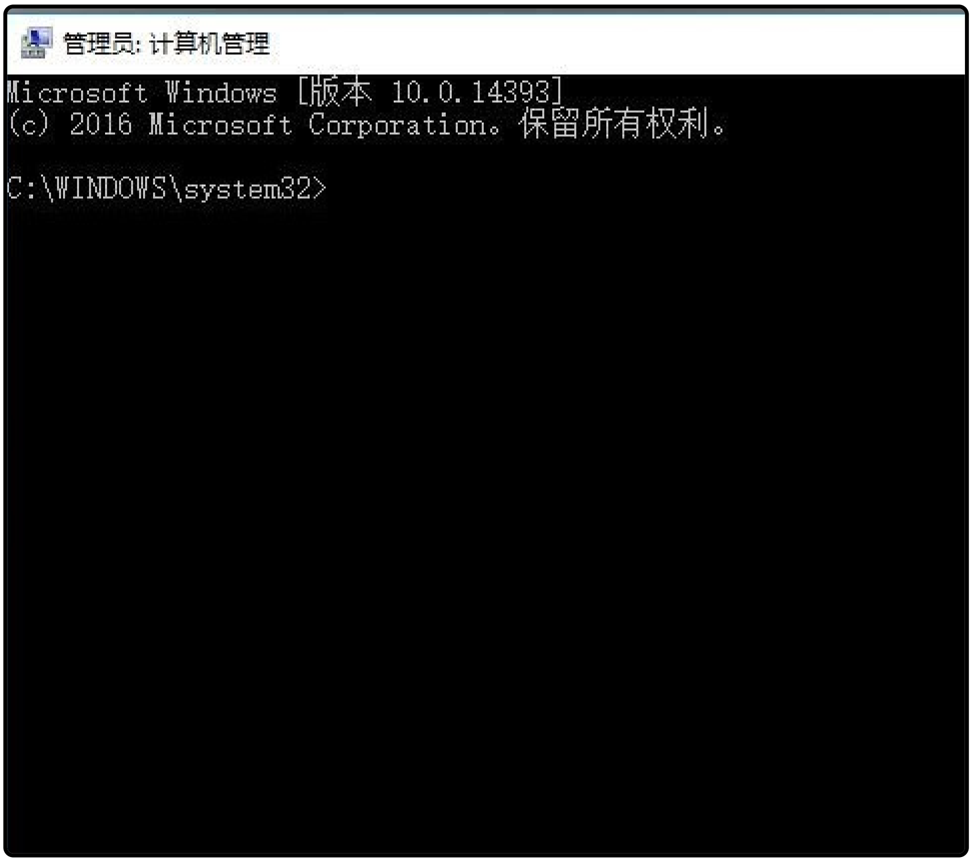
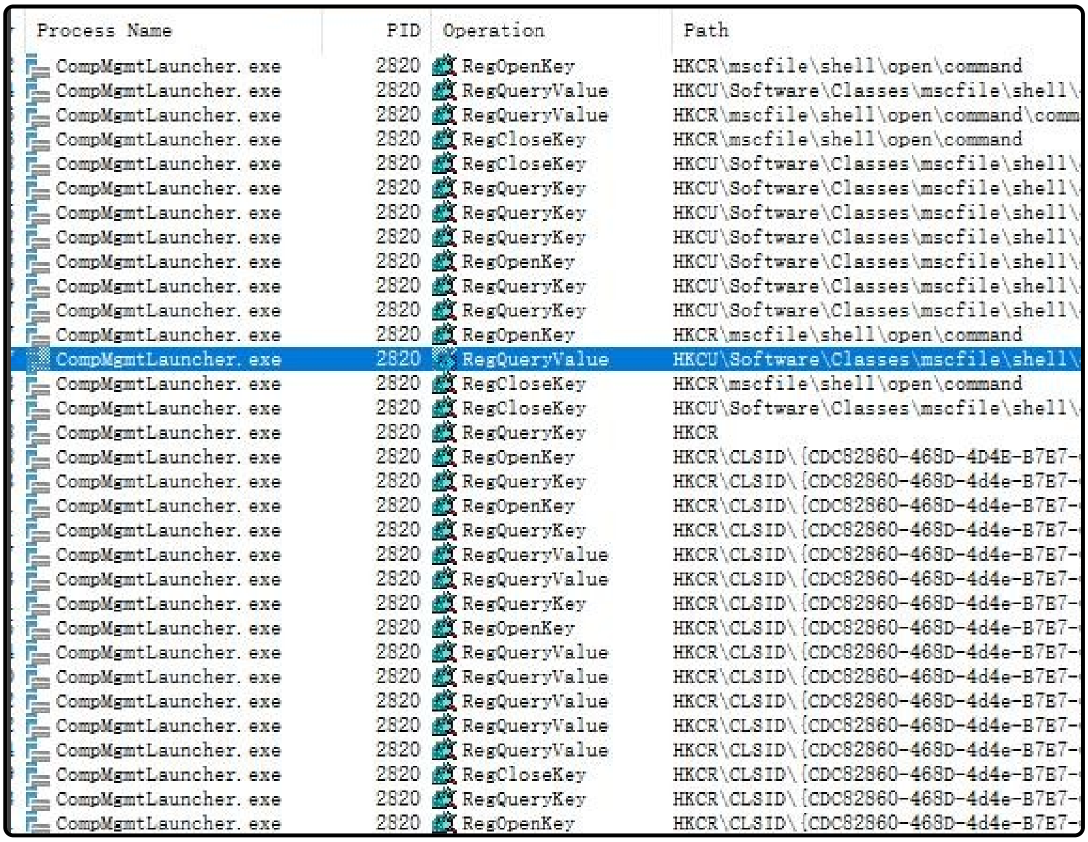
在CompMgmtLauncher.exe启动的过程中，有一个关键的操作就是它会先读取注册表HKCU\Software\Classes\mscfile\shell\open\command的数据。打开系统注册表编辑器regedit.exe，查看相应路径下的注册表，发现该注册表路径确实不存在。所以，如果自己构造该注册表路径，写入启动程序的路径，这样，CompMgmtLauncher.exe便会启动该程序。为了验证这个猜想，自己手动添加该注册表路径，并设置默认的数据为C:\Windows\System32\cmd.exe，然后使用Procmon.exe进行监控并运行CompMgmtLauncher.exe，成功弹出cmd.exe命令行窗口，而且提示管理员权



```
Microsoft Windows [版本 10.0.14393]
(c) 2016 Microsoft Corporation。保留所有权利。

C:\WINDOWS\system32>
```

查看Procmon.exe的监控数据，CompMgmtLauncher.exe确实直接读取HKCU\Software\Classes\mscfile\shell\open\command(Default)注册表路径中的数据并启动，如图6-3所示



```
Process Name               PID  Operation       Path
CompMgmtLauncher.exe       2820 RegOpenKey      HKCR\mscfile\shell\open\command
CompMgmtLauncher.exe       2820 RegQueryValue   HKCU\Software\Classes\mscfile\shell\
CompMgmtLauncher.exe       2820 RegQueryValue   HKCR\mscfile\shell\open\command\comm
CompMgmtLauncher.exe       2820 RegCloseKey     HKCR\mscfile\shell\open\command
CompMgmtLauncher.exe       2820 RegCloseKey     HKCU\Software\Classes\mscfile\shell\
CompMgmtLauncher.exe       2820 RegQueryKey     HKCU\Software\Classes\mscfile\shell\
CompMgmtLauncher.exe       2820 RegQueryKey     HKCU\Software\Classes\mscfile\shell\
CompMgmtLauncher.exe       2820 RegQueryKey     HKCU\Software\Classes\mscfile\shell\
CompMgmtLauncher.exe       2820 RegOpenKey      HKCU\Software\Classes\mscfile\shell\
CompMgmtLauncher.exe       2820 RegQueryKey     HKCU\Software\Classes\mscfile\shell\
CompMgmtLauncher.exe       2820 RegQueryKey     HKCU\Software\Classes\mscfile\shell\
CompMgmtLauncher.exe       2820 RegOpenKey      HKCR\mscfile\shell\open\command
CompMgmtLauncher.exe       2820 RegQueryValue   HKCU\Software\Classes\mscfile\shell\
CompMgmtLauncher.exe       2820 RegCloseKey     HKCR\mscfile\shell\open\command
CompMgmtLauncher.exe       2820 RegCloseKey     HKCU\Software\Classes\mscfile\shell\
CompMgmtLauncher.exe       2820 RegQueryKey     HKCR
CompMgmtLauncher.exe       2820 RegOpenKey      HKCR\CLSID\{CDC82860-468D-4D4E-B7E7-
CompMgmtLauncher.exe       2820 RegQueryKey     HKCR\CLSID\{CDC82860-468D-4d4e-B7E7-
CompMgmtLauncher.exe       2820 RegOpenKey      HKCR\CLSID\{CDC82860-468D-4d4e-B7E7-
CompMgmtLauncher.exe       2820 RegQueryKey     HKCR\CLSID\{CDC82860-468D-4d4e-B7E7-
CompMgmtLauncher.exe       2820 RegQueryValue   HKCR\CLSID\{CDC82860-468D-4d4e-B7E7-
CompMgmtLauncher.exe       2820 RegQueryValue   HKCR\CLSID\{CDC82860-468D-4d4e-B7E7-
CompMgmtLauncher.exe       2820 RegQueryKey     HKCR\CLSID\{CDC82860-468D-4d4e-B7E7-
CompMgmtLauncher.exe       2820 RegOpenKey      HKCR\CLSID\{CDC82860-468D-4d4e-B7E7-
CompMgmtLauncher.exe       2820 RegQueryValue   HKCR\CLSID\{CDC82860-468D-4d4e-B7E7-
CompMgmtLauncher.exe       2820 RegQueryValue   HKCR\CLSID\{CDC82860-468D-4d4e-B7E7-
CompMgmtLauncher.exe       2820 RegQueryValue   HKCR\CLSID\{CDC82860-468D-4d4e-B7E7-
CompMgmtLauncher.exe       2820 RegQueryValue   HKCR\CLSID\{CDC82860-468D-4d4e-B7E7-
CompMgmtLauncher.exe       2820 RegCloseKey     HKCR\CLSID\{CDC82860-468D-4d4e-B7E7-
CompMgmtLauncher.exe       2820 RegQueryKey     HKCR\CLSID\{CDC82860-468D-4d4e-B7E7-
CompMgmtLauncher.exe       2820 RegOpenKey      HKCR\CLSID\{CDC82860-468D-4d4e-B7E7-
```

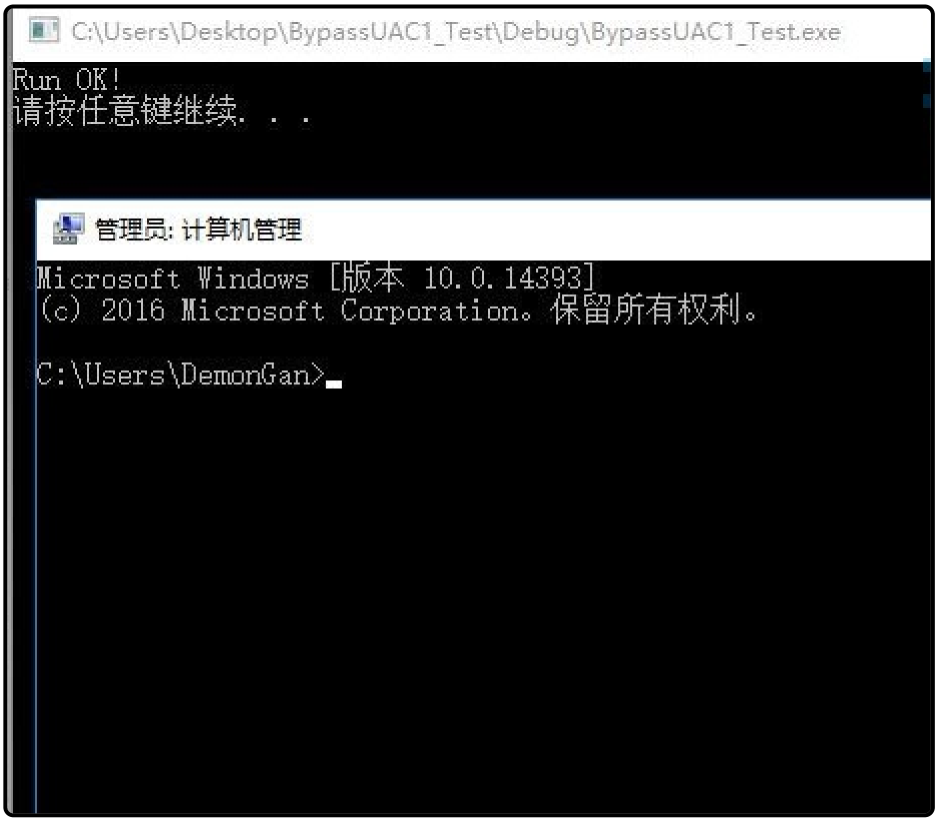
// 修改注册表

```
BOOL SetReg(char *lpszExePath)
```

```
{
HKEY hKey = NULL;
// 创建项
::RegCreateKeyEx(HKEY_CURRENT_USER, "Software\\Classes\\mscfile\\Shell\\Open\\Command",
0, NULL, 0, KEY_WOW64_64KEY | KEY_ALL_ACCESS, NULL, &hKey, NULL);
if (NULL == hKey)
{
ShowError("RegCreateKeyEx");
return FALSE;
}
// 设置键值
::RegSetValueEx(hKey, NULL, 0, REG_SZ, (BYTE *)lpszExePath, (1 +
::lstrlen(lpszExePath)));
// 关闭注册表
::RegCloseKey(hKey);
return TRUE;
}
```

测试

直接运行上述程序，向注册表HKCU\Software\Classes\mscfile\shell\open\command(Default)中写入cmd.exe的路径，启动cmd.exe进程。cmd.exe成功启动，窗口标题显示管理员字样，如图6-4所示。



```
Run OK!
请按任意键继续. . .
```

```
Microsoft Windows [版本 10.0.14393]
(c) 2016 Microsoft Corporation。保留所有权利。

C:\Users\DemonGan>_
```