国家互联网应急中心

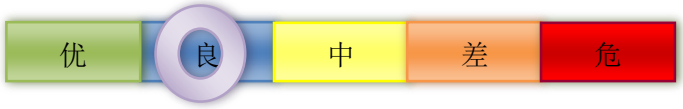
# 网络安全信息与动态周报

2020 年第 2 期

1 月 6 日-1 月 12 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 | • 58.9万 | ↓ 6.2% |
| 境内被篡改网站总数<br>其中政府网站数量 | • 8774<br>• 32 | ↓ 10.7%<br>↓ 5.9% |
| 境内被植入后门网站总数<br>其中政府网站数量 | • 2777<br>• 18 | ↓ 0.7%<br>↑ 5.9% |
| 针对境内网站的仿冒页面数量 | • 1479 | ↓ 8.7% |
| 新增信息安全漏洞数量<br>其中高危漏洞数量 | • 295<br>• 133 | ↑ 37.2%<br>↑ 56.5% |

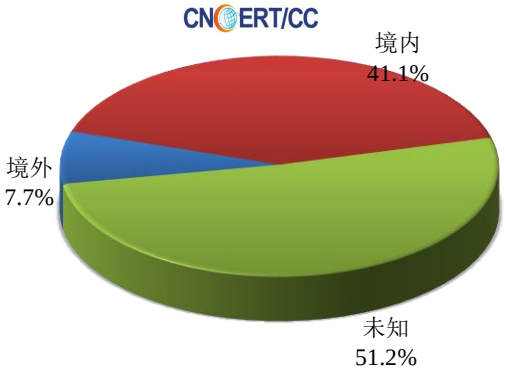
*= 表示数量与上周相同　↑ 表示数量较上周环比增加　↓ 表示数量较上周环比减少*

## 本周网络病毒活动情况

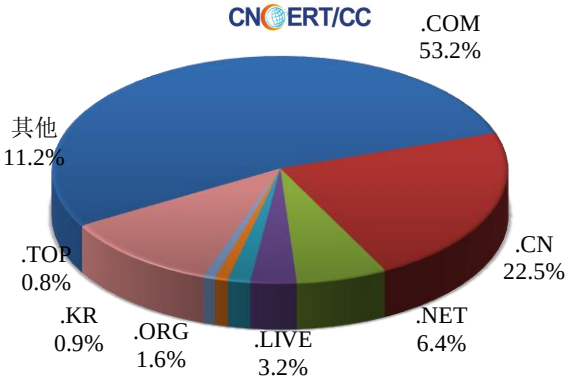
本周境内感染网络病毒的主机数量约为 58.9 万个，其中包括境内被木马或被僵尸程序控制的主机约 51.2 万以及境内感染飞客（conficker）蠕虫的主机约 7.7 万。

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 1078 个，涉及 IP 地址 2589 个。在 1078 个域名中，有 7.7%为境外注册，且顶级域为.com 的约占 53.2%；在 2589 个 IP 中，有约 22.9%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 282 个 IP。

**本周放马站点域名注册所属境内外分布**
**(1/6-1/12)**




**本周放马站点域名所属顶级域的分布**
**(1/6-1/12)**




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。

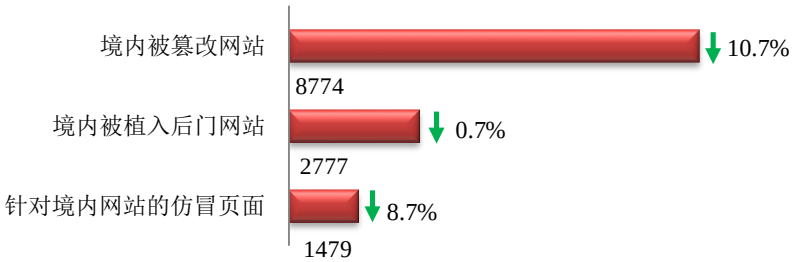
**ANVA恶意地址黑名单发布地址**

**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。*

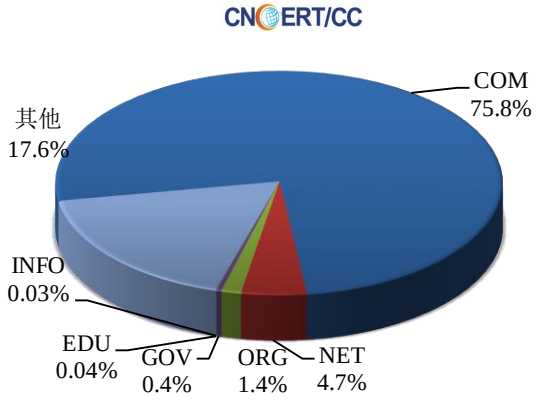
## 本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 8774 个；被植入后门的网站数量为 2777 个；针对境内网站的仿冒页面数量 1479 个。

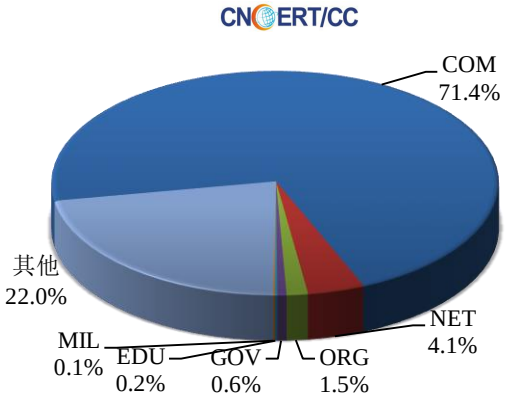


本周境内被篡改政府网站（GOV 类）数量为 32 个（约占境内 0.4%），较上周下降了 5.9%；境内被植入后门的政府网站（GOV 类）数量为 18 个（约占境内 0.6%），较上周上涨了 5.9%。

**本周我国境内篡改网站按类型分布**
**(1/6-1/12)**



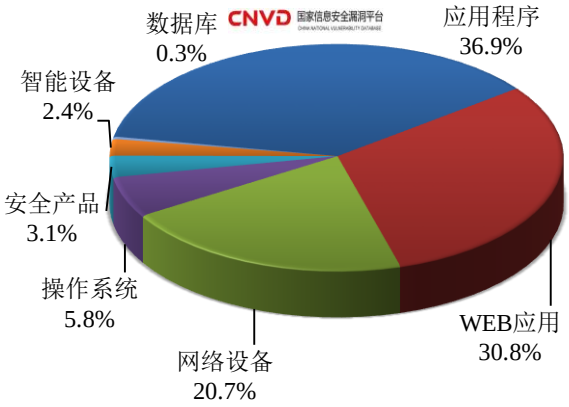

**本周我国境内被植入后门网站按类型分布**
**(1/6-1/12)**




## 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 295 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**
**(1/6-1/12)**




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 应用和网络设备。

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**

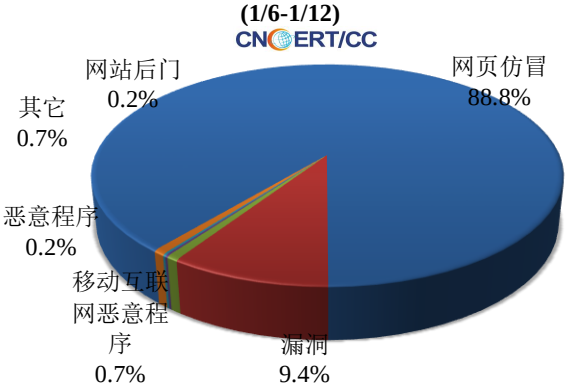
http://www.cnvd.org.cn/webinfo/list?type=4

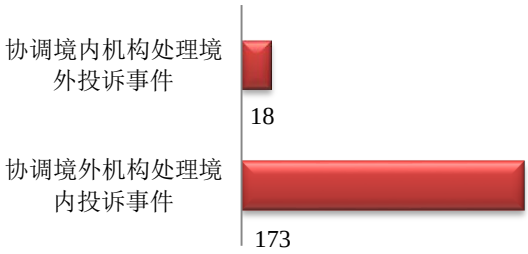
*国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。*

## 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 563 起，其中跨境网络安全事件 191 起。

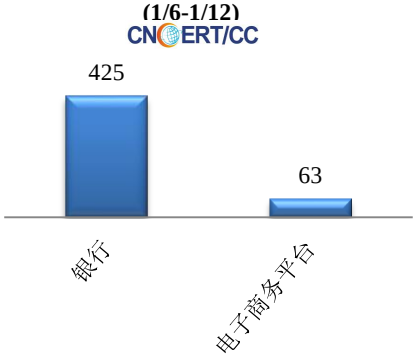
**本周CNCERT处理的事件数量按类型分布**
**(1/6-1/12)**



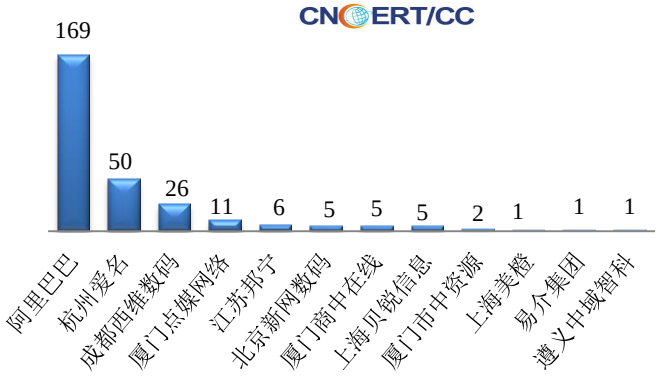




本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 500 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包括银行仿冒事件 425 起和电子商务平台仿冒事件 63 起。

**本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计**
**(1/6-1/12)**

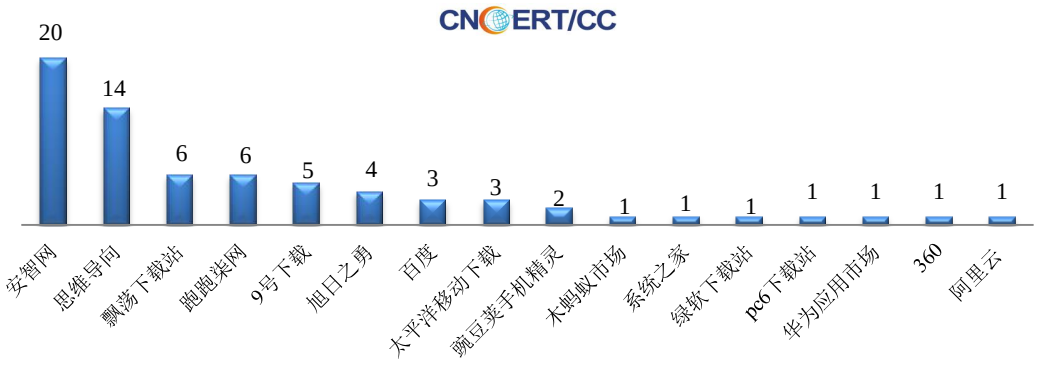



**本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (1/6-1/12)**



本周，CNCERT 协调 16 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 70 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**
**(1/6-1/12)**




## 业界新闻速递

### 1、 工信部通报第二批侵害用户权益行为的 App 名单，15 款产品在列

1 月 8 日，工信部官网消息，工信部信息通信管理局通报第二批侵害用户权益行为的 App 名单，15 款产品在列。第二批存在问题且未完成整改的 15 款 App 中，有云南招考、知米背单词、金程网校旗舰版三款教育类 App 上榜。除了教育类 App 外，第二批被通报的还有天涯社区、风行视频、一点资讯、luckin coffee、绿城生活等 App，涉及社交、媒体、生活应用等多个领域。第一批未按要求完成整改的 3 家企业，已于 1 月 3 日依法组织下架。

### 2、 美国加州“物联网安全法案”开始实施

1 月 9 日，据外媒报道，近日，美国加州立法委员会颁布的《加利福尼亚州的物联网网络安全法案》（SB 327）开始实施，加州成为全美国第一个拥有智能物联网设备安全法的州政府。法案正式生效后，所有联网设备的制造商都要为其产品配备安全设置，以防止信息被未授权访问或者修改泄露。另外，如果设备可以使用密码在局域网外访问，那么制造商需要为用户提供唯一的密码，或强制用户在第一次连接时设置密码。这也就意味着黑客们将没有机会通过默认设置的漏洞来对设备进行攻击或者监视。

### 3、 微软 Access 数据库存在可能泄露敏感数据的漏洞

1 月 7 日，据外媒报道，研究人员发现微软的 Access 数据库应用程序存在一个漏洞，可能会导致敏感信息泄露。据分析，该漏洞与 2019 年在 Microsoft Office 中发现的漏洞非常相似。该漏洞的产生与应用程序对系统内存的不当管理有关，可能导致系统内存中的敏感数据无意中保存在数据库文件中，泄露敏感信息。该漏洞会影响 Office 2010、2013、2016、2019 和 365 ProPlus，可能会使用户面临敏感数据泄漏的风险。微软已经在 201912 月份的微软安全更新中修复，希望尽快下载并安装该补丁。

## 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 2018 年，CNCERT 与 76 个国家和地区的 233 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：王小群

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315