به نام خدا

نحوه­ی عملکرد درایور و چگونگی لاگ گیری از برنامه ها

درایور ProcessHooking.sys اقدام به رهگیری 42 تابع، لیست شده در فایل xlsx موجود در همین دایرکتوری، می­کند. به منظور استفاده از این درایور یک برنامه کنسول با نام UseDriver.exe در سطح کاربر ایجاد شده است که اطلاعات مربوط به پروسه ای که باید تحت نظر قرار گیرد را به داخل درایور ارسال می کند. در ضمن خود این درایور اقدام به بارگذاری و راه­اندازی این درایور در کرنل سیستم­عامل می­کند. برای این منظور بایستی فایل ProcessHooking.sys را در مسیر ریشه درایو C قرار دهید.

به عنوان مثال برای رهگیری برنامه­ی notepad.exe بایستی مراحل زیر را انجام دهید:

1. مطمئن باشید که فایل ProcessHooing.sys در ریشه درایو C قرار گرفته است.
2. برنامه cmd را در سطح امتیاز مدیر (گزینه­ی Run as administrator) اجرا کنید و به داخل پوشه­ای که شامل فایل UseDriver.exe است تغییر مسیر دهید. سپس دستور زیر را اجرا کنید.

>"UseDriver.exe" "C:\Windows\system32\notepad.exe"

1. برنامه UseDriver پارامتر ارسالی را بررسی می­کند تا ببیند که آیا چنین فایلی وجود دارد یا خیر. در صورتی که همه چیز درست پیش برود اقدام به اجرای پردازه­ی مربوطه در حالت Suspend می­کند و از شما درخواست فشردی دکمه Enter را می­کند تا عملیات رهگیری از همان ابتدای اجرای یک برنامه انجام شود. عملیات رهگیری تا زمانی ادامه می­یابد که شما مجددا کلید Enter را بفشارید.
2. فایل نهایی گزارش ایجاد شده از رهگیری در مسیر ریشه درایو C با همان نام پردازه ایجاد می­شود. مثلا در این جا فایل notepad.txt در درایو C با فرمت Unicode ایجاد می­شود.