PowerShell para el análisis del registro

# Análisis de Registro w/ Pwsh

### \*\*Navegando y preguntando al registro\*\*

Antes de sumergirnos en la parte de investigación de PowerShell, me gustaría mostrarles dos maneras de abrir el Editor del Registro en Windows 10:

- Encuentre el cuadro de búsqueda en la barra de tareas, escriba regedit y luego seleccione Editor del Registro (aplicación de escritorio) de los resultados.

![](https://i.imgur.com/OrOXuwj.png)

![](https://i.imgur.com/vVQyLEI.png)

- \*\*Inicio\*\* de \*\*derecha\*\* (ícono de ventanas), luego \*\*seleccione\*\* Ejecute. Escriba regedit en la caja Abrir: y luego seleccione Aceptar.

![](https://i.imgur.com/cY3jnad.png)

![](https://i.imgur.com/qCUOjfa.png)

Por último, vamos a consultar el registro de Windows con Get-ItemProperty. El siguiente comando ayudará a enumerar los valores del registro en una clave específica:

```plaintext

Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"

```

![](https://i.imgur.com/l7LNIJd.png)

La clave de registro HKLM:-SOFTWARE-Microsoft-Windows-CurrentVersion-Run contiene entradas para programas que se configuran para ejecutarse automáticamente cuando un usuario inicia sesión. Cada entrada dentro de esta clave normalmente especifica la ruta a un archivo ejecutable que se lanzará. Ahora, vamos a entrar en lo bueno. La siguiente porción tendrá lugar de la última lección Análisis diferencial con la máquina de Windows infectada.

### \*\*Claves de inicio de registro\*\*

Como se mencionó anteriormente, los atacantes tratarán de utilizar métodos de persistencia como crear un valor de registro en Windows `Run`o o `RunOnce`las claves del registro. Estas claves de registro se conocen como [Puntos de Extensibilidad Autostart (ASEP),](https://www.notion.so/f2bdd702b3fb440ea591fcafd11cbc38?pvs=21) utilizados para iniciar un proceso automáticamente cuando el sistema arranca o un usuario inicia sesión. Windows incluye soporte para múltiples claves de registro ASEP, pero cuatro comunes incluyen:

- `HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`

- `HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce`

- `HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run`

- `HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce`

El `Run`las claves especifican los programas que se ejecutan cada vez que Windows comienza, mientras que el `RunOnce`Las claves especifican los programas que se ejecutan una sola vez en la próxima startup.

Usamos el comando PowerShell Get-ChildItem para enumerar la unidad de PowerShell HKCU:

```plaintext

Get-ChildItem HKCU:

```

![](https://i.imgur.com/hzlb0bp.png)

\_La imagen ha sido redactada para mayor claridad\_

En esta salida, verá la columna Nombre, que serán las claves del registro, y la columna Propiedad, que será los valores de registro en las claves de nivel superior para la colmena HKEY-CURRENT-USER AKA HKCU.

### \*\*Investigando el Registro w/ PowerShell\*\*

Corramos los siguientes comandos a continuación, respectivamente:

```plaintext

Get-ItemProperty "HKLM:\Software\Microsoft\Windows\CurrentVersion\Run"

```

```plaintext

Get-ItemProperty "HKLM:\Software\Microsoft\Windows\CurrentVersion\RunOnce"

```

```plaintext

Get-ItemProperty "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run"

```

```plaintext

Get-ItemProperty "HKCU:\Software\Microsoft\Windows\CurrentVersion\RunOnce"

```

![](https://i.imgur.com/prBnR96.png)

![](https://i.imgur.com/KjX13Zt.png)

En esta salida, vemos que no hay valores de registro en ninguna de las claves de RunOnce, pero hay valores tanto en las teclas HKLM como HKCU Run. Para la tecla HKLM Run, vemos un programa (SecurityHealth), seguido de valores de propiedad específicos de la clave interrogada.

Para el comando HKCU Run, vemos una entrada para \*\*Calcache\*\* (el malware introducido en la sección anterior). Conociendo su naturaleza maliciosa, el siguiente paso sería eliminarlo.

\*\*Dato divertido:\*\* tenemos otro laboratorio en nuestra Sección Capstone titulado \_"Using PowerShell for Windows Examination"\_ que también cubre el mismo malware.Si usted tiene curiosidad acerca de su naturaleza.

De su sesión de PowerShell, retire el valor Calcache de la tecla Run usando `Remove-ItemProperty`, como se muestra aquí:

```plaintext

Remove-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run" -Name "Calcache"

```

```plaintext

Get-ItemProperty "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run\Calcache"

```

![](https://i.imgur.com/qtuHrKv.png)

Niza, el valor ASEP fue eliminado. Lo confirmamos comprobando la propiedad con Get-ItemProperty (que devuelve un error, porque el valor ya no existe). A continuación, retire el programa \_calcache.exe\_ de la máquina utilizando el comando Remove-Item.