Fun with processes - Suspend and Resume

cyberstoph.org/posts/2021/05/fun-with-processes-suspend-and-resume

May 3, 2021

Did you ever wonder how process suspension in Windows works? Nevermind, I'm writing this anyway.

Since you're reading this blog you're either totatlly lost or into Windows anyway. So I assume you alread tried suspending and resuming a process with process explorer for example. There are actually different ways to suspend a process and we'll go with the one that's officially undocumented (more fun).

NTSuspendProcess

The API we're using is called **NTSuspendProcess** and lives inside NTDLL. It is not documented officially as mentioned above, however it is already well known for years and you find a lot of information about it on the internet. It looks like this:

```
[DllImport("ntdll.dll", PreserveSig = false)]
public static extern void NtSuspendProcess(IntPtr processHandle);
```

Quite simple, the only thing we need is a process handle with the appropriate (= ALL) permissions. And you might already guessed it, resuming the process works the same way.

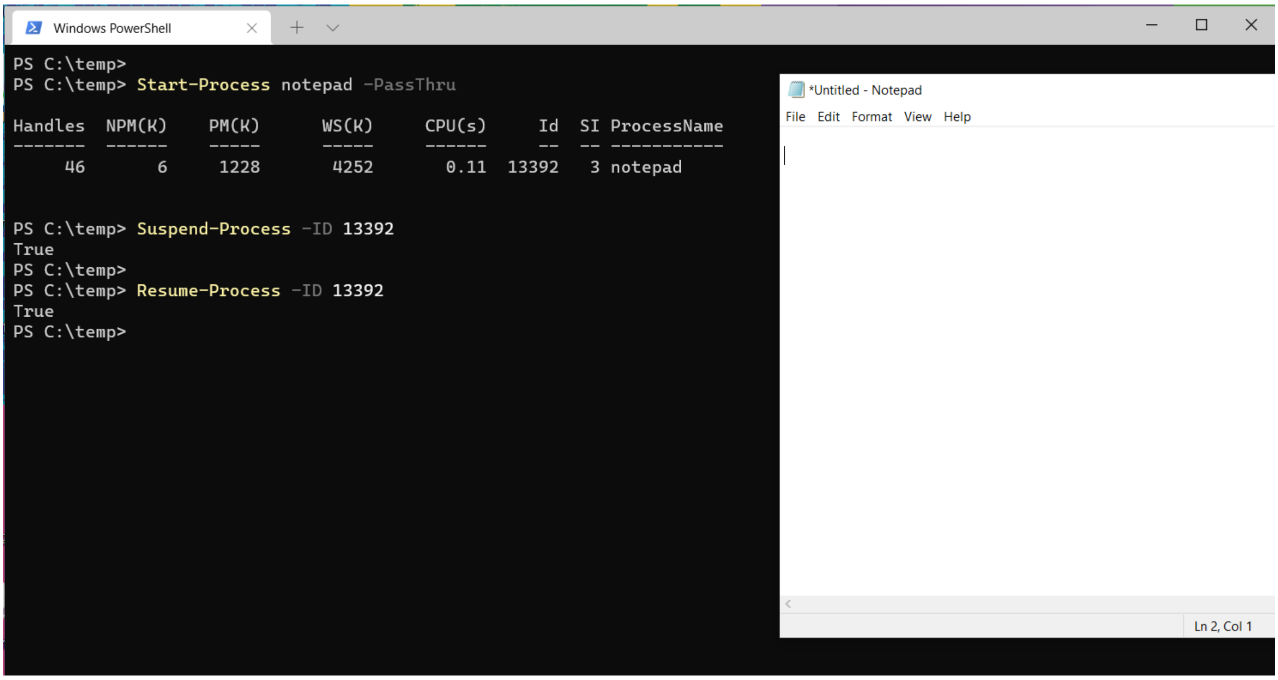
```
[DllImport("ntdll.dll", PreserveSig = false, SetLastError = true)]
public static extern void NtResumeProcess(IntPtr processHandle);
```

To make things work, we also need **OpenProcess** and **CloseHandle** from kernel32 to acquire and release the process handle.

```
[DllImport("kernel32.dll", SetLastError = true)]
public static extern IntPtr OpenProcess(ProcessAccessFlags processAccess,bool
bInheritHandle,int processId);
[DllImport("kernel32.dll", SetLastError=true)]
public static extern bool CloseHandle(IntPtr hObject)
```

And that's it. Nothing fancy here today ;-)

If you're interested, here's a Powershell function to play with.



```
PS C:\temp>
PS C:\temp> Start-Process notepad -PassThru

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
     46       6     1228       4252       0.11  13392   3 notepad


PS C:\temp> Suspend-Process -ID 13392
True
PS C:\temp>
PS C:\temp> Resume-Process -ID 13392
True
PS C:\temp>
```