

## 本周网络安全基本态势



▬ 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

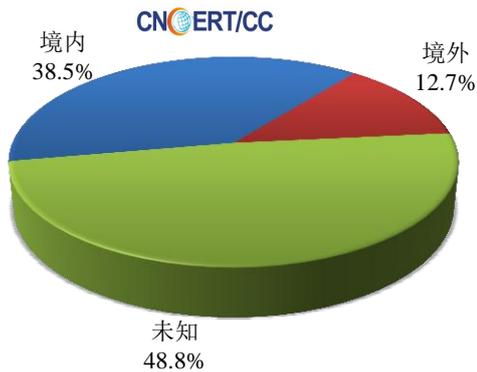
本周境内感染网络病毒的主机数量约为 22.0 万个，其中包括境内被木马或被僵尸程序控制的主机约 13.7 万以及境内感染飞客（conficker）蠕虫的主机约 8.3 万。



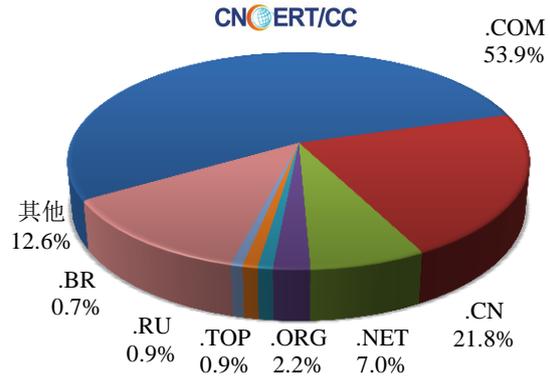
<sup>1</sup>本期境内被篡改网站总数受监测数据范围扩大影响，波动较大

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 2661 个，涉及 IP 地址 4043 个。在 2661 个域名中，有 12.7% 为境外注册，且顶级域为 .com 的约占 53.9%；在 4043 个 IP 中，有约 51.0% 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 545 个 IP。

本周放马站点域名注册所属境内外分布  
(6/10-6/16)



本周放马站点域名所属顶级域的分布  
(6/10-6/16)



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。

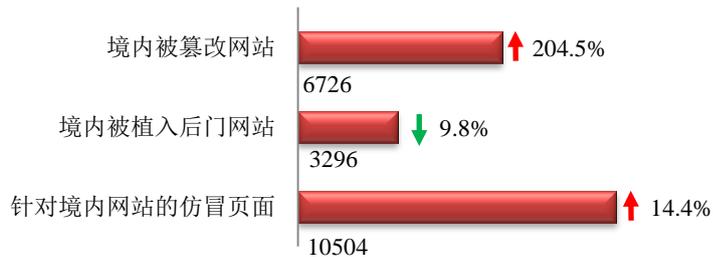
ANVA 恶意地址黑名单发布地址

<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

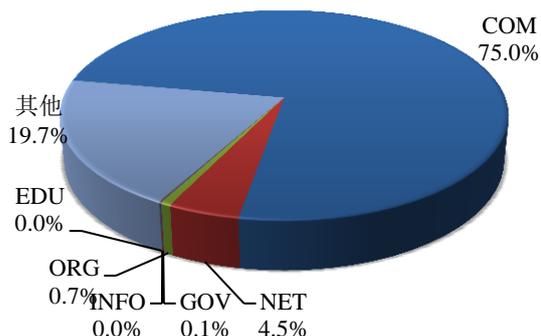
本周 CNCERT 监测发现境内被篡改网站数量 6726 个；境内被植入后门的网站数量为 3296 个；针对境内网站的仿冒页面数量 10504 个。



本周境内被篡改政府网站（GOV 类）数量为 8 个（约占境内 0.1%），较上周环比上升 116.7%；境内被植入后门的政府网站（GOV 类）数量为 45 个（约占境内 1.4%），较上周环比下降 10.0%；针对境内网站的仿冒页面涉及域名 957 个，IP 地址 662 个，平均每个 IP 地址承载了约 16 个仿冒页面。

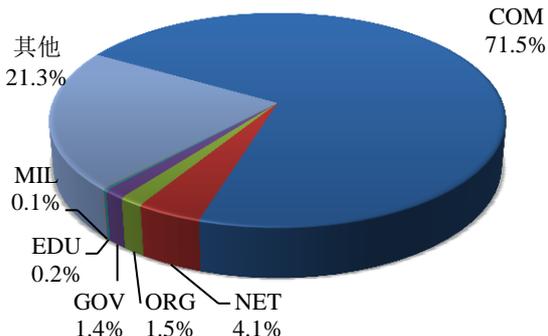
本周我国境内被篡改网站按类型分布  
(6/10-6/16)

CN CERT/CC



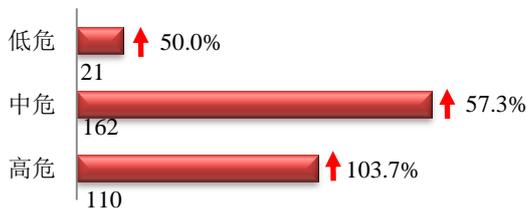
本周我国境内被植入后门网站按类型分布  
(6/10-6/16)

CN CERT/CC



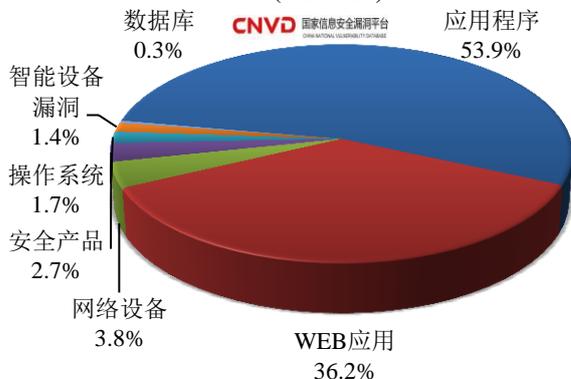
### 本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 293 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  
(6/10-6/16)

CNVD 国家信息安全漏洞平台



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>

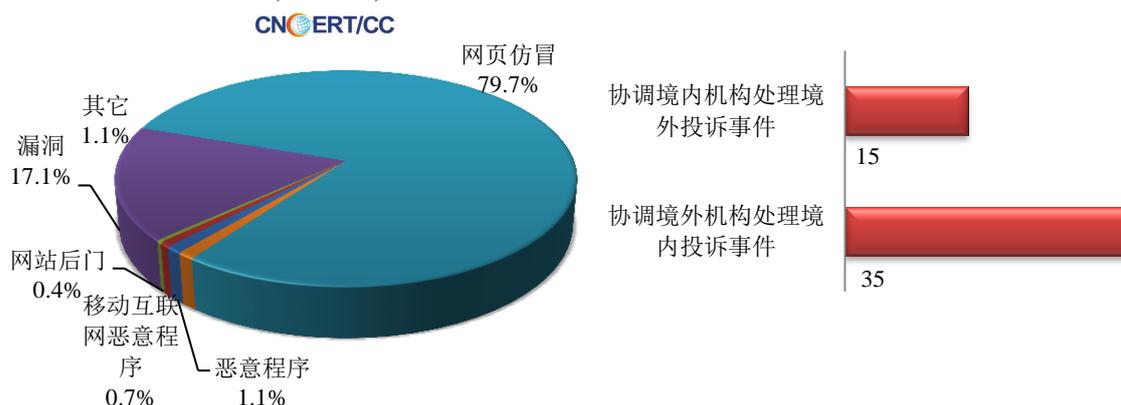
国家信息安全漏洞共享平台(缩写CNVD)是CNCERT联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。



## 本周事件处理情况

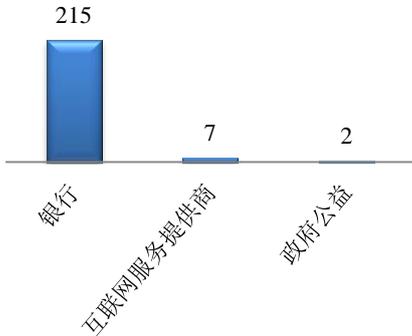
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 281 起，其中跨境网络安全事件 50 起。

本周CNCERT处理的事件数量按类型分布  
(6/10-6/16)

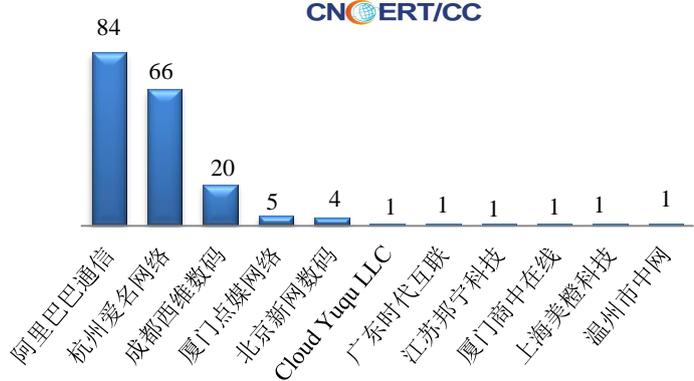


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 224 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 215 起和互联网移动供应商仿冒事件 7 起。

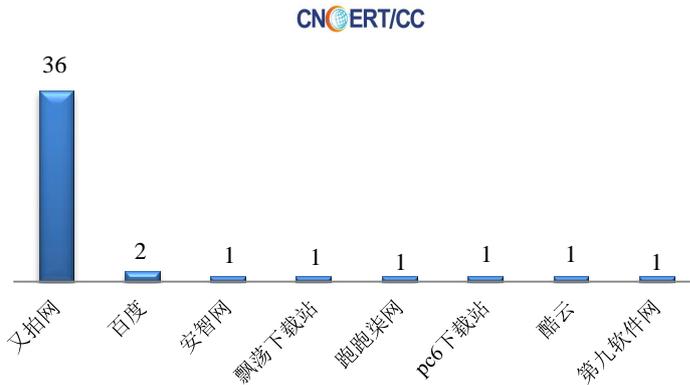
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (6/10-6/16)  
CNCERT/CC



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 (6/10-6/16)  
CNCERT/CC



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 (6/10-6/16)  
CNCERT/CC



本周，CNCERT 协调 8 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 44 个。



## 业界新闻速递

### 1、中央网信办等四部委联合开展互联网网站安全专项整治

新华网北京 6 月 11 日消息 中央网信办、工业和信息化部、公安部、市场监管总局四部门于 2019 年 5 月至 2019 年 12 月，联合开展全国范围的互联网网站安全专项整治工作，对未备案或备案信息不准确的网站进行清理，对攻击网站的违法犯罪行为进行严厉打击，对违法违规网站进行处罚和公开曝光。此次专项整治的一大特点是加大对未履行网络安全义务，发生事件的网站开办者的处罚力度，督促其切实落实安全防护责任，加强网站安全管理和防护。各地通信管理局、公安机关将根据《网络安全法》，对落实网络安全义务不到位，发生网页篡改、被植入后门木马、大量公民个人信息被窃取等网络安全事件，以及存在非法获取、出售或提供个人

信息等行为的网站，依据情节严重程度，采取约谈主要负责人、停业整顿、关闭网站、注销备案等措施并公开曝光，涉企行政处罚信息将依法纳入市场监管总局国家企业信用信息公示系统予以公示。

## 2、美国国土安全部成立网络事件响应小组

安全内参 6 月 10 日消息 美国众议院以口头表决方式通过了一项法案，将在美国国土安全部(DHS)内设立网络事件响应小组。该小组将负责在网络事件发生后，向资产所有者和运营商提供援助和支持。私营部门的网络专家将可能成为该团队的成员。该法案的主要发起人、众议院外交事务委员会资深成员 R-Texas 表示，网络事件响应小组的设立将有助于促进公共部门和私营部门之间的合作，并将网络团队形容为袭击后的“第一反应者”。当网络攻击发生时，需要立即获得专业知识，以减轻损失。此次立法确保美国能够继续适应网络环境的不断变化。该法案在参议院有一项配套措施，已于 4 月得到美国国土安全和政府事务委员会的批准，正在等待众议院投票。

## 3、欧盟宣布斥资 8.4 亿欧元新建 8 个超算中心

Cnbeta.COM 6 月 10 日消息 欧盟委员会日前发布公报，“欧洲高性能计算共同计划”已从欧盟成员国中选定 8 处地点建设“世界级”超级计算机中心，来自各方的项目总预算高达 8.4 亿欧元。8 个超算中心将设在保加利亚的索菲亚、捷克的俄斯特拉发、芬兰的卡亚尼、意大利的博洛尼亚、卢森堡的比森、葡萄牙的米尼奥、斯洛文尼亚的马里博尔和西班牙的巴塞罗那。

## 4、美国食品慈善组织被勒索软件攻陷

安全内参 6 月 11 日消息 位于华盛顿州金县的奥本食品银行成为名为 GlobeImposter 2.0 的勒索软件的受害者，后者加密了网络中的所有计算机，该勒索软件其主要通过 RDP 远程桌面弱口令进行爆破攻击，由于很多用户设置的密码过于简单，因此密码在破解成功后，攻击者会将勒索病毒植入受害者设备并加密指定后缀名的文件。

## 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：马莉雅

网址：[www.cert.org.cn](http://www.cert.org.cn)

email：[cncert\\_report@cert.org.cn](mailto:cncert_report@cert.org.cn)

电话：010-82990315

