国家互联网应急中心

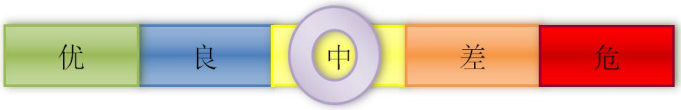
# 网络安全信息与动态周报

2020 年第 23 期

6 月 1 日-6 月 7 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 | •14.7万 | 51.2% |
| 境内被篡改网站总数<br>其中政府网站数量 | •7473<br>•36 | 9.1%<br>50.0% |
| 境内被植入后门网站总数<br>其中政府网站数量 | •1350<br>•8 | 18.4%<br>33.3% |
| 针对境内网站的仿冒页面数量 | •686 | 8.4% |
| 新增信息安全漏洞数量<br>其中高危漏洞数量 | •465<br>•150 | 49.0%<br>63.0% |

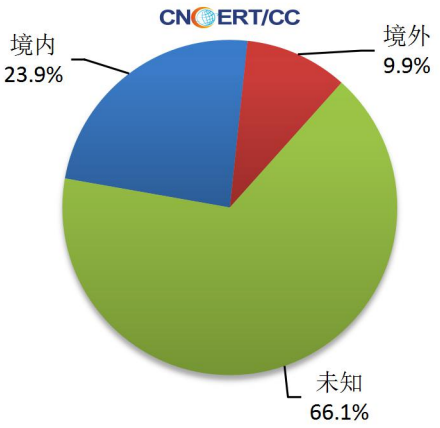
*表示数量与上周相同* *表示数量较上周环比增加* *表示数量较上周环比减少*

## 本周网络病毒活动情况

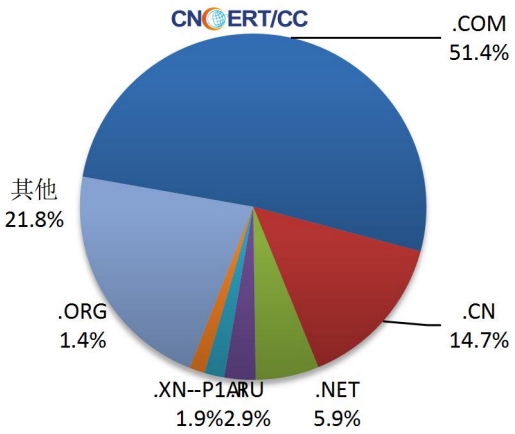
本周境内感染网络病毒的主机数量约为 14.7 万个，其中包括境内被木马或被僵尸程序控制的主机约 8.1 万以及境内感染飞客（conficker）蠕虫的主机约 6.6 万。

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 1610 个，涉及 IP 地址 4808 个。在 1610 个域名中，有 9.9%为境外注册，且顶级域为.com 的约占 51.4%；在 4808 个 IP 中，有约 61.9%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 379 个 IP。

本周放马站点域名注册所属境内外分布
(6/1-6/7)




本周放马站点域名所属顶级域的分布
(6/1-6/7)




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。

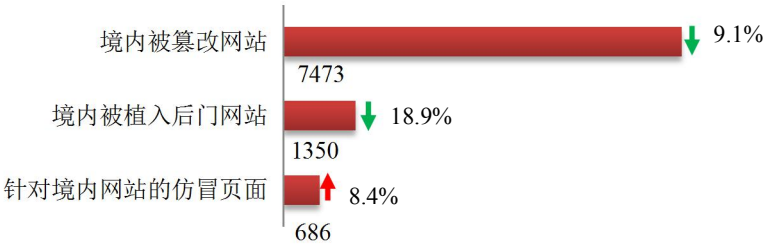
**ANVA网络安全威胁信息共享平台**

**https://share.anva.org.cn/web/publicity/listurl**

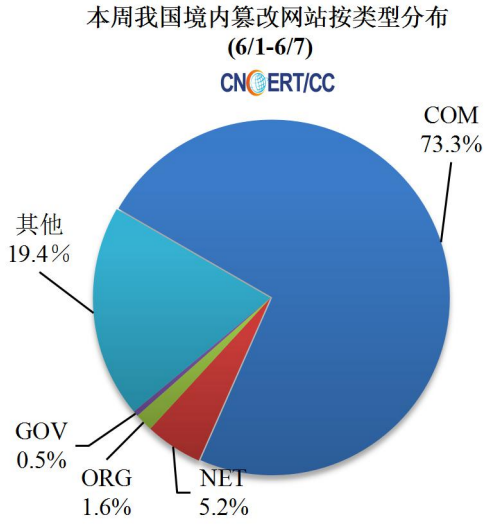
*中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由 CNCERT 发起并组织运作的行业联盟。*

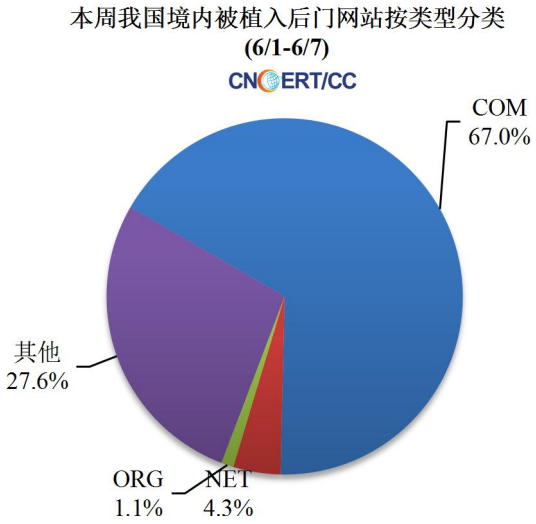
## 本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 7473 个；被植入后门的网站数量为 1350 个；针对境内网站的仿冒页面数量 686 个。



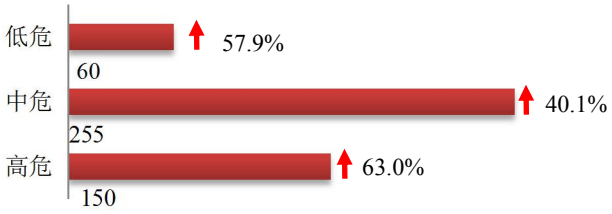
本周境内被篡改政府网站（GOV 类）数量为 36 个（约占境内 0.5%），较上周上涨了 50.0%；境内被植入后门的政府网站（GOV 类）数量为 8 个（约占境内 0.6%），较上周上涨了 33.3%。

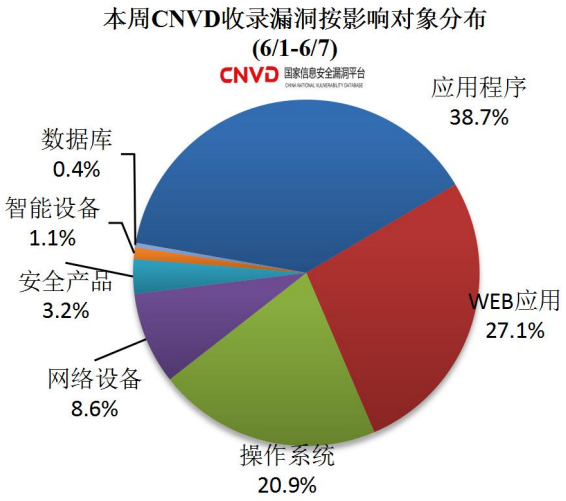



## 本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 465 个，信息安全漏洞威胁整体评价级别为中。




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 应用和操作系统。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

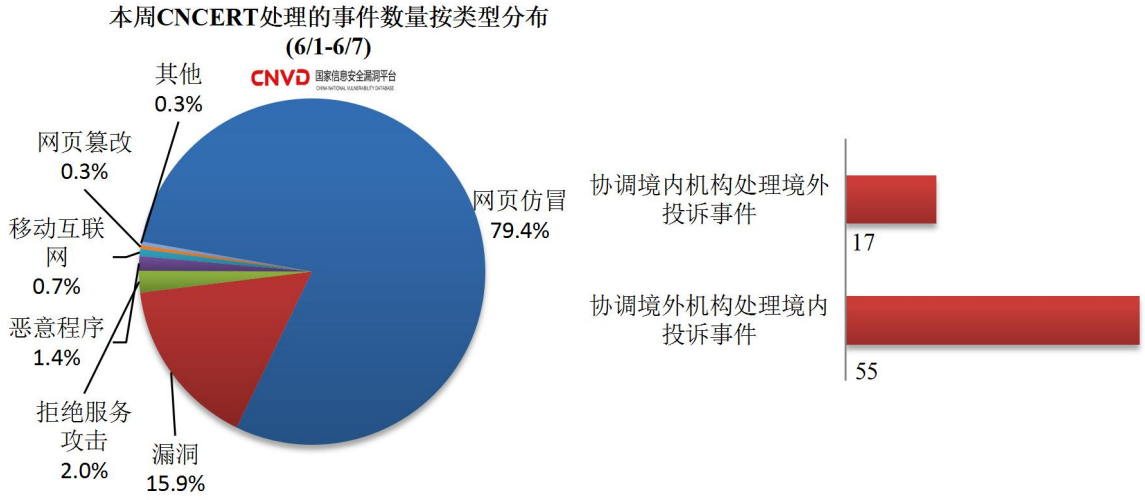
**CNVD漏洞周报发布地址**

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

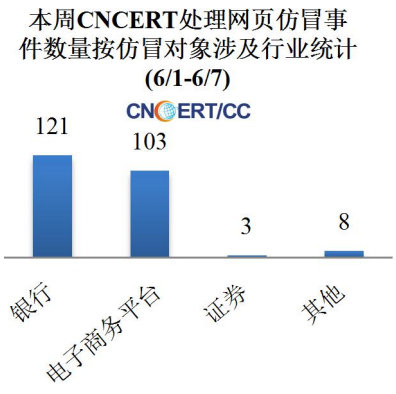
*国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。*

## 本周事件处理情况

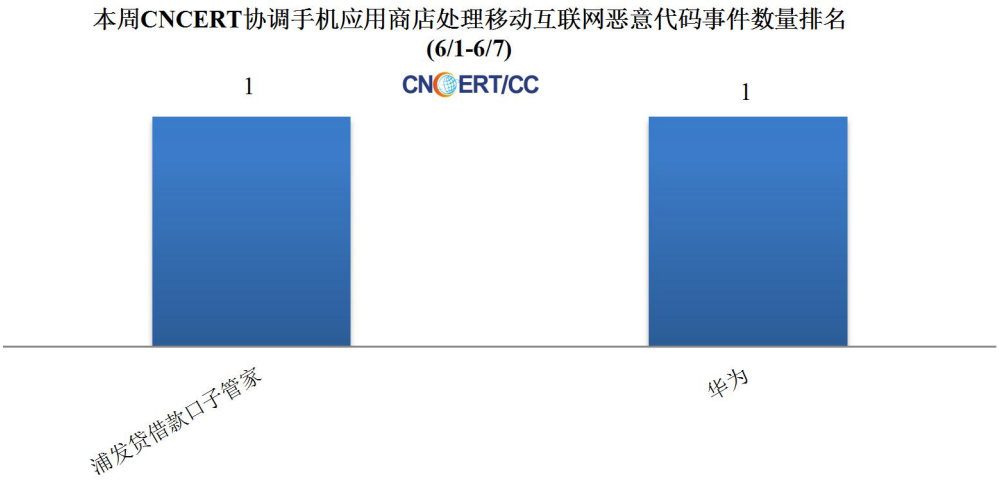
本周，CNCERT 协调基础电信企业、云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 296 起，其中跨境网络安全事件 72 起。




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 235 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 121 起、电子商务平台 103 起、证券 3 起和其他事件 8 起。




本周，CNCERT 协调 2 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 2 个。




## 业界新闻速递

### 1、《网络安全审查办法》6 月 1 日起正式生效

由国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、国家安全部、财政部、商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管理局联合制定的《网络安全审查办法》已于今年 6 月 1 日起正式实施。

网络安全审查重点评估关键信息基础设施运营者采购网络产品和服务可能带来的国家安全风险，包括：产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或破坏，以及重要数据被窃取、泄露、毁损的风险；产品和服务供应中断对关键信息基础设施业务连续性的危害；产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险；产品和服务提供者遵守中国法律、行政法规、部门规章情况；其他可能危害关键信息基础设施安全和国家安全的因素。

### 2、英国武装部队启动首个专用网络军团

近日，据英国国防部官方网站消息，英国国防部长本·华莱士宣布，随着国防部继续进行现代化改造以应对明天的威胁，新的网络军团已启动，以保护前线作战免受数字攻击。英国国防部已经启动了第 13 信号团，这是英国武装部队的第一个专用网络军团，它将保护国内和海外行动中的重要国防网络。该部队于 6 月 1 日星期一在皇家信号装置之家布兰福德举行的仪式上正式成立。第 13 信号军团是英国第 6 师下属的第 1 英军信号旅

中的英军团，负责进行情报机动和非常规战争，以支持整个武装部队。该专家单位将提供新的陆军网络信息安全运营中心的基础，重点是保护国防的网络领域，并将与皇家海军和皇家空军合作，为所有军事通信提供安全的网络。

### 3、加拿大 CPA 披露数据泄露暴露 32.9 万人信息

加拿大注册专业会计师协会（CPA）6 月 4 日披露，该网站遭到网络攻击，未经授权的第三方访问了超过 329,000 名成员和其他利益相关者的个人信息。加拿大注册专业会计师协会在尚未公开的日期发现数据泄露后，采取措施保护受损系统，遏制了事件的发生，并在确认受损系统后通知受影响的个人。违规通知中写道:“涉及的信息主要与 CPA 杂志的发行有关，包括姓名、地址、电子邮件地址和雇主姓名等个人信息。”这些组织表示，事件中还暴露了密码和完整的信用卡号，但它们都“受到加密保护”。

### 4、中国台湾地区发生重大个人数据泄露事件，84%公民信息出现在暗网

6 月 4 日，据威胁情报机构 Cyble 消息，研究人员在暗网上发现圈内知名卖家放出了一个“台湾全省房屋登记数据库”的数据库，大约 3.5GB，包含 2000 万条记录。目前中国台湾地区人口为 2380 万人，这意味着 84%中国台湾地区人员的个人数据都遭到了泄露。Cyble 称，3.5GB 的数据库包含个人的全名、邮政地址、电话号码、身份 ID、性别和出生日期，这则泄漏将成为有史以来最大规模的公众数据泄露事件之一。到目前为止，尚未无法确定数据泄露的时间。

### 5、VMware Cloud Director 严重漏洞可导致黑客接管企业服务器

6 月 2 日，据外媒报道，网络安全研究员在 VMware 的 Cloud Director 平台上发现了一个新漏洞，可导致攻击者获得对敏感信息的访问权限并控制整个基础设施中的私有云。该漏洞的编号是 CVE-2020-3956，是一个代码注入缺陷，因不正确的输入处理而导致，可被通过身份验证的攻击者将恶意流量发送给 Cloud Director，从而导致任意代码执行的后果。该漏洞的 CVSS v3 评分为 8.8 分，属于“严重”漏洞级别。VMware 公司指出，该漏洞可通过基于 HTML5 和 Flex 的 UI、API Explorer 接口和 API 访问权限遭利用。该漏洞影响 VMware Cloud Director10.0.0.2 之前的 10.0.x 版本、9.7.0.5 之前的 9.7.0.x 版本、9.5.0.6 之前的 9.5.0.x 版本以及 9.1.0.4 之前的 9.1.0.x 版本。

## 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 2019 年，CNCERT 已与 78 个国家和地区的 260 个组织建立了“CNCERT 国际合作伙伴”关系。CNCERT 还积极参加亚太经合组织、国际电联、上合组织、东盟、金砖等政府层面国际和区域组织的网络安全相关工作。

## 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：文静

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315