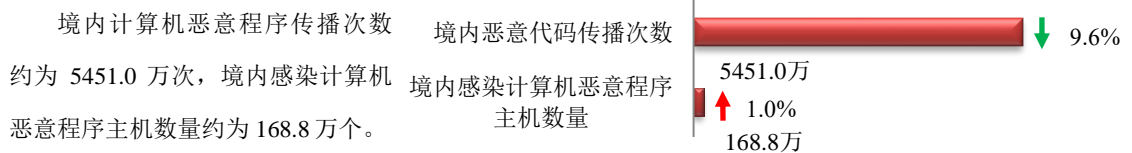


本周网络安全基本态势



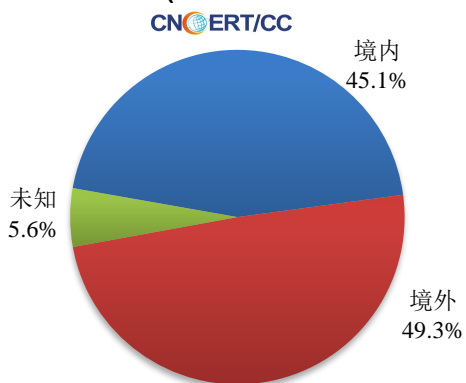
■ 表示数量与上周相同 ↑ 表示数量较上周环比增加 ↓ 表示数量较上周环比减少

本周网络病毒活动情况

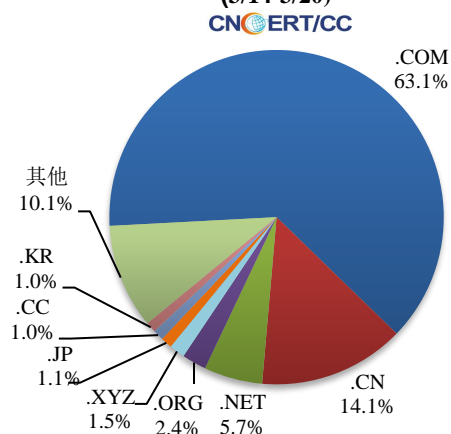


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 5372 个，涉及 IP 地址 29052 个。在 5372 个域名中，有 49.3% 为境外注册，且顶级域为 .com 的约占 63.1%；在 29052 个 IP 中，有约 87.0% 位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 500 个。

本周放马站点域名注册所属境内外分布
(3/14-3/20)



本周放马站点域名注册所属顶级域分布
(3/14-3/20)



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

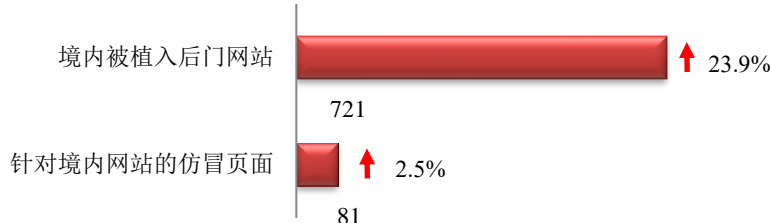
<https://share.anva.org.cn/web/publicity/listurl>

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

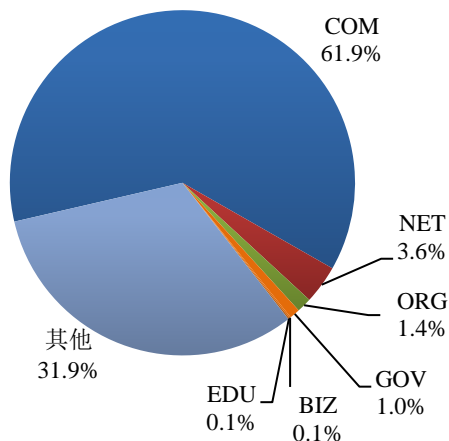
本周 CNCERT 监测境内被植入后门的网站数量为 721 个；针对境内网站的仿冒页面数量 81 个。



本周境内被植入后门的政府网站（GOV类）数量为7个（约占境内1.0%），与上周相比上升250.0%。

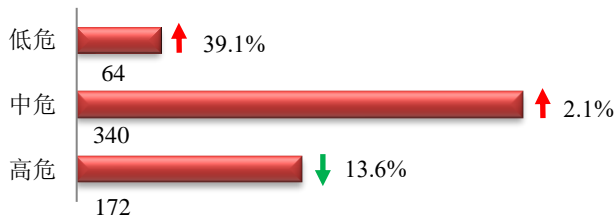
本周我国境内被植入后门网站按类型分布
(3/14-3/20)

CNCERT/CC



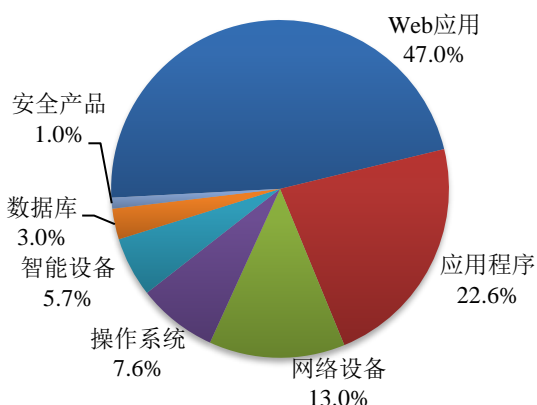
本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 576 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
(3/14-3/20)

CNVD 国家信息安全漏洞平台



本周 CNVD 发布的网络安全漏洞中，Web 应用占比最高，其次是应用程序和网络设备。

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

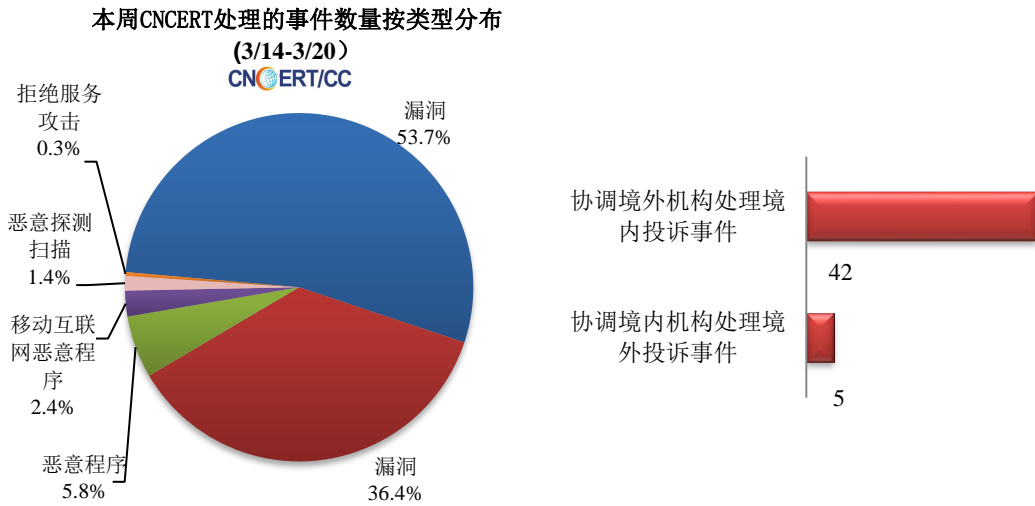
<http://www.cnvd.org.cn/webinfo/list?type=4>

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。

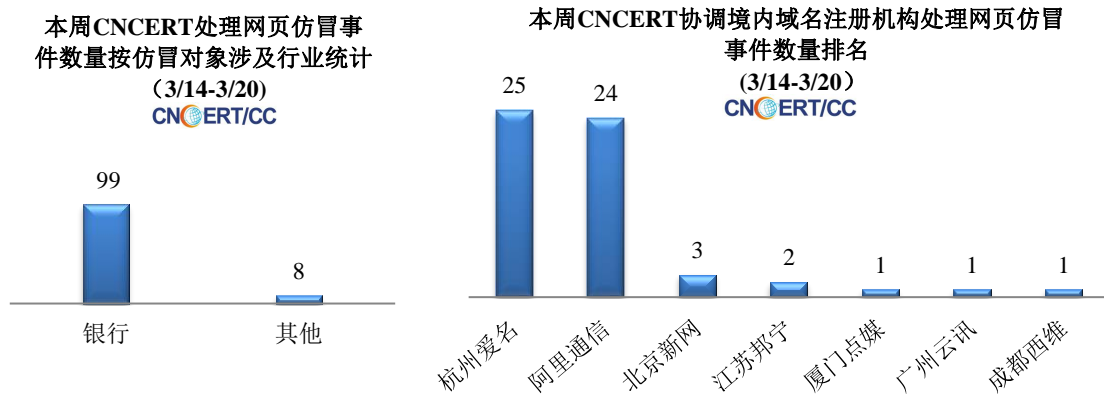


本周事件处理情况

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网络安全事件 294 起，其中跨境网络安全事件 47 起。

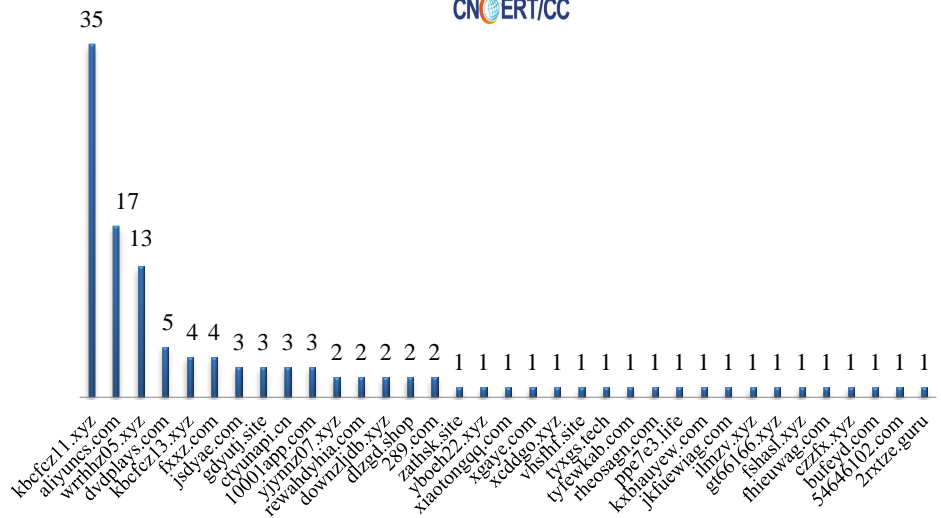


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理 107 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，银行仿冒事件 99 起，其他事件 8 起。



本周，CNCERT 协调 35 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 120 个。

本周CNCERT协调应用程序下载服务平台处理移动互联网恶意代码事件数量排名 (3/14-3/20)
CNCERT/CC



业界新闻速递

1. 国家计算机病毒应急处理中心公布美国国家安全局开发的网络武器

3月14日，据国家计算机病毒应急处理中心消息，近日，国家计算机病毒应急处理中心对名为“NOPEN”的木马工具进行了攻击场景复现和技术分析。该木马工具针对 Unix/Linux 平台，可实现对目标的远程控制。根据“影子经纪人”泄露的 NSA 内部文件，该木马工具为美国国家安全局开发的网络武器。“NOPEN”木马工具是一款功能强大的综合型木马工具，也是美国国家安全局接入技术行动处（TAO）对外攻击窃密所使用的主战网络武器之一。“NOPEN”木马工具为针对 Unix/Linux 系统的远程控制工具，主要用于文件窃取、系统提权、网络通信重定向以及查看目标设备信息等，是 TAO 远程控制受害单位内部网络节点的主要工具。通过技术分析，我单位认为，“NOPEN”木马工具编码技术复杂、功能全面、隐蔽性强、适配多种处理器架构和操作系统，并且采用了插件式结构，可以与其他网络武器或攻击工具进行交互和协作，是典型的用于网络间谍活动的武器工具。

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：李明

网址：www.cert.org.cn

Email：cncert_report@cert.org.cn

电话：010-82990315