

**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**

在使用R77的基础上，撰写技术分析，要求描述使用过程中看到的行为如何技术实现。

1. **实验过程**

## 1、R77概述：

r77 Rootkit 是一个无文件ring 3级别的rootkit。它的主要目的是隐藏文件、目录、进程、服务、注册表项等。

此外，rootkit 附带一个安装程序，该安装程序在操作系统上保留 r77。安装是完全无文件的，这意味着不会将任何文件写入磁盘。

R77 完全依赖于内存操作，并始终保留在系统内存中。安装程序的持久性机制允许它在 Windows 重新启动后继续运行。

对于 r77 的部署，只需要一个只需要执行一次的可执行文件。

## 2、部署和配置：

##### 安装：

运行Install.exe将r77注入到所有正在运行的进程中，并在系统上持久化rootkit。

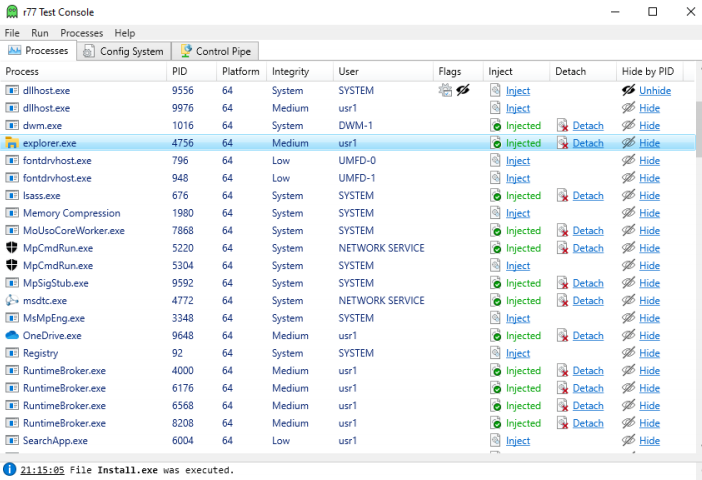
安装完成后，新创建的进程在执行任何自己的指令之前会被注入。通过钩子进程创建来实现。安装完成后，r77被设置为在重启后启动，并在第一个用户登录之前注入所有进程。

##### 卸载：

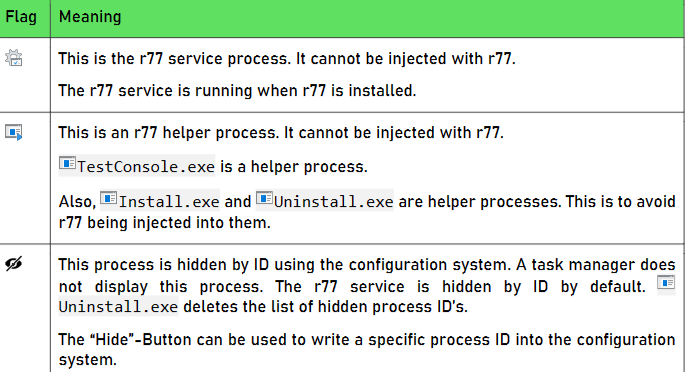
运行Uninstall.exe可以完全从系统中移除r77，它会从所有正在运行的进程中分离rootkit，并从注册表中删除r77的配置信息。不需要重新启动。

## 3、测试控制台：

Test Console是一个用于测试r77功能的工具。它可以用于注入r77到特定进程或从特定进程中分离r77。



标识含义：



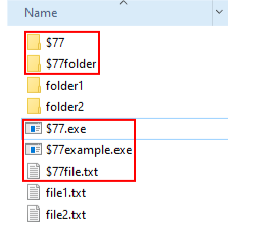
1. r77 服务流程。它不能注射 r77。
2. r77 帮助程序进程。它不能注射 r77。
3. 使用配置系统按 ID 隐藏。任务管理器不显示此过程。默认情况下，r77 服务按 ID 隐藏。Uninstall.exe 删除隐藏进程 ID 的列表。

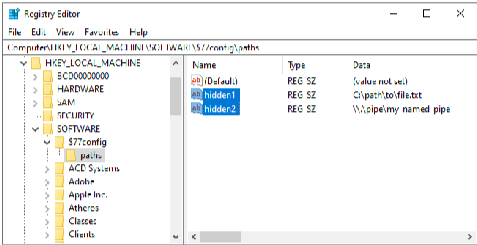
## 4、隐藏实体：

隐藏实体是指r77 Rootkit隐藏的系统组件，包括文件系统、进程、注册表、服务以及TCP和UDP连接。

##### 文件系统

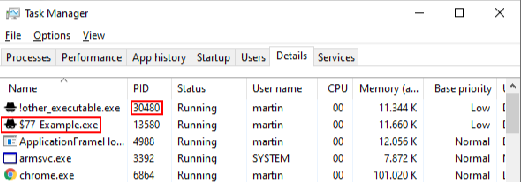
r77 Rootkit可以隐藏指定的文件、目录、符号链接和命名管道。





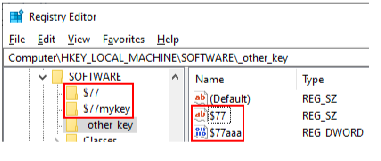
##### 进程

r77 Rootkit可以通过进程ID或进程名称来隐藏指定的进程。



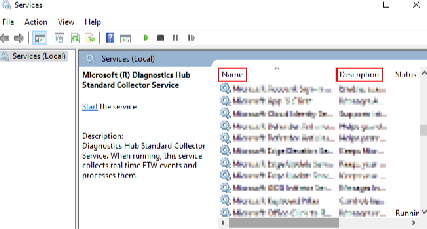
##### 注册表

r77 Rootkit可以隐藏注册表中指定的键值。



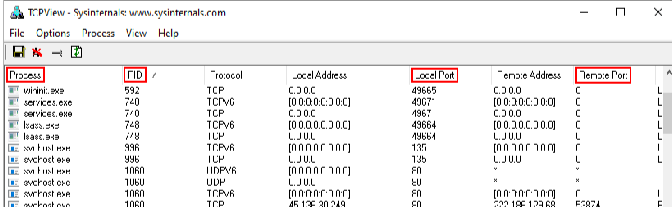
##### 服务

r77 Rootkit可以隐藏指定的服务，包括服务的名称和显示名称。



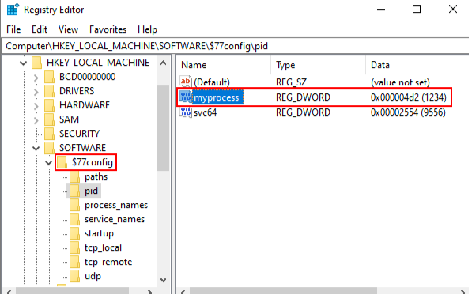
##### TCP和UDP连接

r77 Rootkit可以隐藏指定的本地TCP端口、远程TCP端口和UDP端口。



##### 配置系统

配置系统是用于配置r77 Rootkit行为的一组设置。



##### 其他：

通过设置特定的进程ID、进程名称、路径、服务名称、启动路径，可以隐藏相关的对象及其相关的网络连接。

## 技术实现：

##### Rootkit 的DLL

r77 Rootkit 是一个 DLL 文件，单独编译32 位和 64 位进程。注入到进程中后，此进程将不会显示隐藏的实体。

r77 实现反射式 DLL 注入。任何时候都不需要将 DLL 写入磁盘。相反，文件将写入远程进程内存，并调用 ReflectiveDllMain 导出以最终加载 DLL 并调用 DllMain。因此，DLL 未在 PEB 中列出。

将 DLL 注入到已注入的进程中没有任何影响。DllMain 将检测到这一点，并返回 FALSE 以自行卸载。

##### 子进程挂钩

挂钩进程的创建：

通过挂钩NtResumeThread函数，在新进程执行之前将r77注入到该进程中。如果是32位进程创建64位子进程，则使用命名管道处理注入请求。

定期挂钩新进程：

通过定期检查新创建的进程列表，确保所有新创建的进程都被注入。这是因为某些进程无法直接注入，但它们会创建子进程。

##### Shellcode安装

Shellcode安装是通过执行一个装载器可执行文件来实现的。该装载器在内存中执行过程空洞化(hollowing)操作，然后运行安装程序。

1. **实验结论及心得体会**

在本次实验中，我深入研究了R77，并通过实际操作探索了其在网络安全方面的关键功能和性能。

通过这次实验，我不仅提升了对R77的理论认识，而且通过实际操作获得了宝贵的经验。这将对我们更好地理解和运用网络安全工具和技术产生积极的影响。总体而言，本次实验为我们打开了网络安全领域的大门，为今后的学习和研究奠定了坚实的基础。