

南开大学

《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 孙璐

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。

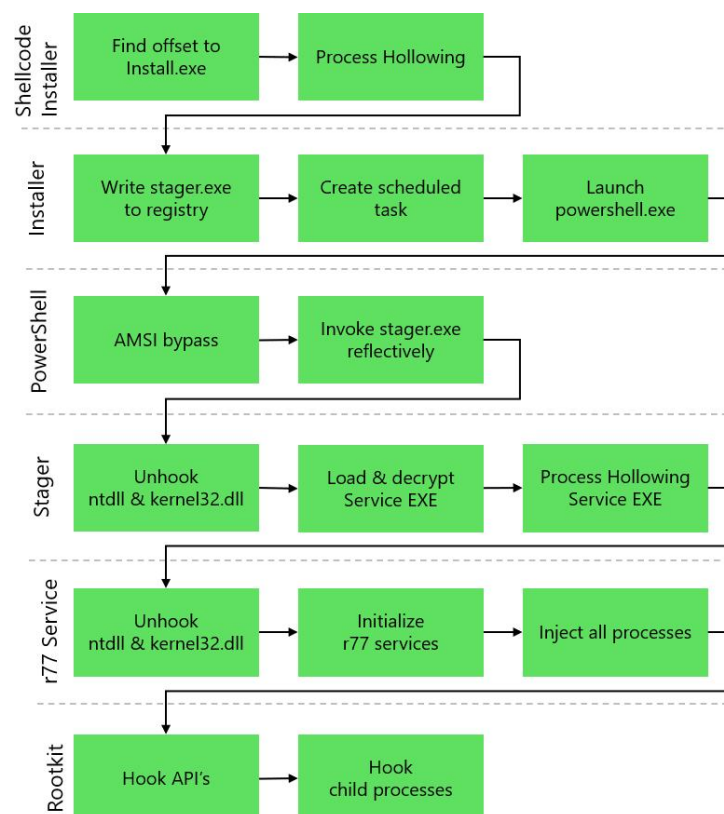
对实验结果进行截图，完成实验报告。

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。

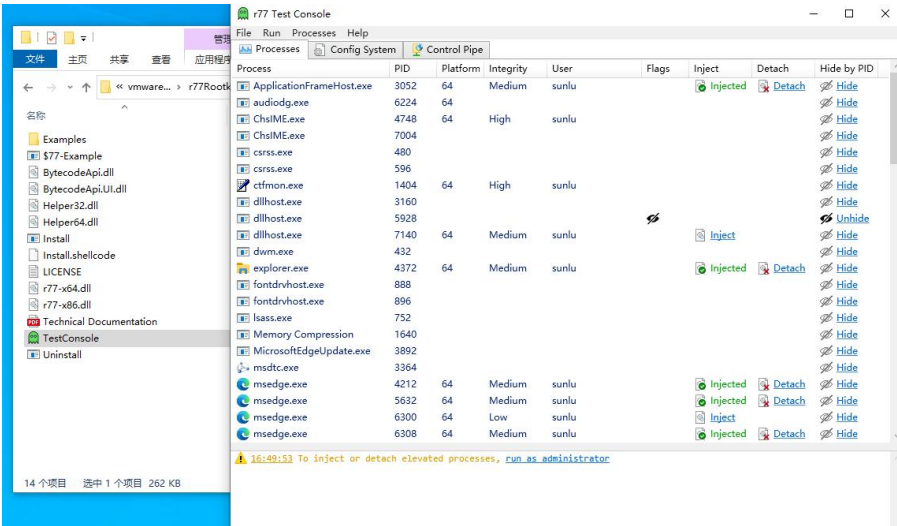


三、实验过程

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。

vmware... > r77Rootkit 1.5.0				搜索"r77Rootkit 1.5.0"
名称	修改日期	类型	大小	
Examples	2023/11/19 15:25	文件夹		
\$77-Example	2023/8/29 3:10	应用程序	48 KB	
BytecodeApi.dll	2022/10/14 22:16	应用程序扩展	318 KB	
BytecodeApi.UI.dll	2022/10/14 22:16	应用程序扩展	77 KB	
Helper32.dll	2023/8/29 3:10	应用程序扩展	9 KB	
Helper64.dll	2023/8/29 3:10	应用程序扩展	11 KB	
Install	2023/8/29 3:10	应用程序	162 KB	
Install.shellcode	2023/8/29 3:10	SHELLCODE 文件	163 KB	
LICENSE	2023/6/7 4:21	文本文档	2 KB	
r77-x64.dll	2023/8/29 3:10	应用程序扩展	143 KB	
r77-x86.dll	2023/8/29 3:10	应用程序扩展	108 KB	
Technical Documentation	2023/11/19 15:23	Microsoft Edge ...	849 KB	
TestConsole	2023/8/29 3:10	应用程序	263 KB	
Uninstall	2023/8/29 3:10	应用程序	13 KB	

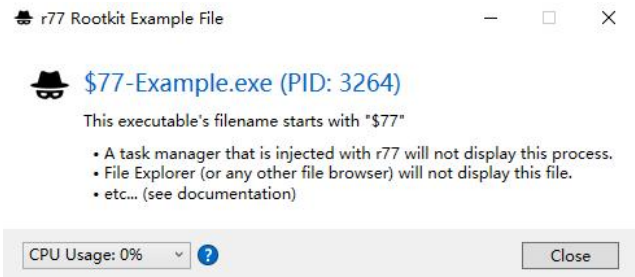
TestConsole.exe 是一个用于测试 r77 功能的工具。它可用于在不安装 rootkit 的情况下将 r77 注入或从单个进程中分离 r77。但是，某些功能只有在完全安装 rootkit 后才能使用



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. <code>TestConsole.exe</code> is a helper process. Also, <code>Install.exe</code> and <code>Uninstall.exe</code> 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. <code>Uninstall.exe</code> 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



vmware... > r77Rootkit 1.5.0					搜索"r77Rootkit 1.5.0"
名称	修改日期	类型	大小		
Examples	2023/11/19 15:25	文件夹			
\$77-Example	2023/8/29 3:10	应用程序	48 KB		
BytecodeApi.dll	2022/10/14 22:16	应用程序扩展	318 KB		
BytecodeApi.Ui.dll	2022/10/14 22:16	应用程序扩展	77 KB		
Helper32.dll	2023/8/29 3:10	应用程序扩展	9 KB		
Helper64.dll	2023/8/29 3:10	应用程序扩展	11 KB		
Install	2023/8/29 3:10	应用程序	162 KB		
Install.shellcode	2023/8/29 3:10	SHELLCODE 文件	163 KB		
LICENSE	2023/6/7 4:21	文本文件	2 KB		
r77-x64.dll	2023/8/29 3:10	应用程序扩展	143 KB		
r77-x86.dll	2023/8/29 3:10	应用程序扩展	108 KB		
Technical Documentation	2023/11/19 15:23	Microsoft Edge ...	849 KB		
TestConsole	2023/8/29 3:10	应用程序	263 KB		
Uninstall	2023/8/29 3:10	应用程序	13 KB		

名称	修改日期	类型	大小		
Examples	2023/11/19 15:25	文件夹			
BytecodeApi.dll	2022/10/14 22:16	应用程序扩展	318 KB		
BytecodeApi.Ui.dll	2022/10/14 22:16	应用程序扩展	77 KB		
Helper32.dll	2023/8/29 3:10	应用程序扩展	9 KB		
Helper64.dll	2023/8/29 3:10	应用程序扩展	11 KB		
Install	2023/8/29 3:10	应用程序	162 KB		
Install.shellcode	2023/8/29 3:10	SHELLCODE 文件	163 KB		
LICENSE	2023/6/7 4:21	文本文件	2 KB		
r77-x64.dll	2023/8/29 3:10	应用程序扩展	143 KB		
r77-x86.dll	2023/8/29 3:10	应用程序扩展	108 KB		
Technical Documentation	2023/11/19 15:23	Microsoft Edge ...	849 KB		
TestConsole	2023/8/29 3:10	应用程序	263 KB		
Uninstall	2023/8/29 3:10	应用程序	13 KB		

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

Process Name	Process ID	Protocol	State	Local Address	Local Port	Process	PID	Platform	Integrity	User	Flags	Inject	Detach	Hide by PID
svchost.exe	972	TCP	Listen	0.0.0.0	135	SecurityHealthSystray.exe	3352	64	Medium	sunlu		Injected		Hide
System	4	TCP	Listen	192.168.175.135	139	services.exe	724					Injected		Hide
svchost.exe	1116	TCP	Listen	0.0.0.0	5040	SettingUpHost.exe	5088	64	Medium	sunlu		Injected		Hide
lsass.exe	752	TCP	Listen	0.0.0.0	48664	SgmBroker.exe	5372					Injected		Hide
wininit.exe	584	TCP	Listen	0.0.0.0	48665	ShellExperienceHost.exe	7924	64	Low	sunlu		Injected		Hide
svchost.exe	476	TCP	Listen	0.0.0.0	48666	smartscreen.exe	8096	64	Medium	sunlu		Injected		Hide
svchost.exe	1900	TCP	Listen	0.0.0.0	48667	smss.exe	392					Injected		Hide
spoolsv.exe	1532	TCP	Listen	0.0.0.0	48668	spoolsv.exe	1532					Injected		Hide
services.exe	724	TCP	Listen	0.0.0.0	48669	svchost.exe	1548					Injected		Hide
svchost.exe	476	TCP	Established	192.168.175.135	48889	StartMenuExperienceHost.exe	4848	64	Low	sunlu		Injected		Hide
msedge.exe	6008	TCP	Established	192.168.175.135	48948	svchost.exe	476					Injected		Hide
svchost.exe	476	TCP	Established	192.168.175.135	50331	svchost.exe	892					Injected		Hide
SearchApp.exe	3852	TCP	Established	192.168.175.135	50439	svchost.exe	1052					Injected		Hide
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50441	svchost.exe	1080					Injected		Hide
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50442	svchost.exe	1080					Injected		Hide
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50443	svchost.exe	1116					Injected		Hide
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50444	svchost.exe	1308					Injected		Hide
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50445	svchost.exe	1516					Injected		Hide
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50447	svchost.exe	1672	64	Medium	sunlu		Injected		Hide
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50448	svchost.exe	1772					Injected		Hide
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50449							Injected		Hide

Endpoints: 93 Established: 9 Listening: 20 Time Wait: 33 Close Wait: 10 Update: 2

12.88.88 To inject or detach elevated processes, run as administrator

12.12.12 svchost.exe (PID 4552) is marked as hidden.

12.12.12 svchost.exe (PID 4551) is marked as not hidden.

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port
System	4	TCP	Listen	192.168.175.135	135	0.0.0.0	0
svchost.exe	1116	TCP	Listen	0.0.0.0	5040	0.0.0.0	0
lsass.exe	752	TCP	Listen	0.0.0.0	49664	0.0.0.0	0
wininit.exe	584	TCP	Listen	0.0.0.0	49665	0.0.0.0	0
svchost.exe	476	TCP	Listen	0.0.0.0	49666	0.0.0.0	0
svchost.exe	1060	TCP	Listen	0.0.0.0	49667	0.0.0.0	0
spoolsv.exe	1532	TCP	Listen	0.0.0.0	49668	0.0.0.0	0
services.exe	724	TCP	Listen	0.0.0.0	49669	0.0.0.0	0
svchost.exe	476	TCP	Established	192.168.175.135	49889	192.168.175.135	49890
msedge.exe	6308	TCP	Established	192.168.175.135	49948	192.168.175.135	49949
svchost.exe	476	TCP	Established	192.168.175.135	50331	192.168.175.135	50332
SearchApp.exe	3852	TCP	Established	192.168.175.135	50429	192.168.175.135	50430
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50441	192.168.175.135	50442
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50442	192.168.175.135	50443
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50443	192.168.175.135	50444
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50444	192.168.175.135	50445
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50445	192.168.175.135	50446
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50446	192.168.175.135	50447
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50447	192.168.175.135	50448
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50448	192.168.175.135	50449
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50449	192.168.175.135	50450

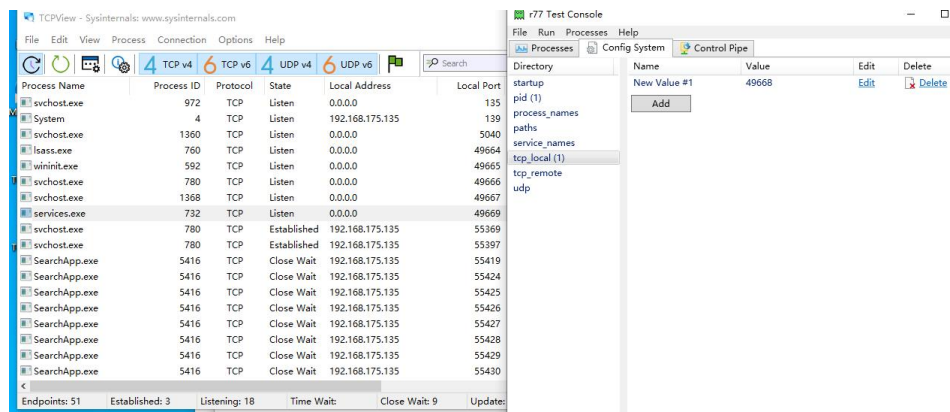
隐藏了PID=972 的进程

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port
System	4	TCP	Listen	192.168.175.135	135	0.0.0.0	0
svchost.exe	1116	TCP	Listen	0.0.0.0	5040	0.0.0.0	0
lsass.exe	752	TCP	Listen	0.0.0.0	49664	0.0.0.0	0
wininit.exe	584	TCP	Listen	0.0.0.0	49665	0.0.0.0	0
svchost.exe	476	TCP	Listen	0.0.0.0	49666	0.0.0.0	0
svchost.exe	1060	TCP	Listen	0.0.0.0	49667	0.0.0.0	0
spoolsv.exe	1532	TCP	Listen	0.0.0.0	49668	0.0.0.0	0
services.exe	724	TCP	Listen	0.0.0.0	49669	0.0.0.0	0
svchost.exe	476	TCP	Established	192.168.175.135	49889	192.168.175.135	49890
msedge.exe	6308	TCP	Established	192.168.175.135	49948	192.168.175.135	49949
svchost.exe	476	TCP	Established	192.168.175.135	50331	192.168.175.135	50332
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50439	192.168.175.135	50440
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50441	192.168.175.135	50442
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50442	192.168.175.135	50443
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50443	192.168.175.135	50444
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50444	192.168.175.135	50445
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50445	192.168.175.135	50446
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50446	192.168.175.135	50447
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50447	192.168.175.135	50448
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50448	192.168.175.135	50449
SearchApp.exe	3852	TCP	Close Wait	192.168.175.135	50449	192.168.175.135	50450

隐藏了PID=476 的进程

(3) 隐藏网络连接

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port
svchost.exe	972	TCP	Listen	0.0.0.0	135	0.0.0.0	0
System	4	TCP	Listen	192.168.175.135	139	0.0.0.0	0
svchost.exe	1360	TCP	Listen	0.0.0.0	5040	0.0.0.0	0
lsass.exe	760	TCP	Listen	0.0.0.0	49664	0.0.0.0	0
wininit.exe	592	TCP	Listen	0.0.0.0	49665	0.0.0.0	0
svchost.exe	780	TCP	Listen	0.0.0.0	49666	0.0.0.0	0
svchost.exe	1368	TCP	Listen	0.0.0.0	49667	0.0.0.0	0
spoolsv.exe	2092	TCP	Listen	0.0.0.0	49668	0.0.0.0	0
services.exe	732	TCP	Listen	0.0.0.0	49669	0.0.0.0	0
svchost.exe	780	TCP	Established	192.168.175.135	53399	20.198.162.78	443
svchost.exe	780	TCP	Established	192.168.175.135	53399	20.198.162.78	443
SearchApp.exe	5416	TCP	Close Wait	192.168.175.135	55419	111.31.22.3	443
SearchApp.exe	5416	TCP	Close Wait	192.168.175.135	55424	111.31.22.3	443
SearchApp.exe	5416	TCP	Close Wait	192.168.175.135	55425	111.31.22.3	443
SearchApp.exe	5416	TCP	Close Wait	192.168.175.135	55426	111.31.22.3	443
SearchApp.exe	5416	TCP	Close Wait	192.168.175.135	55427	111.31.22.3	443
SearchApp.exe	5416	TCP	Close Wait	192.168.175.135	55428	111.31.22.3	443
SearchApp.exe	5416	TCP	Close Wait	192.168.175.135	55429	111.31.22.3	443



(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。

