

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:

```
Find result - 6 hits
Search "Trial" (6 hits in 1 file)
new 1 (6 hits)
Line 180: 00292579 PUSH OFFSET 004802C0 UNICODE "Trial expired"
Line 181: 0029257E PUSH OFFSET 004802E0 UNICODE "This trial version is expired. Please buy and activate to get the full feature. Thank you!"
Line 211: 00292F9A PUSH OFFSET 004806BC UNICODE " - Free Trial %d Days Left."
Line 215: 002930E3 PUSH OFFSET 00480730 UNICODE "This is an free trial version with time and/or function limitations."
Line 216: 00293137 PUSH OFFSET 004807BC UNICODE " Trial period left: %d days."
Line 347: 00298D03 PUSH OFFSET 00483798 UNICODE "Only the first %d files on the file list will be renamed in this trial version. Please purchase to unlock all the features."
```

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*

002930AB 002930AE 002930AF 002930B0 002930B2 002930B5 002930BA 002930C1 002930C6 002930CD 002930D1 002930D6 002930D9 002930DB 002930E1 002930E3 002930E8 002930EA 002930EF 002930F4 002930F6 002930F8 002930FD 002930FF 00293101 00293103 00293108 0029310A 0029310C 0029310F 00293111 00293113 00293118 0029311D 0029311F 00293121 00293124 00293126 00293129 0029312C 00293133 00293134 00293137 0029313C 0029313D 00293142 00293145 00293148 0029314B 0029314C 0029314D 0029314F 00293154 00293156 0029315B 0029315D 00293162 00293164	897D FC 57 51 8BCC 8965 E4 68 5CE54700 C745 EC 0100 E8 2A26FFFF C745 FC 0200 C645 FC 00 E8 4A9BFFFF 83C4 08 84C0 0F85 10010000 6A 44 68 30074800 8BCE E8 9119FFFF E8 4C90FFFF 3BC7 7C 0B BF 1E000000 2BF8 79 02 33FF E8 58B20100 33C9 85C0 0F95C1 85C9 75 0A 68 05400000 E8 932DFFFF 8B10 8BC8 8B42 0C FFD0 8945 F0 C745 FC 0400 57 8D4D F0 68 BC074800 51 0029313D 8B7D F0 8B47 F4 83C4 0C 50 57 8BCE E8 2C19FFFF 6A 46 68 F8074800 8BCE E8 1E19FFFF 6A 24 68 86084800	MOV DWORD PTR SS:[LOCAL.1],EDI PUSH EDI PUSH ECX MOV ECX,ESP MOV DWORD PTR SS:[LOCAL.7],ESP PUSH OFFSET 0047F55C MOV DWORD PTR SS:[LOCAL.5],1 CALL 002856F0 MOV DWORD PTR SS:[LOCAL.1],2 MOV BYTE PTR SS:[LOCAL.1],0 CALL 0028CC20 ADD ESP,8 TEST AL,AL JNZ 002931F1 PUSH 44 PUSH OFFSET 00480730 MOV ECX,ESI CALL 00284A80 CALL 0028CE40 CMP EAX,EDI JL SHORT 00293103 MOV EDI,IE SUB EDI,EAX JMS SHORT 00293103 XOR EDI,EDI CALL 0028E360 XOR ECX,ECX TEST EAX,EAX SETNZ CL TEST ECX,ECX JNZ SHORT 0029311D PUSH 80004005 CALL 00285EB0 MOV EDX,DWORD PTR DS:[EAX] MOV ECX,EAX MOV EAX,DWORD PTR DS:[EDX+0C] CALL EAX ADD EAX,10 MOV DWORD PTR SS:[LOCAL.4],EAX MOV DWORD PTR SS:[LOCAL.1],4 PUSH EDI LEA ECX,[LOCAL.4] PUSH OFFSET 004807BC PUSH ECX CALL 002852F0 MOV EDI,DWORD PTR SS:[LOCAL.4] MOV EAX,DWORD PTR DS:[EDI-0C] ADD ESP,0C PUSH EAX PUSH EDI MOV ECX,ESI CALL 00284A80 PUSH 46 PUSH OFFSET 004807F8 MOV ECX,ESI CALL 00284A80 PUSH 24 PUSH 24 PUSH OFFSET 00480888	Arg2 Arg1 Arg1 = UNICODE "BRP" BatchRename4.002856F0 BatchRename4.0028CC20 Arg2 = 44 Arg1 = UNICODE "This is an free trial version with time and/or function limitations." BatchRename4.00284A80 BatchRename4.0028CE40 Arg1 = 80004005 BatchRename4.00285EB0 <%d> Format = " Trial period left: %d days." Arg1 => OFFSET LOCAL.4 BatchRename4.002852F0 Arg2 Arg1 => [LOCAL.4] BatchRename4.00284A80 Arg2 = 46 Arg1 = UNICODE "Please activate this product to unlock all the features including:" BatchRename4.00284A80 Arg2 = 24 Arg1 = UNICODE "No time or function limitations."
--	---	---	---

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:

0028CC20	55	PUSH EBP	BatchRename4.0028CC20(guessed Arg1,Arg2)
0028CC21	8BEC	MOV EBP,ESP	
0028CC23	6A FF	PUSH -1	
0028CC25	68 683C4400	PUSH 00443C68	Entry point
0028CC2A	64:A1 00000000	MOV EAX,DWORD PTR FS:[0]	
0028CC30	59	PUSH EAX	
0028CC31	53EC 14	SUB ESP,14	
0028CC34	53	PUSH EBX	
0028CC35	56	PUSH ESI	
0028CC36	57	PUSH EDI	
0028CC37	A1 709C4B00	MOV EAX,DWORD PTR DS:[4B9C70]	
0028CC3C	33C5	XOR EAX,EBP	
0028CC3E	58	PUSH EAX	
0028CC3F	8D45 F4	LEA EAX,[LOCAL.3]	
0028CC42	64:A3 00000000	MOV DWORD PTR FS:[0],EAX	
0028CC48	C745 FC 0000	MOV DWORD PTR SS:[LOCAL.1],0	
0028CC4F	8D45 F0	LEA EAX,[LOCAL.4]	
0028CC52	50	PUSH EAX	[Arg1 => OFFSET LOCAL.4 BatchRename4.0028D7C0]
0028CC53	E8 680B0000	CALL 0028D7C0	
0028CC58	83C4 04	ADD ESP,4	
0028CC5B	C45 F0 01	MOV BYTE PTR SS:[LOCAL.1],1	
0028CC5F	68 FCF54700	PUSH OFFSET 0047F5FC	UNICODE "pid.bin"
0028CC64	50	PUSH EAX	
0028CC65	8D4D EC	LEA ECX,[LOCAL.5]	
0028CC68	51	PUSH ECX	
0028CC69	E8 020CFFFF	CALL 00285870	
0028CC6E	83C4 0C	ADD ESP,0C	
0028CC71	C645 FC 03	MOV BYTE PTR SS:[LOCAL.1],3	
0028CC75	8B45 F0	MOV EAX,DWORD PTR SS:[LOCAL.4]	
0028CC78	83C0 F0	ADD EAX,-10	
0028CC7B	8D50 0C	LEA EDX,[EAX+0C]	
0028CC7E	83C9 FF	OR ECX,FFFFFFFF	
0028CC81	F0:0FC10A	LOCK XADD DWORD PTR DS:[EDX],ECX	
0028CC85	49	DEC ECX	
0028CC86	85C9	TEST ECX,ECX	
0028CC88	7F 0A	JS SHORT 0028CC94	
0028CC8A	8B08	MOV ECX,DWORD PTR DS:[EAX]	
0028CC8C	8B11	MOV EDX,DWORD PTR DS:[ECX]	
0028CC8E	50	PUSH EAX	
0028CC8F	8B42 04	MOV EAX,DWORD PTR DS:[EDX+4]	
0028CC92	FFD0	CALL EAX	
0028CC94	E8 C7160200	CALL 0028E360	
0028CC99	83C9	XOR ECX,ECX	
0028CC9B	85C0	TEST EAX,EAX	
0028CC9D	0F95C1	SETNZ CL	
0028CCA0	85C9	TEST ECX,ECX	
0028CCA2	75 0A	JNZ SHORT 0028CCAE	
0028CCA4	68 05400000	PUSH 80004005	[Arg1 = 80004005 BatchRename4.00285EB0]
0028CCA9	E8 0292FFFF	CALL 00285EB0	
0028CCAE	8B10	MOV EDX,DWORD PTR DS:[EAX]	
0028CCB0	8B45 F0	MOV ECX,DWORD PTR DS:[LOCAL.4]	
0028CCB2	8B42 0C	MOV EAX,DWORD PTR DS:[EDX+0C]	
0028CCB5	FFD0	CALL EAX	
0028CCB7	83C0 10	ADD EAX,10	
0028CCBA	8945 F0	MOV DWORD PTR SS:[LOCAL.4],EAX	
0028CCBD	B3 06	MOV BL,6	
0028CCBF	8B5D FC	MOV BYTE PTR SS:[LOCAL.1],BL	
0028CCD2	8B45 FC	MOV EAX,DWORD PTR SS:[LOCAL.5]	
Stack [010AF914]=0			
EBP=010AF938			
Local calls from 29199E,2919DE,29288A,292F41,2930D1,293A06,298CC7,298D47,29B90E,29D4D3,2AC316			

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:

0028CE26	FFD0	CALL EAX	Registers (FPU)
0028CE28	32C0	XOR AL,AL	EAX 00000001
0028CE2A	8B4D F4	MOV ECX,DWORD PTR SS:[LOCAL.3]	ECX 015E8FC0
0028CE2D	64:890D 0000	MOV DWORD PTR FS:[0],ECX	EDX 00000000
0028CE34	59	POP ECX	EBX 00000006
0028CE35	5F	POP EDI	ESP 010AF8E4
0028CE36	5E	POP ESI	EBP 010AF8E4
0028CE37	5B	POP EBX	ESI 010AF8E0
0028CE38	8BE5	MOV ESP,EBP	EDI 010AF904 ASCII "0EK"
0028CE3A	5D	POP EBP	EIP 0028CE28 BatchRename4.0028CE28
0028CE3B	C3	RETN	

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**:

002930D1	E8 4A9BFFFF	CALL ProCheck	BatchRename4.ProCheck
002930D6	83C4 08	ADD ESP,8	
002930D9	84C0	TEST AL,AL	
002930DB	75 0A	JNZ 002930E1	

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:

00292F41	E8 DA9CFFFF	CALL ProCheck	BatchRename4.ProCheck
00292F46	83C4 08	ADD ESP,8	
00292F49	84C0	TEST AL,AL	
00292F4B	75 0A	JNZ 002930E1	
00292F51	E8 EA9EFFFF	CALL 0028CE40	BatchRename4.0028CE40

Registers (FPU)	
EAX	00000001
ECX	DDCD14B0
EDX	00000000
EBX	00000000
ESP	0116F1EC
EBP	0116F218
ESI	012E7FE8 ASCII "4IH"
EDI	0116F240 ASCII "0EK"
EIP	00292F4B BatchRename4.00292F4B
C 0	ES 002B 32bit 0(FFFFFFFF)
P 0	CS 002B 32bit 0(FFFFFFFF)
A 0	SS 002B 32bit 0(FFFFFFFF)
Z 0	DS 002B 32bit 0(FFFFFFFF)
S 0	FS 0053 32bit 7E89E000(FFF)
T 0	GS 002B 32bit 0(FFFFFFFF)
D 0	
O 0	LastErr 00000002 ERROR_FILE_NOT_FOUND

Boala!

Solo nos resta modificar dicha función para que siempre nos devuelva **AL** en 1:

0028CE26	FFD0	CALL EBX
0028CE28	90	NOP
0028CE29	90	NOP
0028CE2A	8B4D F4	MOV ECX,DWORD PTR SS:[LOCAL.3]
0028CE2D	64:8900 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	C3	RET

Listo!

