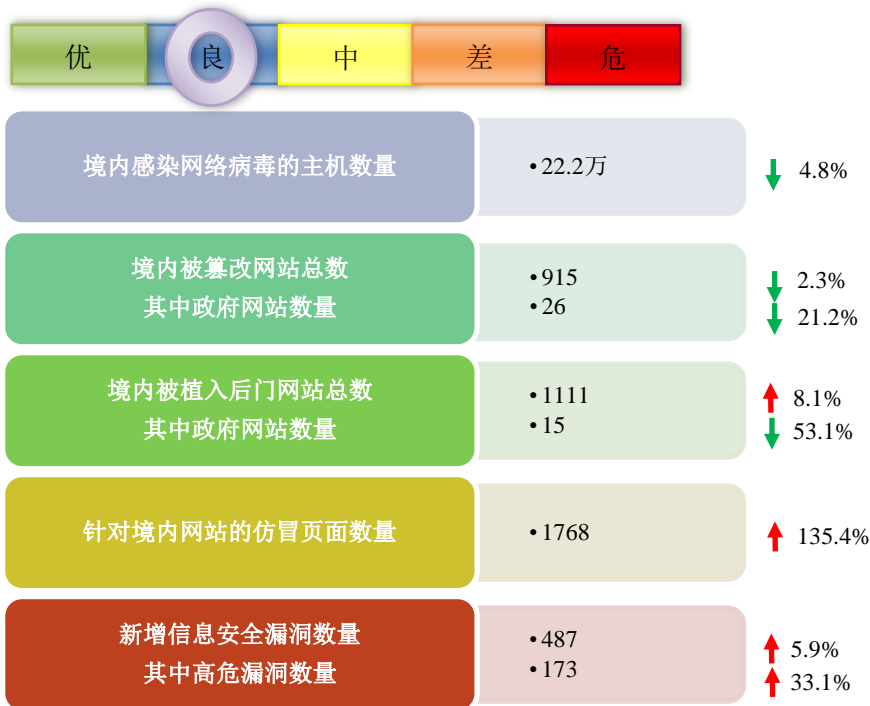


# 网络安全信息与动态周报

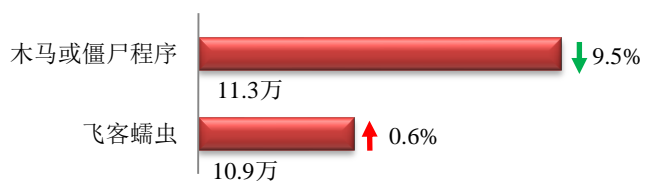
## 本周网络安全基本态势



▬ 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

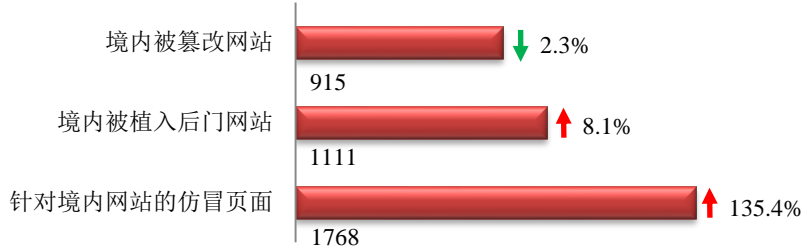
## 本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 22.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 11.3 万以及境内感染飞客（conficker）蠕虫的主机约 10.9 万。



## 本周网站安全情况

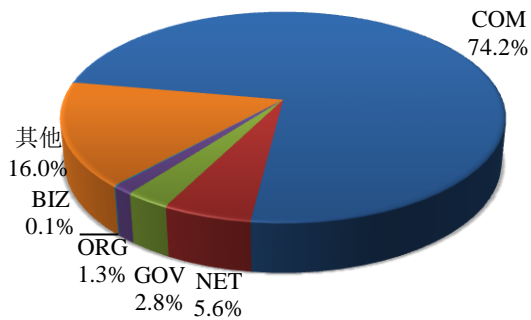
本周 CNCERT 监测发现境内被篡改网站数量为 915 个；境内被植入后门的网站数量为 1111 个；针对境内网站的仿冒页面数量为 1768。



本周境内被篡改政府网站（GOV 类）数量为 26 个（约占境内 2.8%），较上周环比下降了 21.2%；境内被植入后门的政府网站（GOV 类）数量为 15 个（约占境内 1.4%），较上周环比下降了 53.1%；针对境内网站的仿冒页面涉及域名 986 个，IP 地址 170 个，平均每个 IP 地址承载了约 10 个仿冒页面。

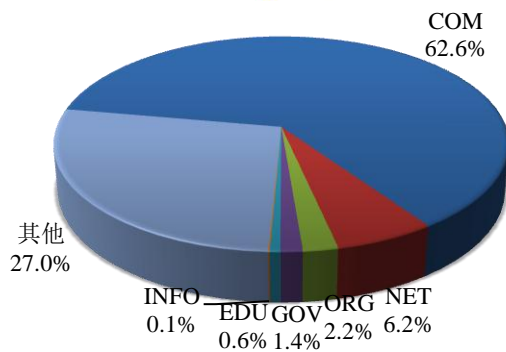
本周我国境内被篡改网站按类型分布 (3/19-3/25)

CNCERT/CC



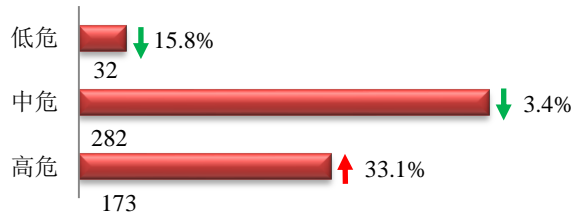
本周我国境内被植入后门网站按类型分布 (3/19-3/25)

CNCERT/CC

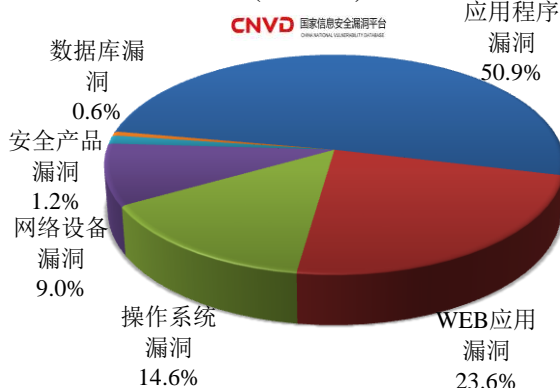


## 本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 487 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  
(3/19-3/25)



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

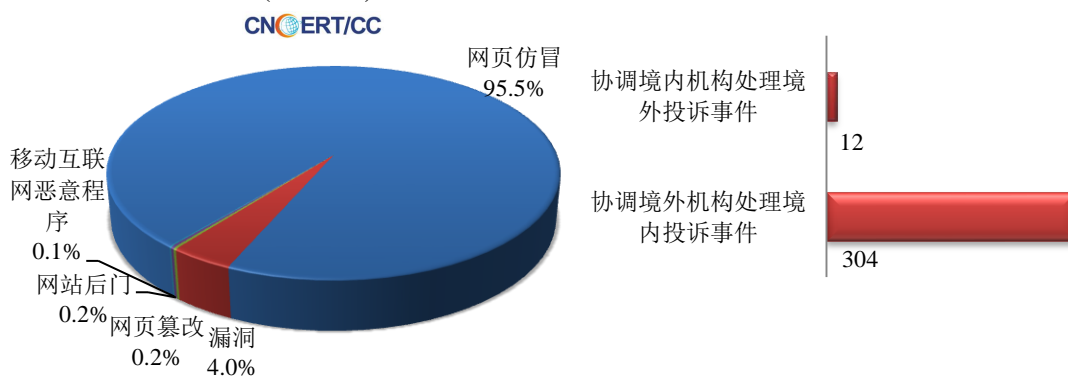
<http://www.cnvd.org.cn/webinfo/list?type=4>

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

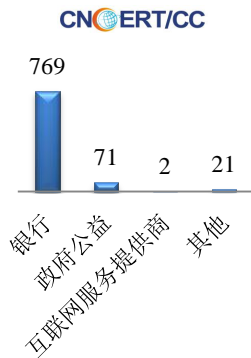
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 904 起，其中跨境网络安全事件 316 起。

本周CNCERT处理的事件数量按类型分布  
(3/19-3/25)

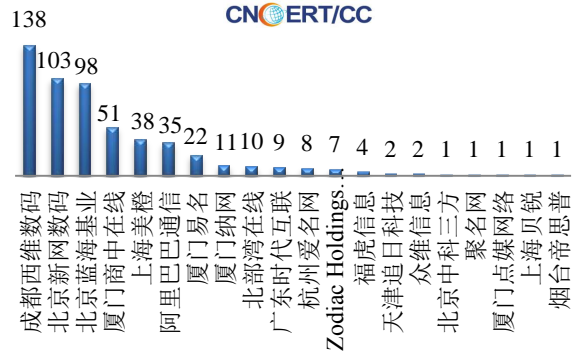


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 863 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 769 起和政府公益仿冒事件 71 起。

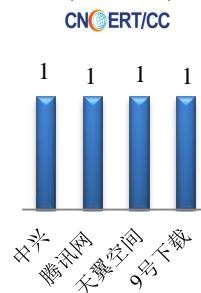
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(3/19-3/25)



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(3/19-3/25)



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(3/19-3/25)



本周，CNCERT 协调 4 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 4 个。

## 业界新闻速递

### 1、美国通过“关键基础设施”最新法案

E 安全 3 月 21 日消息 美国众议院当地时间 2018 年 3 月 19 日通过《2018DHS 网络事件响应小组法案》，提出授权由美国国土安全部（DHS）国家网络安全与通信整合中心（简称 NCCIC）下的“网络狩猎及事件响应小组”（简称 HIRT）帮助保护联邦网络和关键基础设施免于遭受网络攻击。这项法案授权 HIRT 帮助关键基础设施的所有者和运营者响应网络攻击，并提供缓解网络安全风险的策略。它还允许 DHS 部长尼尔森将私营企业的网络安全专家纳入到 HIRT 当中。此外，这项法案还要求在其成为法律之后的四年内，NCCIC 必须不断评估 HIRT，并在每个财年结束时向美国国会汇报评估结果。

## 2、韩国电信宣布在网络安全中应用区块链技术

3月22日消息 韩国著名移动运营商韩国电信（KT）在周二宣布计划采用基于区块链安全解决方案的新型电信系统。该公司的一位首席研究人员 Seo Young-il 表示，被称为“未来互联网”的韩国电信数字基础设施项目将允许人们和企业使用他们自己的数据获得奖励，而不是像 Google 这样的门户运营商垄断私人数据的访问权。融合技术研究所的区块链中心负责人在接受《韩国先驱报》采访时表示：“使用区块链技术，通过不可伪造的区块链网络传输数据可以抵御黑客的攻击，并且用户将基于信任互相传送他们自己的数据，无需依赖第三方 OTT 业务。”韩国电信的最终目标是在未来几年利用区块链技术重建韩国的网络基础设施。

## 3、亚特兰大市政支付处理系统遭黑客攻击

3月23日消息 根据 Fortune 报道，美国亚特兰大市的重要系统受到了黑客攻击，该系统是用于处理支付和访问政府信息的。根据亚特兰大市市长 Keisha Lance Bottoms 在新闻发布会上透露，目前还不知道被攻击的程度如何，但任何与亚特兰大市做生意的人——包括消费者和企业——都有可能面临风险。根据亚特兰大市当地电视台 WXIA 发布的消息，黑客称必须提供价值 51,000 美元的比特币，才能恢复系统工作。本次袭击事件最初是在本周四（3月22日）上午 5 点被发现的，之后大量企业内部和面向客户的应用程序无法使用，其中就包括一些用于支付账单或访问政府信息的应用程序。

## 4、波多黎各电力局（PREPA）遭遇黑客入侵

3月23日消息 外媒 3月21日消息，波多黎各电力局（PREPA）本周一证实其计算机基础设施曾在周末遭受了黑客入侵。目前 PREPA 确认此次事件没有对用户带来风险，因为黑客并没有访问其客户服务系统，数据信息也没有受到破坏。值得注意的是，美国政府几天前曾发出警告称俄罗斯资助黑客组织发起针对美国关键基础设施的网络攻击。不过目前并没有证据表明俄罗斯黑客参与了 PREPA 的攻击事件，因为黑客人士采用了复杂的技术来隐藏自己，使得调查该网络攻击变得非常困难。根据 PREPA 发言人的说法，目前有关部门正在对该事件进行调查，但拒绝透露有哪些政府部门参与。

## 5、Facebook 最大规模资料外泄！5000 万用户或“被助选”

3月19日消息 美国总统特朗普在 2016 年大选时曾聘用一家数据分析公司，传媒揭发它从 2014 年起，违法收集社交网脸书网 Facebook 上 5000 万名美国用户的数据，用来设计软件，预测和影响选民的大选投票取向，协助特朗普取胜。该数据分析公司被指与俄罗斯有关连，已成“通俄门”特别检察官米勒的调查对象。外媒称，脸书网对这宗历来最大用户数据外泄事件早已知情，但未有采取补救措施。报道称，事件主角是一家名为“剑桥分析”（Cambridge Analytica）的数据分析公司，早于 2013 年底，它已获得特朗普支持者、保守派金主默瑟投资，并获得后来成为白宫首席策略师的班农支持，尝试通过收集大数据及心理分析，操控美国选举结果。2014 年美国中期选举前，公司开始与剑桥大学美籍俄裔心理学家科甘合作，通过后者设计的心理测验脸书应用程序，在脸书上收集用户数据。“剑桥分析”将 Facebook 用户数据被窃归咎于科甘，并声称已经删除所得数据，而且从没使用来为特朗普助选。不过揭发事件的《纽约时报》及《观察家报》指出，“剑桥分析”还未删除这些数据。英国国会媒体委员会批评脸书网误导国会，隐瞒用户在未经授权下遭盗用数据的风险，有议员要

求脸书网创办人扎克伯格到国会接受质询。

## 6、Expedia 旗下在线旅行社“Orbitz”88 万用户信用卡数据泄露

HackerNews.cc 3 月 21 日消息 外媒 3 月 20 日消息，美国在线旅游巨头 Expedia 旗下的旅游网站 Orbitz 于本周二披露了一项安全漏洞，致使约 88 万 Orbitz 用户受到数据泄露影响，其中包括姓名、出生日期、性别、电话号码、电子邮件地址、账单地址以及支付卡数据等详细信息。据调查人员称，受到数据泄露影响的可能是 2016 年 1 月 1 日至 2017 年 12 月 22 日期间在 Orbitz 平台上进行过交易的用户。不过目前没有证据表明 Orbitz 网站受到此次事件的影响，并且用户的护照和旅行行程信息也被认为未曾遭到泄露。Orbitz 方面表示已通知受影响的客户和合作伙伴，并免费为其客户以及合作伙伴提供一年的信用监控和身份保护服务。

## 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：朱天

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：010-82990158