

恶意代码分析与防治技术实验报告

Lab10-2 R77

网络空间安全学院 信息安全专业

2112492 刘修铭 1063

https://github.com/lxmliu2002/Malware_Analysis_and_Prevention_Techniques

一、实验目的

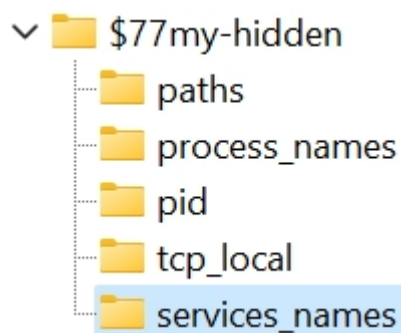
了解 R77 Rootkit 恶意软件

二、实验环境


已关闭病毒防护的 Windows11

三、实验过程

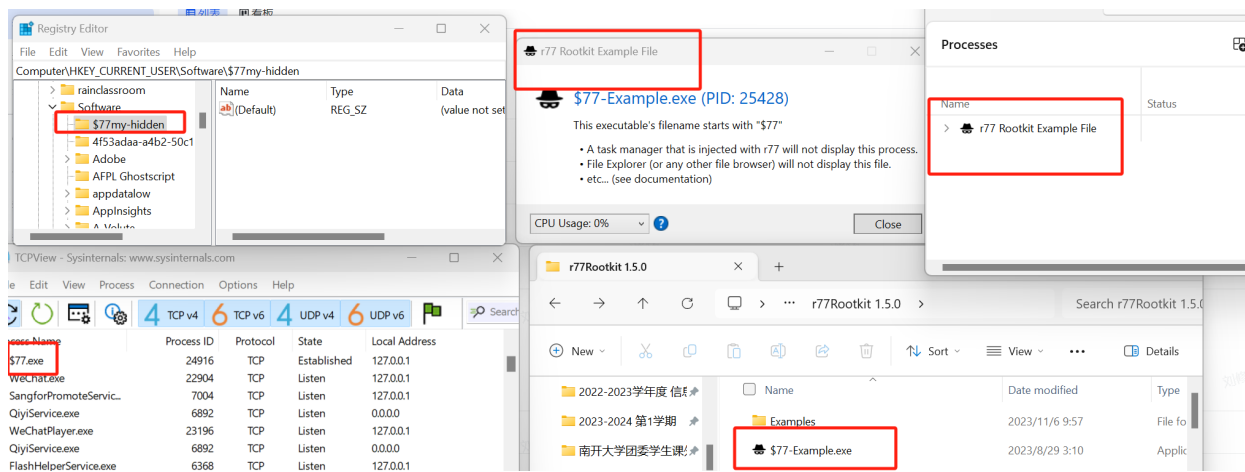
按照 Technical Document 说明，创建并将 File、Named pipes、Process、Registry、Services 等写入 configuration system。



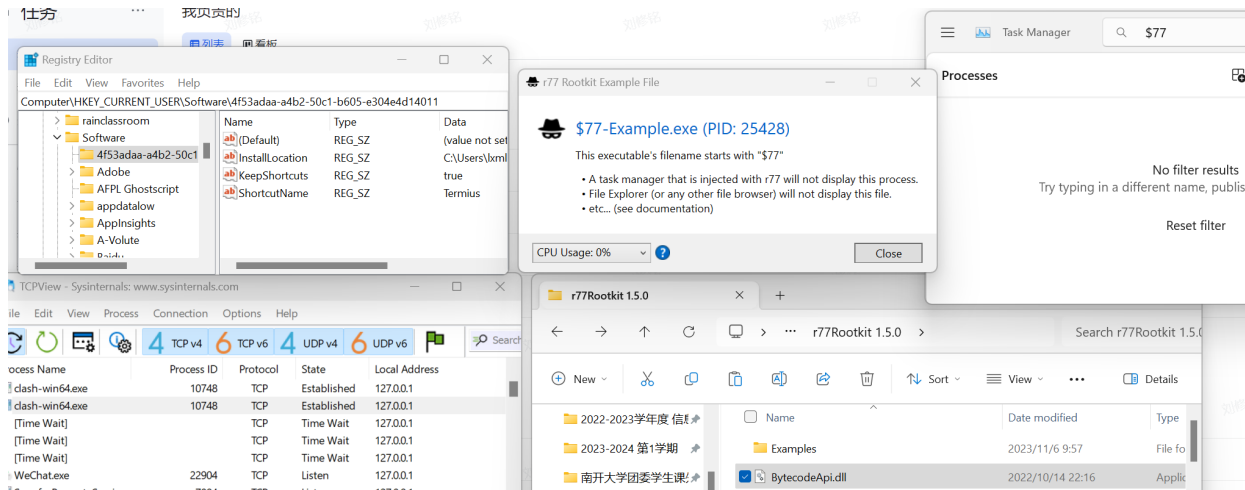
启动 \$77-Example.exe，可以看到任务管理器中出现该进程。

Process	PID	Pla
 \$77-Example.exe	23128	64

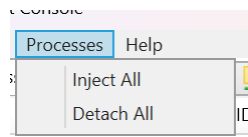
打开相关监视窗口，可以看到均能正常显示。



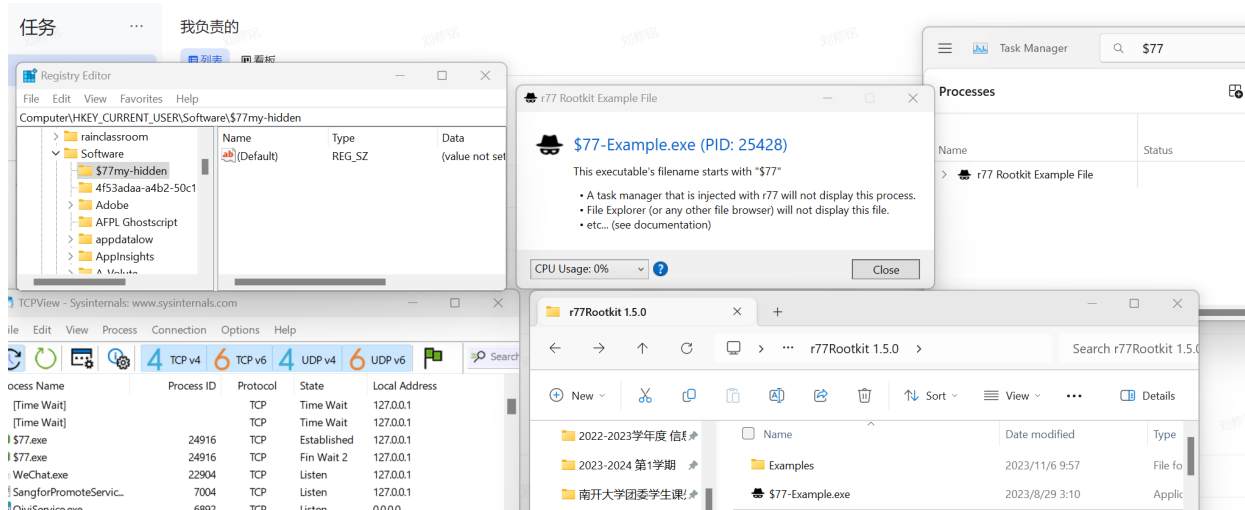
运行 Install.exe 文件，将 r77 注入到正在运行的进程中，并将 rootkit 保存在系统中。接着刷新相关监视窗口，可以看到，所有以 \$77 开头的都被隐藏，包括进程、文件、注册表及网络连接等。



点击 Detach All，取消隐藏。



可以看到，被隐藏的均重新显示。



四、实验结论及心得

了解了 R77 Rootkit 的功能。