MDE_ : Macrorit Disk Partition Expert Server

by Apuromafo

Encontré curioso el programa ^^

CLS
19/08/2013

Hola, no tengo mucho tiempo pero Hoy vamos a revisar un programa “de pago” que da soporte en varias versiones, atacaré solo la que me llamó la atención (server) este escrito es con fines educacionales, un saludo gigante a la lista de CLS

Historia:

Conversaba con +erisoft el me comentó que viera este programa,le he dicho que no practico el cracking hace bastante, pero el confia en mis conocimientos y me ha instado en escribir otro tute así que aquí el resultado

Así que manos a la obra ,espero les guste ^^

Descarga

Primero la descarga solo existe en versión Free y las demás son “demo”

License Expiry Date	For Free, Forever!	30 days	Lifetime	30 days	Lifetime	Lifetime	Lifetime & Free lifetime upgrade service
License	Free for Use (Home User)	USD $ 9.99	USD $ 29.99	USD $ 39.99	USD $ 99.99	USD $ 359.99	USD $ 499.99
Tech-support	By Email	By Email	By Email	By Email	By Email	By Email	By Email
Download/Purchase	Download Now	BUY NOW	BUY NOW	BUY NOW	BUY NOW	BUY NOW	BUY NOW

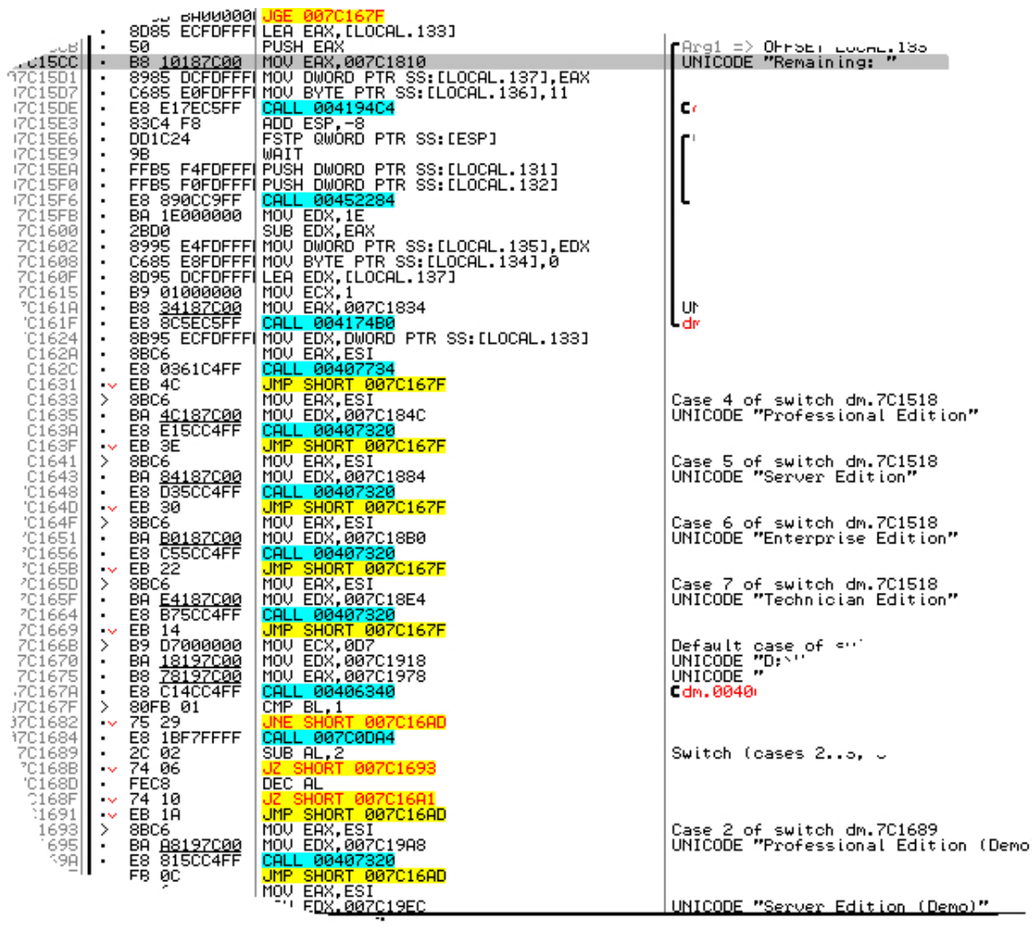
Pero de igual forma bajaré la opción de Server edition

mde_setup_ser_DEMO.zip
http://www.macrorit.com/download/mde/mde_setup_ser_DEMO.zip

Luego de instalar, vemos algunas cosas importantes ya que se esta versión :

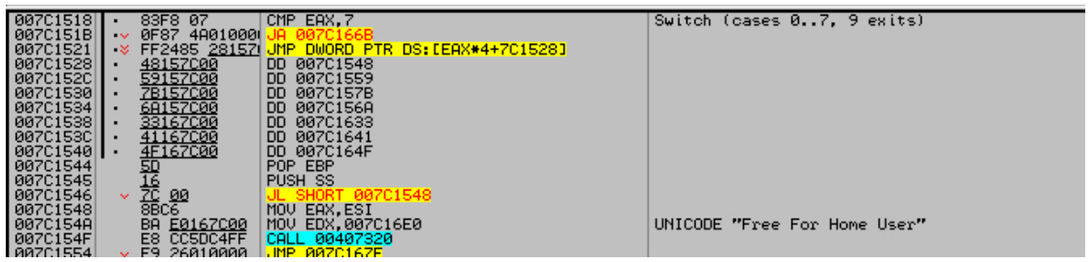
```
007C1528  |.  48157C00    DD 007C1548
007C152C  |.  59157C00    DD 007C1559
007C1530  |.  7B157C00    DD 007C157B
007C1534  |.  6A157C00    DD 007C156A
007C1538  |.  33167C00    DD 007C1633
007C153C  |.  41167C00    DD 007C1641
007C1540  |.  4F167C00    DD 007C164F
007C1544     5D           POP EBP
007C1545     16           PUSH SS
007C1546  .  7C 00        JL SHORT 007C1548
007C1548     8BC6         MOV EAX,ESI
007C154A     BA E0167C00  MOV EDX,007C16E0                UNICODE "Free For Home User"
007C154F     E8 CC5DC4FF  CALL 00407320
007C1554  .  E9 26010000  JMP 007C167F
007C1559     8BC6         MOV EAX,ESI
007C155B  .  BA 14177C00  MOV EDX,007C1714                UNICODE "Trial Edition"
007C1560  .  E8 BB5DC4FF  CALL 00407320
007C1565  .  E9 15010000  JMP 007C167F
007C156A  >  8BC6         MOV EAX,ESI                     Case 3 of switch dm.7C1518
007C156C  .  BA 3C177C00  MOV EDX,007C173C                UNICODE "Expired (30-days)"
007C1571  .  E8 AA5DC4FF  CALL 00407320
007C1576  .  E9 04010000  JMP 007C167F
007C157B  >  8BC6         MOV EAX,ESI                     Case 2 of switch dm.7C1518
007C157D  .  BA 6C177C00  MOV EDX,007C176C                UNICODE "Registered (30-days)"
007C1582  .  E8 995DC4FF  CALL 00407320
007C1587  .  8D95 F0FDFFFF LEA EDX,[LOCAL.132]
007C158D  .  B8 A4177C00  MOV EAX,007C17A4                UNICODE "SOFTWARE\Microsoft\Windows\CurrentVersion\MDE_"
007C1592  .  E8 AD6EFFFF  CALL 007B8444                   dm.007B8444
007C1597  .  84C0         TEST AL,AL
007C1599  .  0F84 E000000( JZ 007C167F
007C159F  .  E8 207FC5FF  CALL 004194C4                   dm.004194C4
007C15A4  .  83C4 F8      ADD ESP,-8
007C15A7  .  DD1C24       FSTP QWORD PTR SS:[ESP]         Arg3_4
007C15AA  .  9B           WAIT
007C15AB  .  FFB5 F4FDFFFF PUSH DWORD PTR SS:[LOCAL.131]  Arg2 => [LOCAL.131]
007C15B1  .  FFB5 F0FDFFFF PUSH DWORD PTR SS:[LOCAL.132]  Arg1 => [LOCAL.132]
007C15B7  .  E8 C80CC9FF  CALL 00452284                   dm.00452284
007C15BC  .  83F8 1E      CMP EAX,1E
007C15BF  .  0F8D BA00000( JGE 007C167F
007C15C5  .  8D85 FCFDFFFF LEA EAX,[LOCAL.133]
```

Bajando encuentro más (posiblemente parece un lugar estratégico



Ya me refiere los “remaining” osea el tiempo restante y puedo ver todas las versiones

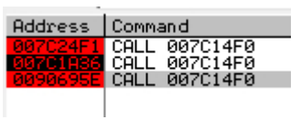
Entro y veo esto (es el switch case 0 y ahora pasa por free for home user)



Pero luego en la segunda llamada va a versión de server edition (más abajo)

Ahora veo cuantas llamadas tenemos a estos tipos de licencia

Asi que solo tenemos 3 llamadas



Address	Command
007C24F1	CALL 007C14F0
007C1A86	CALL 007C14F0
0090695E	CALL 007C14F0

Luego de ello comenzaremos una a una “claramente arriba dice splash frm” por ende este es la versión del comienzo

```
0090691A   .  09            DB 09
0090691B   .  73 70 6C 61   ASCII "splashFrm"                    ASCII "splashFrm"
00906924      00            DB 00
00906925      00            DB 00
00906926      00            DB 00
00906927      00            DB 00
00906928      02            DB 02
00906929      00            DB 00
0090692A      8BC0          MOV EAX,EAX
0090692C  r$  55            PUSH EBP                            dm.0090692C(guessed void)
0090692D  .   8BEC          MOV EBP,ESP
0090692F  .   6A 00         PUSH 0
00906931  .   33C0          XOR EAX,EAX
00906933  .   55            PUSH EBP
00906934  .   68 A3699000   PUSH 009069A3
00906939  .   64:FF30       PUSH DWORD PTR FS:[EAX]
0090693C  .   64:8920       MOV DWORD PTR FS:[EAX],ESP          Installs SE handler 9069A3
0090693F  .   33C9          XOR ECX,ECX
00906941  .   B2 01         MOV DL,1
00906943  .   A1 DC649000   MOV EAX,DWORD PTR DS:[9064DC]
00906948  .   E8 1F2FC0FF   CALL 0050986C
0090694D  .   A3 4CC99300   MOV DWORD PTR DS:[93C94C],EAX
00906952  .   8D55 FC       LEA EDX,[LOCAL.1]
00906955  .   A1 70539300   MOV EAX,DWORD PTR DS:[935370]
0090695A  .   0FB640 28     MOVZX EAX,BYTE PTR DS:[EAX+28]      para splash
0090695E  .   E8 8DABEBFF   CALL 007C14F0
00906963  .   8B55 FC       MOV EDX,DWORD PTR SS:[LOCAL.1]
00906966  .   A1 4CC99300   MOV EAX,DWORD PTR DS:[93C94C]
```

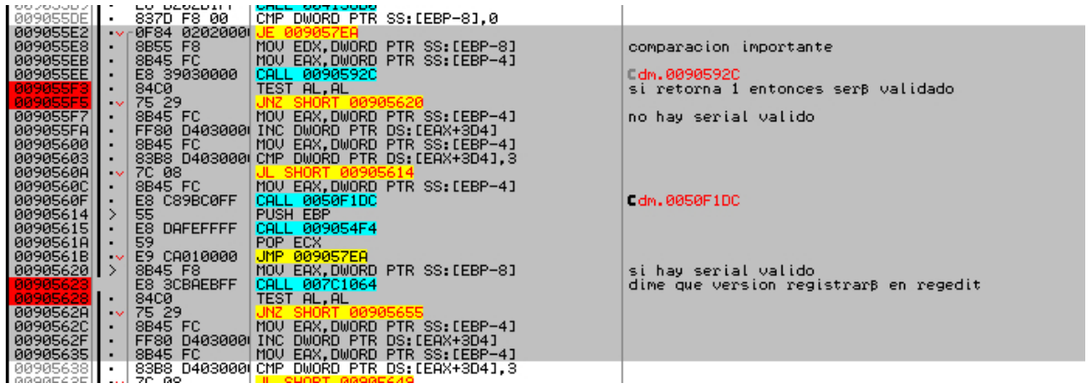
Tipo de licencia

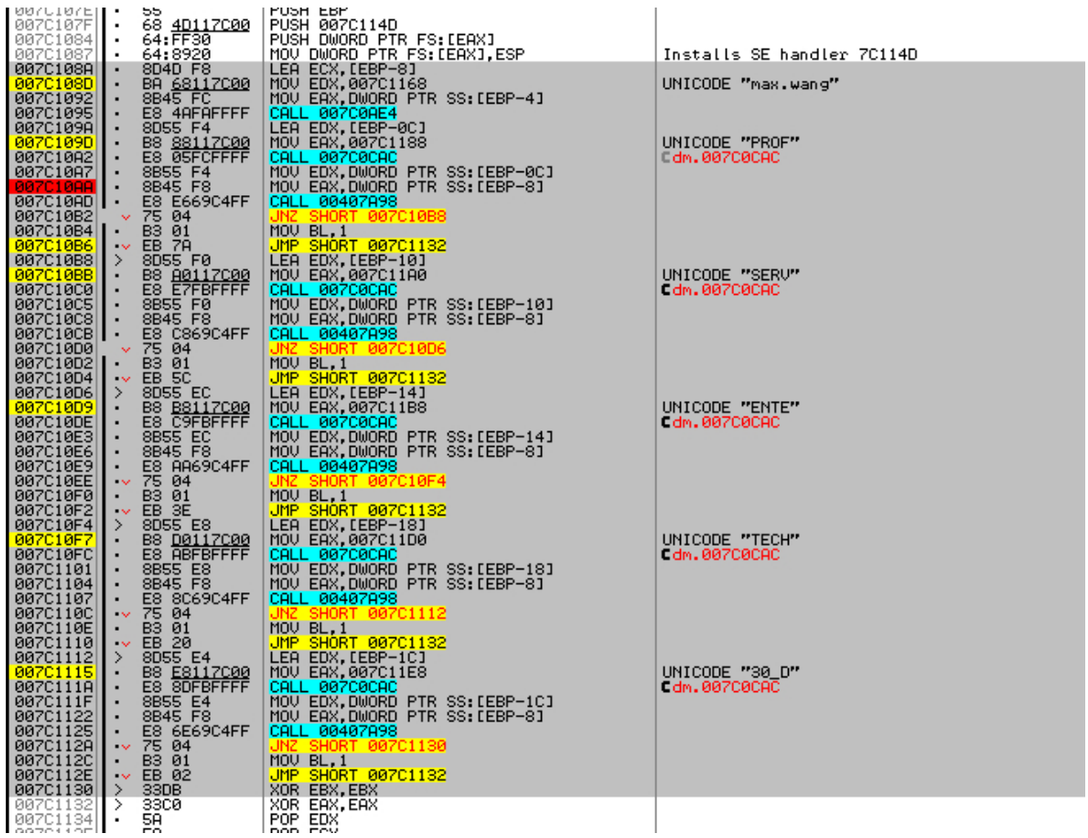
```
007C19EB      00            DB 00
007C19EC  .   5300 6500 72  UNICODE "Server E"                  UNICODE "Server Edition (Demo)"
007C19FC  .   6400 6900 74  UNICODE "dition ("
007C1A0C  .   4400 6500 6D  UNICODE "Demo)",0
007C1A18  r$  55            PUSH EBP                            dm.007C1A18(guessed void)
007C1A19  .   8BEC          MOV EBP,ESP
007C1A1B  .   6A 00         PUSH 0
007C1A1D  .   53            PUSH EBX
007C1A1E  .   56            PUSH ESI
007C1A1F  .   8BF2          MOV ESI,EDX
007C1A21  .   8BD8          MOV EBX,EAX
007C1A23  .   33C0          XOR EAX,EAX
007C1A25  .   55            PUSH EBP
007C1A26  .   68 601A7C00   PUSH 007C1A60
007C1A2B  .   64:FF30       PUSH DWORD PTR FS:[EAX]
007C1A2E  .   64:8920       MOV DWORD PTR FS:[EAX],ESP          Installs SE handler 7C1A60
007C1A31  .   8D55 FC       LEA EDX,[LOCAL.1]
007C1A34  .   8BC3          MOV EAX,EBX
007C1A36  .   E8 B5FAFFFF   CALL 007C14F0
007C1A3B  .   8B4D FC       MOV ECX,DWORD PTR SS:[LOCAL.1]
007C1A3E  .   8BC6          MOV EAX,ESI
007C1A40  .   BA 781A7C00   MOV EDX,007C1A78                   UNICODE "License type: "
007C1A45  .   E8 AA5DC4FF   CALL 004077F4
007C1A4A  .   33C0          XOR EAX,EAX
007C1A4C  .   5A            POP EDX
007C1A4D  .   59            POP ECX
007C1A4E  .   59            POP ECX
007C1A4F  .   64:8910       MOV DWORD PTR FS:[EAX],EDX
007C1A52  .   68 671A7C00   PUSH 007C1A67                       Entry point
007C1A57  >   8D45 FC       LEA EAX,[EBP-4]
007C1A5A  .   E8 B158C4FF   CALL 00407310
007C1A5F  L.v C3            RETN                                Jump to 7C1A67
007C1A60  $^  E9 CB40C4FF   JMP 00405B30                        SE handling routine
007C1A65  .^  EB F0         JMP SHORT 007C1A57
007C1A67  r>  5E            POP ESI
007C1A68  .   5B            POP EBX
```

Y el titulo

```
007C24B7      90            NOP
007C24B8  r$  55            PUSH EBP
007C24B9  .   8BEC          MOV EBP,ESP
007C24BB  .   6A 00         PUSH 0
007C24BD  .   6A 00         PUSH 0
007C24BF  .   53            PUSH EBX
007C24C0  .   8BD8          MOV EBX,EAX
007C24C2  .   33C0          XOR EAX,EAX
007C24C4  .   55            PUSH EBP
007C24C5  .   68 20257C00   PUSH 007C2520
007C24CA  .   64:FF30       PUSH DWORD PTR FS:[EAX]
007C24CD  .   64:8920       MOV DWORD PTR FS:[EAX],ESP          Installs SE handler 7C2520
007C24D0  .   8D55 FC       LEA EDX,[EBP-4]
007C24D3  .   A1 144A9300   MOV EAX,DWORD PTR DS:[934A14]
007C24D8  .   E8 CF86C4FF   CALL 0040ABAC
007C24DD  .   FF75 FC       PUSH DWORD PTR SS:[EBP-4]
007C24E0  .   68 38257C00   PUSH 007C2538                       UNICODE " - "
007C24E5  .   8D55 F8       LEA EDX,[EBP-8]
007C24E8  .   A1 70539300   MOV EAX,DWORD PTR DS:[935370]
007C24ED  .   0FB640 28     MOVZX EAX,BYTE PTR DS:[EAX+28]
007C24F1  .   E8 FAEFFFFF   CALL 007C14F0
007C24F6  .   FF75 F8       PUSH DWORD PTR SS:[EBP-8]
007C24F9  .   8BC3          MOV EAX,EBX
007C24FB  .   BA 03000000   MOV EDX,3
007C2500  .   E8 D353C4FF   CALL 004078D8
007C2505  .   33C0          XOR EAX,EAX
007C2507  .   5A            POP EDX
007C2508  .   59            POP ECX
007C2509  .   59            POP ECX
007C250A  .   64:8910       MOV DWORD PTR FS:[EAX],EDX
007C250D  .   68 27257C00   PUSH 007C2527                       Entry point
```

Veamos si podemos ver algo del serial:





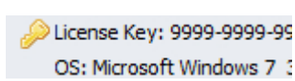
Si logro que cualquiera mov bl,1 sea verdadero entonces logro un licence key para guardar con un interesante texto

---------- Macrorit Disk Partition Expert 2013 ----------

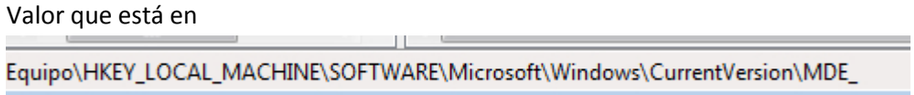
Your activation has been successful, Thank you for choosing Macrorit.

---------- Aceptar ----------

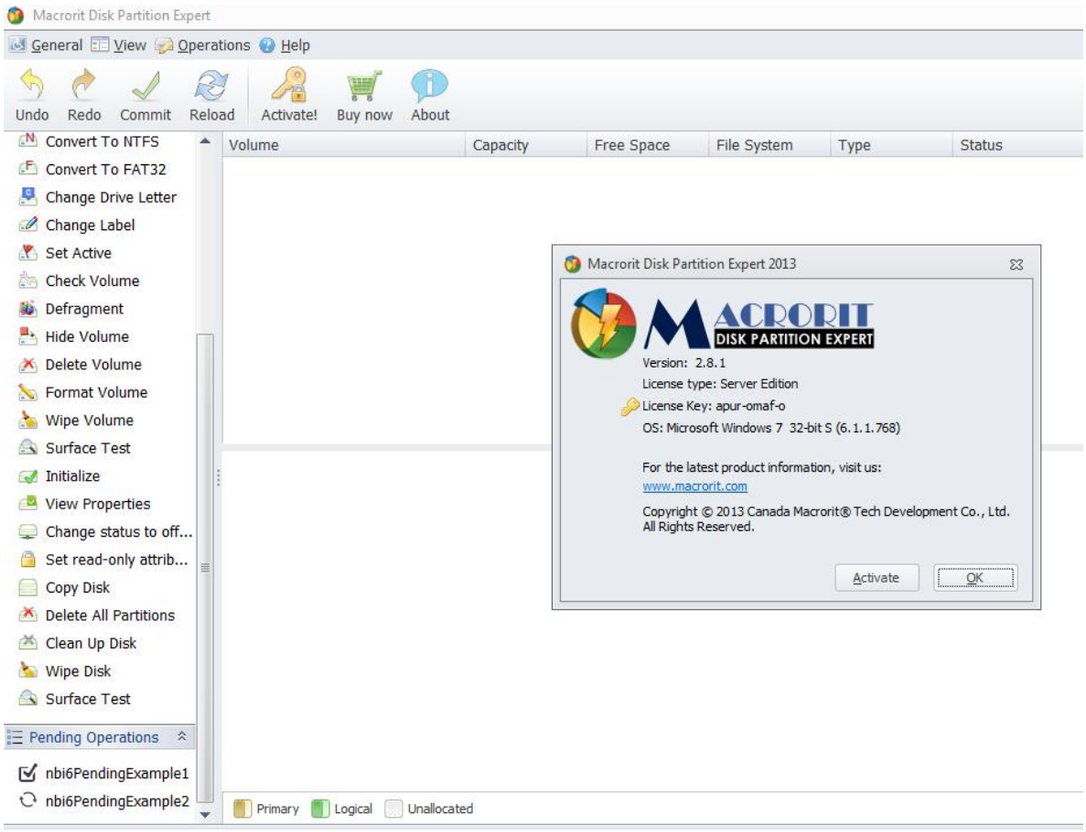
Y luego la licencia aparece guardada



Valor que está en



El primer intento fue intentar Apuromafo (copy paste apuromafo) y que me aceptara el serial, luego lo re-formateó y genero uno y cientos de errores porque el string Apuromafo es manipulado directamente y cuando llama da divisiones por cero y cuanto otro error, por ende da errores de valores (MALA IDEA)



Asi que si es de registrar, mejor intentar con numeritos o bien el formato que acepte el programa (escribirlos directo, no hacer copy paste de algún valor)

Ahora me voy a realmente ver las versiones, meditando de como intentaré parchar

```
14EE     00              DB 00
14EF     00              DB 00
14F0 r$  55              PUSH EBP
14F1  .  8BEC            MOV EBP,ESP
14F3  .  81C4 DCFDFFFF  ADD ESP,-224
14F9  .  53              PUSH EBX
14FA  .  56              PUSH ESI
14FB  .  33C9            XOR ECX,ECX
14FD  .  898D ECFDFFFF  MOV DWORD PTR SS:[LOCAL.133],ECX
1503  .  8BF2            MOV ESI,EDX
1505     8BD8            MOV EBX,EAX
1507     33C0            XOR EAX,EAX
1509     55              PUSH EBP
150A     68 C6167C00     PUSH 007C16C6
150F     64:FF30         PUSH DWORD PTR FS:[EAX]
1512     64:8920         MOV DWORD PTR FS:[EAX],ESP
1515  .  0FB6C3          MOVZX EAX,BL
1518  .  83F8 07         CMP EAX,7                        Switch (cases 0..7, 9 exits)
151B  .v 0F87 4A010000  JA 007C166B
1521  .v FF2485 28157C  JMP DWORD PTR DS:[EAX*4+7C1528]
1528  .  48157C00        DD 007C1548
152C  .  59157C00        DD 007C1559
1530  .  7B157C00        DD 007C157B
1534  .  6A157C00        DD 007C156A
1538  .  33167C00        DD 007C1633
153C  .  41167C00        DD 007C1641
1540  .  4F167C00        DD 007C164F
```

Tenemos del 0 al 7

Asi que tenemos en las manos donde parcharemos:

Quiero que observen la siguiente instrucción(no involucra solo eax, sino además bl)

```
007C1512     64:8920         MOV DWORD PTR FS:[EAX],ESP
007C1515  .  0FB6C3          MOVZX EAX,BL
007C1518  .  83F8 07         CMP EAX,7                        Switch
007C151B  .v 0F87 4A010000  JA 007C166B
```

Tenemos que manipular los 2 valores el de (bl) y el valor de eax que sean iguales, luego saltar a la versión que quiero.

Asi que donde dice “server edition trial “ le coloco los valores de eax y de BL pues llegaré ahí tarde o temprano

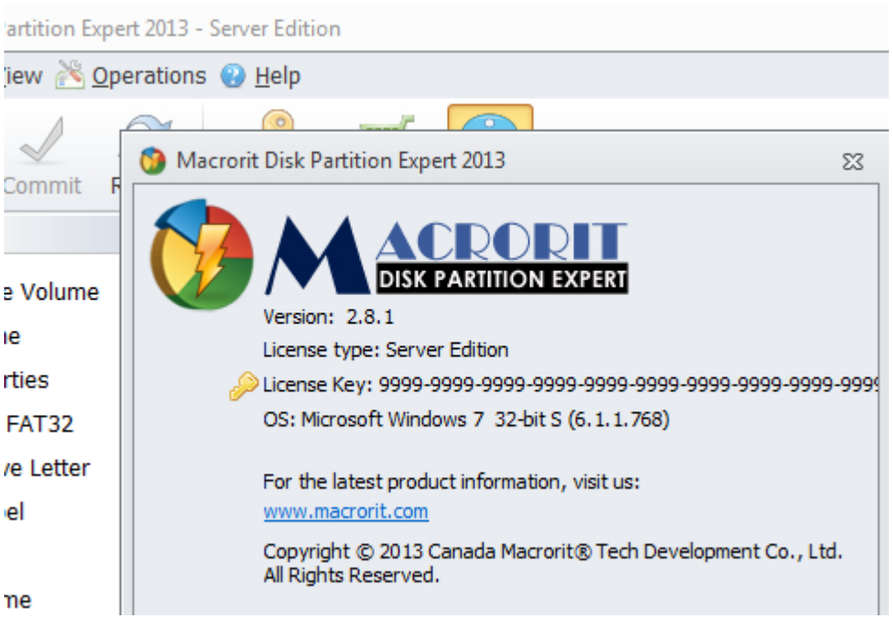
```
007C163F  EB 3E       JMP SHORT 007C167F
007C1641  8BC6        MOV EAX,ESI                 Case 5 of switch dm.7C1518
007C1643  BA 84187C00 MOV EDX,007C1884            UNICODE "Server Edition"
007C1648  E8 D35CC4FF CALL 00407320
007C164D  EB 30       JMP SHORT 007C167F
007C164F  8BC6        MOV EAX,ESI                 Case 6 of switch dm.7C1518
007C1651  BA B0187C00 MOV EDX,007C18B0            UNICODE "Enterprise Edition"
007C1656  E8 C55CC4FF CALL 00407320
007C165B  EB 22       JMP SHORT 007C167F
007C165D  8BC6        MOV EAX,ESI                 Case 7 of switch dm.7C1518
007C165F  BA E4187C00 MOV EDX,007C18E4            UNICODE "Technician Edition"
007C1664  E8 B75CC4FF CALL 00407320
007C1669  EB 14       JMP SHORT 007C167F
007C166B  B9 D7000000 MOV ECX,0D7                 Default case of switch dm.7C1518
007C1670  BA 18197C00 MOV EDX,007C1918            UNICODE "D:\Work\projects\dm\ui\comm\dmActiv.pas"
007C1675  B8 28197C00 MOV EAX,007C1928            UNICODE "Assertion failure"
007C167A  E8 C14CC4FF CALL 00406340               dm.00406340
007C167F  80FB 01     CMP BL,1
007C1682  75 29       JNE SHORT 007C16AD
007C1684  E8 1BF7FFFF CALL 007C0DA4               Switch (cases 2..3, 3 exits)
007C1689  2C 02       SUB AL,2
007C168B  74 06       JZ SHORT 007C1693
007C168D  FEC8        DEC AL
007C168F  74 10       JZ SHORT 007C16A1
007C1691  EB 1A       JMP SHORT 007C16AD
007C1693  8BC6        MOV EAX,ESI                 Case 2 of switch dm.7C1689
007C1695  BA A8197C00 MOV EDX,007C19A8            UNICODE "Professional Edition (Demo)"
007C169A  E8 815CC4FF CALL 00407320
007C169F  EB 0C       JMP SHORT 007C16AD
007C16A1  B3 05       MOV BL,5
007C16A3  B8 05000000 MOV EAX,5
007C16A8  EB 97       JMP SHORT 007C1641
007C16AA  90          NOP
007C16AB  90          NOP
```

Asi que ahora a testear

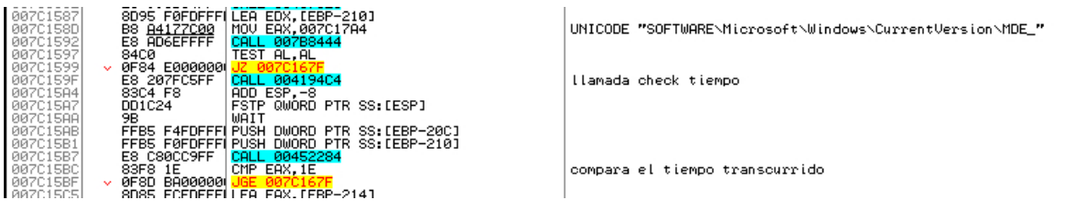
Intentemos algunos numeritos y logro:

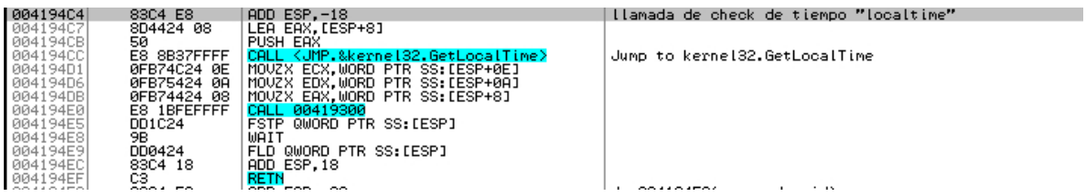
luego intento con otros números (reinicio denuevo)

Y luego

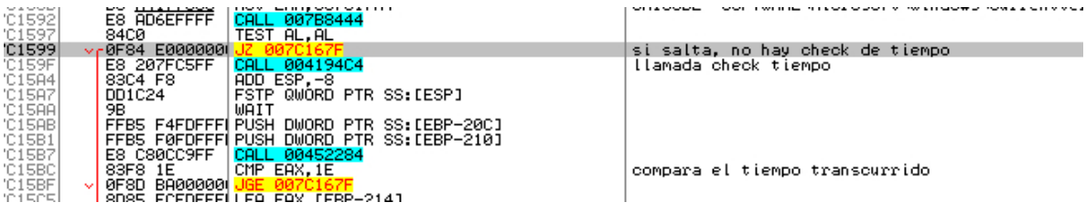


Así que damos por revisado esta aplicación, puedo continuar si tiene algún check de tiempo





Por lo cual debemos forzar que no exista check de tiempo:



Luego quedo mas tranquilo que está registrado a la versión que quiera(mov numero de versión y parchado por si algún dia quiera expirar) el programa corre de lo más bien .

Nota: este programa acompaña unos archivos .api (realmente son .dll , pero el programa los carga con su nombre) en el cual tiene todas las funciones del programa en sí.

Saludos a la lista de Crackslatinos y amigos ^^

Saludos Apuromafo