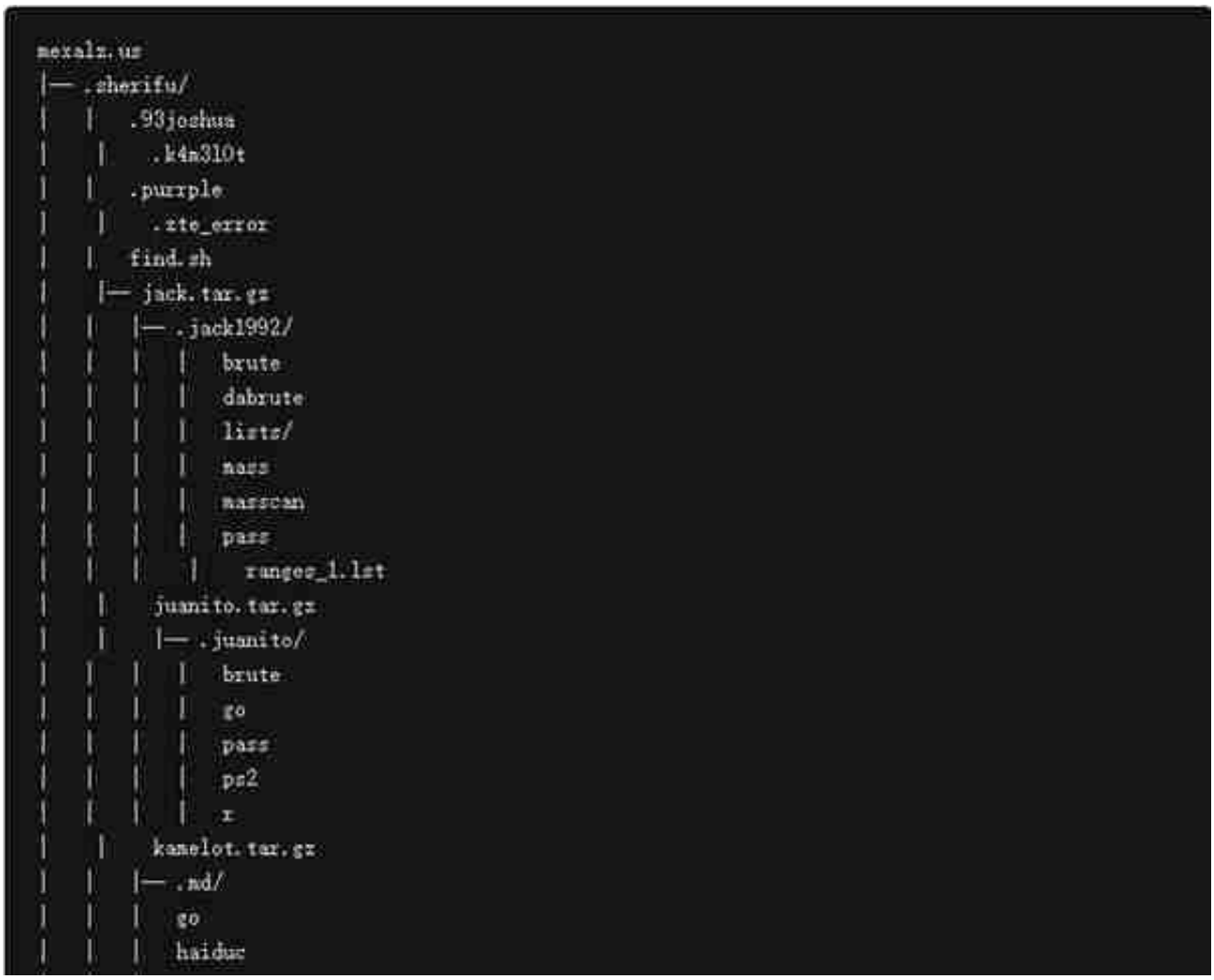

黑客是如何利用该工具包进行攻击的呢？

整个过程可以分为三个阶段：

- 侦察：通过端口扫描和横幅抓取识别SSH服务器。
- 凭据访问：通过暴力识别有效凭据。
- 初始访问：通过SSH连接并进行感染。

攻击者发现并进入弱SSH凭据的Linux设备后，他们会部署并执行loader从而

收集系统信息，并使用HTTP POST将其转发给webhook的攻击者。黑客将在此步骤收集到的信息用于判断被攻击设备的利用价值。

黑客通过bash禁用了几个shell命令，目的是使shell不被后来者操作。至此，黑客已成功安装门罗币恶意挖矿软件。

据悉，这个工具目前仍有效。据BitDefender称，已查明的IP地址属于一个相对较小的集合，说明本次事件的黑客组织尚未使用受攻击的系统来传播恶意软件。

那么该如何防止SSH 暴力破解呢？

1、足够复杂的密码

2、修改默认端口号

3、不允许Root账号直接登陆

4、不允许密码登陆，只能通过认证的秘钥来登陆系统

5、借助第三方工具fail2ban防御

以上方法便是防止SSH暴力破解的一些措施，可供大家参考哦～

阅读原文：

Linux设备沦为矿机，黑客暴力破解SSH