背景

CreateProcessAsUser

https://blog.csdn.net/xiaoyafang123/article/details/110087387

UAC（User Account Control）是微软在 Windows Vista 以后版本引入的一种安全机制，通过 UAC，应用程序和任务可始终在非管理员帐户的安全上下文中运行，除非管理员特别授予管理员级别的系统访问权限。UAC 可以阻止未经授权的应用程序自动进行安装，并防止无意中更改系统设置。

UAC需要授权的动作包括：配置Windows Update；增加或删除用户账户；改变用户的账户类型；改变UAC设置；安装ActiveX；安装或移除程序；安装设备驱动程序；设置家长控制；将文件移动或复制到Program Files或Windows目录；查看其他用户文件夹等。

在触发 UAC 时，系统会创建一个consent.exe进程，该进程通过白名单程序和用户选择来判断是否创建管理员权限进程。请求进程将要请求的进程cmdline和进程路径通过LPC接口传递给appinfo的RAiLuanchAdminProcess函数，该函数首先验证路径是否在白名单中，并将结果传递给consent.exe进程，该进程验证被请求的进程签名以及发起者的权限是否符合要求，然后决定是否弹出UAC框让用户进行确认。这个UAC框会创建新的安全桌面，屏蔽之前的界面。同时这个UAC框进程是SYSTEM权限进程，其他普通进程也无法和其进行通信交互。用户确认之后，会调用CreateProcessAsUser函数以管理员权限启动请求的进程。

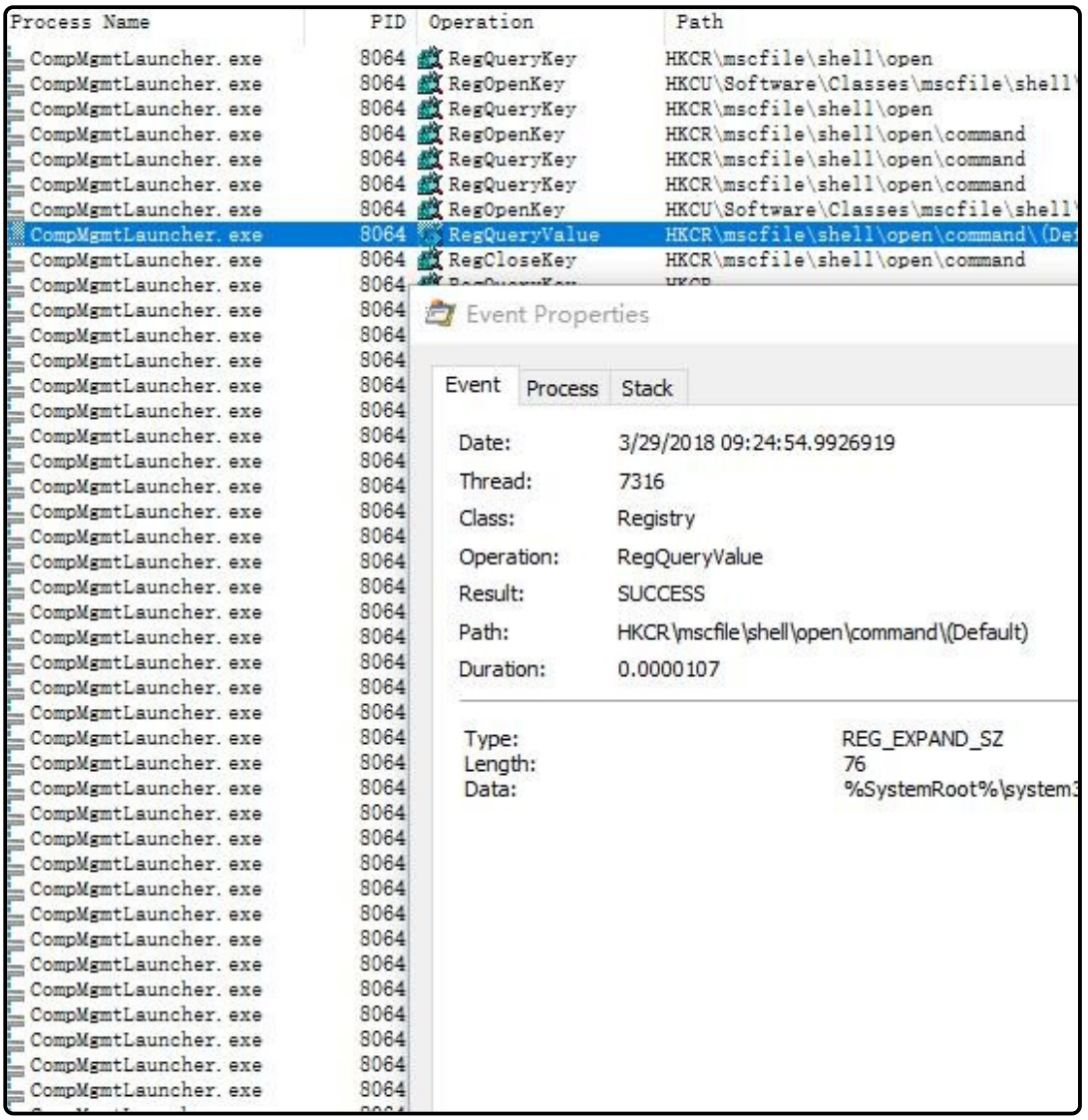
所以，病毒木马想要实现更多权限操作，那么就不得不绕过UAC弹窗，在没有通知用户情况下，静默地将程序普通权限提升为管理员权限，从而程序可以实现一些需要权限的操作。目前实现Bypass UAC的方法主要有两种方法，一种是利用白名单提权机制，另一种是利用COM组件接口技术。接下来，分别介绍这两种Bypass UAC的实现方法。

基于白名单程序Bypass UAC

有些系统程序是直接获取管理员权限，而不会触发UAC弹框，这类程序称为白名单程序。例如，slui.exe、wusa.exe、taskmgr.exe、msra.exe、eudcedit.exe、eventvwr.exe、CompMgmtLauncher.exe等等。可以通过对这些白名单程序进行DLL劫持、注入或是修改注册表执行命令的方式启动目标程序，实现Bypass UAC提权操作。

接下来，选取白名单程序CompMgmtLauncher.exe计算机管理程序进行详细分析，利用它实现Bypass UAC提权。下述的分析过程是在64位Windows 10操作系统上完成的，使用到的关键工具软件是进程监控器Procmon.exe。

实现过程
首先，直接到System32目录下运行CompMgmtLauncher.exe程序，并没有出现UAC弹窗，直接显示计算机管理的窗口界面。其中，使用进程监控器Procmon.exe来监控CompMgmtLauncher.exe进程的所有操作行为，主要是监控注册表和文件的操作。通过分析Procmon.exe的监控数据发现，CompMgmtLauncher.exe进程会先查询注册表HKCU\Software\Classes\mscfile\shell\open\command中数据，发现该路径不存在后，继续查询注册表HKCR\mscfile\shell\open\command(Default)中的数据并读取，该注册表路径中存储着mmc.exe进程的路径信息，如图6-1所示。然后，CompMgmtLauncher.exe会根据读取到的路径启动程序，显示计算机管理的窗口界面。


Process Name PID Operation Path
CompMgmtLauncher.exe 8064 RegQueryKey HKCR\mscfile\shell\open
CompMgmtLauncher.exe 8064 RegOpenKey HKCU\Software\Classes\mscfile\shell
CompMgmtLauncher.exe 8064 RegQueryKey HKCR\mscfile\shell\open
CompMgmtLauncher.exe 8064 RegOpenKey HKCR\mscfile\shell\open\command
CompMgmtLauncher.exe 8064 RegQueryKey HKCR\mscfile\shell\open\command
CompMgmtLauncher.exe 8064 RegQueryKey HKCR\mscfile\shell\open\command
CompMgmtLauncher.exe 8064 RegOpenKey HKCU\Software\Classes\mscfile\shell
CompMgmtLauncher.exe 8064 RegQueryValue HKCR\mscfile\shell\open\command\(De
CompMgmtLauncher.exe 8064 RegCloseKey HKCR\mscfile\shell\open\command
Event Properties
Event Process Stack
Date: 3/29/2018 09:24:54.9926919
Thread: 7316
Class: Registry
Operation: RegQueryValue
Result: SUCCESS
Path: HKCR\mscfile\shell\open\command\(Default)
Duration: 0.0000107
Type: REG_EXPAND_SZ
Length: 76
Data: %SystemRoot%\system