国家互联网应急中心

# 网络安全信息与动态周报

2022 年第 26 期

6 月 20 日-6 月 26 日

CNCERT/CC

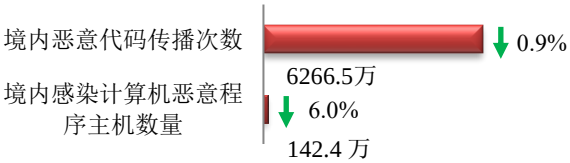
## 本周网络安全基本态势


| | | |
|---|---|---|
| 境内计算机恶意程序传播次数<br>境内感染计算机恶意程序主机数量 | • 6266.5万<br>• 142.4万 | ↓ 0.9%<br>↓ 6.0% |
| 境内被篡改网站总数<br>其中政府网站数量 | • 1835<br>• 9 | ↑ 155.9% |
| 境内被植入后门网站总数<br>其中政府网站数量 | • 670<br>• 0 | ↑ 8.9% |
| 针对境内网站的仿冒页面数量 | • 13001 | ↓ 1.3% |
| 新增信息安全漏洞数量<br>其中高危漏洞数量 | • 383<br>• 149 | ↓ 19.2%<br>↑ 2.1% |

*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

境内计算机恶意程序传播次数约为 6266.5 万次，境内感染计算机恶意程序主机数量约为 142.4 万个。



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 2423 个，涉及 IP 地址 5503 个。在 2423 个域名中，最多的顶级域为.com 类。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 194 个。

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。

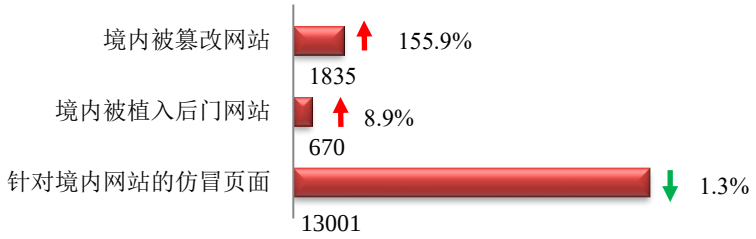
**ANVA网络安全威胁信息共享平台**

**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。*

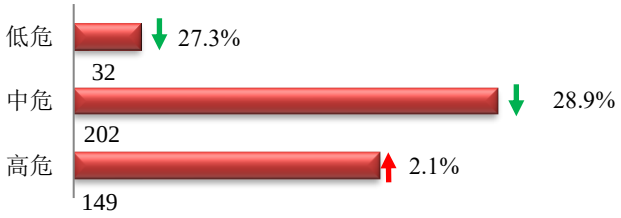
## 本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 1835 个；被植入后门的网站数量为 670 个；针对境内网站的仿冒页面数量 13001 个。




## 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 383 个，信息安全漏洞威胁整体评价级别为中。其中，Web 应用占比最高，其次是应用程序和网络设备。



**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。*

更多漏洞有关的详细情况，请见CNVD漏洞周报。

## 本周事件处理情况

本周，CNCERT协调云服务商、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网络安全事件2990起，含跨境网络安全事件2755起。其中，协调境内外域名注册机构、境外CERT等机构重点处理2810起页仿冒投诉事件。协调41个提供恶意移动应用程序下载服务的平台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1521个。

## 业界新闻速递

### 1. 国务院印发《关于加强数字政府建设的指导意见》

6月23日，据中国政府网消息，国务院发布《关于加强数字政府建设的指导意见》。意见要求全面强化数字政府安全管理责任，落实安全管理制度，加快关键核心技术攻关，加强关键信息基础设施安全保障，强化安全防护技术应用，切实筑牢数字政府建设安全防线。包括建立健全数据分类分级保护、风险评估、检测认证等制度，加强数据全生命周期安全管理和技术防护。加大对涉及国家秘密、工作秘密、商业秘密、个人隐私和个人信息等数据的保护力度，完善相应问责机制，依法加强重要数据出境安全管理。加强关键信息基础设施安全保护和网络安全等级保护，建立健全网络安全、保密监测预警和密码应用安全性评估的机制，定期开展网络安全、保密和密码应用检查，提升数字政府领域关键信息基础设施保护水平。建立健全动态监控、主动防御、协同响应的数字政府安全技术保障体系。充分运用主动监测、智能感知、威胁预测等安全技术，强化日常监测、通报预警、应急处置，拓展网络安全态势感知监测范围，加强大规模网络安全事件、网络泄密事件预警和发现能力。

### 2. 国家网信办网络安全审查办公室对知网启动网络安全审查

6月24日，据中国网信网消息，国家互联网信息办公室网络安全审查办公室有关负责人表示，为防范

国家数据安全风险，维护国家安全，保障公共利益，依据《国家安全法》《网络安全法》《数据安全法》，按照《网络安全审查办法》，2022 年 6 月 23 日，网络安全审查办公室约谈同方知网（北京）技术有限公司负责人，宣布对知网启动网络安全审查。据悉，知网掌握着大量个人信息和涉及国防、工业、电信、交通运输、自然资源、卫生健康、金融等重点行业领域重要数据，以及我重大项目、重要科技成果及关键技术动态等敏感信息。

### 3. 全国信安标委发布《网络安全标准实践指南个人信息跨境处理活动安全认证规范》

6 月 24 日，据全国信安标委官网消息，为落实《个人信息保护法》关于建立个人信息保护认证制度的相关要求，指导个人信息处理者规范开展个人信息跨境处理活动，全国信安标委秘书处组织编制了《网络安全标准实践指南—个人信息跨境处理活动安全认证规范》。本《实践指南》提出了个人信息跨境处理活动安全的基本原则，规定了个人信息跨境处理活动的基本要求和个人信息主体权益保障要求。全文请参见官方网站。

## 关于国家互联网应急中心（CNCERT）

国家计算机网络应急技术处理协调中心（英文简称 CNCERT/CC），成立于 2001 年 8 月，为非政府非盈利的网络安全技术中心，是中国计算机网络应急处理体系中的牵头单位。作为国家级应急中心，CNCERT/CC 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，运行和管理国家信息安全漏洞共享平台（CNVD），维护公共互联网安全，保障关键信息基础设施的安全运行。

CNCERT/CC 在中国大陆 31 个省、自治区、直辖市设有分支机构，并通过组织网络安全企业、学校、社会组织和研究机构，协调骨干网络运营单位、域名服务机构和其他应急组织等，构建中国互联网安全应急体系，共同处理各类互联网重大网络安全事件。CNCERT/CC 积极发挥行业联动合力，发起成立了中国反网络病毒联盟（ANVA）和中国互联网网络安全威胁治理联盟（CCTGA）。

同时，CNCERT/CC 积极开展网络安全国际合作，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 2021 年，已与 81 个国家和地区的 274 个组织建立了“CNCERT/CC 国际合作伙伴”关系。CNCERT/CC 是国际应急响应与安全组织 FIRST 的正式成员，以及亚太计算机应急组织 APCERT 的发起者之一，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：王小群

网址： www.cert.org.cn

Email：cncert_report@cert.org.cn

电话： 010-82990315