国家互联网应急中心

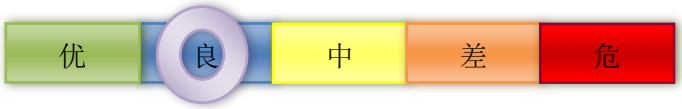
# 网络安全信息与动态周报

**2019 年第 10 期**

**3 月 4 日-3 月 10 日**

CNCERT/CC

## 本周网络安全基本态势

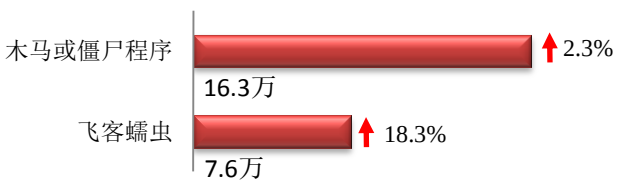



| | | |
|---|---|---|
| 境内感染网络病毒的主机数量 | •23.9万 | ↑6.9% |
| 境内被篡改网站总数<br>其中政府网站数量 | •700<br>•33 | ↑16.7%<br>↑6.5% |
| 境内被植入后门网站总数<br>其中政府网站数量 | •564<br>•13 | ↑10.6%<br>↑62.5% |
| 针对境内网站的仿冒页面数量 | •1700 | ↑12.0% |
| 新增信息安全漏洞数量<br>其中高危漏洞数量 | •240<br>•105 | ↓36.7%<br>↓30.9% |

*=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*

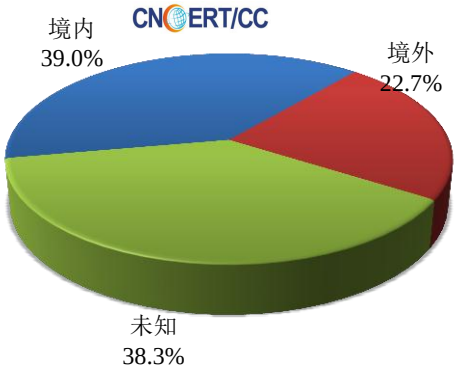
## 本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 23.9 万个，其中包括境内被木马或被僵尸程序控制的主机约 16.3 万以及境内感染飞客（conficker）蠕虫的主机约 7.6 万。

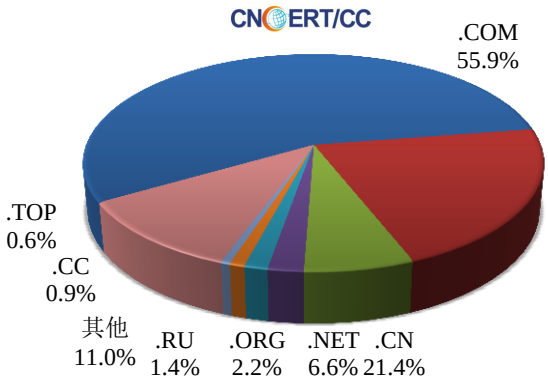


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1767 个，涉及 IP 地址 3385 个。在 1767 个域名中，有 22.7%为境外注册，且顶级域为.com 的约占 55.9%；在 3385 个 IP 中，有约 54.9%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 390 个 IP。

**本周放马站点域名注册所属境内外分布**
**(3/4-3/10)**




**本周放马站点域名所属顶级域的分布**
**(3/4-3/10)**




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。

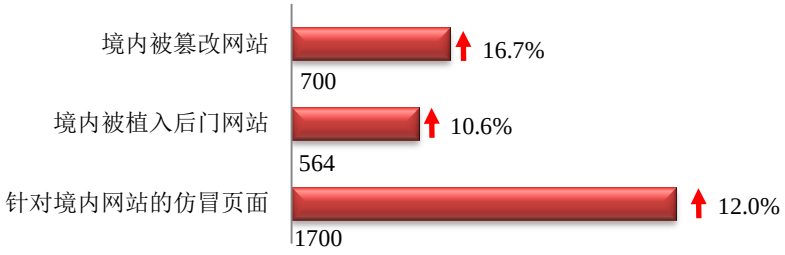
**ANVA恶意地址黑名单发布地址**

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。*

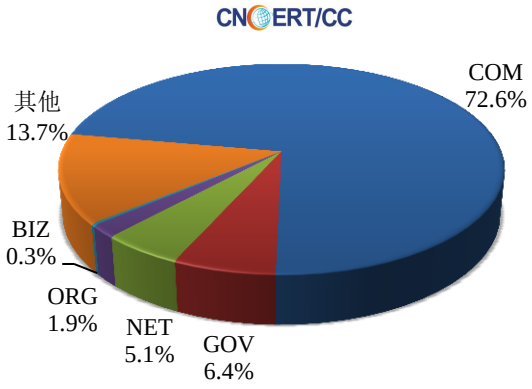
## 本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 700 个；境内被植入后门的网站数量为 564 个；针对境内网站的仿冒页面数量 1700 个。

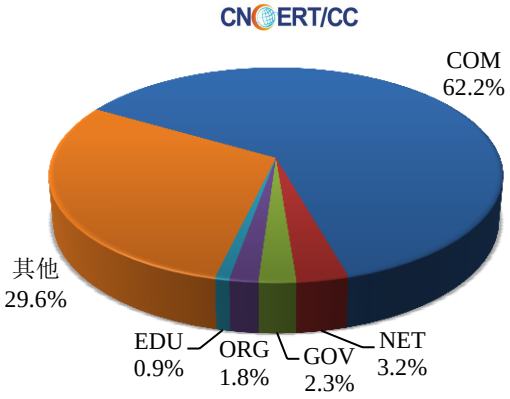


本周境内被篡改政府网站（GOV 类）数量为 33 个（约占境内 4.7%），较上周环比上升了 6.5%；境内被植入后门的政府网站（GOV 类）数量为 13 个（约占境内 2.3%），较上周环比上升了 62.5%；针对境内网站的仿冒页面涉及域名 398 个，IP 地址 273 个，平均每个 IP 地址承载了约 6 个仿冒页面。

**本周我国境内被篡改网站按类型分布**
**(3/4-3/10)**

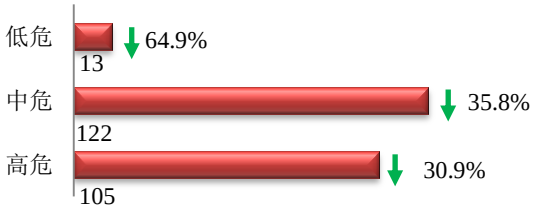



**本周我国境内被植入后门网站按类型分布**
**(3/4-3/10)**

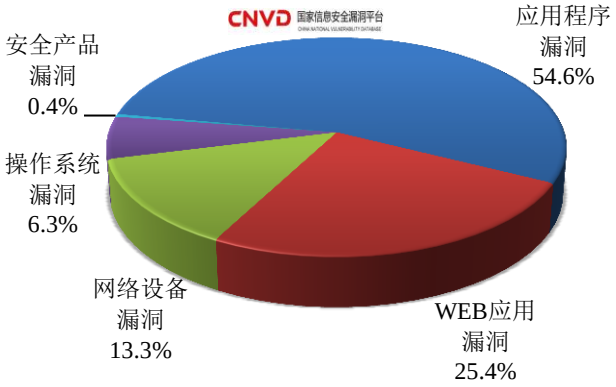



## 本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 240 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**
**(3/4-3/10)**




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**

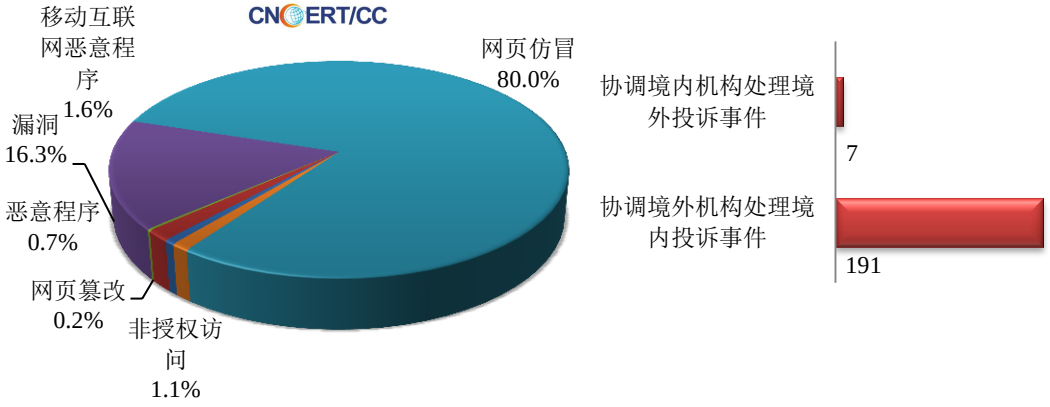
http://www.cnvd.org.cn/webinfo/list?type=4

*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 436 起，其中跨境网络安全事件 198 起。

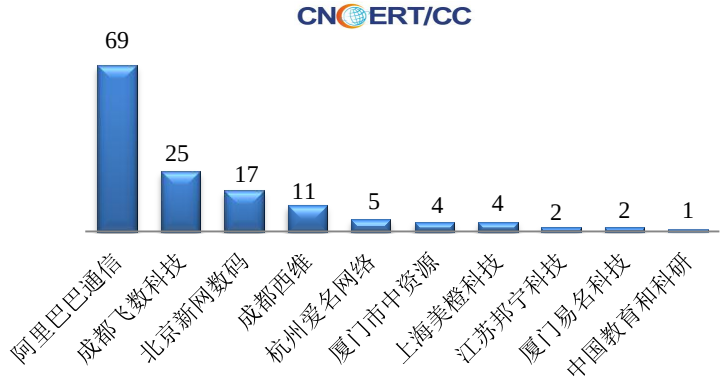
**本周CNCERT处理的事件数量按类型分布 (3/4-3/10)**




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 436 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 325 起和其他事件 10 起。

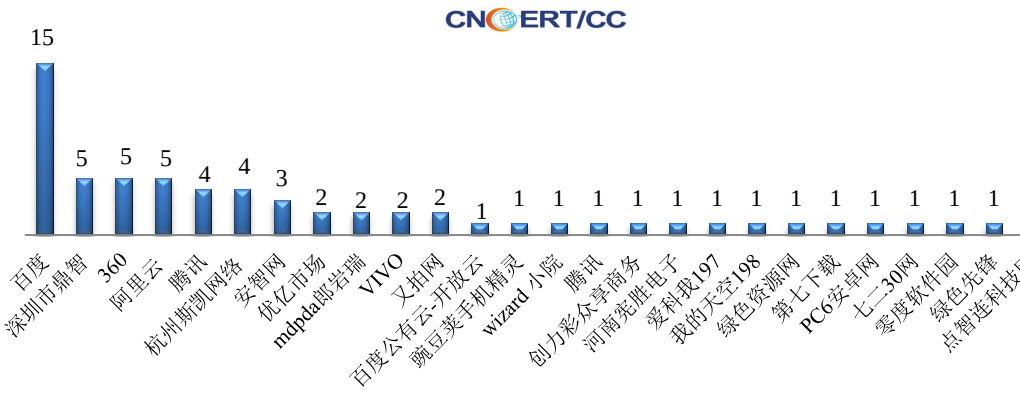
**本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (3/4-3/10)**


**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 (3/4-3/10)**



本周，CNCERT 协调 26 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 64 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 (3/4-3/10)**




## 业界新闻速递

### 1、日本拟对 IT 巨头收集个人信息追责

参考消息网 3 月 10 日报道 日本公平交易委员会基本决定，在美国谷歌和脸书等 IT 巨头非法收集、使用个人信息时，对其适用《反垄断法》。日本公平交易委员会考虑，把企业与个人之间的服务和信息交换看作交易，并视为触犯《反垄断法》中规定的“滥用优势地位”条款。对 IT 巨头，日本此前一直以企业间交易为中心重点监视，今后将目光扩大至个人。报道称，IT 巨头有强势地位，在人们使用信息检索和社交网站时收集个人信息，日本公平交易委员会将认定这种行为属于触犯规定，加以管制。

### 2、委内瑞拉电力系统再遭攻击

新华社 3 月 9 日消息 委内瑞拉总统马杜罗 9 日在首都加拉加斯表示，委电力系统当天再次遭受攻击，电力供应恢复受到极大影响据报道，7 日开始的大范围停电影响委全国 23 个州中的 18 个州。这是 2012 年以来，委持续时间最长、影响地区最广的一次停电。委新闻和通信部长指出，停电原因是古里水电站遭反对派蓄意破坏。委内瑞拉电力供应逾六成来自水力发电，其中绝大多数发电量由古里水电站提供。

### 3、沙特智能电话本应用 Dalil 被爆严重漏洞：500 万以上用户信息被泄露

cnBata.COM 年 3 月 6 日消息 Dalil 是一款类似于 Truecaller 的智能电话本应用程序，但仅限于沙特和其他阿拉伯地区用户。由于该应用所使用的 MongoDB 数据库可以在不输入密码的情况下在线访问，导致用户数据持续泄露一周时间。安全研究人员发现，在数据库中包含了这款 APP 的所有数据，从用户个人详细信息到活动

日志。 外媒对样本进行审查之后，发现该数据库中包括以下信息:用户手机号码、应用注册数据（完整姓名、电子邮件地址、Viber 账号、性别等等）、设备信息（生产日期和型号、序列号、IMEI、MAC 地址、SIM 号码、系统版本等等）、电信运营商细节、 GPS 坐标（不适用于所有用户）、个人通话详情和号码搜索。基于与每个条目相关联的国家/地区代码，数据库中包含的大多数数据属于沙特用户，此外还有少部分用户来自埃及，阿联酋，欧洲甚至一些以色列/巴勒斯坦人。数据非常的敏感，甚至可以通过 GPS 坐标数据进行跟踪。

### 4、Verifications.io 遭遇数据库泄露 邮件地址等 8 亿记录被曝光

HakerNews3 月 8 日次搜次 安全研究人员刚刚披露了一个可被公开访问的 MongoDB 数据库，其中包含了超过 8.08 亿个电子邮件地址、以及其它纯文本记录。数据库大小为 150GB，剩余的是涉及个人信息的数据缓存。该漏洞与 Verifications.io 的电子邮件验证服务相关，但于 2 月 25 日被曝光到互联网上，且允许被公众访问。泄露信息包含了 7.98 亿的电子邮件记录、超过 400 万备注了电话号码的 E-mail 地址、以及超过 600 万条被识别为‘商业线索’的信息。这些记录中的信息，包括了电子邮件、用户 IP 地址、出生日期、邮政编码、地址、性别、电话号码等内容。安全专家称之为‘一组完全独特的数据’。

## 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：何能强

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158