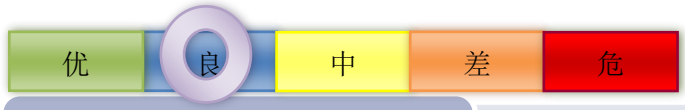
国家互联网应急中心

2022 年第 25 期

6 月 13 日-6 月 19 日

网络安全信息与动态周报

本周网络安全基本态势

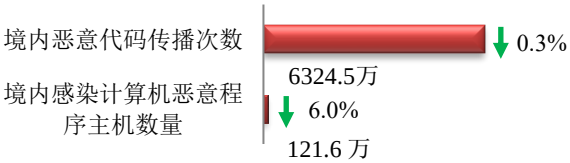


境内计算机恶意程序传播次数 境内感染计算机恶意程序主机数量	• 6342.5万 • 121.6万	↓ 0.3% ↓ 6.0%
境内被篡改网站总数 其中政府网站数量	• 717 • 1	↓ 117.5%
境内被植入后门网站总数 其中政府网站数量	• 615 • 0	↑ 56.1%
针对境内网站的仿冒页面数量	• 13176	↑ 176.3%
新增信息安全漏洞数量 其中高危漏洞数量	• 474 • 146	↓ 12.5% ↓ 13.6%

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 6342.5 万次，境内感染计算机恶意程序主机数量约为 121.6 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 7334 个，涉及 IP 地址 15382 个。在 7334 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 279 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。

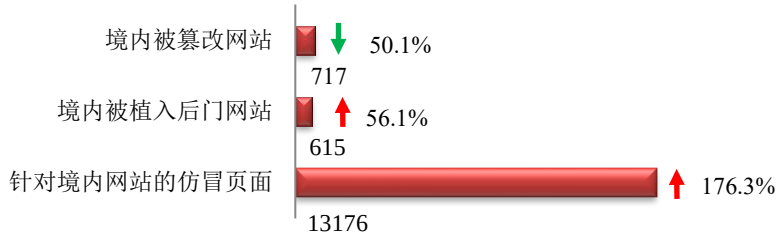
ANVA网络安全威胁信息共享平台

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。

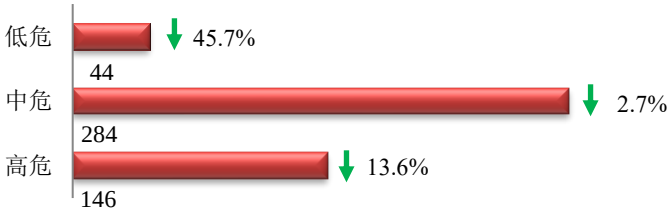
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 717 个；被植入后门的网站数量为 615 个；针对境内网站的仿冒页面数量 13176 个。



本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞474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2094起，含跨境网络安全事件1913起。其中，协调境内外域名注册机构、境外CERT等机构重点处理1914起页仿冒投诉事件。 协调 15 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49个。

业界新闻速递

1. 关于Mirai变种Miori僵尸网络大规模传播的风险提示

6月14日，据CNCERT官网消息，CNCERT与奇安信科技集团股份有限公司（奇安信）共同发布《关于Mirai变种Miori僵尸网络大规模传播的风险提示》。近期，CNCERT和奇安信共同监测发现一个在互联网上快速传播新的DDoS僵尸网络，通过跟踪监测发现其每日上线境内肉鸡数（以IP数计算）最多已超过1万、且每日会针对多个攻击目标发起攻击，给网络空间带来较大威胁。该僵尸网络为Mirai变种，包括针对mips、arm、x86等CPU架构的样本，由于该僵尸网络样本均以miori命名，因此将其命名为Mirai_miori。在2个月的时间中，捕获到Mirai_miori僵尸网络样本至少迭代过3个版本，具有9个传播源，涉及6个C2服务器，传播方式主要为弱口令爆破以及1 day和N day漏洞。Mirai_miori僵尸网络出现以来所投递的样本变动很小，运营者将主要精力投入到漏洞搜集利用以及更换C2服务器上。报告详情请参见官网。

2. 国家互联网信息办公室修订《移动互联网应用程序信息服务管理规定》发布施行

6月14日，据中国网信网消息，国家互联网信息办公室6月14日发布新修订的《移动互联网应用程序信息服务管理规定》（以下简称新《规定》）。新《规定》自2022年8月1日起施行。国家互联网信息办公室有关负责人表示，修订发布新《规定》旨在进一步依法监管移动互联网应用程序，促进应用程序信息服

务健康有序发展。《移动互联网应用程序信息服务管理规定》自 2016 年 8 月 1 日施行以来，对于维护网络信息内容生态，保护公民、法人和其他组织的合法权益发挥了积极作用。但随着移动应用程序快速发展、广泛应用，新情况新问题不断出现，需要适应形势发展进行修订完善。新《规定》共 27 条，包括信息内容主体责任、真实身份信息认证、分类管理、行业自律、社会监督及行政管理等条款。详情请参见中国网信网。

3. Microsoft 发布 2022 年 6 月安全更新

6 月 15 日，据国家信息安全漏洞共享平台 CNVD 消息，6 月 14 日，微软发布了 2022 年 6 月份的月度例行安全公告，修复了多款产品存在的 56 个安全漏洞。受影响的产品包括：Windows 11（28 个）、Windows Server 2022（29 个）、Windows 10 21H2（29 个）、Windows 10 21H1（29 个）、Windows 10 20H2 & Windows Server v20H2（31 个）、Windows Server 2012（23 个）、Windows RT 8.1（21 个）和 Microsoft Office-related software（7 个）。CNVD 提醒广大 Microsoft 用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

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：胡俊

网址： www.cert.org.cn

Email：cncert_report@cert.org.cn

电话： 010-82990315