虚拟货币“挖矿”排查及防范方法

1. **挖矿行为分类：**

挖矿行为可以分为主动挖矿和被动挖矿。

1.主动挖矿是指个人或团体通过在专业机器或普通电脑安装挖矿软件、超频工具等，主动进行挖矿行为。

2.被动挖矿是指攻击者通过各种手段将挖矿程序植入受害者的计算机中，在受害者不知情的情况下利用其计算机的算力进行挖矿，从而获取利益，这类非法植入用户计算机的挖矿程序就是挖矿病毒。

1. **处置原则：**

☆主动挖矿坚决清零，被动挖矿一经发现立即清零。

1. **排查方法**

主动挖矿是个人主动行为，由计算机使用人自行清理。

被动挖矿是在计算机所有人不知情的情况下被植入挖矿病毒木马，挖矿病毒木马具有伪装性，往往伪装成其他程序，整治挖矿的重点和难点。

☆发现计算机感染挖矿病毒木马应立即断开计算机网络，避免病毒木马通过网络传播到附近其他计算机。

windows：安装杀毒软件升级到最新版本，更新最新病毒库进行全盘深度查杀。推荐杀毒软件有奇安信天擎、360杀毒、火绒杀毒。

奇安信在线版（[点击下载](https://222.200.96.174:19345/about/download)） 奇安信离线版（[点击下载](http://222.200.96.174/install.exe)）

360杀毒（[点击下载](https://sd.360.cn/)） 火绒杀毒（[点击下载](https://www.huorong.cn/person5.html)）

**说明**：奇安信天擎是收费的专业软件，“挖矿”病毒木马查杀能力要远远强于一般免费杀毒软件，推荐使用。360杀毒、火绒杀毒病毒库更新稍微滞后，适合于日常使用。**为避免冲突，在安装新的杀毒软件前，请卸载已安装的杀毒软件，多个杀毒软件不但不能提升查杀能力，反而会导致功能失常。**

linux：专业性较强，建议个人计算机由所有人操作，网站或应用系统服务器则由服务商操作。排查和清理详见附件《虚拟货币“挖矿”自查参考方法》。

1. **挖矿病毒木马清理不了怎么办？**

若windows系统的计算机经过病毒全盘查杀、linux系统的计算机按《虚拟货币“挖矿”自查参考方法》排查清理后依然无法完全清理的顽固挖矿病毒木马，主要体现：消耗大量的CPU或GPU资源，如CPU使用率高达90%，有大量对外进行网络连接（特别是境外）的日志记录。

可在做好数据备份情况下格式化计算机磁盘、重装操作系统，并在新系统做好防护措施，或联系网络中心提供技术支持。

1. **挖矿病毒木马如何防范？**
2. 培养良好的计算机使用习惯。计算机长时间不使用的情况下或下班时，及时进行关机或断网。
3. 通过技术手段做好服务器主机绑定隔离措施，阻止主机间非授权访问。使用正版操作系统，及时更新操作系统补丁。
4. 安装安全防护软件或者杀毒软件，开启自动更新功能，定期全盘扫描。
5. 计算机登录口令要有足够的长度和复杂性，建议密码长度10位以上，并定期更换，严禁使用弱口令、空口令和缺省出厂口令。
6. 非必要不要开启远程控制；如必须使用应在使用完后立即关闭服务。
7. 从正规渠道下载安装软件，不安装未知来源的第三方软件；
8. 不打开来源不明的链接、文档、邮件、邮件附件等。
9. 不浏览被安全软件提示为恶意或存在风险的网站。
10. 不使用未经杀毒的U盘、移动硬盘等存储设备。
11. 个人用户应推荐使用非管理员帐户活动，必要时根据系统提示或自行提权。公共服务器应限制用户对管理员权限的使用，不允许私自安装软件，降低用户服务运行权限。
12. 建议服务器采用最小访问控制策略，禁止或删除不需要的服务，包括内网网络服务、互联网网络服务，仅允许授权IP地址访问。
13. 开启系统日志记录功能，并按照规定留存相关的网络日志不少于六个月。