这项计划的银行，需根据自身规模每年支付 250 美元到 25000 美元不等的费用。据悉，这项名为 Sheltered Harbor 的计划在今年早些时候启动，目前参与进来的银行和信用联盟总共拥有约 4 亿账户。该计划要求成员公司各自备份数据，以便在某家银行的网络陷入瘫痪时，其他公司可以使用备份数据为其客户提供服务。Sheltered Harbor 计划的参与者范围很广，既包含小型本地机构，也包括美国银行、花旗集团和摩根大通这样的金融巨头。Sheltered Harbor 计划的董事会由来自大型银行、小企业团体、行业协会、结算机构和券商的 34 名代表组成。成员必须遵循具体的数据格式要求，建造备份保管库并接受审计。其目标是能在 48 小时内启用备份数据，为受影响的机构的客户提供保护。

## 3、德国准备起草法律要求所有设备包含后门

cnBeta.COM12 月 6 日消息 德国当局正着手起草法律强制性要求所有设备制造商在其产品中包含后门，允许执法机关在法律调查中根据需要使用。法律将针对所有现代设备，包括汽车、手机、计算机、物联网产品等等。官员预计将会在本周递交法律提议进行辩论。德国内政部长 Thomas de Maizier 支持这项立法，他在过去几个月对此谈及了执法机构调查恐怖分子袭击和其它犯罪活动上的困难。

## 4、北约“网络联盟”演习关键词：恶意软件、混合攻击和移动攻击

E 安全 12 月 4 日消息 上周，北约在爱沙尼亚举行为期三天的“网络联盟”（Cyber Coalition）演习，25 个北约成员国、北约盟国、欧盟、行业及学术界 700 多人参加此次演习。Cyber Coalition 演习今年迎来第十个年头，主要测试并训练北约网络防御者防御北约和国家网络的能力。今年的演习内容包括针对基础设施的恶意软件攻击，涉及社交媒体的混合挑战，以及针对移动设备的攻击。训练内容包括运营和法律程序的测试。北约表示，这次演习具有挑战性，现实的场景有助于网络防御者为真实网络挑战做准备。网络防御是北约联合防御的核心任务。北约的最高优先事项是在网络防御方面保持领先地位。Cyber Coalition 这类演习有助于提升北约和盟国防御网络的能力，以及遭遇网络攻击时的协调能力。近几年，随着数字攻击威胁日益严峻，此类网络防御演习的重要性愈发凸显。作为全球最大的军事联盟，北约过去几年逐渐加大了对网络战的关注。本月初，北约曾表示希望将成员国的网络战能力纳入军事行动。

## 5、北卡罗来纳州服务器遭勒索软件攻击 政府拒绝支付赎金

新浪网 12 月 9 日消息 据外媒报道，美国北卡罗来纳州夏洛特所在地——梅克伦堡县的重要服务器本周遭到勒索软件网络攻击，进而导致该城市的政府工作人员不得不回到老式的纸笔办公年代。据悉，政府网络在一名工作者打开一份带有恶意软件附件的邮件之后遭到感染。黑客要求政府支付 2.3 万美元来恢复系统，不过截止到目前当地政府拒绝了这一要求。发起这次网络攻击的黑客被认为来自伊朗或乌克兰。眼下，包括税务部门、监狱在内的多个城市机构所用的服务器都被勒索软件锁住。尽管梅克伦堡县的许多服务器受到了影响，但夏洛特市的政府计算机系统并未受到波及，显然这非常幸运，毕竟这座城市拥有 100 多万名居民。另外，紧急服务

电话也没有受到影响，不过像处理家庭暴力这样的热线已无法正常运转。

**6、汇丰等知名银行 APP 存在关键漏洞，或致数百万用户易遭黑客中间人（MitM）攻击**

HackerNews.cc12 月 10 日消息 英国伯明翰大学的安全研究人员 Chris McMahon Stone、Tom Chothia 和 Flavio Garcia 近期在佛罗里达州奥兰多举行的 2017 计算机安全应用会议 上发表了一篇学术论文，宣称他们通过测试数百款 iOS 与 Android 设备的不同银行应用程序中发现多家知名银行的主要移动应用程序均存在一处关键漏洞，可导致数百万用户的银行凭证易遭黑客中间人（MitM）攻击，其中受影响的银行包括爱尔兰联合银行、Co-op、汇丰银行、NatWest 和桑坦德银行等。调查显示，即使该移动银行应用程序使用了 SSL pinning 功能，黑客也可通过该漏洞连接至与受害用户同一网络后拦截 SSL 连接，并检索用户银行凭证（例如：用户名与密码等）。目前，研究人员已经与国家网络安全中心（NCSC）合作，通知所有受影响银行尽快解决问题，以避免造成客户信息与财产的损失。

## 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：曹攀攀

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158