



网 络 空 间 安 全 学 院

恶意代码分析与防治技术 实验报告

Lab 10.5 : R77-Rootkit



姓名：辛浩然

学号：2112514

年级：2021 级

专业：信息安全、法学

班级：信息安全、法学

实验内容	
实验环境及实验工具	
实验原理	
隐藏进程	
隐藏名称以\$77为前缀的进程	
在测试工具中指定特定进程	
在测试工具中依据PID和名称隐藏进程	
写注册表隐藏特定进程	
隐藏文件	
文件前缀隐藏	
指定文件路径隐藏	
隐藏注册表	
隐藏计划任务	
隐藏服务	
隐藏网络连接	
实验结论及心得体会	

实验内容

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。

实验环境及实验工具

关闭病毒防护的Windows 10 操作系统。

实验工具：r77 Rootkit、Process Explorer、TCPView等

实验原理

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。

下载R77压缩包解压后：

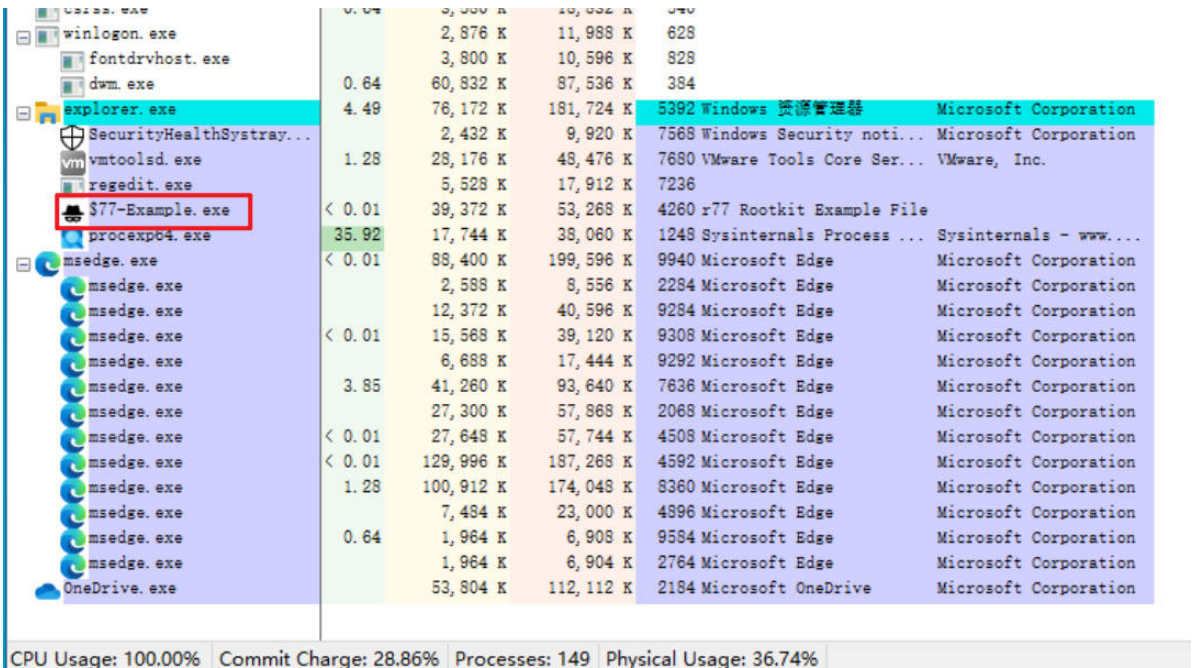
- 运行 `Install.exe` 将 r77 注入每个正在运行的进程中，并将 rootkit 保留在系统上。
- `TestConsole.exe` 是一个用于测试r77功能的工具。它可用于将 r77 注入或将 r77 从各个进程中分离出来。可以在其中停止R77的运行。
- 运行 `Uninstall.exe` 将 r77 彻底移除。

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。`$77config` 键在注册表编辑器被注入了Rootkit之后会自动隐藏。测试工具 `TestConsole.exe` 实际上也是写入注册表。

隐藏进程

隐藏名称以\$77为前缀的进程

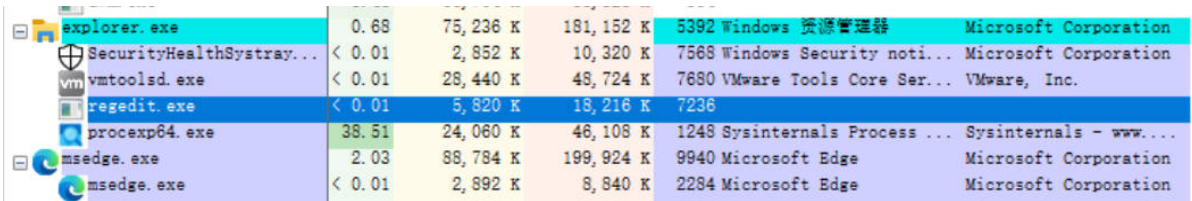
首先运行 `$77-Example.exe`，在 Process Explorer 中可以观察到该进程：



winlogon.exe		2,876 K	11,988 K	628	
fontdrvhost.exe		3,800 K	10,596 K	828	
dm.exe	0.64	60,832 K	87,536 K	384	
explorer.exe	4.49	76,172 K	181,724 K	5392	Windows 资源管理器 Microsoft Corporation
SecurityHealthSystray.exe		2,432 K	9,920 K	7568	Windows Security notification icon Microsoft Corporation
vmtoolsd.exe	1.28	28,176 K	48,476 K	7680	VMware Tools Core Services VMware, Inc.
regedit.exe		5,528 K	17,912 K	7236	
\$77-Example.exe	< 0.01	39,372 K	53,268 K	4260	r77 Rootkit Example File
procexp64.exe	35.92	17,744 K	38,060 K	1248	Sysinternals Process Explorer Sysinternals - www.sysinternals.com
msedge.exe	< 0.01	88,400 K	199,596 K	9940	Microsoft Edge Microsoft Corporation
msedge.exe		2,588 K	8,556 K	2284	Microsoft Edge Microsoft Corporation
msedge.exe		12,372 K	40,596 K	9284	Microsoft Edge Microsoft Corporation
msedge.exe	< 0.01	15,568 K	39,120 K	9308	Microsoft Edge Microsoft Corporation
msedge.exe		6,688 K	17,444 K	9292	Microsoft Edge Microsoft Corporation
msedge.exe	3.85	41,260 K	93,640 K	7636	Microsoft Edge Microsoft Corporation
msedge.exe		27,300 K	57,868 K	2068	Microsoft Edge Microsoft Corporation
msedge.exe	< 0.01	27,648 K	57,744 K	4508	Microsoft Edge Microsoft Corporation
msedge.exe	< 0.01	129,996 K	187,268 K	4592	Microsoft Edge Microsoft Corporation
msedge.exe	1.28	100,912 K	174,048 K	8360	Microsoft Edge Microsoft Corporation
msedge.exe		7,484 K	23,000 K	4896	Microsoft Edge Microsoft Corporation
msedge.exe	0.64	1,964 K	6,908 K	9584	Microsoft Edge Microsoft Corporation
msedge.exe		1,964 K	6,904 K	2764	Microsoft Edge Microsoft Corporation
OneDrive.exe		53,804 K	112,112 K	2184	Microsoft OneDrive Microsoft Corporation

CPU Usage: 100.00% Commit Charge: 28.86% Processes: 149 Physical Usage: 36.74%

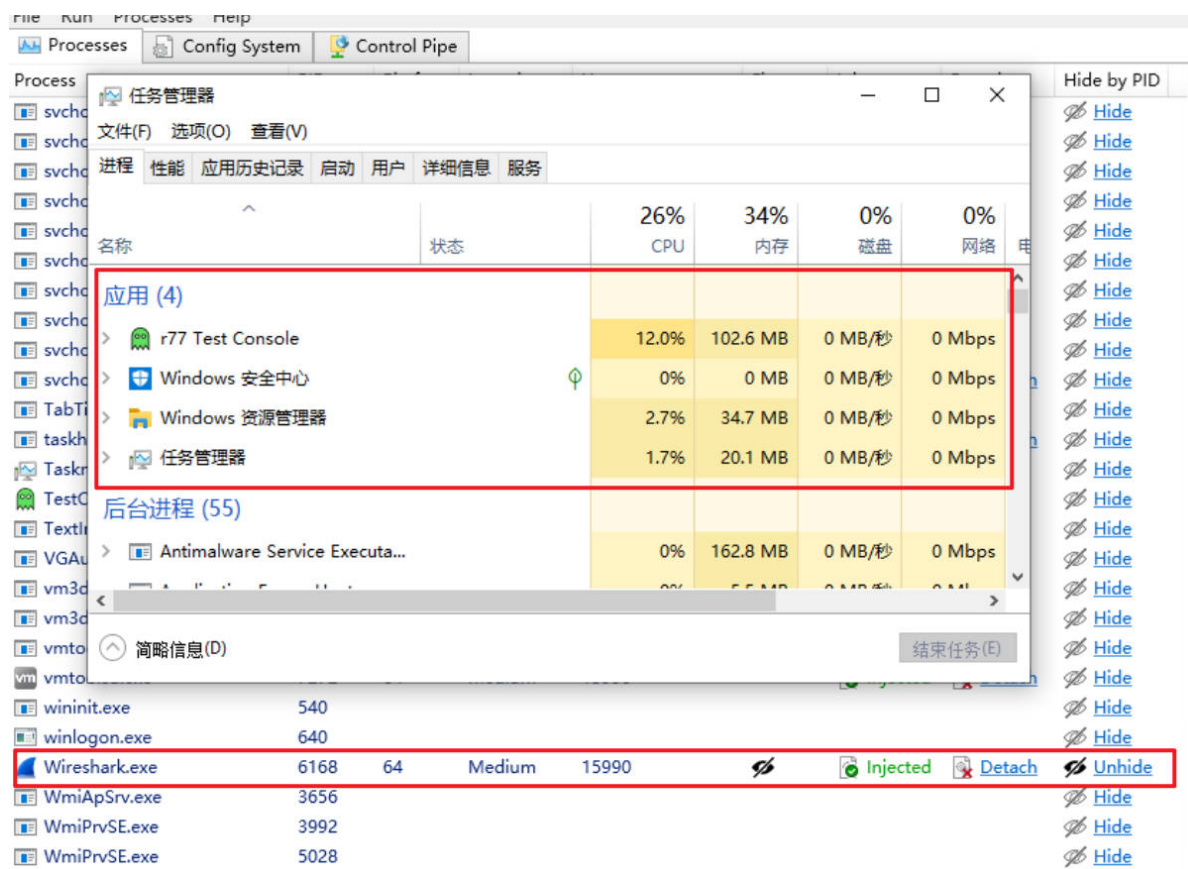
运行 `Install.exe` 安装R77，成功发现进程 `$77-Example.exe` 被隐藏。说明 R77 能够隐藏名称以 `$77` 为前缀的进程。



explorer.exe	0.68	75,236 K	181,152 K	5392	Windows 资源管理器 Microsoft Corporation
SecurityHealthSystray.exe	< 0.01	2,852 K	10,320 K	7568	Windows Security notification icon Microsoft Corporation
vmtoolsd.exe	< 0.01	28,440 K	48,724 K	7680	VMware Tools Core Services VMware, Inc.
regedit.exe	< 0.01	5,820 K	18,216 K	7236	
procexp64.exe	38.51	24,060 K	46,108 K	1248	Sysinternals Process Explorer Sysinternals - www.sysinternals.com
msedge.exe	2.03	88,784 K	199,924 K	9940	Microsoft Edge Microsoft Corporation
msedge.exe	< 0.01	2,892 K	8,840 K	2284	Microsoft Edge Microsoft Corporation

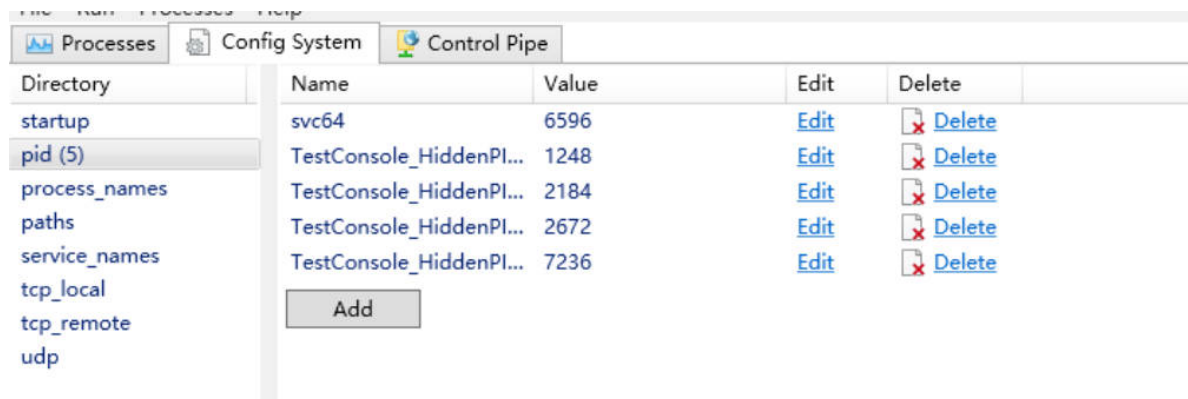
在测试工具中指定特定进程

在测试工具中可以查看当前进程列表，对每个进程实施通过PID的隐藏操作。比如，在测试工具中对 `Wireshark.exe` 进行隐藏，然后发现在任务管理器中无法发现该进程。

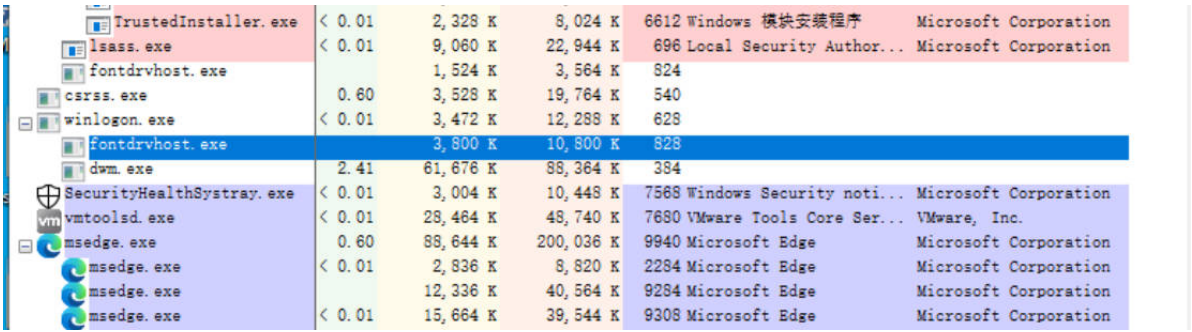


在测试工具中依据PID和名称隐藏进程

在测试工具中，可以添加隐藏的进程的PID：



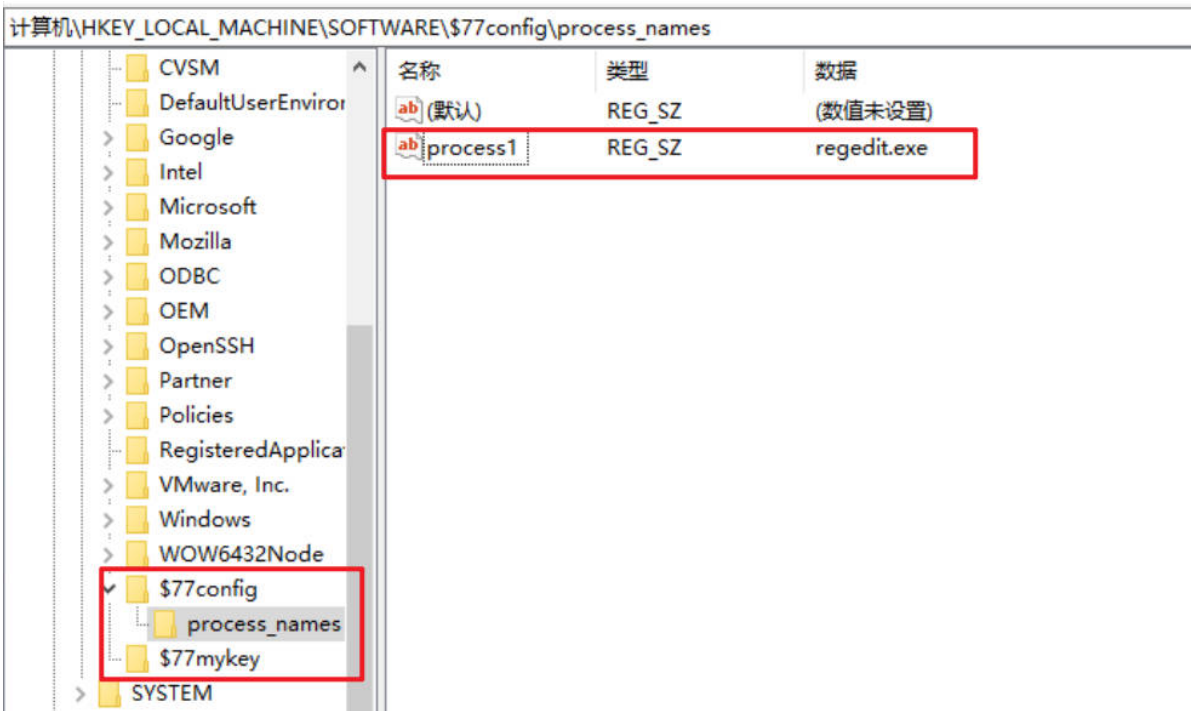
添加之后，在Process Explorer中成功发现特定进程被隐藏。



TrustedInstaller.exe	< 0.01	2,328 K	8,024 K	6612 Windows 模块安装程序	Microsoft Corporation
lsass.exe	< 0.01	9,060 K	22,944 K	696 Local Security Author...	Microsoft Corporation
fontdrvhost.exe		1,524 K	3,564 K	824	
csrss.exe	0.60	3,528 K	19,764 K	540	
winlogon.exe	< 0.01	3,472 K	12,288 K	628	
fontdrvhost.exe		3,800 K	10,800 K	828	
dwm.exe	2.41	61,676 K	88,364 K	384	
SecurityHealthSystray.exe	< 0.01	3,004 K	10,448 K	7568 Windows Security noti...	Microsoft Corporation
vmtoolsd.exe	< 0.01	28,464 K	48,740 K	7680 VMware Tools Core Ser...	VMware, Inc.
msedge.exe	0.60	88,644 K	200,036 K	9940 Microsoft Edge	Microsoft Corporation
msedge.exe	< 0.01	2,836 K	8,820 K	2284 Microsoft Edge	Microsoft Corporation
msedge.exe		12,336 K	40,564 K	9284 Microsoft Edge	Microsoft Corporation
msedge.exe	< 0.01	15,664 K	39,544 K	9308 Microsoft Edge	Microsoft Corporation

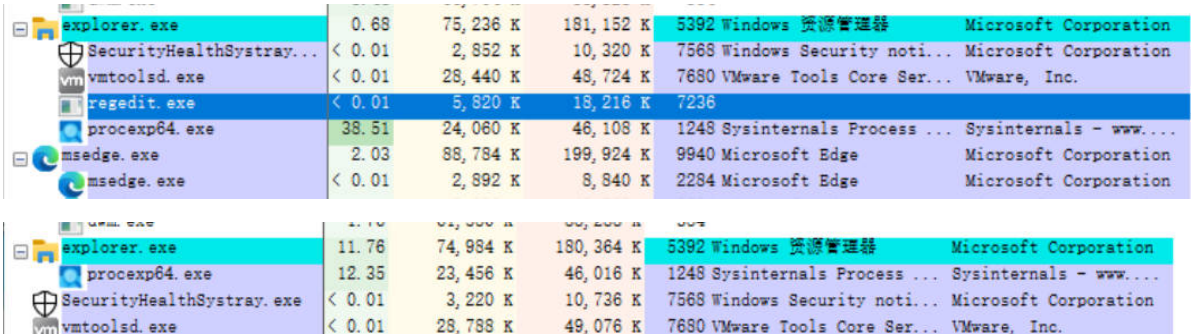
写注册表隐藏特定进程

在未运行R77之前，可以手动在 `HKEY_LOCAL_MACHINE\SOFTWARE\` 下新增项 `$77config\process_names`，并增加值为 `regedit.exe`。



计算机\HKEY_LOCAL_MACHINE\SOFTWARE\\$77config\process_names		
名称	类型	数据
(默认)	REG_SZ	(数值未设置)
process1	REG_SZ	regedit.exe

在运行R77之后，能够发现，该注册表被隐藏，而写入的名为 `regedit.exe` 进程也被隐藏。下图为运行前后Process Explorer进程对比，其中 `regedit.exe` 进程被隐藏。



explorer.exe	0.68	75,236 K	181,152 K	5392 Windows 资源管理器	Microsoft Corporation
SecurityHealthSystray.exe	< 0.01	2,852 K	10,320 K	7568 Windows Security noti...	Microsoft Corporation
vmtoolsd.exe	< 0.01	28,440 K	48,724 K	7680 VMware Tools Core Ser...	VMware, Inc.
regedit.exe	< 0.01	5,820 K	18,216 K	7236	
procexp64.exe	38.51	24,060 K	46,108 K	1248 Sysinternals Process ...	Sysinternals - www....
msedge.exe	2.03	88,784 K	199,924 K	9940 Microsoft Edge	Microsoft Corporation
msedge.exe	< 0.01	2,892 K	8,840 K	2284 Microsoft Edge	Microsoft Corporation

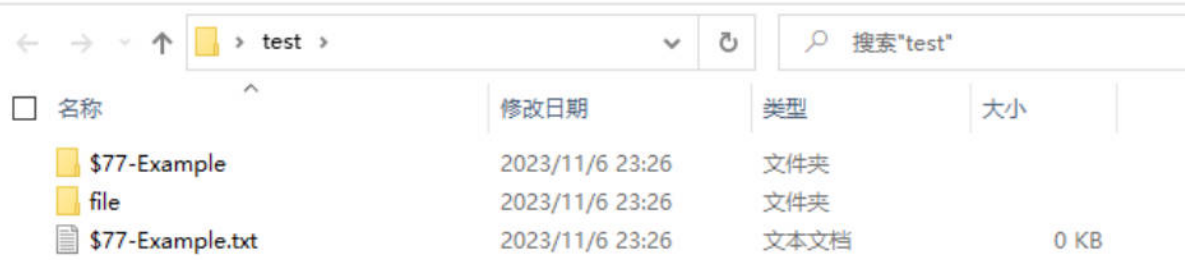
explorer.exe	11.76	74,984 K	180,364 K	5392 Windows 资源管理器	Microsoft Corporation
procexp64.exe	12.35	23,456 K	46,016 K	1248 Sysinternals Process ...	Sysinternals - www....
SecurityHealthSystray.exe	< 0.01	3,220 K	10,736 K	7568 Windows Security noti...	Microsoft Corporation
vmtoolsd.exe	< 0.01	28,788 K	49,076 K	7680 VMware Tools Core Ser...	VMware, Inc.

同样，也可以在注册表中增加 `pid` 项，写入要隐藏的进程 `pid`。在测试工具中依据PID和名称隐藏进程，就是测试工具修改了注册表。

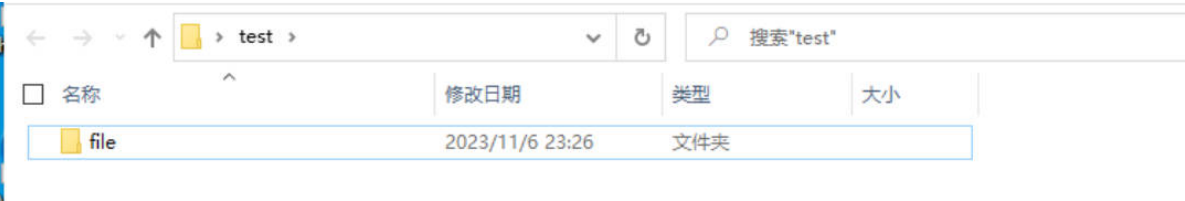
隐藏文件

文件前缀隐藏

在 R77 运行后，`$77` 开头的文件和文件夹会被隐藏。下图为运行前创建的测试文件夹。



运行后查看该文件夹，发现 `$77` 开头的文件和文件夹都被隐藏。



指定文件路径隐藏

在未运行时在注册表项 `$77config\paths` 中写入要隐藏的文件路径，或者直接在测试工具中写入文件路径（测试工具中的记录与注册表中的键值是同步的），可以隐藏指定路径的文件/文件夹。比如，隐藏 `C:\Windows` 目录。



这是运行前的文件目录：

<div> <div> <div>←</div> <div>→</div> <div>⬆</div> <div>⬇</div> <div>⬇</div> <div>⬆</div> </div> <div> <div>本地磁盘 (C:)</div> <div>本地磁盘 (C:)</div> </div> <div> <div>搜索"本地磁盘 (C:)"</div> </div> </div>			
<input type="checkbox"/> 名称	修改日期	类型	大小
\$WinREAgent	2023/11/3 18:16	文件夹	
OneDriveTemp	2023/10/26 17:46	文件夹	
PerfLogs	2019/12/7 17:14	文件夹	
phpstudy_pro	2023/10/26 17:54	文件夹	
Program Files	2023/11/3 18:16	文件夹	
Program Files (x86)	2021/4/9 21:57	文件夹	
ProgramData	2023/11/3 18:06	文件夹	
<input checked="" type="checkbox"/> Windows	2023/11/9 19:21	文件夹	
用户	2023/10/26 17:45	文件夹	

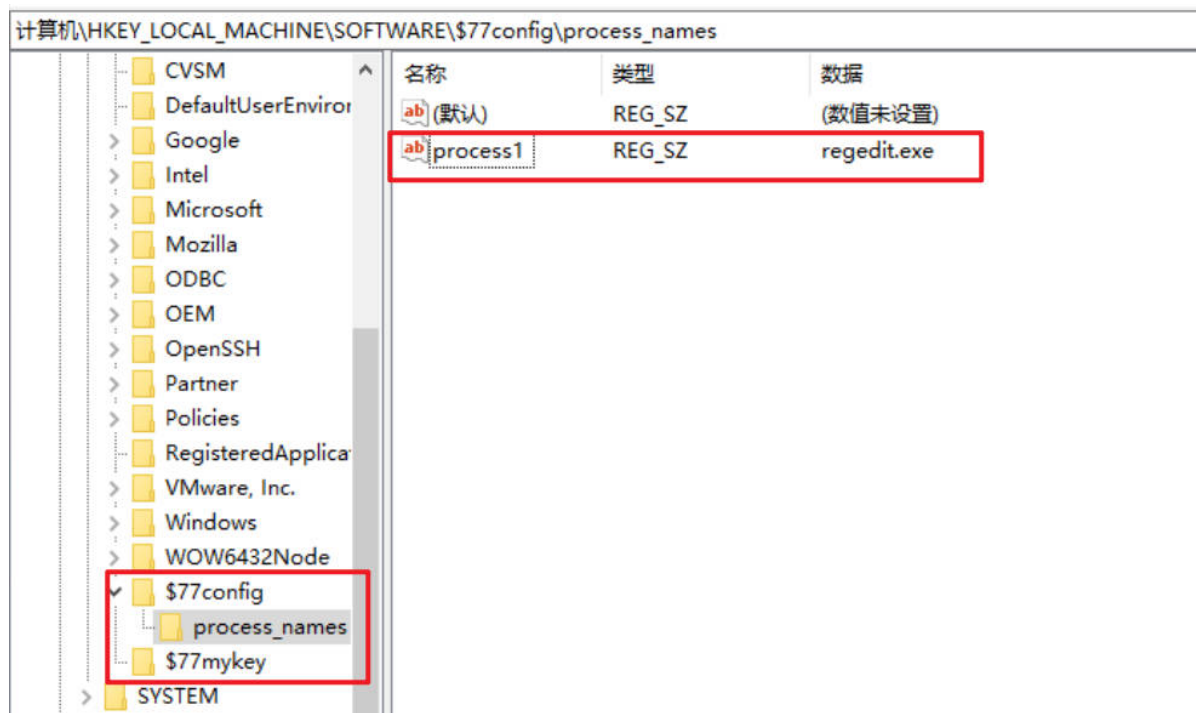
这是运行后的文件目录，成功隐藏了 `C:\Windows`。

<div> <div> <div>←</div> <div>→</div> <div>⬆</div> <div>⬇</div> <div>⬇</div> <div>⬆</div> </div> <div> <div>本地磁盘 (C:)</div> <div>本地磁盘 (C:)</div> </div> <div> <div>搜索"本地磁盘 (C:)"</div> </div> </div>			
<input type="checkbox"/> 名称	修改日期	类型	大小
\$WinREAgent	2023/11/3 18:16	文件夹	
OneDriveTemp	2023/10/26 17:46	文件夹	
PerfLogs	2019/12/7 17:14	文件夹	
phpstudy_pro	2023/10/26 17:54	文件夹	
Program Files	2023/11/3 18:16	文件夹	
Program Files (x86)	2021/4/9 21:57	文件夹	
ProgramData	2023/11/3 18:06	文件夹	
用户	2023/10/26 17:45	文件夹	

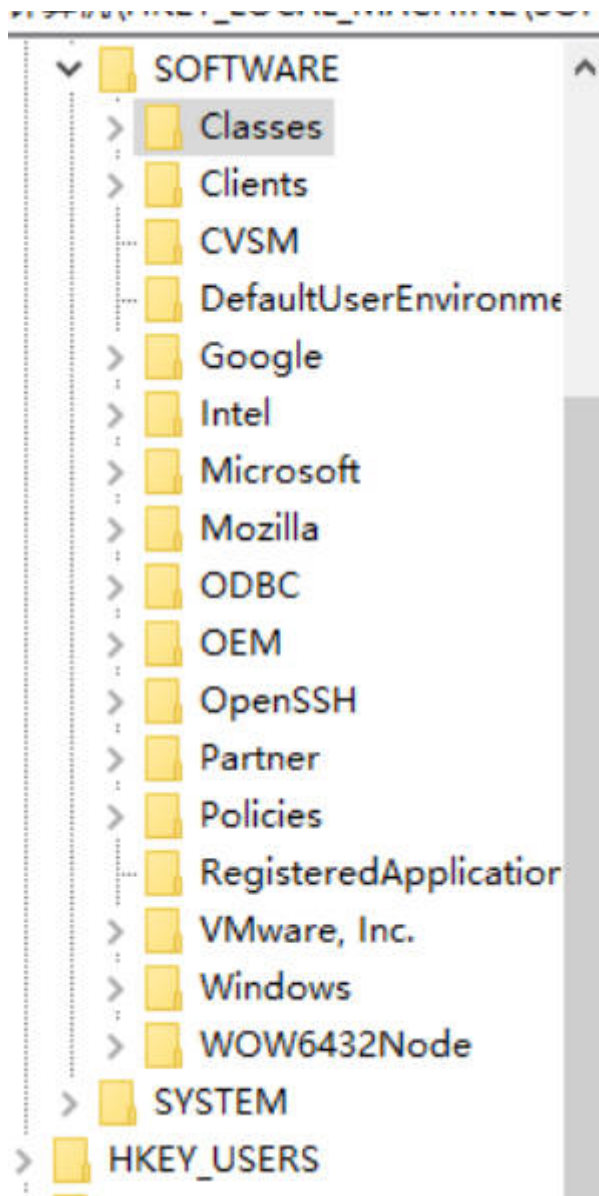
隐藏注册表

注册表项可以根据前缀 `$77` 隐藏。

运行前写注册表项，以 `$77` 开头：



运行后可以发现，以 \$77 开头的注册表项被隐藏。



隐藏计划任务

计划任务同样可以根据前缀 `$77` 隐藏。

名称	状态	触发器	下次运行
\$77task	准备就绪	在 2023/11/9 的 19:23 时	
\$77test	准备就绪	在 2023/11/10 的 19:18 时	2023/1
\$77test sch...	准备就绪		
MicrosoftE...	准备就绪	已定义多个触发器	2023/1
MicrosoftE...	准备就绪	在每天的 18:51 - 触发后, 在 1 天 期间每隔 1 小时 重复一次。	2023/1
MicrosoftE...	准备就绪	已定义多个触发器	2023/1
MicrosoftE...	准备就绪	在每天的 18:14 - 触发后, 在 1 天 期间每隔 1 小时 重复一次。	2023/1
npcapwatc...	准备就绪	在系统启动时	
OneDrive R...	准备就绪	在 2023/11/5 的 13:28 时 - 触发后 无限期地每隔 1 00:00:00 重复一次	2023/1

运行后，可以发现 `$77` 开头的计划任务被隐藏。

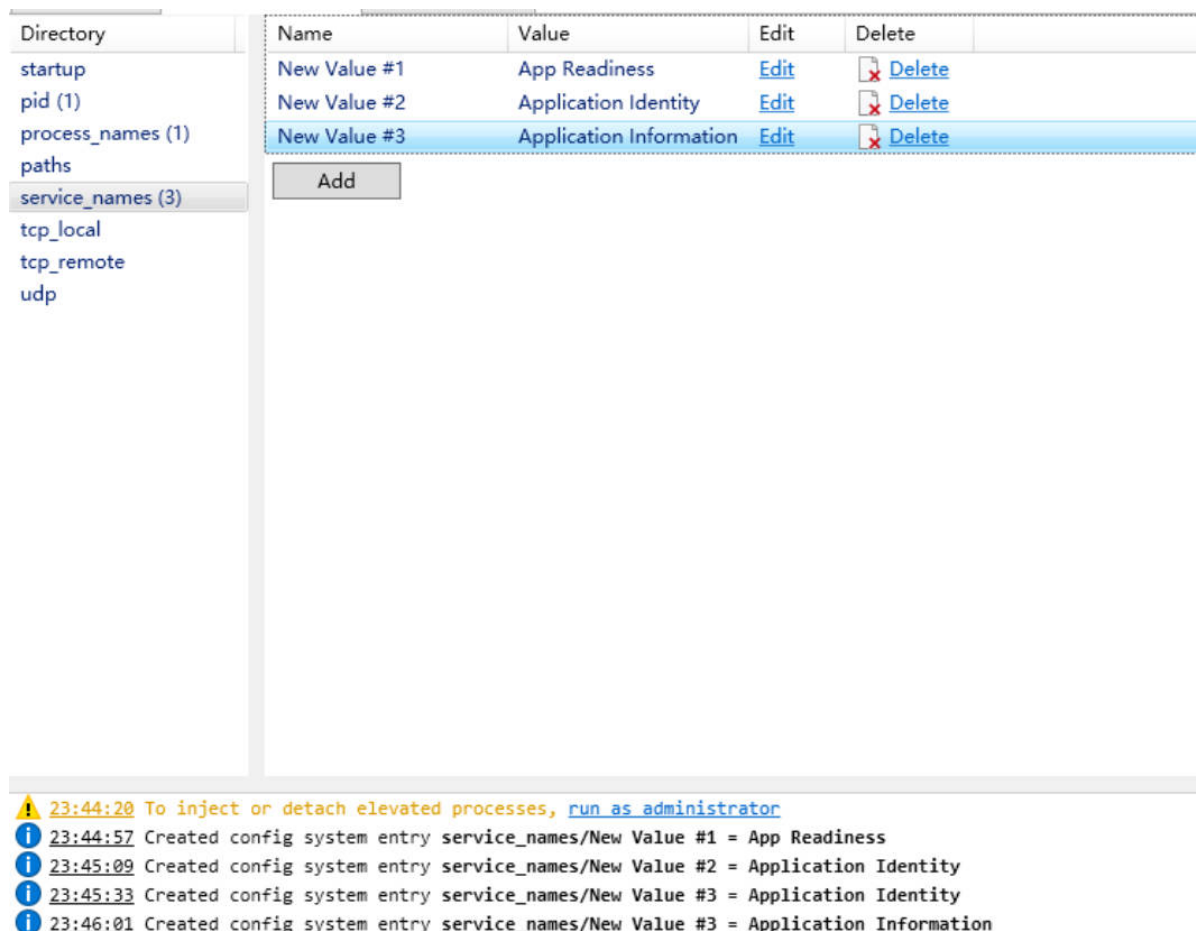
名称	状态	触发器	下次运行时
MicrosoftE...	准备就绪	已定义多个触发器	2023/11/1
MicrosoftE...	准备就绪	在每天的 18:51 - 触发后，在 1 天 期间每隔 1 小时 重复一次。	2023/11/9
MicrosoftE...	准备就绪	已定义多个触发器	2023/11/1
MicrosoftE...	准备就绪	在每天的 18:14 - 触发后，在 1 天 期间每隔 1 小时 重复一次。	2023/11/9
npcapwatc...	准备就绪	在系统启动时	
OneDrive R...	准备就绪	在 2023/11/5 的 13:29 时 - 触发后，无限期地每隔 1.00:00:00 重复一次。	2023/11/1
OneDrive S...	准备就绪	在 1992/5/1 的 12:00 时 - 触发后，无限期地每隔 1.00:00:00 重复一次。	2023/11/1
task	准备就绪	在 2023/11/9 的 19:22 时	

隐藏服务

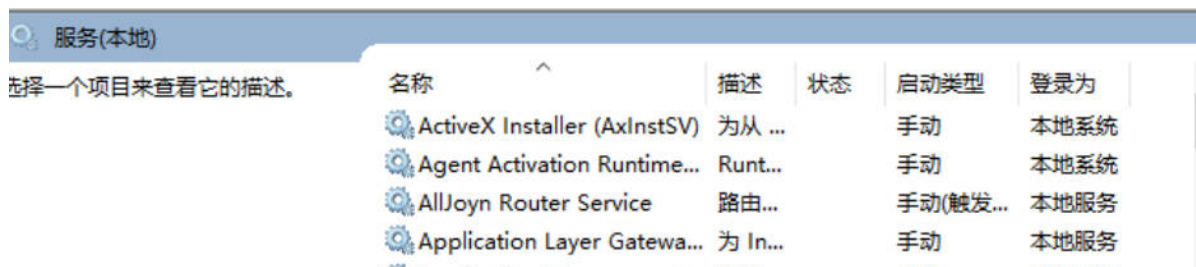
查看存在的服务。

服务(本地)					
选择一个项目来查看它的描述。					
名称	描述	状态	启动类型	登录为	
ActiveX Installer (AxInstSV)	为从 ...		手动	本地系统	
Agent Activation Runtime...	Runt...		手动	本地系统	
AllJoyn Router Service	路由...		手动(触发...	本地服务	
App Readiness	当用...		手动	本地系统	
Application Identity	确定...		手动(触发...	本地服务	
Application Information	使用...	正在...	手动(触发...	本地系统	
Application Layer Gatewa...	为 In...		手动	本地服务	

根据名称，在注册表的 `service_names` 子项下增加要隐藏的服务。



运行后，能够发现指定名称的服务被隐藏。



隐藏网络连接

使用TCPView查看TCP连接。

svcnost.exe	7888	TCP	Established	192.168.188.142	50437	20.191.46.109
msedge.exe	9308	TCP	Established	192.168.188.142	50263	20.194.180.20
msedge.exe	9308	TCP	Close Wait	192.168.188.142	50440	20.231.53.73
msedge.exe	9308	TCP	Close Wait	192.168.188.142	50439	20.231.53.73
msedge.exe	9940	UDP		0.0.0.0	5353	*
msedge.exe	9940	UDP		0.0.0.0	5353	*
msedge.exe	9940	UDpv6		::	5353	*

在注册表中的 `tcp_local` 子项增加要隐藏的TCP连接的 `Local Port`，这里写入端口 50263。



运行后，本地端口5063的tcp连接被隐藏。

msedge.exe	9308	TCP	Close Wait	192.168.188.142	50440	20.231.53.73
msedge.exe	9308	TCP	Close Wait	192.168.188.142	50439	20.231.53.73
msedge.exe	9940	UDP		0.0.0.0	5353	*

实验结论及心得体会

通过本次实验，运行R77程序，实现对指定的进程、文件、注册表、网络连接、计划任务、服务的隐藏，对 Rootkit 有了更为深入的认识。