cmd watcher

السلام عليكم بالمقاله هذي بتكلم عن برنامج cmd watcher

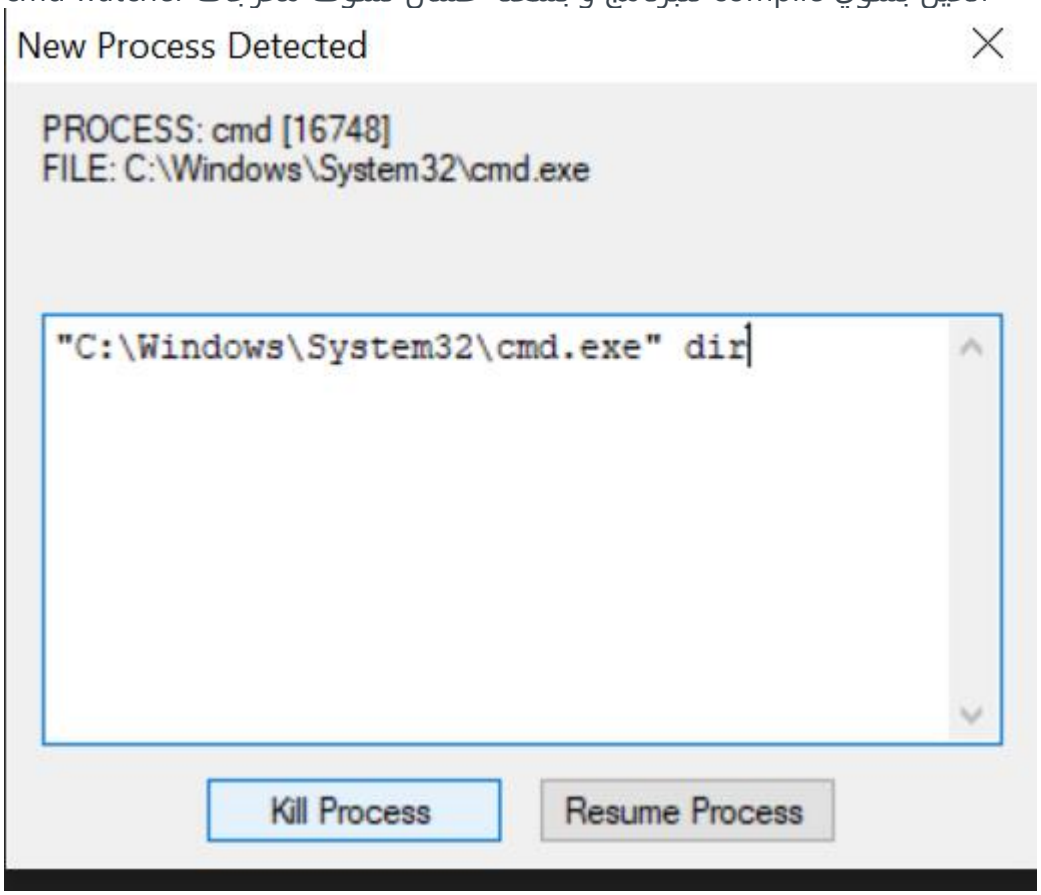
البرنامج هذا وظيتفه كالتالي اذا جا البرنامج ينفذ اوامر عن طريق cmd.exe راح يبين لك انه يكتب وبكذا تقدر تعرف الاوامر اللي يسويها الmalware في حاله انه شغل cmd.exe

simple demo

هنا عندي برنامج بسيط ب C# وظيفته بنفذ dir فقط

```
namespace HelloWorld
{
    class Hello
    {
        static void Main(string[] args)
        {
            System.Console.WriteLine("Hello World!");
            System.Diagnostics.Process.Start("CMD.exe", "dir");
        }
    }
}
```

الحين بسوي compile للبرنامج و بشغله عشان نشوف مخرجات cmd watcher



عطاني ان فيه بروسيس ل cmd.exe اشتغلت و تنفذ امر dir و بالطريقه هذي تقدر تعرف وش يسوي البرنامج بشكل ابسط من procmon