广州理工学院

广州理工网函〔2024〕16号

信息与网络中心关于警惕“银狐”木马程序传播的预警通报

校属各单位：

根据上级网络与信息安全部门通报，近期以来，境外黑客组织通过非法入侵控制我境内多个电子邮箱、即时通讯软件账号，伪装成为税务部门发送远程木马，诱导用户点击运行后监听设备运行情况，伺机实施网络诈骗等犯罪活动。

为保障我校网络安全和数据安全，防止此类事件在我校发生，特此发布预警通报。

一、高度重视，加强网络安全宣传和教育培训

各单位要高度重视网络安全工作，加强网络安全宣传和教育培训，提升我校师生的网络安全防范意识。要定期组织网络安全培训，使广大师生了解网络安全的重要性，掌握基本的网络安全防范措施和应对方法。

二、强化网络安全技术防护措施

信息与网络中心将协助各二级单位强化网络安全技术防护措施，包括但不限于定期检测分析异常网络行为，及

时发现并清除木马程序，定期更新和升级网络安全设备和技术。

三、加强对不明邮件、即时通讯软件、可疑文件的检测和预警

各单位要加强对我校师生收到的邮件、即时通讯软件、可疑文件的监测和预警，防止社工和钓鱼攻击。对于不明来源的邮件、链接和附件要特别小心，不要轻易点击或下载。

四、立即消除危害

如有师生发现网络设备、软件系统感染上木马程序，请立即参考附件《“银狐”木马程序清查方法》或联系信息与网络中心吴昊老师提供技术协助消除危害。

附件：“银狐”木马程序清查方法

广州理工学院信息与网络中心

2024年12月2日

广州理工学院信息与网络中心　　2024年12月3日印发

附件

“银狐”木马程序清除方法

近日，多地出现黑客组织通过微信投放"银狐"木马程序情况。设备感染后会自动将钓鱼文件添加进微信收藏中，并自动转发到微信群聊。建议已经感染的设备立即采取以下步骤消除风险：

一、电脑端清除步骤

（一）删除钓鱼文件及以下文件，若电脑中添加了用户或修改了管理员用户名，请至对应用户名文件夹下操作：

C :\ Users \ Administrator \ AppDataLocal \ OneDrive \ cache \ Run \微软 OneDrive . Ink

C :\ Users \ Administrator \ AppData \ Local \ OneDrive \ cachelnw _ elf . dll

C :\ Users \ Public \ Downloads \1.dll

C :\ Users \ Public \ Downlcads \ QQgames . exe

（二）关闭电脑端微信的自动缓存功能，关闭自动下载同步在其他设备中查看过的照片、视频和文件的功能。

（三）重新启动电脑，打开杀毒软件对全盘进行扫描，如扫描出木马程序则立刻清除。

（四）如果有必要，可以进行系统还原或者系统重装。

二、手机端清除步骤

（一）删除微信收藏中的钓鱼文件。

（二）立即停止在已感染手机使用微信，并清除缓存。打开微信，点击"我"-"设置"-"通用"-"清除缓存"，清除微信缓存，然后退出微信账号。

（三）中断手机网络，使用其他设备更改微信密码，在微信登录界面，选择"忘记密码"，按照提示进行密码重置。

（四）使用手机杀毒软件扫描手机，清除病毒。

（五）如果发现微信聊天记录中有可疑的信息或者联系人，请立即删除。

（六）关闭手机端微信的自动缓存功能，关闭自动下载同步在其他设备中查看过的照片、视频和文件的功能。

（七）停用其他设备上的微信。如微信账号同时登录在其他设备上，建议停用其他设备上的微信，以免木马程序通过其他设备继续感染微信账号。