南開大學

《恶意代码分析与防治技术》课程实验报告

实验 10-2

学　　院　网络空间安全学院

专　　业　信息安全

学　　号　2112060

姓　　名　孙蕗

一、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。

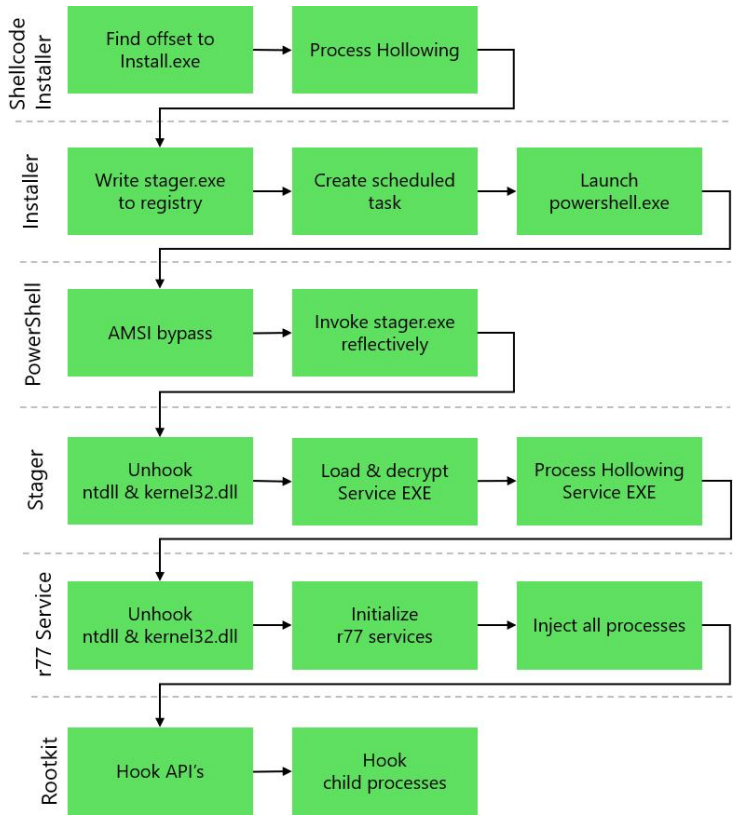
对实验结果进行截图，完成实验报告。

二、实验原理

r77-Rootkit 是一个 Ring3 级别的 Rootkit。Rootkit 是一种特殊的恶意软件，它的功能是在安装目标上隐藏自身及指定的文件、进程和网络链接等信息，比较多见到的是 Rootkit 一般都和木马、后门等其他恶意程序结合使用。Rootkit 并不一定是用作获得系统 root 访问权限的工具。比起攻击，Rootkit 更倾向于被使用于隐藏踪迹和保留 root 访问权限的工具。至于 Ring3 则是 CPU 的四个特权级别之一，Windows 只使用其中的两个级别 Ring0 和 Ring3，Ring0 上运行操作系统（内核）代码，Ring3 上运行应用程序代码，不能执行受控操作。如果普通应用程序企图执行 Ring0 指令，则 Windows 会显示“非法指令”错误信息。

rootkit 驻留在系统内存中，不会将任何文件写入磁盘。这是分多个阶段实现的。

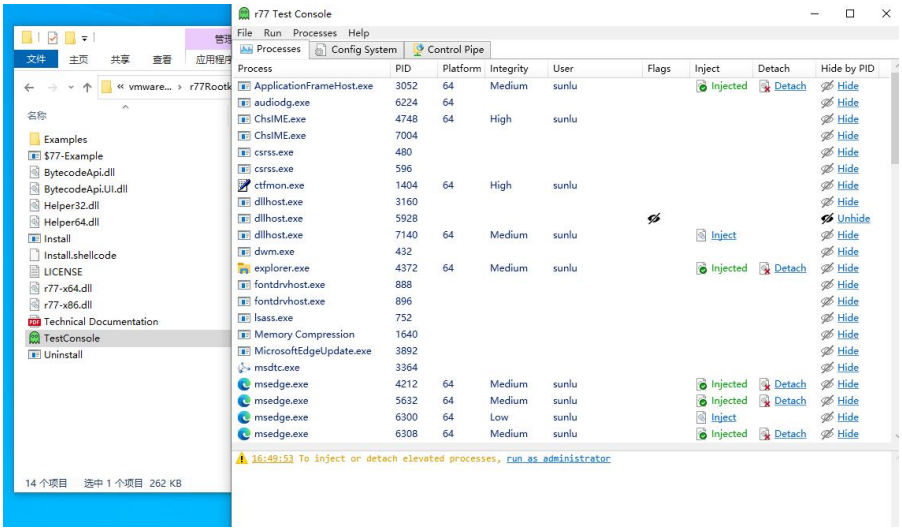
此图显示了从安装程序的执行一直到每个进程中运行的 rootkit DLL 的每个阶段。



三、实验过程

使用 install.exe 安装.exe，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。

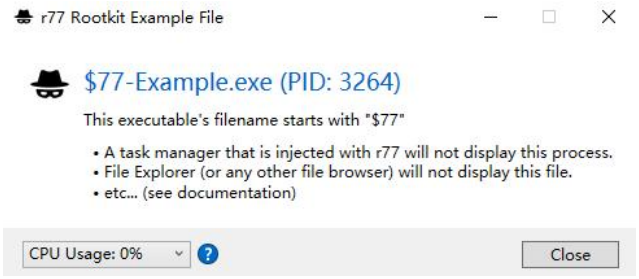
TestConsole.exe 是一个用于测试 r77 功能的工具。它可用于在不安装 rootkit 的情况下将 r77 注入或从单个进程中分离 r77。但是，某些功能只有在完全安装 rootkit 后才能使用

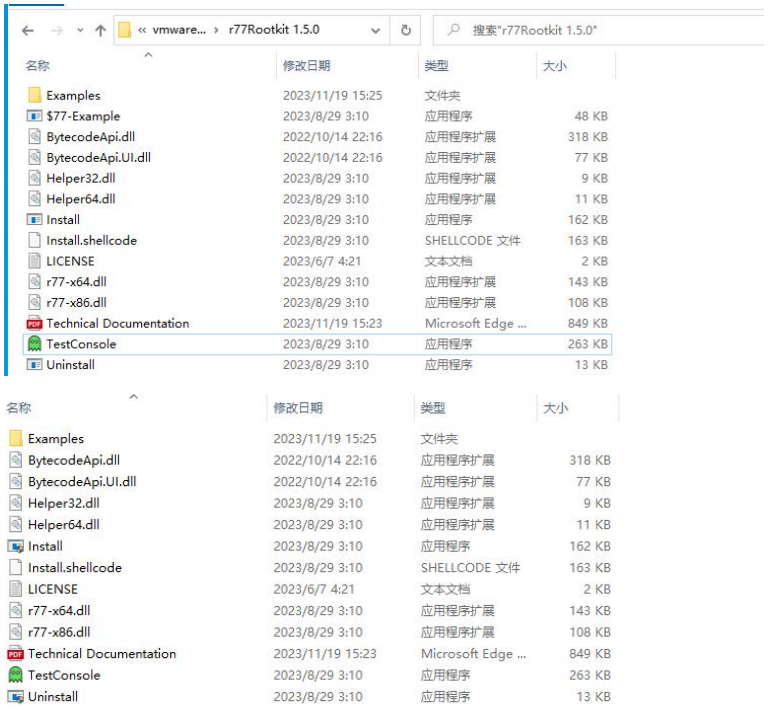


Flag	Meaning
	This is the r77 service process. It cannot be injected with r77. The r77 service is running when r77 is installed.
	This is an r77 helper process. It cannot be injected with r77. `TestConsole.exe` is a helper process. Also, `Install.exe` and `Uninstall.exe` are helper processes. This is to avoid r77 being injected into them.
	This process is hidden by ID using the configuration system. A task manager does not display this process. The r77 service is hidden by ID by default. `Uninstall.exe` deletes the list of hidden process ID's. The "Hide"-Button can be used to write a specific process ID into the configuration system.

$77- Example.exe 可用于测试任务管理器和文件查看器。要对进程隐藏执行快速测试，启动此可执行文件，然后使用测试控制台向任务管理器注入 r77。该进程在注入的任务管理器中不再可见。要隐藏该文件，可使用测试控制台注入资源管理器，但需要将文件名重命名为以前缀 $77 开头。

（1） 隐藏文件





r77 每 1000 毫秒读取一次配置，其中包含以下信息：

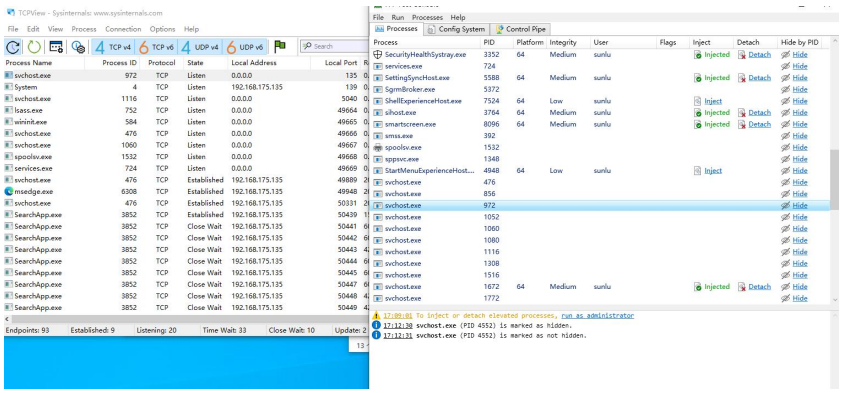
隐藏进程 ID 列表、隐藏进程名称列表、隐藏路径列表、隐藏服务名称列表、隐藏的本地 TCP 端口列表、隐藏的远程 TCP 端口列表、隐藏的 UDP 端口列表、启动路径列表

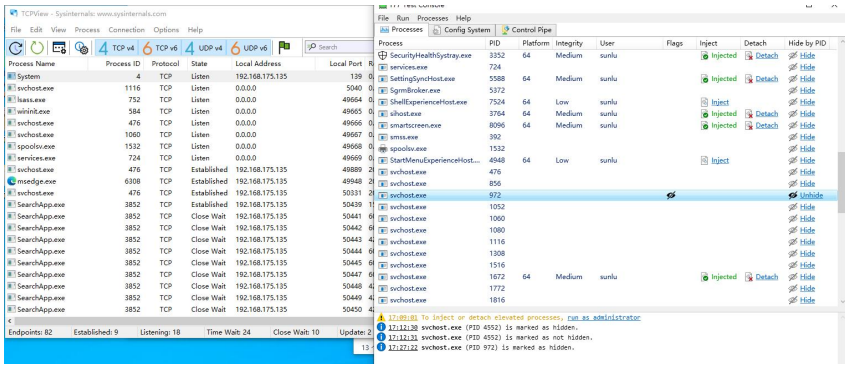
除了 $77 前缀之外，此配置还用于隐藏基于自定义配置的实体。任何进程都可以在没有提升权限的情况下写入配置系统。

值的名称通常会被忽略。值 $77configpidsvc32 和 $77configpidsvc64 保留给 r77 服务，不应修改。它们是在 r77 服务启动时自动创建的。

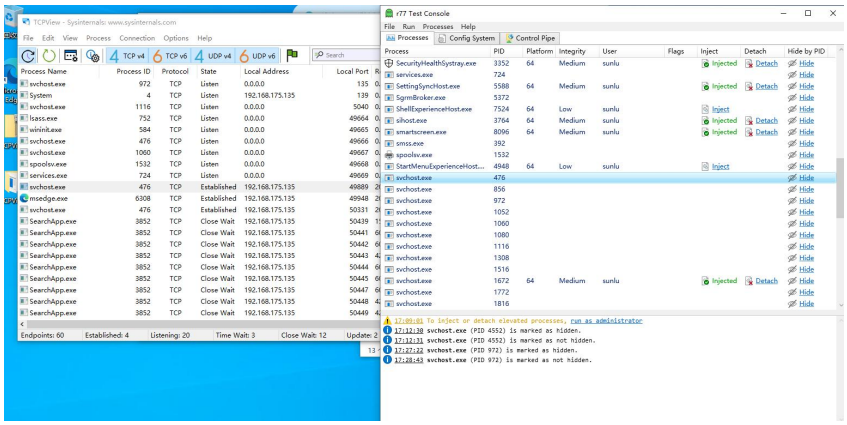
测试控制台可用于将 r77 注入单个进程或从单个进程中分离 r77。

（2） 隐藏指定进程



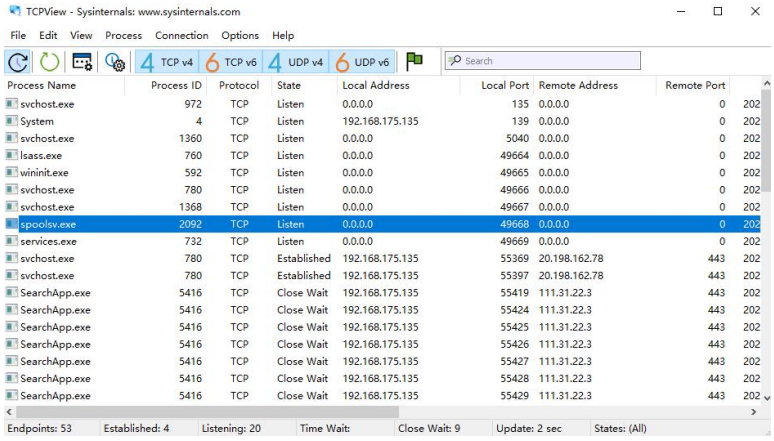


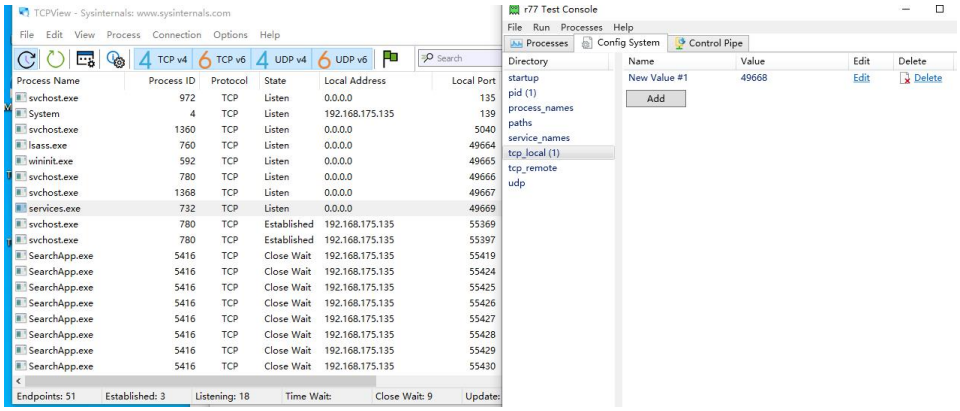
隐藏了 PID=972 的进程



隐藏了 PID=476 的进程

(3) 隐藏网络连接





（4） 隐藏注册表

服务通过前缀和配置系统中指定的名称隐藏。根据该列表检查名称和显示名称。