Quickpost: SelectMyParent or Playing With the Windows Process Tree

Published: 2009-11-22 · Archived: 2026-04-05 15:25:18 UTC

Quickpost: SelectMyParent or Playing With the Windows Process Tree

I read something very interesting in "Windows via C/C++" today: starting with Windows Vista, CreateProcess can start a program where you specify the parent process! This is something forensic investigators must be aware of when they analyse processes running on a Windows machine.

Normally the parent process of a new process is the process that created the new process (via CreateProcess). But when using STARTUPINFOEX with the right LPPROC_THREAD_ATTRIBUTE_LIST to create a process, you can arbitrarely specify the parent process, provided you have the rights (i.e. it's your process or you have debug rights).

I developed a small tool to start a program while specifying its parent process: SelectMyParent. Here I use it to start notepad as a child of lsass.exe:

```
C:\>SelectMyParent notepad 864
SelectMyParent v0.0.0.1: start a program with a selected parent process
Source code put in public domain by Didier Stevens, no Copyright
https://DidierStevens.com
Use at your own risk

Process created: 5156

C:\>
```

lsass.exe	864	Local Security Authority Proc...	Microsoft Corporation	NT AUTHORITY\SYSTEM
notepad.exe	5156	Notepad	Microsoft Corporation	NT AUTHORITY\SYSTEM
lsm.exe	872	Local Session Manager Serv...	Microsoft Corporation	NT AUTHORITY\SYSTEM
csrss.exe	816	Client Server Runtime Process	Microsoft Corporation	NT AUTHORITY\SYSTEM
winlogon.exe	920	Windows Logon Application	Microsoft Corporation	NT AUTHORITY\SYSTEM

2 remarks about this example:

1. to make lsass.exe a parent process, you need to use SelectMyParent with admin rights and elevate its rights (Run as administrator)
2. the notepad process takes over the parent process' account: NT AUTHORITY\SYSTEM

I don't know how one can detect that a process' parent is not the process that created it, because a process has no access to its extended startup info (only to its startup info). And it is the extended startup info that contains the attribute list with the handle to the parent process.

SelectMyParent version 0.0.0.1 is available here.

Quickpost info
