自2021年9月国家发展改革委等11部门联合发布《关于整治虚拟货币“挖矿”活动的通知》以来，各行各业都在加快整治虚拟货币“挖矿”活动。由于高校校园网计算机多，用户量大，用户安全意识参差不齐，因此深受“挖矿”困扰。

将“挖矿”治理纳入校园安全整体考虑

高校“挖矿”活动的治理不是一项完全独立的专项行动，其与学校的网络安全体制机制建设、监测预警通报处置体系建设、网络安全宣传教育、网络安全队伍建设等都密切相关，治理“挖矿”需要将其纳入学校校园安全综合治理体系进行整体考虑，打出一套“挖矿”治理的组合拳。

在网络安全体制机制建设上，
学校的高度重视将有利于“挖矿”活动治理的顺利开展，成立工作专班或工作小组，明确统筹部门，统一部署“挖矿”治理工作，有利于在短期内改善“挖矿”高发的态势。

在监测预警通报处置体系建设上，
升级技术防护手段，加强“挖矿”活动的常态化监测能力，实现监测、通报、整改、反馈闭环管理（如图1所示）。一方面提前发现、及时处置，尽量避免出现通报；另一方面发现一起处置一起，实现动态清零。

图1 “挖矿”活动监测预警通报处置闭环管理

在网络安全宣传教育上，
教育师生在数字时代掌握一定的网络安全技能。攻击者虽然能发现并利用一切可利用的途径成功入侵进行“挖矿”，但“苍蝇不叮无缝的蛋”，主要还是因为我们自身存在漏洞或薄弱环节。例如，计算机操作系统未及时更新、使用了常见弱密码、点击钓鱼邮件感染木马、从非官网下载内嵌木马的软件、使用带病毒的U盘等。对此，学校可以网络安全宣传周为契机，重点宣传和常态化宣传双管齐下，通过线上线下讲座、多媒体推送、形势教育思政课、开展安全演练等多种形式，将“挖矿”活动的风险危害、政策形势、安全防护技能传授给广大师生，使其“拒绝主动‘挖矿’，防范被动‘挖矿’”。“挖矿”木马入侵传播途径如图2所示。

图2 “挖矿”木马入侵传播途径

在网络安全队伍建设上，
除专业安全人员外，学校网络运维人员、信息系统开发运维人员和二级单位信息化

联络员也是学校网络安全保障工作的中坚力量。工作人员可以通过各类专题讲座、培训认证、开展安全演练等形式提升校园师生的网络安全意识和个人处置能力。

与此同时，“挖矿”活动的治理还需要监管部门、高校之间、学校自身、安全厂商等多方合作交流、共享情报，打造统一战线，从而提高教育系统整体对“挖矿”活动的治理能力。

打造高效闭环的处置体系

上海交通大学通过自主研发“挖矿”监测平台，提升对“挖矿”活动的监测预警能力，建立一套从发现、处置到预防的高效闭环工作机制，将负面影响控制在最小范围内。图3为“挖矿”监测平台部署示意。

图3 “挖矿”监测平台部署示意

□事前，
一是在校园网络域名解析系统（DNS）中配置“矿池”相关域名黑名单并定期更新，及时阻断校内主机与“矿池”的通讯渠道；二是向用户提供3种终端防病毒软件，供用户自行选择下载安装，抵御“挖矿”木马侵害；三是加强网络安全宣传教育，提高师生安全意识。此外，还需开展专业技能培训，提升学校网信队伍的安全能力。

□事中，
利用“挖矿”监测平台及时跟踪处置，实现动态清零。根据“挖矿”程序多使用域名连接至公共矿池或矿池代理的特性，研发“挖矿”监测平台。通过采集请求时间、客户端IP地址、请求域名等DNS相关日志信息，与收集的“矿池”域名信息进行比对，检查请求是否命中，并进行相关的统计和预警，实现对“挖矿”活动的实时监测。

“矿池”域名黑名单对检测的准确性和及时性起着重要作用。目前，平台根据相关恶意域名通报、互联网上公开的“挖矿”域名列表、主动工具采集三种方式，收集“矿池”域名信息并不定期更新。例如，目前公开的“矿池”域名和“矿池”代理不少采用stratum+tcp或stratum+ssl格式，利用工具采集互联网上包含“stratum+tcp://”或“stratum+ssl://”的内容，即可提取整理出部分“矿池”域名清单。

和漏洞威胁处置一样，“挖矿”处置要讲究时效性。一方面要在第一时间采取措施，阻断“挖矿”木马在网内进一步传播。另一方面，要彻底清理“挖矿”程序，避免“挖矿”木马死灰复燃。除了检查异常进程、异常网络连接、定位清除“挖矿”

程序之外，还要检查远程登录配置文件、开机启动项、定时任务、隐藏权限、系统用户设置等事项，采取授权IP地址访问、使用强密码、安全配置系统及应用等措施进一步加固系统。

值得一提的是，在“挖矿”处置过程中，要避免一刀切的做法。高校不乏研究区块链技术的科研活动，可能会产生类似“挖矿”的行为，安全工作要服务于学校教学科研等各项事业的发展，因此处置时要充分了解实际情况，具体问题具体分析，这也对学校网络安全人员的能力提出了更高要求。

□事后，
通过统一日志分析等手段归纳总结“挖矿”活动的共性问题，举一反三，发现一个阻断一类。相信只要高校进行持续治理，校园内的“挖矿”活动就成不了气候，动态清零的目标也终将实现。

作者：吴芳 上海交通大学信息化推进办公室