附件

挖矿木马防范指南

一、虚拟货币“挖矿”活动危害

虚拟货币“挖矿”活动指依据特定算法，通过运算去获得虚拟的加密数字货币，常见的有比特币、以太坊币、门罗币、EOS币等。由于虚拟货币“挖矿”需要借助计算机高速运算，消耗大量计算力和电力资源，国家已经明确其为高能耗的淘汰类产业，且虚拟货币相关业务活动属于非法金融活动。

同时虚拟货币“挖矿”活动常伴随安全问题，不法分子为了获取暴利，大量通过植入挖矿木马，控制受害者计算机进行虚拟货币“挖矿”，为自己牟利，对受害计算机及其网络安全构成严重威胁，国内挖矿木马攻击事件呈爆发式增长。

国家将对虚拟货币“挖矿”活动开展全面整治，严查严处国有单位机房涉及的“挖矿”活动，并采取相关惩处措施，如收取惩罚性电费，相关参与人员将面临违法违纪风险。

二、挖矿木马如何防范

挖矿木马大多利用计算机常见漏洞，如未授权访问、远程命令执行漏洞、弱口令、零日0Day漏洞等，做好日常防范非常关键。

1.安装正版操作系统，及时更新操作系统补丁。

2.安装安全防护软件并升级病毒和规则库，定期检测电脑、服务器的安全状况，定期全盘扫描，保持实时防护，安全检测范围包括但不限于：

（1）是否有新增账户、未知进程；

（2）系统日志是否存在异常；

（3）安全防护软件是否存在异常拦截情况。

3.多台终端设备不要使用相同的账号和口令，登录口令要有足够的长度和复杂性，并定期更换登录口令。

4.从正规渠道下载安装软件，不安装未知来源的第三方软件，不点击未知的链接。

5.不打开来源不明的文档、邮件、邮件附件等。

6.不浏览被安全软件提示为恶意或存在风险的网站。

7.不使用未经杀毒的U盘、移动硬盘等存储设备。

8.开启防火墙，服务器配置访问控制，仅允许授权IP地址访问。

9.不共享使用上网账号，避免使用远程控制类软件，非必要不通过远程手段进行运维。

10.如无法自行处理“挖矿”木马，尝试备份必要文件并重装正版操作系统。