

**恶意代码分析与防治课程实验报告**

**R77-Rootkit**

****

专 业 信息安全

学 号 2113662

姓 名 张丛

班 级 信安一班

1. **实验目的**

运行R77程序，实现对指定的进程、文件、注册表、网络连接的隐藏。

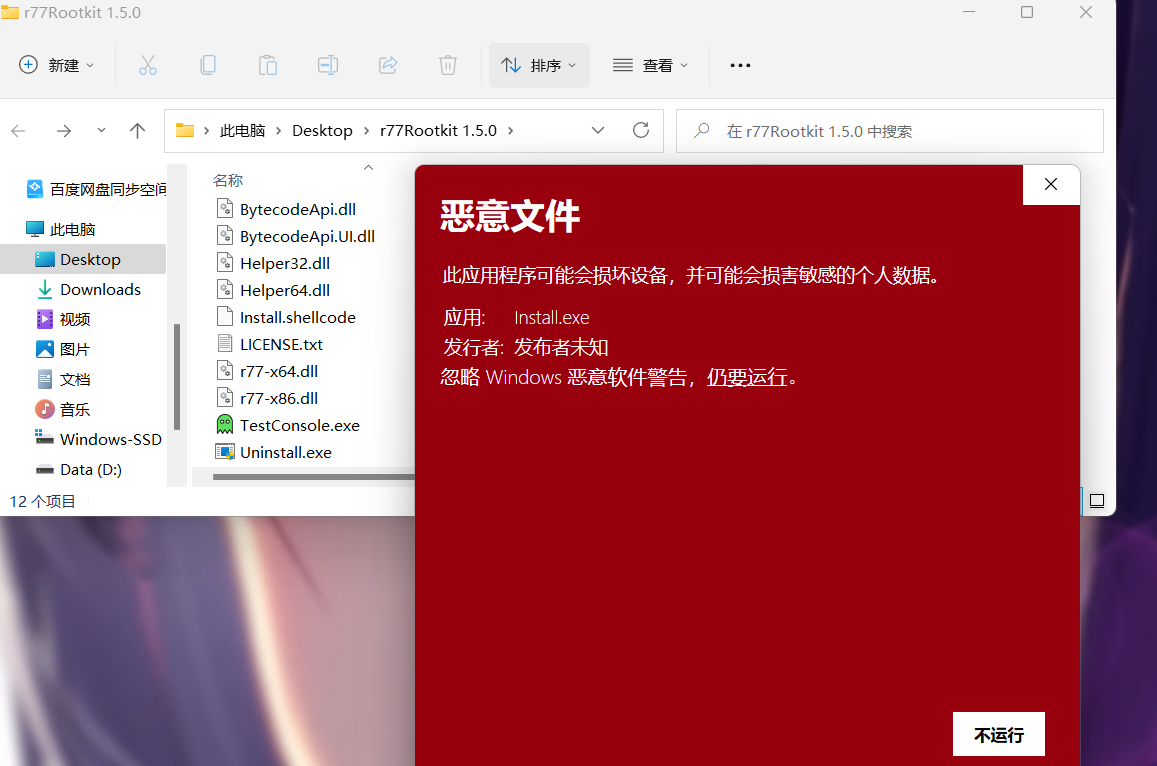
对实验结果进行截图，完成实验报告。

1. **实验过程**

r77-Rootkit是一款功能强大的无文件Ring 3 Rootkit，并且带有完整的安全工具和持久化机制，可以实现进程、文件和网络连接等操作及任务的隐藏。

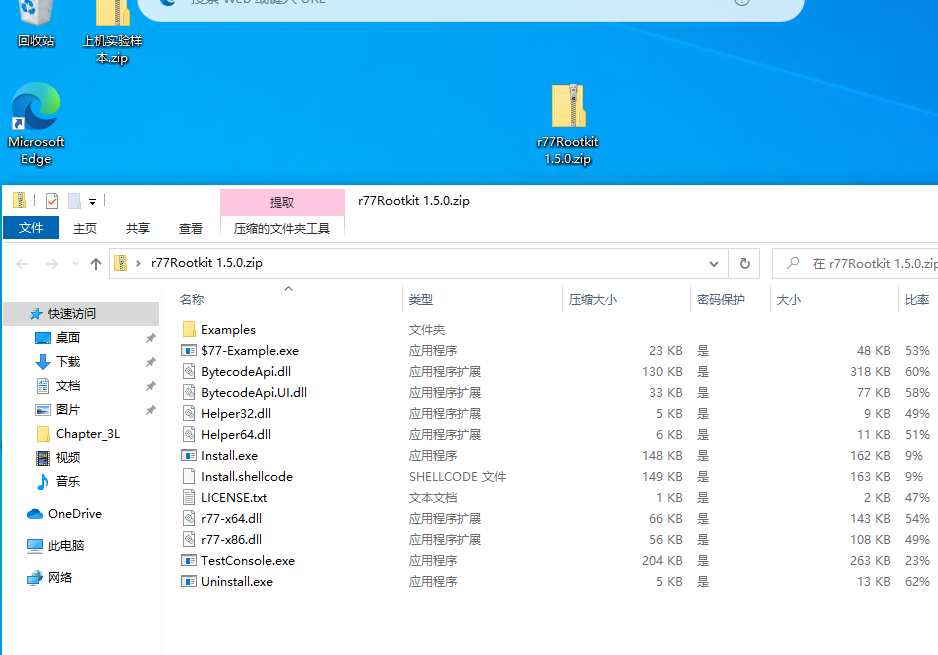
r77能够在所有进程中隐藏以下实体：文件、目录、连接、命名管道、计划任务； 进程； CPU用量； 注册表键&值； 服务； TCP&UDP连接。

尝试在本机运行R77:



然鹅事实上就算点击 仍要运行 其实还是不能运行。

**虚拟机中：**



## 运行install.exe：

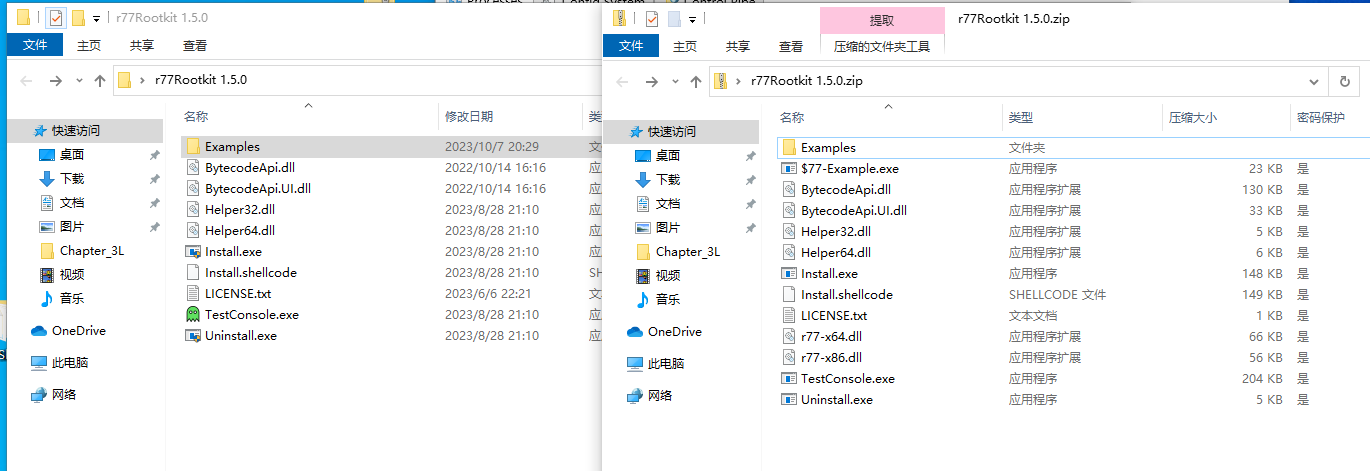
r77可以直接使用单独的“Install.exe”进行安装，安装工具会将r77服务在用户登录之前开启，后台进程会向所有当前正在运行以及后续生成的进程中注入命令。

## 通过前缀隐藏

所有以“$77”为前缀命名的实体都将被隐藏：

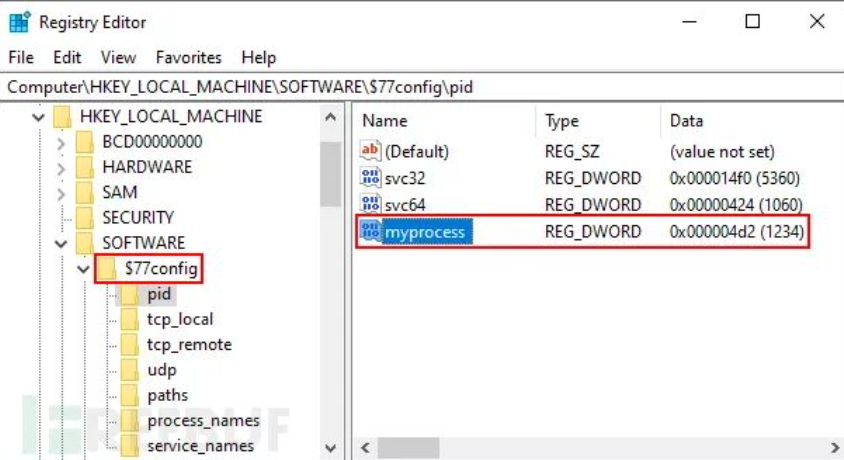
下图是压缩包文件和运行后的文件对比：

可以看到$77-Example.exe和r77-x64.dll和r77-x86.dll这些文件被隐藏了。



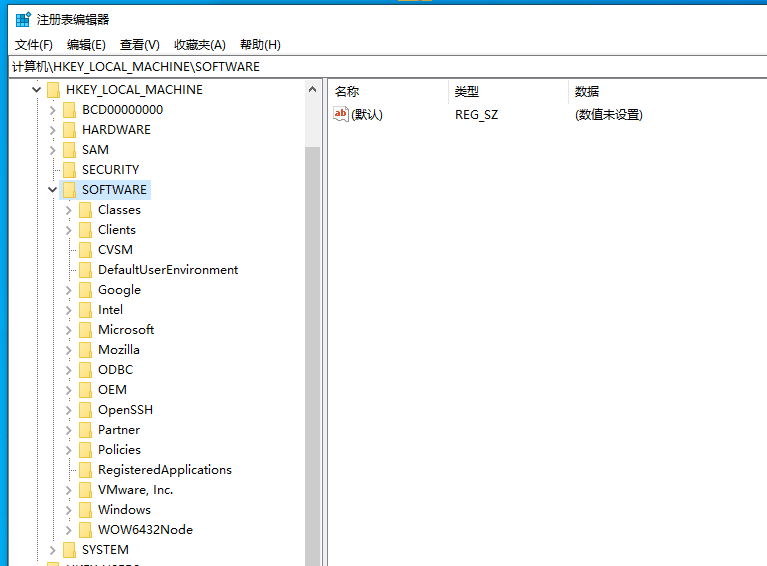
动态配置系统允许研究人员通过PID来隐藏进程，通过完整路径来隐藏文件系统，或通过指定端口隐藏TCP&UDP连接：

配置信息存储在“HKEY\_LOCAL\_MACHINE\SOFTWARE$77config”中，并且可以在未提权状态下由任何进程写入。这个键的DACL被设置为可以给任意用户授予完整访问权。



“$77config”键在注册表编辑器被注入了Rootkit之后会自动隐藏。

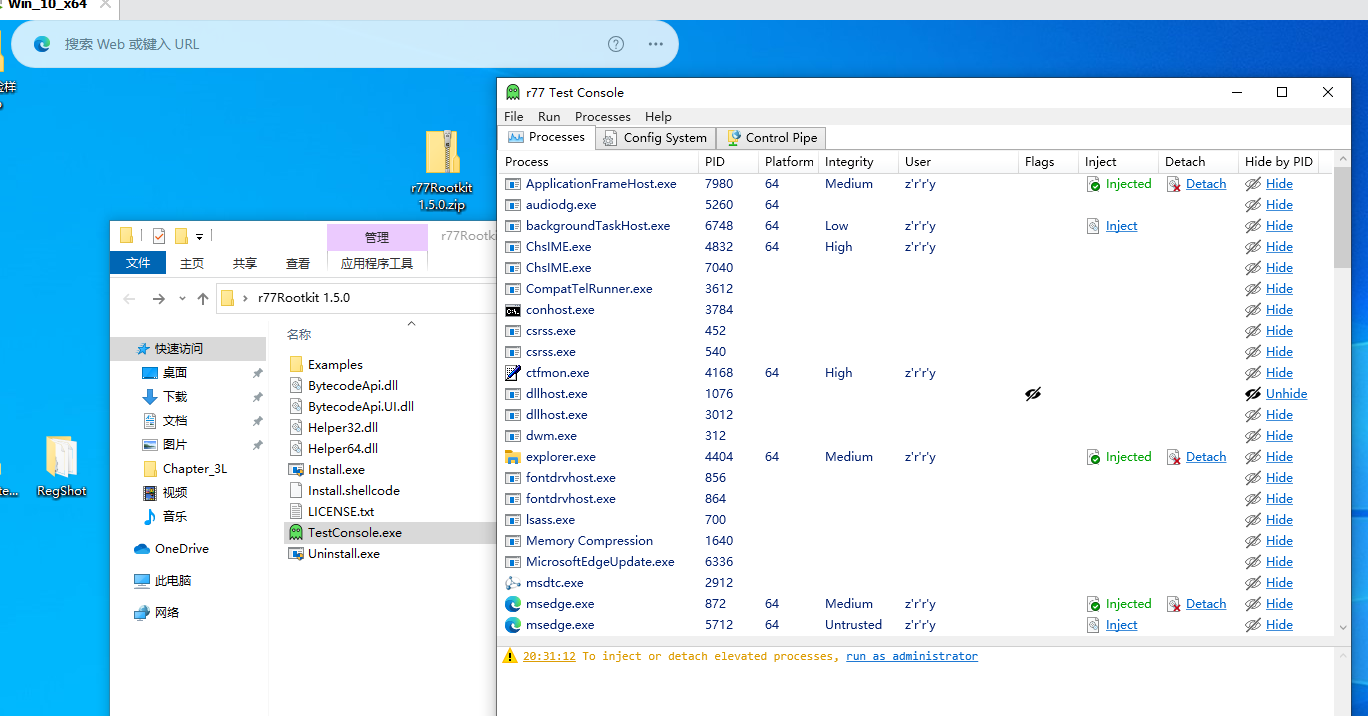
下图中“$77config”键就被隐藏了：



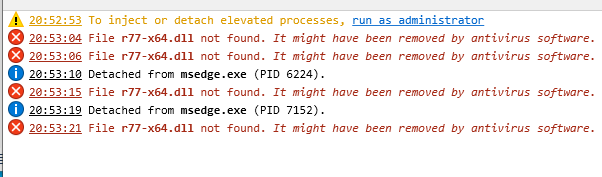
使用配置系统通过特定名称隐藏进程：

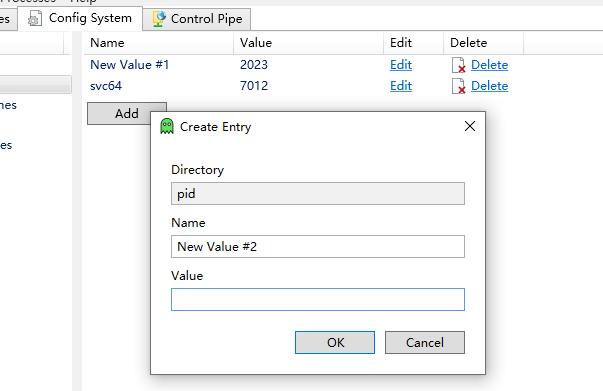


下面是R77的控制台：



测试控制台可以用来向单独进程注入r77，或接触进程跟Rootkit的绑定关系。





## 网络连接隐藏

基于以下任一情况隐藏 TCP 和 UDP 连接：

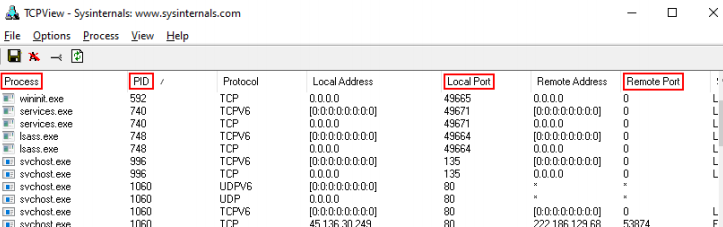
具体情况：

* 进程被前缀隐藏。
* 进程被ID 隐藏。
* 该进程按名称隐藏。

或者具体配置：

* 在配置系统中找到TCP 或TCPv6 连接的本地或远程端口。
* UDP 或UDPv6 连接的端口在配置系统中找到。UDP 连接没有远程端口。

要隐藏传出 TCP 连接，将远程端口写入配置系统。



同样的，要隐藏指定的注册表项，可以将注册表项添加到配置系统中。

1. **实验结论及心得体会**

学习使用R77-Rootkit。

但是怎么使用全靠摸索，以及网上不全的教程，以及看不懂的官方技术文档。课上学习的R77和实验不是一回事。

然后，R77这个程序的下载和安装也花费了很多时间，很无助。

这就说明，理论和实践确实不是一回事，以及我的网络安全技术水平可能确实不高。

再接再厉吧。