国家互联网应急中心

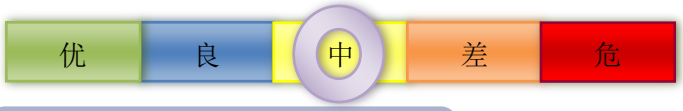
网络安全信息与动态周报

2021 年第 13 期

3 月 22 日-3 月 28 日

CNCERT/CC

本周网络安全基本态势

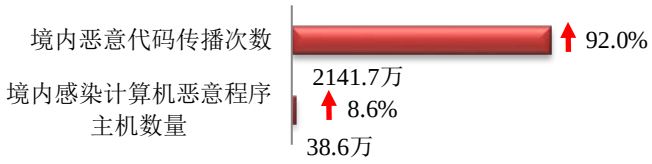


境内计算机恶意程序传播次数 境内感染计算机恶意程序主机数量	•2141.7万 •38.6万	↑92.0% ↑8.6%
境内被篡改网站总数 其中政府网站数量	•3198 •13	↑73.8% ↑44.4%
境内被植入后门网站总数 其中政府网站数量	•563 •9	↑7.9% ↑350%
针对境内网站的仿冒页面数量	•982	↑155.1%
新增信息安全漏洞数量 其中高危漏洞数量	•719 •166	↑5.9% ↑38.3%

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

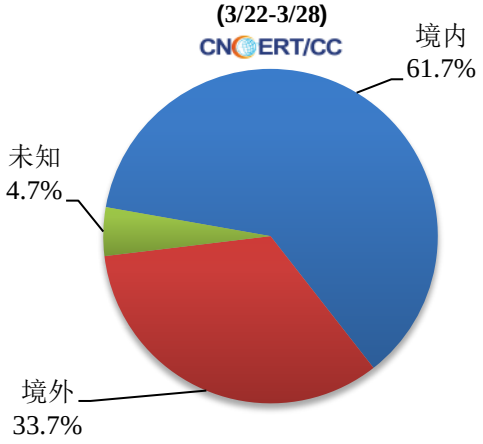
本周网络病毒活动情况

境内计算机恶意程序传播次数约为 2141.7 万次，境内感染计算机恶意程序主机数量约为 38.6 万个。

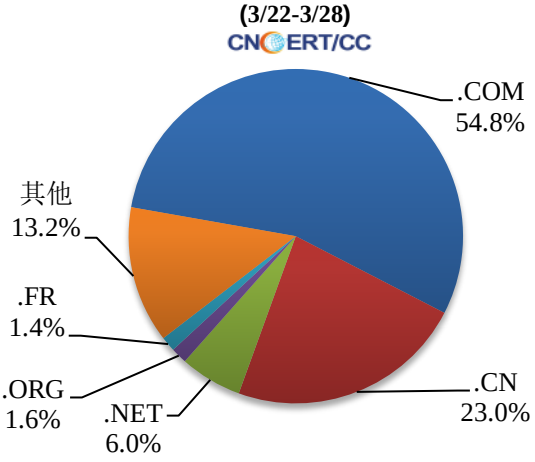


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 832 个，涉及 IP 地址 4408 个。在 832 个域名中，有 33.7%为境外注册，且顶级域为.com 的约占 54.8%；在 4408 个 IP 中，有约 40.8%于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 420 个。

本周放马站点域名注册所属境内外分布
(3/22-3/28)



本周放马站点域名注册所属顶级域分布
(3/22-3/28)



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。

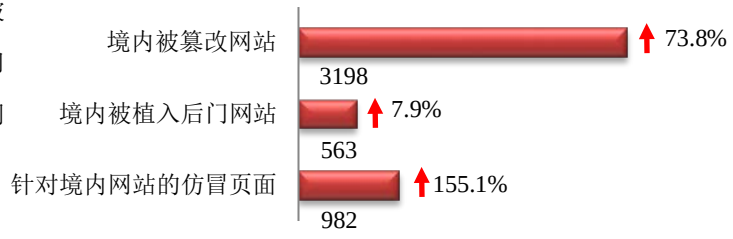
ANVA网络安全威胁信息共享平台

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。

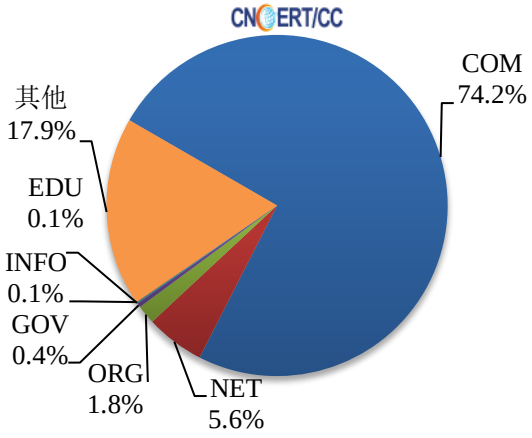
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 3198 个；被植入后门的网站数量为 563 个；针对境内网站的仿冒页面数量为 982 个。

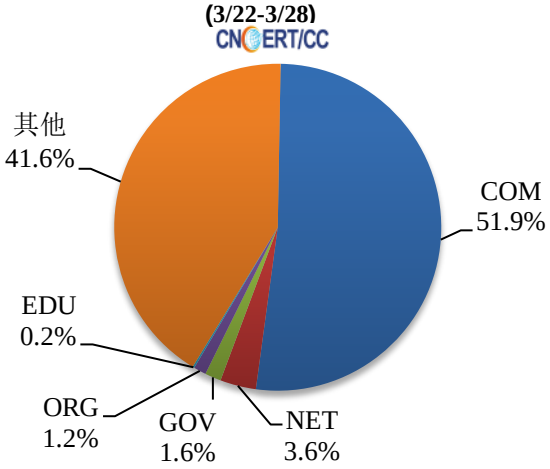


本周境内被篡改政府网站（GOV 类）数量为 13 个（约占境内 0.6%），较上周上升了 44.4%；境内被植入后门的政府网站（GOV 类）数量为 9 个。

本周我国境内篡改网站按类型分布
(3/22-3/28)

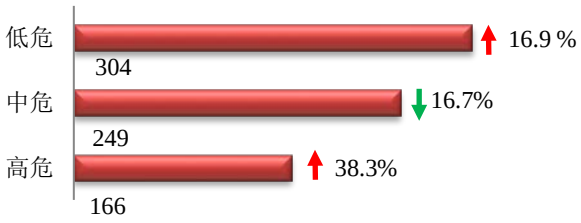


本周我国境内被植入后门网站按类型分布
(3/22-3/28)

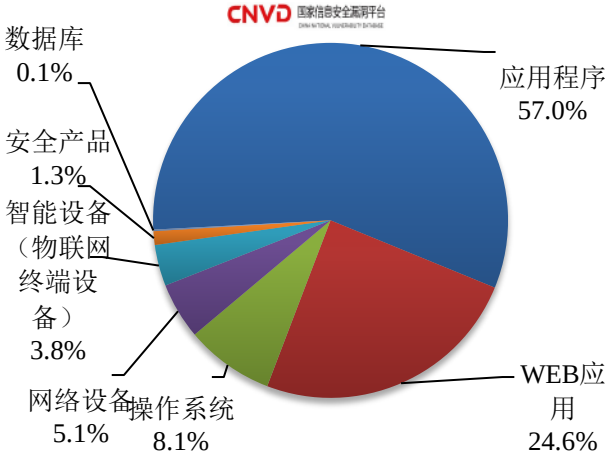


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 719 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分布
(3/22-3/28）



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。

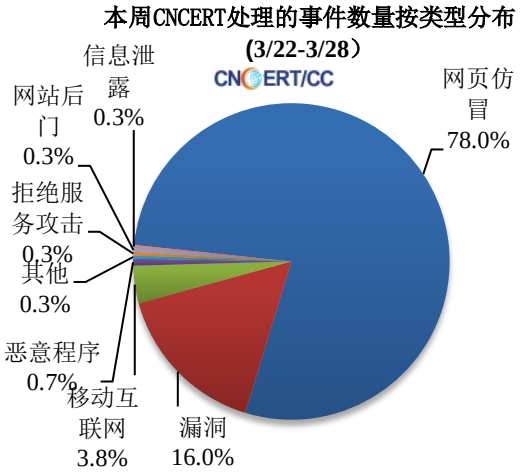
CNVD漏洞周报发布地址

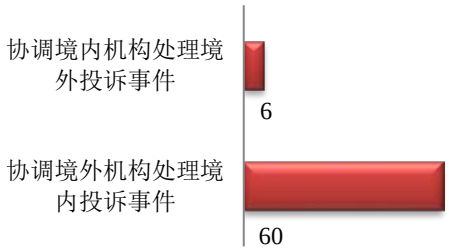
http://www.cnvd.org.cn/webinfo/list?type=4

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。

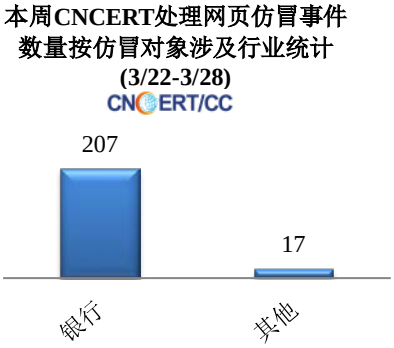
本周事件处理情况

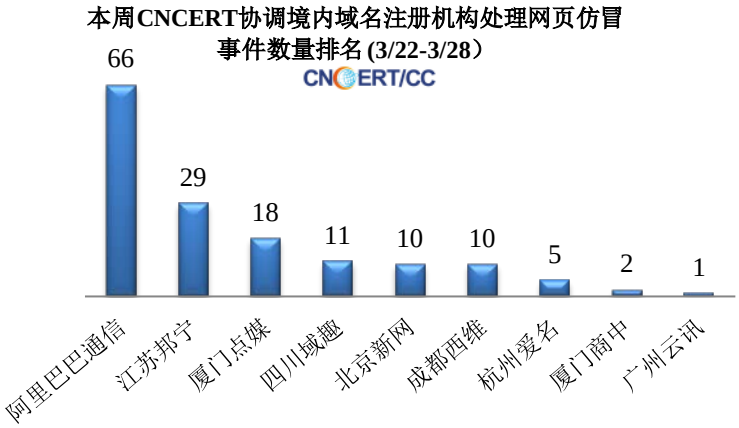
本周，CNCERT 协调云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 287 起，其中跨境网络安全事件 66 起。





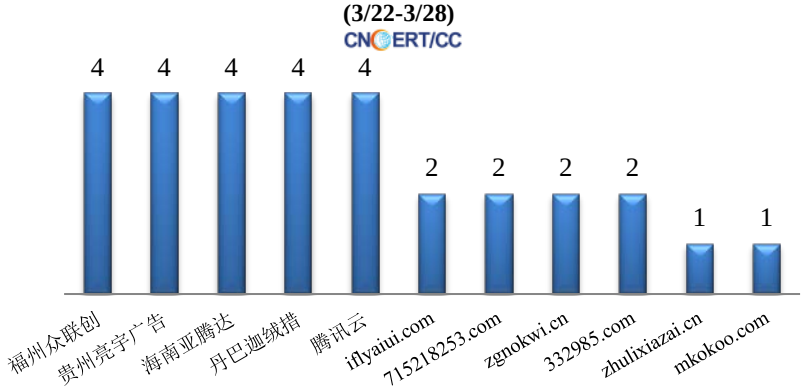
本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理 224 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，银行仿冒事件 207 起，其他事件 17 起。





本周，CNCERT 协调 12 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 30 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
(3/22-3/28)



业界新闻速递

1. Microsoft 发布 2021 年 3 月安全更新

3 月 22 日，据国家信息安全漏洞共享平台（CNVD）官网消息，近日微软发布了 2021 年 3 月份的月度例行安全公告，修复了其多款产品存在的 89 个安全漏洞。受影响的产品包括：Windows 10 20H2 & Windows Server v20H2（48 个）、Windows 10 2004 &Windows Server v2004（48 个）、Windows 10 1909 &Windows Server v1909（47 个）、Windows 8.1 & Server 2012 R2（27 个）、Windows Server 2012（26 个）和 Microsoft Office-related software（9 个）。利用上述漏洞，攻击者可以绕过安全功能限制，获取敏感信息，提升权限，执行远程代码，或发起拒绝服务攻击等。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。

2. 推动金融网关建设 提升跨境金融网络与信息服务水平

3 月 23 日，据中国人民银行官网消息，随着我国金融业对外开放不断深化，我国境内金融机构越来越多使用环球银行金融电信协会（SWIFT）提供的跨境金融网络与信息服务，参与机构、业务规模日益增长，对业务连续性、稳定性和数据的合规性、安全性均提出了更高要求。人民银行高度重视相关要求，于 2018 年发布了《关于加强跨境金融网络与信息服务管理的通知》。为进一步提升跨境金融网络与信息服务水平，保障 SWIFT 境内用户（以下简称用户）合法权益和业务连续性，SWIFT 与 4 家中资机构合资成立金融网关信息服务有限公司，向用户提供金融网关服务，包括建立并运营金融报文服务的本地网络集中点、建立并运营本地数据仓库等服务。SWIFT 与中资机构合作开展金融网关服务有利于实现互利共赢，为用户提供更为稳定、韧性强、安全且合规的服务。下一步，人民银行将加强督促指导，推动各方规范开展金融网关业务。

3. 工信部印发《“双千兆”网络协同发展行动计划（2021-2023 年）》，要求重点强化安全保障

3 月 25 日，据工信部网站消息，工信部发布《“双千兆”网络协同发展行动计划（2021-2023 年）》（以下称“行动计划”）。据了解，制定该“行动计划”是为贯彻落实《政府工作报告》部署要求，推进“双千兆”网络建设互促、应用优势互补、创新业务融合，进一步发挥“双千兆”网络在拉动有效投资、促进信息消费和助力制造业数字化转型等方面的重要作用，加快推动构建新发展格局。作为该“行动计划”的重点任务，工信部要求从提升网络安全防护能力，构筑安全可信的新型信息基础设施，做好跨行业网络安全保障等 3 个方面落实安全保障强化行动。

4. “网络安全万人培训资助计划”启动仪式在武汉举行

3 月 26 日，据国家网信办网站消息，3 月 20 日，“网络安全万人培训资助计划”启动仪式在国家网络安全人才与创新基地举行，预计未来三年内培养超过 1 万名国家网络安全人才。“网络安全万人培训资助计划”是在中央网信办指导下，由武汉市人民政府、中国互联网发展基金会、中国信息安全认证中心、中国信息安全测评中心、国家计算机网络应急技术处理协调中心共同发起，对在国家网安基地内面向党政机关、企事业单位工作人员、大中院校在校学生等开展网络安全培训的机构进行资助，并对优秀学员进行奖励。该计划由武汉市及东西湖区人民政府各出资 2000 万元、中国互联网发展基金会网络安全专项基金出资 2000 万元进行支持，中国信息安全认证中心、中国信息安全测评中心、国家计算机网络应急技术处理协调中心将在人员培训认证方面提供指导支持。目前，奇安信、启迪、开源网安、天融信、网信联盾等多家企业已入驻并正在开展培训。这些具备培训经验的网安企业，将开展普识教育、政策法规、网络安全从业人员认证（注册）和技术提升等方面的培训，力争补齐学历教育与岗位需求不适配的短板，推动解决网安人才急需紧缺难题。

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 2020 年，已与 78 个国家和地区的 265 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：王英

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315