Descodificación de un comando de PowerShell desde un proceso en ejecución

Ejecutar un script en PowerShell (que se ejecute durante un tiempo para poder ser detectado listando procesos)

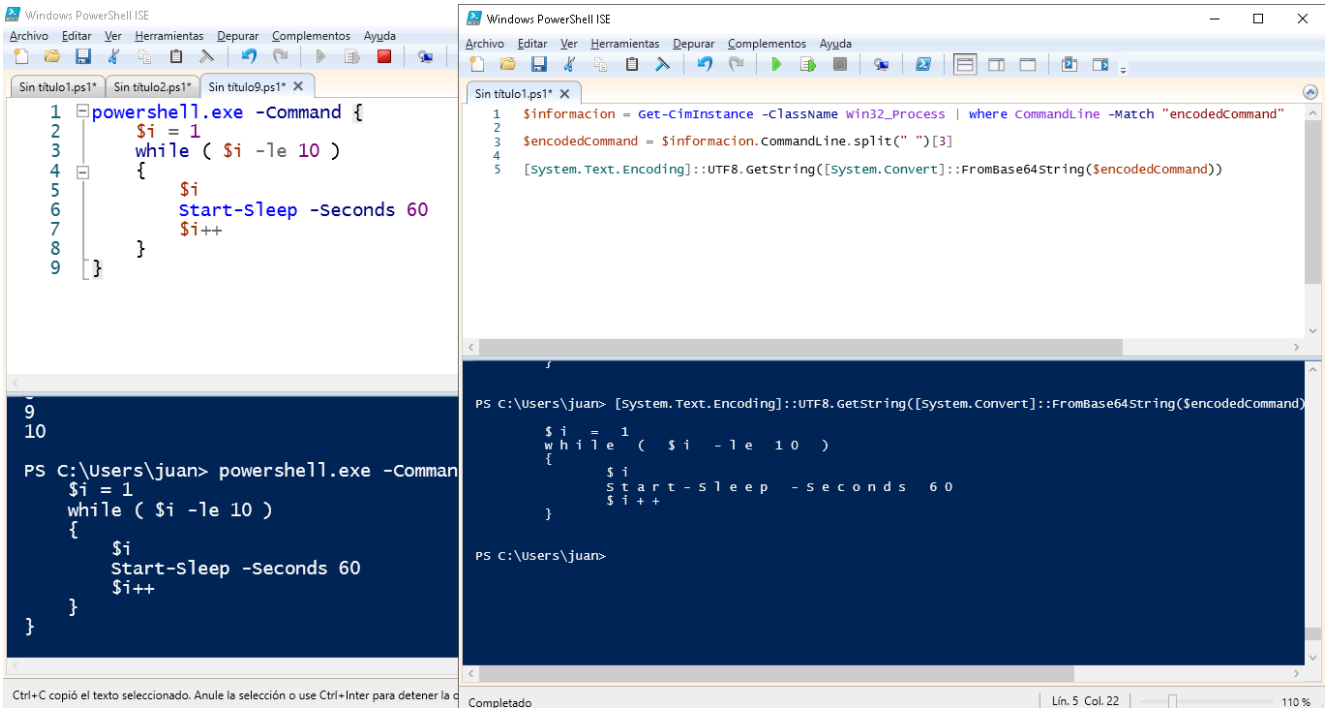
[crayon-6a9d570a5d0bf658429551/]

Analizar los procesos y detectar el proceso que tenga la palabra «encodedCommand» en su propiedad «CommandLine»

[crayon-6a9d570a5d0c7031972949/]

Convertir a base64 (descodificar) el valor «encodedCommand» que se encuentra en la tercera posición

[crayon-6a9d570a5d0c9789153657/]


Windows PowerShell ISE
Archivo Editar Ver Herramientas Depurar Complementos Ayuda
Sin título1.ps1* Sin título2.ps1* Sin título9.ps1*
1 powershell.exe -Command {
2 $i = 1
3 while ($i -le 10)
4 {
5 $i
6 Start-Sleep -Seconds 60
7 $i++
8 }
9 }
9
10
PS C:\Users\juan> powershell.exe -Comman
$i = 1
while ($i -le 10)
{
$i
Start-Sleep -Seconds 60
$i++
}
}
Ctrl+C copió el texto seleccionado. Anule la selección o use Ctrl+Inter para detener la c
Windows PowerShell ISE
Archivo Editar Ver Herramientas Depurar Complementos Ayuda
Sin título1.ps1*
1 $informacion = Get-CimInstance -ClassName Win32_Process | where CommandLine -Match "encodedCommand"
2
3 $encodedCommand = $informacion.CommandLine.split(" ")[3]
4
5 [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($encodedCommand))
}
PS C:\Users\juan> [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($encodedCommand)
$i = 1
while ($i -le 10)
{
$i
Start-Sleep -Seconds 60
$i++
}
PS C:\Users\juan>
Completado
Lín. 5 Col. 22
110 %