它最大的特点是通过劫持动态链接库植入 rootkit 后门。Kworkerds 主要利用 Redis 未授权访问漏洞、SSH 弱密码、WebLogic 远程代码执行等进行入侵，入侵后下载 mr.sh/2mr.sh 恶意脚本运行，植入挖矿程序。该挖矿木马在代码结构未发生重大变化的基础上频繁更换恶意文件下载地址，具备较高的活跃度。

10. Watchdogs

Watchdogs 是 2019 年 4 月爆发的 Linux 系统下的挖矿木马。Watchdogs 利用 SSH 弱密码、WebLogic 远程代码执行、Jenkins 漏洞、ActiveMQ 漏洞等进行入侵，还利用新公开的 Confluence RCE 漏洞大肆传播。其包含自定义版本的 UPX 加壳程序，会尝试获取 root 权限，进行隐藏。

5.1.3 挖矿木马的传播方法

1. 利用漏洞传播

为了追求高效率，攻击者一般会通过自动化脚本扫描互联网上的所有机器，寻找漏洞，然后部署挖矿进程。因此，大部分的挖矿都是由于受害者主机上存在常见漏洞，如 Windows 系统漏洞、服务器组件插件漏洞、中间件漏洞、Web 漏洞等，利用系统漏洞可快速获取相关服务器权限，植入挖矿木马。

2. 通过弱密码暴力破解传播

挖矿木马会通过弱密码暴力破解进行传播，但这种方法攻击时间较长。

3. 通过僵尸网络传播

利用僵尸网络也是挖矿木马重要的传播方法，如利用 Mykings、WannaMine、Glupteba 等控制大量主机。攻击者通过任务计划、数据库存储过程、WMI 等技术进行持久化攻击，很难被清除，还可随时从服务器下载最新版本的挖矿木马，控制主机挖矿。

4. 采用无文件攻击方法传播

通过在 PowerShell 中嵌入 PE 文件加载的形式，达到执行“无文件”形式挖矿攻击。新的挖矿木马执行方法没有文件落地，会直接在 PowerShell.exe 进程中运行，这种注入“白进程”执行的方法更加难以实施检测和清除恶意代码。