近年来，我国正不断加强虚拟货币“挖矿”行为整治力度。2021年9月，国家发展改革委、中央宣传部、中央网信办等11部门印发《关于整治虚拟货币“挖矿”活动的通知》，要求加强虚拟货币“挖矿”活动上下游全产业链监管，严禁新增虚拟货币“挖矿”项目。同年11月10日，国家发改委组织召开虚拟货币“挖矿”治理专题视频会议，要求各省市区要坚决贯彻落实好虚拟货币“挖矿”整治工作，全面对本地区虚拟货币“挖矿”活动进行清理整治。

随着一系列针对虚拟货币“挖矿”活动整治文件和要求的发布，各省市区域相关单位已开始积极响应并开展行动。至此，虚拟币“挖矿”整治行动已转入常态化监管。

那么，到底什么是“挖矿”呢？

虚拟货币“挖矿”活动有什么危害？

如何防范“挖矿”攻击？

请听下文分解~

“挖矿”介绍及危害

“挖矿”活动是指利用硬件计算机系统，通过算法来锁定虚拟货币的对应位置并进行收取。在此过程中，出现了大量利用他人设备进行恶意“挖矿”的不法行为，通过利用目标资产的脆弱性进行攻击入侵，控制目标主机变为挖矿算力，产生诸多危害及不良影响：

能源浪费：
“挖矿”活动会利用目标主机满负荷持续进行计算，造成巨大的能源消耗和碳排放量，与国家“十四五”规划实现碳中和节能减排的目标背道而驰。

业务影响：
一旦被“挖矿”程序控制，挖矿过程需要消耗大量计算资源，影响组织内部业务系统运行，还会造成数据泄露或感染病毒等网络安全问题，比如机密文件、关键资产

的用户名和密码等，导致企事业单位遭受更进一步的资产损失。

金融危害：
“挖矿”活动产出的虚拟货币，在生产、交易过程中绕过国家监管，不仅扰乱金融秩序，还催生了诸多犯罪活动，给社会稳定和国家安全带来严重威胁。

目前国内大多省份已开展“挖矿”专项治理工作，并卓有成效，但由于“挖矿”病毒具有易复发性，应防患未然，构建预防排查手段，及时对脆弱点加固，防止“挖矿”活动死灰复燃。

天融信根据对挖矿入侵行为的分
析，发现并总结出
资产暴露、漏洞利用、弱口令、不安全的配置、容器镜像文件污染等是最常见的攻击入口，因此常态化脆弱性风险排查，是 “挖矿”病毒预防中的重要技术手段。

恶意挖矿活动分析情况如下图所示：

天融信脆弱性扫描与管理系统（以下简称“漏扫系统”）以资产暴露面梳理、漏洞扫描、弱口令检测、
配置核查、镜像扫描五大能力为基本抓手

，并通过与防火墙、态势感知实现强强联合，帮助用户认清风险，实现事前预防，建设立体主动防护体系。

招式一：全量资产梳理

“知己知彼，百战不殆”，要做好预防恶意挖矿的安全防护工作，第一步需要明确“要保护什么”。天融信漏扫系统融合最新的操作系统指纹识别、智能端口服务识别、Web爬虫、子域名收集等技术，发现并评估整个资产面，覆盖传统IT资产、云资产、国产化系统与应用、移动应用、Web应用程序、容器等各类资产，并准确识别资产的IP、MAC、类型、服务、协议、端口等信息，帮助客户对资产信息了如指掌。

招式二：精准漏洞治理/发现

通过对挖矿攻击团队的深入跟踪与分析、归纳总结挖矿病毒常用漏洞清单，研制挖矿病毒漏洞专项检测模板，综合运用预探测、渐进式、多线程等扫描技术，能够快速、精准地发现被检资产的漏洞信息，并提供细致的漏洞修复建议，让客户能够及时修复漏洞隐患，防止漏洞被挖矿病毒利用。

招式三：弱口令检测

“千里之堤，溃于蚁穴”，再完善的安全防御体系只要存在弱口令，就如同一套严密的防盗设施把钥匙留在门上，所有努力付之一炬。天融信漏扫系统内置丰富的协议、服务的口令字典，通过口令字典动态匹配技术，实现无损检测各类服务器、数据库、中间件、网络设备的弱口令，全面掌握弱口令情况，及时消除弱口令隐患。

招式四：配置核查

不安全的配置也是“挖矿”病毒团伙常用的攻击入口。天融信漏扫系统的基线检查功能能够提供信息系统基线的最佳安全实践，针对服务器操作系统、数据库、应用软件和容器等各类信息系统的配置进行安全检测，并提供检查结果和加固建议，帮助客户进行系统安全加固，降低入侵风险并满足安全合规要求。

招式五：镜像扫描

近年来，随着企业上云进程不断推进，容器技术的使用逐渐频繁，如果镜像被污染后部署于组织内部，将会带来重大的安全威胁。天融信漏扫系统提供对容器镜像的风险检测，在容器镜像部署前发现容器镜像存在的风险，使客户能够尽早发现镜像存在的安全问题，便于管理员完成镜像的安全管理和维护。