Lab10 - R77

- 学号：2113203
- 姓名：付政烨

一、实验目的

本次实验旨在深入探究 r77 根工具包的运行机制及其对系统的影响。通过安装和操作 r77，我们将评估其隐藏进程、文件和注册表项的能力，以及如何规遍常见的安全软件检测。此实验也将帮助理解现代根工具包如何在操作系统级别进行操作，探讨它们的安全隐患和可能的防御措施。通过这一过程，我们将加深对网络安全、恶意软件行为和操作系统安全机制的理解。

二、实验原理

r77 根工具包是一个环3级别的恶意软件，它通过操作系统的用户模式运行，而不需要访问更高权限的内核模式。实验的核心在于理解和观察 r77 如何通过用户模式接口与操作系统交互，以及它如何实现隐藏其活动的目的。

1. **隐藏机制：** r77 利用特定前缀（"$77"）来标记需要隐藏的对象，包括文件、进程、注册表项等。这一过程涉及修改系统API的行为，使得标记的对象在正常查询中不可见。

2. **文件无关性：** 实验还将探索 r77 的文件无关性（filelessness），即它不依赖于硬盘上的文件来持久化或执行。这是通过在内存中运行和复制自身实现的，这种方式使得它能够规避传统的基于文件的防病毒检测。

3. **规避技术：** r77 使用了多种技术来规避防病毒软件和端点检测响应（EDR）系统的检测，包括AMSI绕过和DLL取消挂钩。这些技术展示了现代恶意软件如何利用复杂策略来逃避安全检测。

三、实验过程

1. r77 基本介绍

r77 是一个 ring 3 rootkit，所有以 `"$77"` 开头的内容都会被隐藏。r77 能隐藏以下内容：

- 文件、目录
- 进程和 CPU 使用
- 注册表键和值
- 服务
- TCP 和 UDP 连接
- 联接、命名管道、计划任务

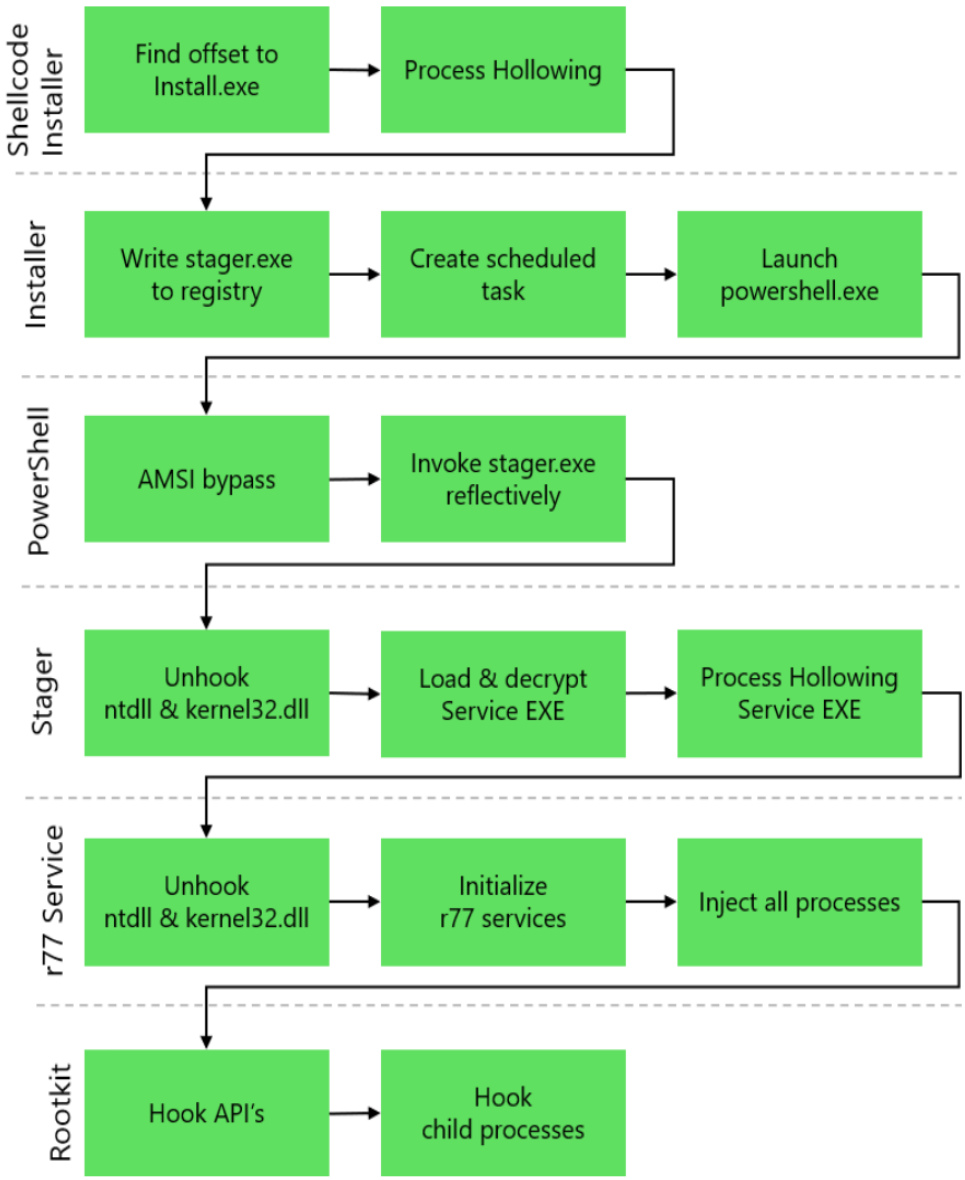
2. r77 配置与安装

配置位于 `HKEY_LOCAL_MACHINE\SOFTWARE\$77config`，任何进程都可以无需提升权限就对其进行写操作。此键的 DACL 被设置为允许任何用户完全访问。此外，`$77config` 键也被根工具包隐藏。

部署 r77 只需要：`Install.exe`。执行后，r77 将在系统中持久化并注入所有运行中的进程。`Uninstall.exe` 可以完全、优雅地从系统中移除 r77。

3. r77 执行流程

本部分详细介绍了 R77 根工具包的执行流程，包括其在系统中的安装、激活和隐藏活动的各个阶段。



1. **Shellcode 安装器阶段**
   - **偏移量定位**: 首先识别 `Install.exe` 的内存偏移量。
   - **进程空洞化**: 应用进程空洞化技术，通过替换已有进程的内存空间实现代码注入。
2. **安装器阶段**
   - **注册表写入**: 安装器将 `stager.exe` 的信息写入系统注册表。
   - **计划任务创建**: 在系统中创建一个计划任务，以便在预定时间执行 `stager.exe`。
   - **PowerShell 启动**: 执行 `powershell.exe`，为下一阶段的 AMSI 绕过做准备。
3. **PowerShell 阶段**
   - **AMSI 绕过**: 实现对 AMSI 的绕过，通过修改 AMSI 函数来禁用恶意软件扫描功能。
   - **反射性调用**: 反射性地调用 `stager.exe`，允许执行无需在磁盘上存在的可执行文件。
4. **Stager 阶段**
   - **DLL 取消挂钩**: 移除 `ntdll.dll` 和 `kernel32.dll` 上的监控挂钩。
   - **服务执行文件加载与解密**: 将服务执行文件加载到内存中，并进行解密。
   - **服务执行文件进程空洞化**: 对服务执行文件应用进程空洞化技术。
5. **R77 服务阶段**

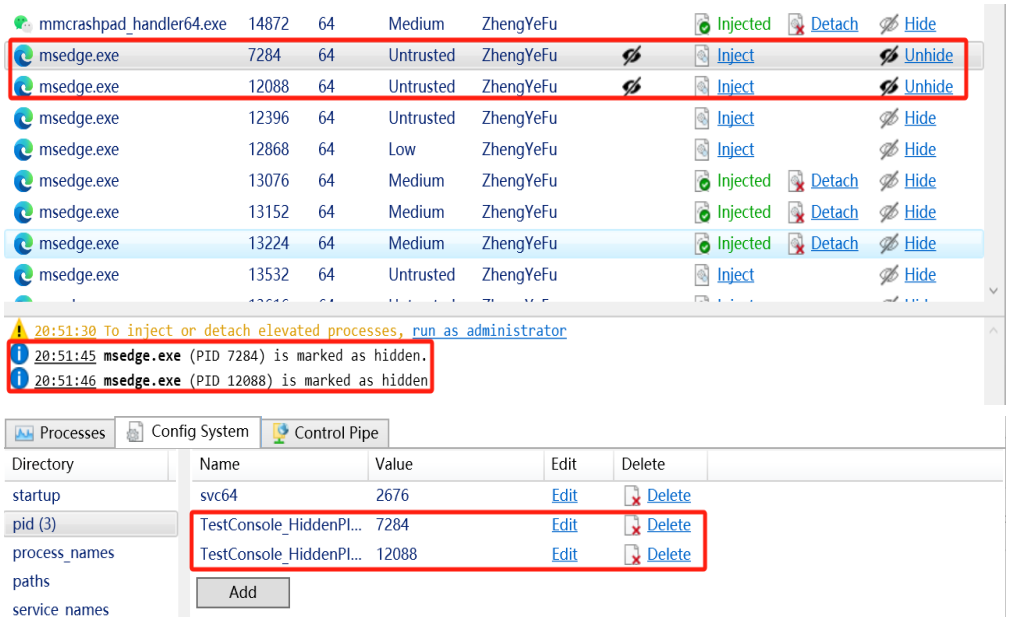
- **系统库文件取消挂钩**: 再次对 `ntdll.dll` 和 `kernel32.dll` 执行取消挂钩操作。
- **R77 服务初始化**: 初始化 R77 根工具包的服务组件。
- **进程注入**: 将 R77 根工具包注入到所有正在运行的进程中。

6. **根工具包阶段**
   - **API 挂钩**: 挂钩系统 API 调用，以隐藏根工具包的活动。
   - **子进程挂钩**: 确保挂钩机制扩展到任何新创建的子进程。

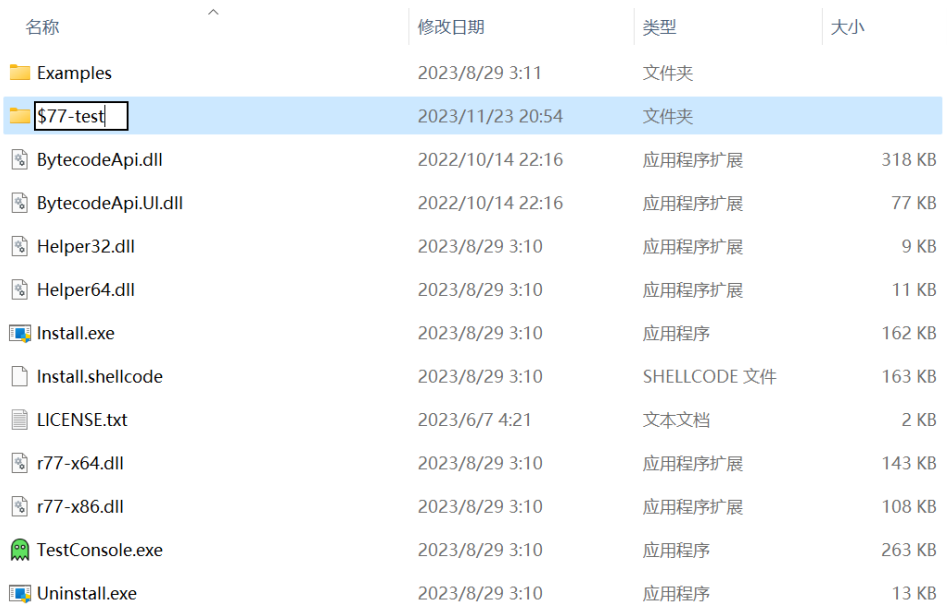
此流程确保了 R77 根工具包在系统中的隐蔽执行，通过各种技术规避安全软件的检测，并在多个系统层面中植入自身，展现了其作为先进持久性威胁（APT）的能力。此分析可作为研究恶意软件行为及其防御策略的基础。

4. r77 测试

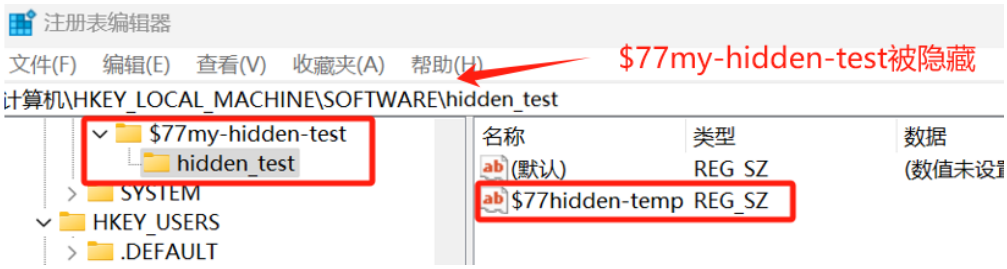
1. **隐藏进程**:
   - 用户可以通过配置系统来指定要隐藏的进程。



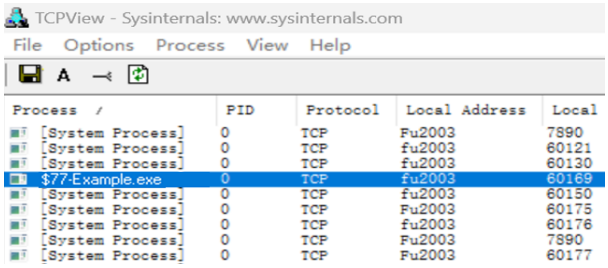
2. **隐藏文件**:
   - r77 允许用户通过前缀 `$77` 隐藏文件。任何以 `$77` 为前缀的文件、目录或进程都会被自动隐藏。



3. **隐藏注册表项和值**：
   - r77 通过修改系统注册表的方式隐藏特定的注册表键和值。



4. **隐藏网络连接**：
   - r77 可以隐藏特定端口的 TCP 和 UDP 网络连接。
   - 用户可以通过动态配置系统指定要隐藏的网络连接的端口。



四、实验心得与体会

通过实验，我深刻理解了 r77 根工具包的复杂性和潜在危害。它的高度隐蔽性和强大的隐藏能力使我意识到了现代恶意软件的先进技术和威胁。同时，这也突显了作为网络安全从业者需要具备的敏锐洞察力和持续学习的重要性。实验中，我特别对 r77 的文件无关性和高级规避技术印象深刻。这些特性不仅展示了恶意软件作者的高技术水平，也为我提供了有关如何改进安全防御策略的洞见。此外，亲手操作和观察这样的根工具包也加强了我的实践技能，让我对理论知识有了更深入的理解和应用。