反“挖矿”复习范围全汇总！
“全校统考卷”干货都在这里

信息网络工程研究中心

2022.5.10

反“挖矿”复习范围全汇总！“全校统考卷”干货都在这里

- 虚拟货币“挖矿”行为违法违规。全校学生、教职工有义务做好个人上网终端安全维护，承担个人上网终端网络安全责任，防范上网终端感染病毒而产生被动“挖矿”行为。
- 为防范和排查上网主机“挖矿”行为，普通上网用户建议安装杀毒软件和防“挖矿”浏览器。公共服务器建议采用“安全登录进阶”方法配置服务器远程登录方式。具备一定计算机能力水平的用户，可以采用“入侵排查进阶”方法手动排查“挖矿”病毒文件。

一、杀毒软件（适用所有用户）

- **1、Windows杀毒软件（选其中一个即可）**
- （1）Windows Defender
- Windows10和11自带安全防护软件，系统占用比例低
- （2）360安全卫士或360杀毒
- 下载链接：https://weishi.360.cn/或 https://sd.360.cn/
- （3）火绒安全
- 下载链接：https://www.huorong.cn/person5.html
- （4）腾讯电脑管家
- 下载链接：https://guanjia.qq.com/

一、杀毒软件（适用所有用户）

- **2、Linux病毒扫描工具**
- （1）ClamAV
- 下载链接：https://www.clamav.net/downloads
- Linux服务器安装杀毒软件ClamAV 并配置邮件告警操作指南：http://web.scut.edu.cn/2022/0321/c32211a464688/page.htm

二、防“挖矿”浏览器（适用所有用户）

- 不同浏览器通过拦截恶意软件/应用或专门挖矿防护实现防“挖矿”。
- **1、Microsoft Edge 浏览器（Windows 10和11自带浏览器）**
- 点击浏览器右上角“…”菜单按钮，再点击“设置”，再点击“隐私、搜索和服务”，启用“Microsoft Defender Smartscreen”和“阻止可能不需要的应用”的选项。
- 参考链接：https://docs.microsoft.com/zh-cn/deployedge/microsoft-edge-potentially-unwanted-apps

二、防“挖矿”浏览器（适用所有用户）

- **2、火狐浏览器**
- 下载地址：http://www.firefox.com.cn/
- 默认开启拦截危险与诈骗内容功能，可点击浏览器右上角“...”菜单按钮，再点击“设置 -> 隐私与安全”，确认开启“欺诈内容和危险软件防护”。
- 参考链接：https://support.mozilla.org/zh-CN/kb/how-does-phishing-and-malware-protection-work#w_e-yi-ruan-jian

二、防“挖矿”浏览器（适用所有用户）

- **3、360安全浏览器**
- 下载地址：https://browser.360.cn/
- 默认开启沙箱防护和挖矿防护，可点击浏览器右上角菜单按钮，再点击“设置”，再点击“安全设置”，确认开启“沙箱防护”和“挖矿防护”。
- 参考链接： https://browser.360.cn/se/help/dig.html

三、主机安全加固（适用服务器用户及具备较高计算机能力的用户）

- Windows和Linux系统可以通过清单式的功能安全设置加固系统防护能力。
- Windows系统安全加固可选择性参考：
- https://help.aliyun.com/document_detail/49781.html
- https://www.safedog.cn/news.html?id=4318
- https://www.freebuf.com/articles/system/280171.html
- Linux系统安全加固可选择性参考：
- https://help.aliyun.com/document_detail/49809.html
- https://www.safedog.cn/news.html?id=4315
- 对于部署应用的服务器，可以自行根据服务器类型或部署应用类型，网上搜索相应的应用加固指南，比如web服务器加固、oracle加固、nigix加固等。

四、入侵排查进阶（适用具备较高计算机能力的用户开展深度排查）

- 对于被通知存在“挖矿”通信的主机，以及自行判断疑似“挖矿”的主机（如CPU/GPU经常异常飙高），如果杀毒软件全盘查杀无法发现木马病毒，可手动进行入侵排查，重点排查外联境外IP的异常进程、异常的启动计划和定时任务，以及异常的系统登录日志。

四、入侵排查进阶（适用具备较高计算机能力的用户开展深度排查）

- **1、可利用的网络资源和工具**
- 网络上有很多关于“挖矿”病毒排查的资源和工具。
- 详细信息见链接：“挖矿”病毒排查之四，可利用的网络资源和工具篇，http://web.scut.edu.cn/2022/0413/c32211a467486/page.htm

四、入侵排查进阶（适用具备较高计算机能力的用户开展深度排查）

- **2、排查异常进程**
- 怀疑主机在进行“挖矿”，杀毒软件全盘查杀又查不出病毒的情况下，可对可疑的网络连接和进程进行重点查杀。
- 具体方法见链接：“挖矿”病毒排查之五，排查异常进程篇，http://web.scut.edu.cn/2022/0413/c32211a467487/page.htm

四、入侵排查进阶（适用具备较高计算机能力的用户开展深度排查）

- **3、检查开机启动服务和定时任务**
- 具体方法见链接：“挖矿”病毒排查之六，检查开机启动服务和定时任务篇，http://web.scut.edu.cn/2022/0413/c32211a467496/page.htm

四、入侵排查进阶（适用具备较高计算机能力的用户开展深度排查）

- **4、日志分析**
- 具体方法见链接：“挖矿”病毒排查之七，日志分析篇，http://web.scut.edu.cn/2022/0413/c32211a467488/page.htm

五、安全登录进阶

- **1、Linux的SSH服务设置免密码的Public Key方式登录**
- 参考链接：http://web.scut.edu.cn/2022/0321/c32211a464686/page.htm
- **2、Windows 远程桌面使用动态口令**
- 参考链接：https://mp.weixin.qq.com/s/jH-7BLo566H0QsKAZFTDzA

谢 谢！