烽火十八台丨助力开展“挖矿”整治行动，盛邦安全发布“挖矿”资产测绘专项方案

9月

今年9月，国家发展改革委等10部门联合发布通知，要求梳理排查虚拟货币“挖矿”活动，加强上下游全产业链监管，全面整治虚拟货币“挖矿”活动，防范处置虚拟货币“挖矿”活动盲目无序发展带来的风险。

什么是虚拟货币“挖矿”

虚拟货币“挖矿”指的是通过专用“矿机”计算生产虚拟货币的过程，其能源消耗和碳排放量大，对国民经济贡献度低，对产业发展、科技进步等带动作用有限，加之虚拟货币生产、交易环节衍生的风险越发突出，其盲目无序发展对经济社会高质量发展和节能减排带来不利影响。

虚拟货币“挖矿”带来的危害巨大

国家发展改革委有关负责人指出，一方面，“挖矿”活动能耗和碳排放强度高，对我国实现能耗双控和碳达峰、碳中和目标带来较大影响，加大部分地区电

力安全保供压力，并加剧相关电子信息产品供需紧张；另一方面，比特币炒作交易扰乱我国正常金融秩序，催生违法犯罪活动，并成为洗钱、逃税、恐怖融资和跨境资金转移的通道，一定程度威胁了社会稳定和国家安全。

可见，整治虚拟货币“挖矿”活动对促进我国产业结构优化、推动节能减排、如期实现碳达峰、碳中和目标具有重要意义。

“挖矿”整治行动正在全国范围内开展

随着一系列针对虚拟货币“挖矿”行为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和开展行动。以江苏省为例，2021年10月，江苏省通信管理局全面排查江苏省虚拟货币“挖矿”行为，监测发现江苏省开展虚拟货币活动的矿池出口流量达136.77Mbps，参与“挖矿”的互联网IP地址总数4502个，消耗算力资源超10PH/s，耗能26万度/天。从IP地址归属和性质看，归属党政机关、高校、企业被入侵利用开展虚拟货币“挖矿”行为的占比约21%。

浙江省也针对“利用党政机关、国有企事业和科研院校等单位公共资源参与‘挖矿’的行为”在全省范围内开展了专项整治工作，对全省涉嫌参与虚拟货币挖矿的4699个IP地址进行了全面筛查，梳理排查出77家单位的184个IP地址存在涉嫌利用公共资源从事“挖矿”行为。

为了配合相关单位开展虚拟货币“挖矿”活动整治，助力企事业单位梳理网络资产、排查“挖矿”病毒风险，盛邦安全近期推出了“挖矿”资产测绘专项方案，助力监管单位和行业客户理清资产边界，绘制辖区内“挖矿”资产分布地图。

盛邦安全“挖矿”资产测绘专项方案

该方案以网络空间资产探测系统（RaySpace）为核心，基于挖矿主机或控制端的指纹特征进行资产识别，结合盛邦安全创新的大数据分析技术和实时的威胁情报数据，能够快速定位存在“挖矿”行为的资产，形成辖区内的“挖矿”

资产地图，便于监管单位及时了解辖区内“挖矿”资产分布情况及潜在安全风险，为下一步的整改
工作提供可靠数据来源和决策依据。
截止到目前，盛邦安全已支持20余种“挖矿”病毒家族的远端检测。

技术优势

基于矿池端口的分析与指纹识别技术

基于盛邦安全对主流挖矿木马的行为分析，形成包括挖矿木马使用和通信、回连采用的常用端口清单，结合网络空间资产系统的探测能力，可快速发现存在“挖矿”行为的网络资产信息，同时与平台接入的“挖矿”资产威胁情报数据关联，快速识别和精准定位管辖区域内的“挖矿”资产。

基于矿池域名的识别技术

为了防止固定IP被封禁导致挖矿行为失败，挖矿木马回连通常采用域名形式进行控制和传播， RaySpace可对已有域名进行分析，并结合WHOIS、PDNS等数据对域名、注册人、注册邮箱、解析地址等进行关联拓展分析，辅助用户快速定位存在“挖矿”行为的资产。

基于特征的资产画像

部分挖矿木马为了避免重复感染目标矿机，会对外开发某些标记端口，一旦木马探测到这些标记端口，挖矿木马在检查端口存活后不会再进行感染；RaySpace在主动型检测挖矿木马时，可利用挖矿木马特性，达到快速普查存在潜在威胁资产的目的。

方案价值

1、绘制高清“挖矿”资产定位地图。完善资产管理体系，建立安全可靠、动态更新的网络资产台账库，从而实现对“挖矿”资产的快速、精准定位。

2、描摹清晰的“挖矿”资产画像；根据线索快速定位风险资产并进行定损分析，从漏洞、弱口令、应用资产合规性等多个维度进行安全评估，形成全面的“挖矿”资产画像。

3、实现安全事件定位更精准、灾情范围定界更快速、安全通报预警更及时。