به نام خدا

نحوه‌ی عملکرد درایور و چگونگی لاگ گیری از برنامه ها

درایور ProcessHooking.sys اقدام به رهگیری ۴۲ 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:

۱. مطمئن باشید که فایل ProcessHooing.sys در ریشه درایو C قرار گرفته است.
۲. 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"
```

۳. 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.
۴. 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.