国家互联网应急中心

网络安全信息与动态周报

2022 年第 10 期

2 月 28 日-3 月 6 日

CNCERT/CC

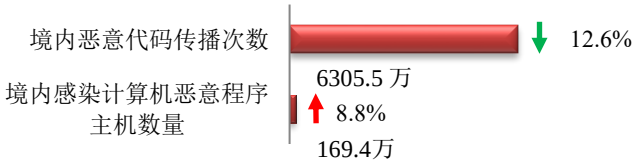
本周网络安全基本态势

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	• 6305.5万 • 169.4万	↓ 12.6% ↑ 8.8%
境内被植入后门网站总数 其中政府网站数量	• 394 • 3	↓ 37.1% ↓ 57.1%
针对境内网站的仿冒页面数量	• 64	↓ 41.8%
新增信息安全漏洞数量 其中高危漏洞数量	• 569 • 160	↑ 32.6% ↑ 5.3%

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

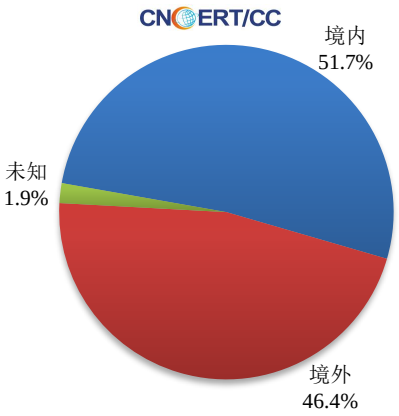
本周网络病毒活动情况

境内计算机恶意程序传播次数约为 6305.5 万次，境内感染计算机恶意程序主机数量约为 169.4 万个。

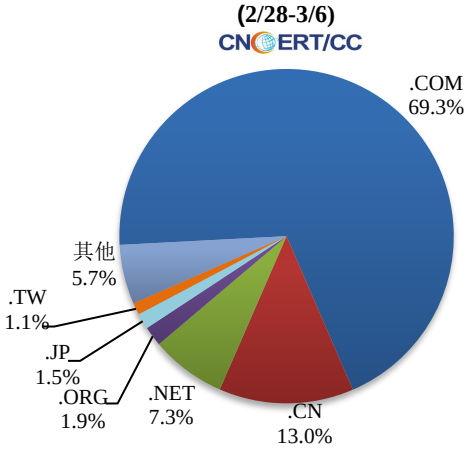


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 261 个，涉及 IP 地址 1179 个。在 261 个域名中，有 46.4%为境外注册，且顶级域为.com 的约占 69.3%；在 1179 个 IP 中，有约 41.7%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 64 个。

本周放马站点域名注册所属境内外分布
(2/28-3/6）



本周放马站点域名注册所属顶级域分布
(2/28-3/6)



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。

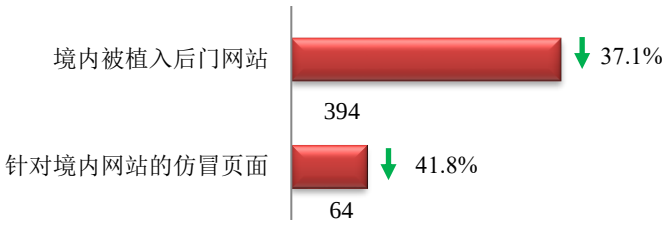
ANVA网络安全威胁信息共享平台

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。

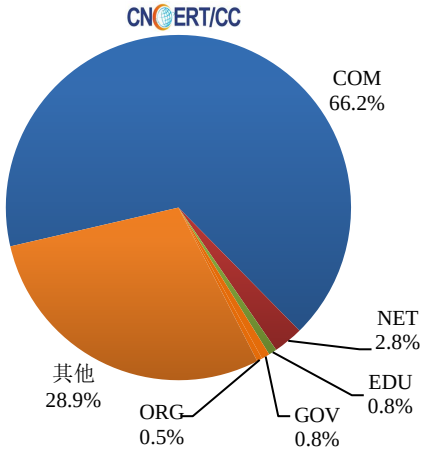
本周网站安全情况

被植入后门的网站数量为 394 个；针对境内网站的仿冒页面数量 64 个。



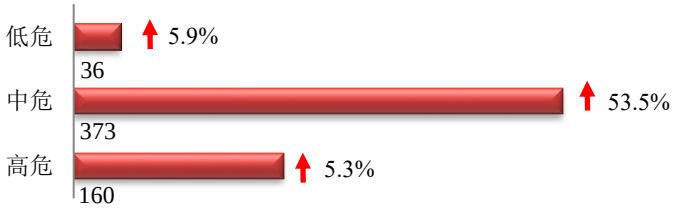
境内被植入后门的政府网站（GOV 类）数量为 3 个（约占境内 0.8%），与上周相比下降 57.1%。

本周我国境内被植入后门网站按类型分布
(2/28-3/6)

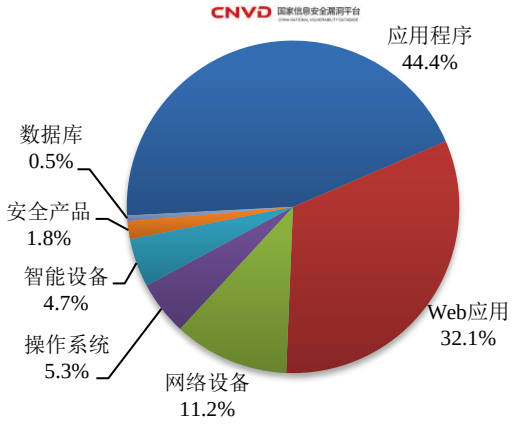


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 569 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
(2/28-3/6）



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

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

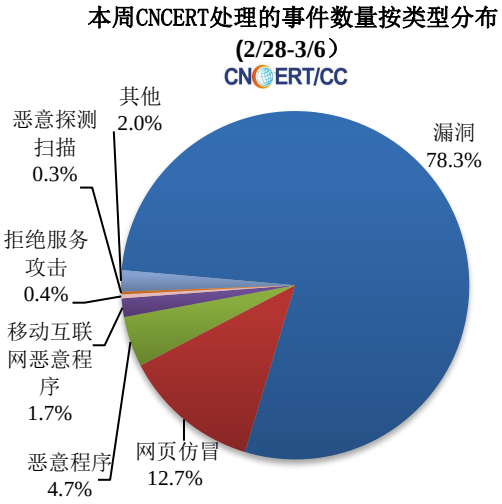
CNVD漏洞周报发布地址

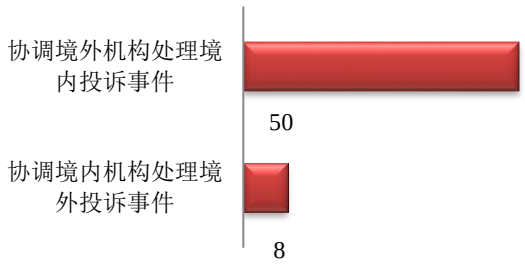
http://www.cnvd.org.cn/webinfo/list?type=4

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。

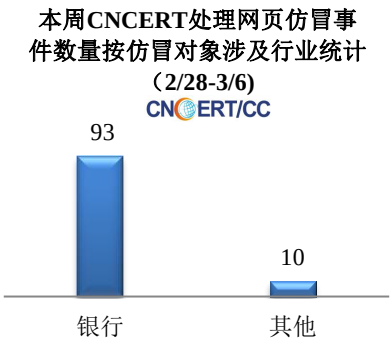
本周事件处理情况

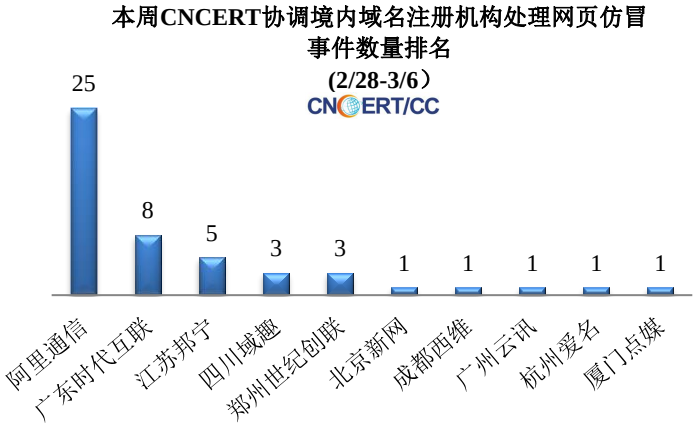
本周，CNCERT 协调云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理网络安全事件 811 起，其中跨境网络安全事件 58 起。



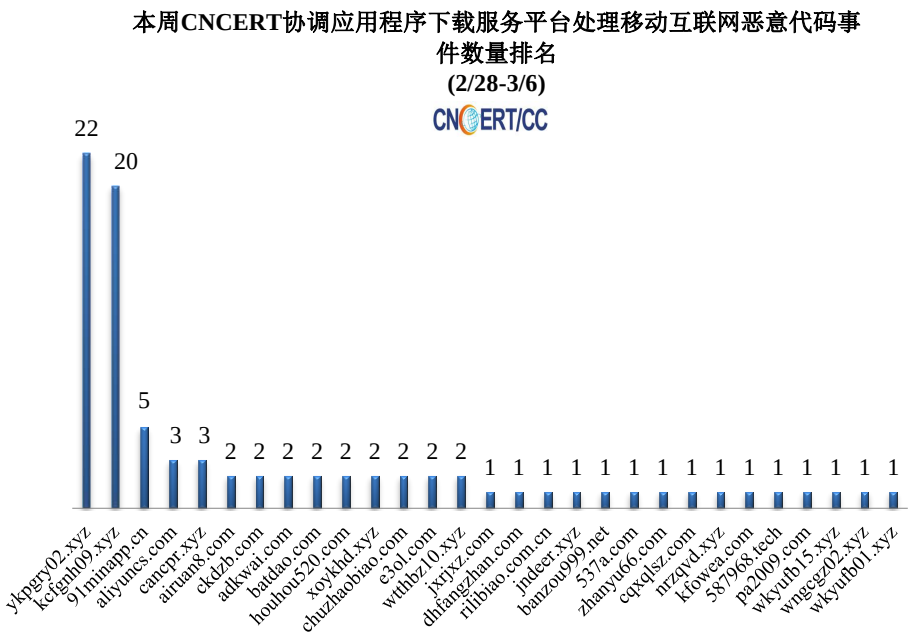


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理 103 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，银行仿冒事件 93 起，其他事件 10 起。





本周， CNCERT 协调 29 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 86 个。



业界新闻速递

1. 关于 BlackMoon 僵尸网络大规模传播的风险提示

近期，CNCERT 监测发现 BlackMoon 僵尸网络在互联网上进行大规模传播，通过跟踪监测发现其 1 月控制规模（以 IP 数计算）已超过 100 万，日上线肉鸡数最高达 21 万，给网络空间带来较大威胁。请广大网民强化风险意识，加强安全防范，避免不必要的经济损失，主要建议包括：1、不要点击来源不明邮件。2、不要打开来源不可靠网站。3、不要安装来源不明软件。4、不要插拔来历不明的存储介质。当发现主机感染僵尸木马程序后，立即核实主机受控情况和入侵途径，并对受害主机进行清理。

2. 关于互联网信息服务算法备案系统上线的通告

2022 年 2 月 28 日，据中国网信网消息，3 月 1 日起，互联网信息服务算法备案系统正式上线运行，官方网址为 https://beian.cac.gov.cn。备案主体通过官网填报备案信息、查看备案状态，普通用户通过官网查询备案信息。具体操作说明访问 https://beian.cac.gov.cn 查看。互联网信息服务算法备案仅对备案主体所提供的算法推荐服务及服务中使用的算法推荐技术进行备案，信息由备案主体自行填报，该备案不代表对有关主体、算法、产品、服务等的认可，任何组织和个人不得将备案结果用于宣传和其他商业用途。

3. 中央网信办等四部门印发《2022 年提升全民数字素养与技能工作要点》

2022 年 3 月 2 日，据中国网信网消息，近日，中央网信办、教育部、工业和信息化部、人力资源社会保障部联合印发《2022 年提升全民数字素养与技能工作要点》（以下简称《工作要点》）。《工作要点》明确了工作目标：到 2022 年底，提升全民数字素养与技能工作取得积极进展，系统推进工作格局基本建立。数字资源供给更加丰富，全民终身数字学习体系初步构建，劳动者数字工作能力加快提升，人民群众数字生活水平不断提高，数字创新活力竞相迸发，数字安全防护屏障更加坚固，数字社会法治道德水平持续提高，全民数字素养与技能发展环境不断优化。

4. 国家互联网信息办公室就《互联网弹窗信息推送服务管理规定（征求意见稿）》公开征求意见

2022 年 3 月 2 日，据中国网信网消息，为了进一步规范互联网弹窗信息推送服务管理，保障公民、法人和其他组织的合法权益，弘扬社会主义核心价值观，营造清朗网络空间，根据《中华人民共和国网络安全法》《中华人民共和国未成年人保护法》《中华人民共和国广告法》《互联网信息服务管理办法》《网络信息内容生态治理规定》等法律法规，国家互联网信息办公室起草了《互联网弹窗信息推送服务管理规定（征求意见稿）》，现向社会公开征求意见。公众可将反馈意见通过电子邮件方式发送至：tcts@cac.gov.cn。意见反馈截止时间为 2022 年 3 月 17 日。

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：王毓骏

网址： www.cert.org.cn

Email：cncert_report@cert.org.cn

电话： 010-82990315