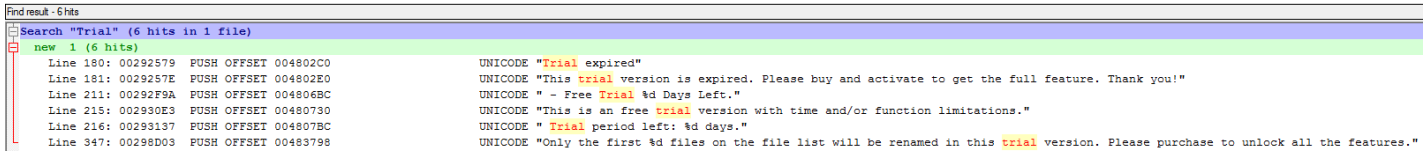
BatchRename Pro v4.51

By Jhonjhon_123

Web	http://www.foryoursoft.com/
Protección	Serial Online
Compiler	C++
Packer	Ninguno
Objetivo	Activarlo

1. Buscando pistas

Bueno, como es común, lo más rápido es buscar entre los *Strings* las palabras clave, **"Trial"** en este caso, esto nos arroja:



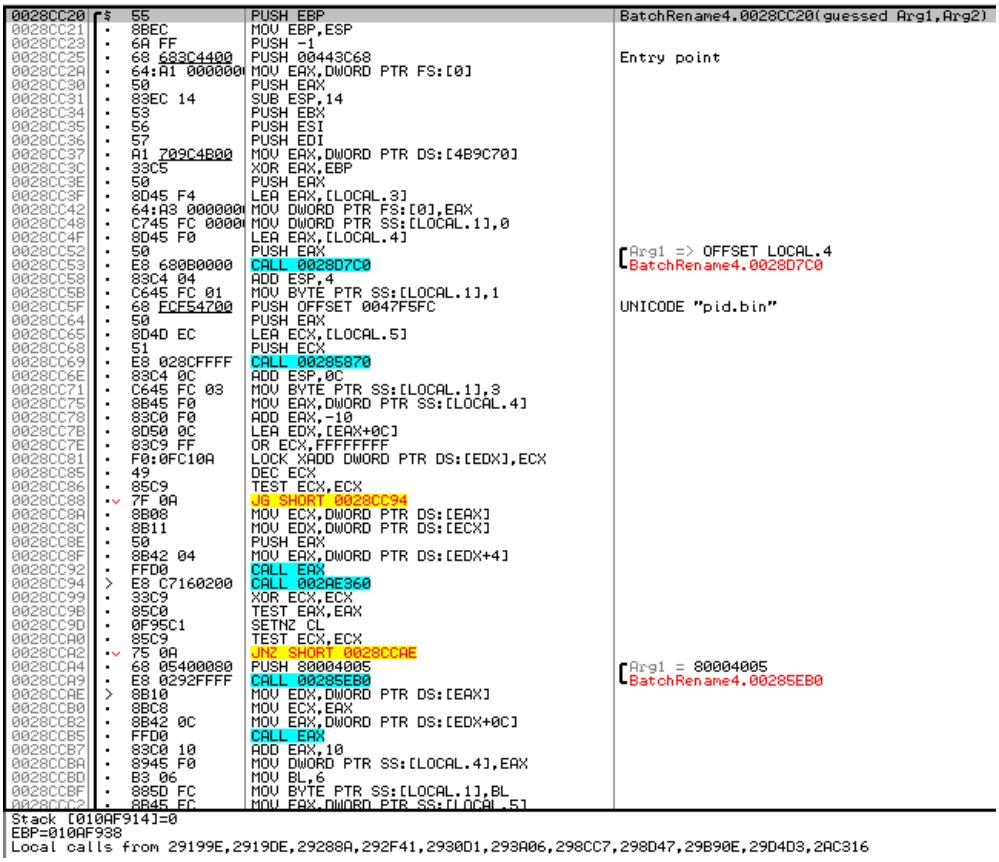
Notemos:

> " Trial period left: %d days."

Aquel *String* aparece en el título de la ventana principal, sería un bueno iniciar por hay para ver que mecanismos de validación aplica para *agregar o no* el *String*

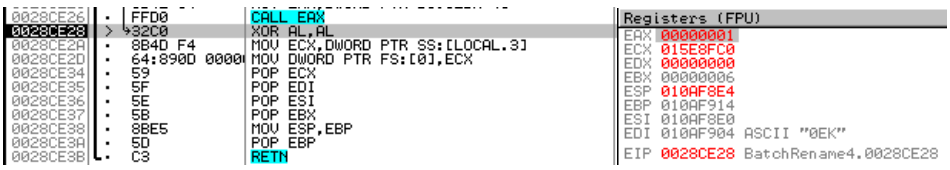
Como vemos en la imagen, en `00293137` esta nuestro *String* y un poco más arriba en la línea seleccionada, notamos un gran salto de código, será esto algo **importante?**

Vamos al primer *Call* antes de dicho salto:



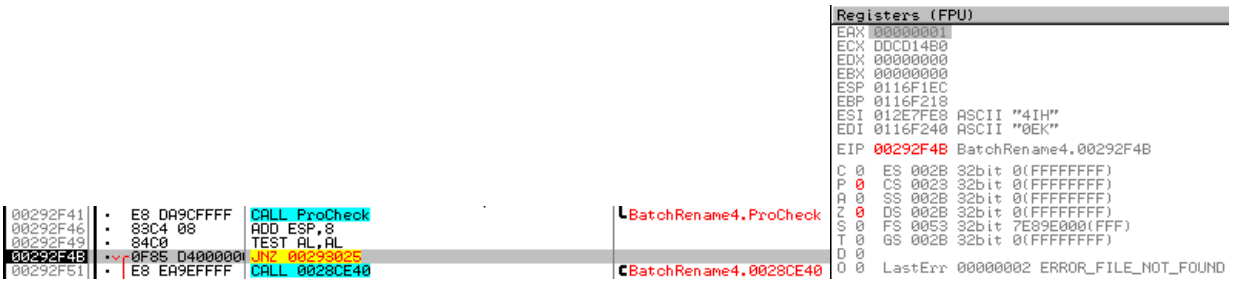
Podemos notar un archivo **"pid.bin"**, algo raro no creen?, a juzgar por las llamadas a dicha función, yo creo que estamos en el **Santo Grial** que le dice al programa si está o no **activado!**

Bueno, pongamos un *BP* en el inicio de tal función y veamos su recorrido:



Mmmm..., como era de esperarse salta al camino del **NO**, pero notemos `EAX` en `1` y ese lindo `XOR AL, AL` antes de salirse de la función. Vamos otra vez a mirar la línea de aquel **gran salto**:

Un `TEST Al, AL` gobierna el salto. Recordemos que `TEST AL, AL` pondrá los *Flags* P y Z en `0` si el resultado es distinto de `0`, ahora modifiquemos `AL` en `1` y ejecutemos:



Boala!

Solo nos resta modificar dicha funcion para que siempre nos devuelva `AL` en `1`:

```
0028CE26  .  FFD0           CALL EAX
0028CE28  >  90             NOP
0028CE29  .  90             NOP
0028CE2A  .  8B4D F4        MOV ECX,DWORD PTR SS:[LOCAL.3]
0028CE2D  .  64:890D 0000(  MOV DWORD PTR FS:[0],ECX
0028CE34  .  59             POP ECX
0028CE35  .  5F             POP EDI
0028CE36  .  5E             POP ESI
0028CE37  .  5B             POP EBX
0028CE38  .  8BE5           MOV ESP,EBP
0028CE3A  .  5D             POP EBP
0028CE3B  L. C3             RETN
```

Listo!