**通过卸载程序触发恶意进程**

参考文章：

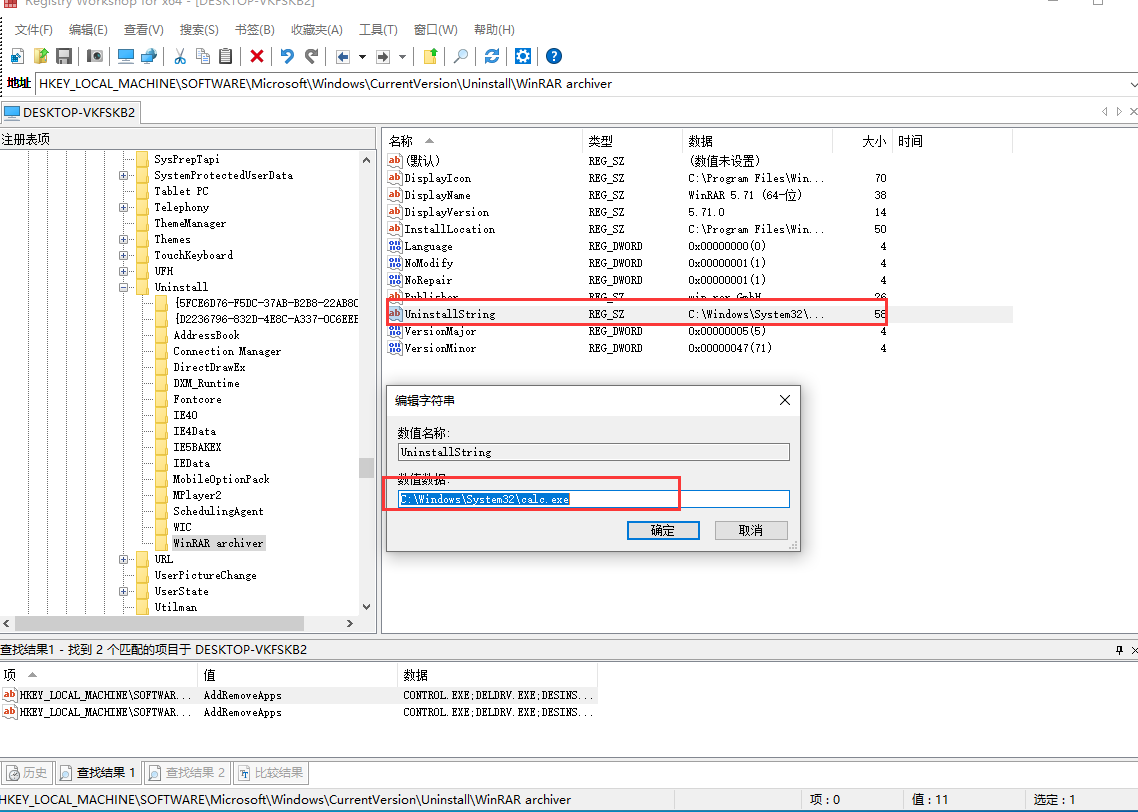
<http://www.hexacorn.com/blog/2019/02/02/beyond-good-ol-run-key-part-101/>

通过修改以下两个路径的程序卸载进程来执行恶意进程

*HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\<program name>=<string>*

*HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\*QuietUninstallString*\<program name>=<string>*

*这里拿Win RAR做例子*



修改UninstallString路径下指定的程序路径为：

C:\Windows\System32\calc.exe

运行卸载程序时便会弹出calc

