



MDE_ : Macrorit Disk Partition Expert Server

by Apuromafo

Encontré curioso el programa ^^

CLS
19/08/2013

7C1500	8085 ECFDFFF	LEA EAX,[LOCAL.133]	Arg1 => Offset Local.133
7C1501	50	PUSH EAX	UNICODE "Remaining: "
7C1502	B8 10187C00	MOV EAX,007C1810	
7C1503	8985 DCFDFFF	MOV DWORD PTR SS:[LOCAL.137],EAX	
7C1504	C685 E0FDFFF	MOV BYTE PTR SS:[LOCAL.136],11	
7C1505	E8 E17EC5FF	CALL 004194C4	
7C1506	83C4 F8	ADD ESP,-8	
7C1507	DD1C24	FSTP QWORD PTR SS:[ESP]	
7C1508	9B	WAIT	
7C1509	FFB5 F4FDFFF	PUSH DWORD PTR SS:[LOCAL.131]	
7C150A	FFB5 F0FDFFF	PUSH DWORD PTR SS:[LOCAL.132]	
7C150B	E8 890CC9FF	CALL 00452284	
7C150C	BA 1E000000	MOV EDX,1E	
7C150D	2BD0	SUB EDX,EAX	
7C150E	8995 E4FDFFF	MOV DWORD PTR SS:[LOCAL.135],EDX	
7C150F	C685 E8FDFFF	MOV BYTE PTR SS:[LOCAL.134],0	
7C1510	8D95 DCFDFFF	LEA EDX,[LOCAL.137]	
7C1511	B9 01000000	MOV ECX,1	
7C1512	B8 34187C00	MOV EAX,007C1834	
7C1513	E8 8C5EC5FF	CALL 004174B0	
7C1514	8B95 ECFDFFF	MOV EDX,DWORD PTR SS:[LOCAL.133]	
7C1515	8BC6	MOV EAX,ESI	
7C1516	E8 0361C4FF	CALL 00407734	
7C1517	EB 4C	JMP SHORT 007C167F	
7C1518	8BC6	MOV EAX,ESI	Case 4 of switch dm.7C1518
7C1519	BA 4C187C00	MOV EDX,007C184C	UNICODE "Professional Edition"
7C151A	E8 E15CC4FF	CALL 00407320	
7C151B	EB 3E	JMP SHORT 007C167F	
7C151C	8BC6	MOV EAX,ESI	Case 5 of switch dm.7C1518
7C151D	BA 84187C00	MOV EDX,007C1884	UNICODE "Server Edition"
7C151E	E8 D35CC4FF	CALL 00407320	
7C151F	EB 30	JMP SHORT 007C167F	
7C1520	8BC6	MOV EAX,ESI	Case 6 of switch dm.7C1518
7C1521	BA 00187C00	MOV EDX,007C18B0	UNICODE "Enterprise Edition"
7C1522	E8 C55CC4FF	CALL 00407320	
7C1523	EB 22	JMP SHORT 007C167F	
7C1524	8BC6	MOV EAX,ESI	Case 7 of switch dm.7C1518
7C1525	BA E4187C00	MOV EDX,007C18E4	UNICODE "Technician Edition"
7C1526	E8 B75CC4FF	CALL 00407320	
7C1527	EB 14	JMP SHORT 007C167F	
7C1528	B9 D7000000	MOV ECX,0D7	Default case of switch dm.7C1518
7C1529	BA 18187C00	MOV EDX,007C1918	UNICODE "D:\\"
7C152A	B8 78187C00	MOV EAX,007C1978	UNICODE "
7C152B	E8 C14CC4FF	CALL 00406340	Case 8 of switch dm.7C1518
7C152C	80FB 01	CMP BL,1	UNICODE "dm.0040"
7C152D	75 29	JNE SHORT 007C16AD	
7C152E	E8 1BF7FFFF	CALL 007C0DA4	
7C152F	2C 02	SUB AL,2	Switch (cases 2..9, 9 exits)
7C1530	74 06	JZ SHORT 007C1693	
7C1531	FEC8	DEC AL	
7C1532	74 10	JZ SHORT 007C16A1	
7C1533	EB 1A	JMP SHORT 007C16AD	
7C1534	8BC6	MOV EAX,ESI	Case 2 of switch dm.7C1689
7C1535	BA 08187C00	MOV EDX,007C19A8	UNICODE "Professional Edition (Demo)"
7C1536	E8 C55CC4FF	CALL 00407320	
7C1537	EB 0C	JMP SHORT 007C16AD	
7C1538	MOV EAX,ESI		UNICODE "Server Edition (Demo)"
7C1539	MOV EDX,007C19EC		

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)

007C1518	83F8 07	CMP EAX,7	Switch (cases 0..7, 9 exits)
007C1519	74 07	JZ 007C166B	
007C151A	FF2485 28157C00	JMP DWORD PTR DS:[EAX*4+7C1528]	
007C151B	48157C00	DD 007C1548	
007C151C	59157C00	DD 007C1559	
007C151D	7B157C00	DD 007C157B	
007C151E	6B157C00	DD 007C156B	
007C151F	3B157C00	DD 007C163B	
007C1520	41157C00	DD 007C1641	
007C1521	4F157C00	DD 007C164F	
007C1522	5D	POP EBP	
007C1523	16	PUSH SS	
007C1524	7C 00	JL SHORT 007C1548	
007C1525	8BC6	MOV EAX,ESI	
007C1526	BA E0187C00	MOV EDX,007C16E0	
007C1527	E8 C55CC4FF	CALL 00407320	UNICODE "Free For Home User"
007C1528	F9 26A10000	JMP 007C167F	

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	• 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 03699000	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 0C649000	MOV EAX,DWORD PTR DS:[9064DC]	
00906948	• E8 1F2FC0FF	CALL 0050986C	
0090694D	• A3 4CC99300	MOV DWORD PTR DS:[93C94C],EAX	
00906952	• 8D55 FC	LEA EDI,[LOCAL.1]	
00906955	• A1 70539300	MOV EAX,DWORD PTR DS:[935370]	
0090695A	• 0FB640 28	MOVBX EAX,BYTE PTR DS:[EAX+28]	para splash
0090695E	• E8 8DABEBFF	CALL 007C14F0	
00906963	• 8B55 FC	MOV EDI,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	• 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 EDI,[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 EDI,007C1A78	Unicode "License type: "
007C1A45	• E8 AA5DC4FF	CALL 004077F4	
007C1A4A	• 33C0	XOR EAX,EAX	
007C1A4C	• 5A	POP EDI	
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	• C3	RET	Jump to 7C1A67
007C1A60	• E9 CB40C4FF	JMP 00405830	SE handling routine
007C1A65	• EB F0	JMP SHORT 007C1A57	
007C1A67	> 5E	POP ESI	
007C1A68	• 5B	POP EBX	

Y el titulo

007C24B7	• 20	MOV EBP,ESP	
007C24B8	• 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	
007C24C9	• 64:FF30	PUSH DWORD PTR FS:[EAX]	
007C24CD	• 64:8920	MOV DWORD PTR FS:[EAX],ESP	Installs SE handler 7C2520
007C24D0	• 8D55 FC	LEA EDI,[EBP-4]	
007C24D3	• A1 144A9300	MOV EAX,DWORD PTR DS:[934A14]	
007C24D8	• E8 CF86C4FF	CALL 0040A8AC	
007C24DD	• FF75 FC	PUSH DWORD PTR SS:[EBP-4]	
007C24E0	• 68 38257C00	PUSH 007C2538	Unicode " - "
007C24E5	• 8D55 F8	LEA EDI,[EBP-8]	
007C24E8	• A1 70539300	MOV EAX,DWORD PTR DS:[935370]	
007C24ED	• 0FB640 28	MOVBX 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 EDI,3	
007C2500	• E8 D353C4FF	CALL 004078D8	
007C2505	• 33C0	XOR EAX,EAX	
007C2507	• 5A	POP EDI	
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:

009055E1	837D F8 00	CMF DWORD PTR SS:[EBP-8],0	
009055E2	0F84 02020000	JE 009057EA	
009055E8	8B55 F8	MOV EDX,DWORD PTR SS:[EBP-8]	comparacion importante
009055EB	8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
009055EE	E8 39030000	CALL 0090592C	cdm.0090592C
009055F3	84C0	TEST AL,AL	si retorna 1 entonces serß valido
009055F5	75 29	JNZ SHORT 00905620	
009055F7	8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	no hay serial valido
009055FA	FF80 D4030000	INC DWORD PTR DS:[EAX+3D4]	
00905600	8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
00905603	83B8 D4030000	CMF DWORD PTR DS:[EAX+3D4],3	
0090560A	7C 08	JL SHORT 00905614	
0090560C	8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
0090560F	E8 C896C0FF	CALL 0050F1DC	cdm.0050F1DC
00905614	55	PUSH EBP	
00905615	E8 DAFFFFFF	CALL 009054F4	
0090561A	59	POP ECX	
0090561B	E9 CA010000	JMP 009057EA	
00905620	8B45 F8	MOV EAX,DWORD PTR SS:[EBP-8]	si hay serial valido
00905623	E8 3CB8EBFF	CALL 007C1064	dime que version registrarß en regedit
00905628	84C0	TEST AL,AL	
0090562A	75 29	JNZ SHORT 00905655	
0090562C	8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
0090562F	FF80 D4030000	INC DWORD PTR DS:[EAX+3D4]	
00905635	8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
00905638	83B8 D4030000	CMF DWORD PTR DS:[EAX+3D4],3	
0090563E	7C 08	JL SHORT 00905648	

007C107E	55	PUSH EBP	
007C107F	68 4D117C00	PUSH 007C114D	
007C1084	64:FF30	PUSH DWORD PTR FS:[EAX]	Installs SE handler 7C114D
007C1087	64:8920	MOV DWORD PTR FS:[EAX],ESP	
007C108A	8D4D F8	LEA ECX,[EBP-8]	
007C108D	BA 68117C00	MOV EDX,007C1168	UNICODE "max.wang"
007C1092	8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
007C1095	E8 4AFBFFFF	CALL 007C0AE4	
007C109A	8D55 F4	LEA EDX,[EBP-0C]	
007C109D	B8 88117C00	MOV EAX,007C1188	UNICODE "PROF"
007C10A2	E8 05FCFFFF	CALL 007C0CAC	cdm.007C0CAC
007C10A7	8B55 F4	MOV EDX,DWORD PTR SS:[EBP-0C]	
007C10AA	8B45 F8	MOV EAX,DWORD PTR SS:[EBP-8]	
007C10AD	E8 E669C4FF	CALL 00407A98	
007C10B2	75 04	JNZ SHORT 007C10B8	
007C10B4	B3 01	MOV BL,1	
007C10B6	EB 7A	JMP SHORT 007C1132	
007C10B8	8D55 F0	LEA EDX,[EBP-10]	
007C10BB	B8 00117C00	MOV EAX,007C11A0	UNICODE "SERV"
007C10C0	E8 E7FBFFFF	CALL 007C0CAC	cdm.007C0CAC
007C10C5	8B55 F0	MOV EDX,DWORD PTR SS:[EBP-10]	
007C10C8	8B45 F8	MOV EAX,DWORD PTR SS:[EBP-8]	
007C10CB	E8 C869C4FF	CALL 00407A98	
007C10D0	75 04	JNZ SHORT 007C10D6	
007C10D2	B3 01	MOV BL,1	
007C10D4	EB 5C	JMP SHORT 007C1132	
007C10D6	8D55 EC	LEA EDX,[EBP-14]	
007C10D9	B8 B8117C00	MOV EAX,007C11B8	UNICODE "ENTE"
007C10DE	E8 C9FBFFFF	CALL 007C0CAC	cdm.007C0CAC
007C10E3	8B55 EC	MOV EDX,DWORD PTR SS:[EBP-14]	
007C10E6	8B45 F8	MOV EAX,DWORD PTR SS:[EBP-8]	
007C10E9	E8 AA69C4FF	CALL 00407A98	
007C10EE	75 04	JNZ SHORT 007C10F4	
007C10F0	B3 01	MOV BL,1	
007C10F2	EB 3E	JMP SHORT 007C1132	
007C10F4	8D55 E8	LEA EDX,[EBP-18]	
007C10F7	B8 D0117C00	MOV EAX,007C11D0	UNICODE "TECH"
007C10FC	E8 ABFBFFFF	CALL 007C0CAC	cdm.007C0CAC
007C1101	8B55 E8	MOV EDX,DWORD PTR SS:[EBP-18]	
007C1104	8B45 F8	MOV EAX,DWORD PTR SS:[EBP-8]	
007C1107	E8 8C69C4FF	CALL 00407A98	
007C110C	75 04	JNZ SHORT 007C1112	
007C110E	B3 01	MOV BL,1	
007C1110	EB 20	JMP SHORT 007C1132	
007C1112	8D55 E4	LEA EDX,[EBP-1C]	
007C1115	B8 E8117C00	MOV EAX,007C11E8	UNICODE "30_D"
007C111A	E8 8DFBFFFF	CALL 007C0CAC	cdm.007C0CAC
007C111F	8B55 E4	MOV EDX,DWORD PTR SS:[EBP-1C]	
007C1122	8B45 F8	MOV EAX,DWORD PTR SS:[EBP-8]	
007C1125	E8 6E69C4FF	CALL 00407A98	
007C112A	75 04	JNZ SHORT 007C1130	
007C112C	B3 01	MOV BL,1	
007C112E	EB 02	JMP SHORT 007C1132	
007C1130	33DB	XOR EBX,EBX	
007C1132	33C0	XOR EAX,EAX	
007C1134	5A	POP EDX	
007C1135	5A	POP ECX	

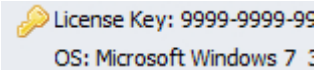
Si logro que cualquiera mov bl,1 sea verdadero entonces logro un licence key para guardar con un interesante texto

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

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

----- Aceptar -----

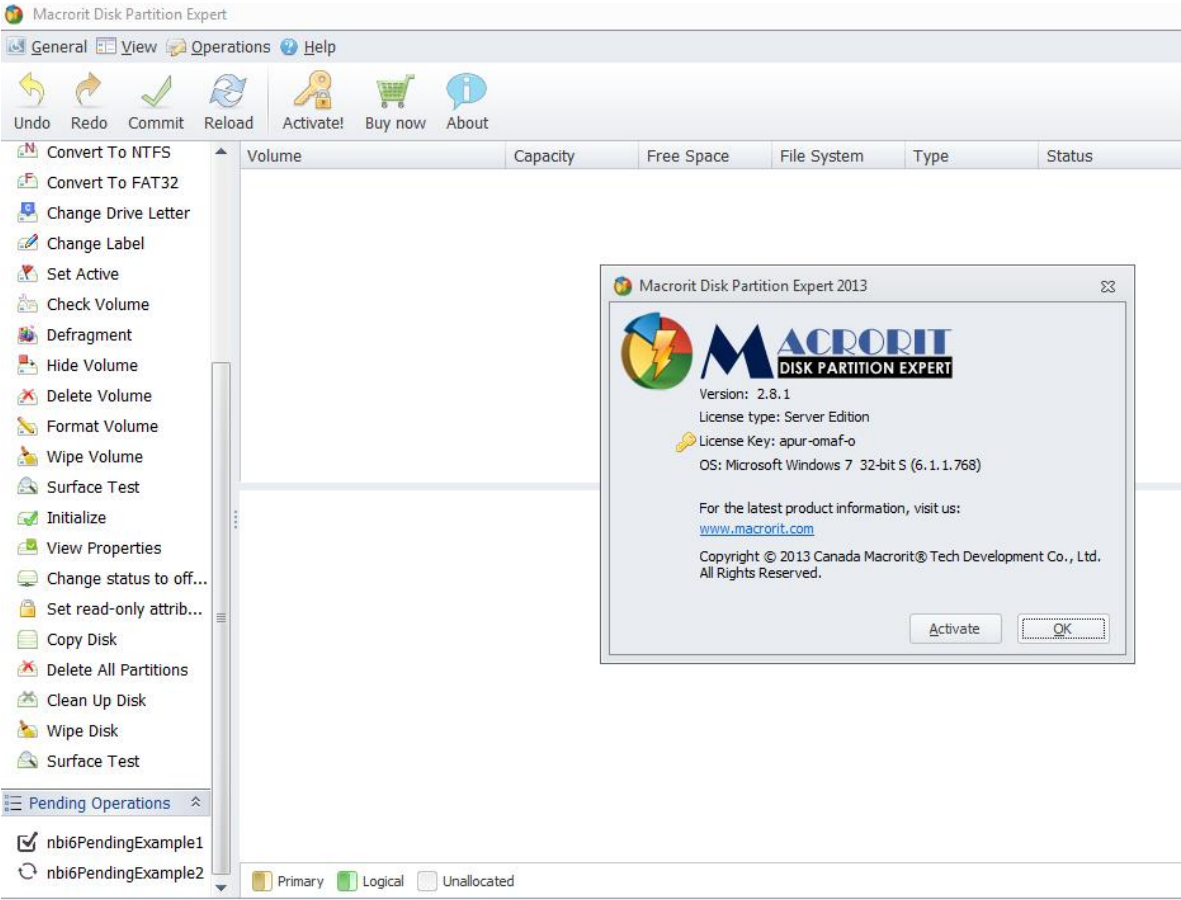
Y luego la licencia aparece guardada



Valor que está en

Equipo\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MDE_

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 55 PUSH EBP
14F1 8BEC MOV EBP,ESP
14F3 81C4 DCFDFF ADD ESP,-224
14F9 53 PUSH EBX
14FA 56 PUSH ESI
14FB 33C9 XOR ECX,ECX
14FD 898D ECFDFF 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
151B 0F87 4A010001 JA 007C166B
1521 FF2485 28157 JMP DWORD PTR DS:[EAX*4+7C1528]
1528 48157C00 DD 007C1548
152C 59157C00 DD 007C1559
1530 7B157C00 DD 007C157B
1534 6B157C00 DD 007C156A
1538 3B157C00 DD 007C1633
153C 41167C00 DD 007C1641
1540 4F167C00 DD 007C164F

Switch (cases 0..7, 9 exits)
```

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
007C151B 0F87 4A010001 JA 007C166B

Switch
```

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	
007C1643	• BA 84187C00	MOV EDX,007C1884	Case 5 of switch dm.7C1518
007C1648	• E8 035CC4FF	CALL 00407320	Unicode "Server Edition"
007C164D	< EB 30	JMP SHORT 007C167F	
007C164F	> 8BC6	MOV EAX,ESI	
007C1651	• BA 80187C00	MOV EDX,007C18B0	Case 6 of switch dm.7C1518
007C1656	• E8 C55CC4FF	CALL 00407320	Unicode "Enterprise Edition"
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 07000000	MOV ECX,007	Default case of switch dm.7C1518
007C1670	• BA 18197C00	MOV EDX,007C1918	Unicode "D:\Work\projects\dm\ui\comm\dmActiv.pas"
007C1675	• B8 78197C00	MOV EAX,007C1978	Unicode "Assertion failure"
007C167A	• E8 C14CC4FF	CALL 00406340	Cdn.00406340
007C167F	> 80FB 01	CMP BL,1	
007C1682	< EB 29	JNE SHORT 007C16AD	
007C1684	• E8 1BF7FFFF	CALL 007C00A4	
007C1689	< EC 02	SUB AL,2	Switch (cases 2..3, 3 exits)
007C168B	< EB 06	JZ SHORT 007C1693	
007C168D	< EC 08	DEC AL	
007C1690	< EB 10	JZ SHORT 007C16A1	
007C1691	< EB 1A	JMP SHORT 007C16AD	
007C1693	> 8BC6	MOV EAX,ESI	Case 2 of switch dm.7C1689
007C1695	• BA 80197C00	MOV EDX,007C19A8	Unicode "Professional Edition (Demo)"
007C169A	• E8 815CC4FF	CALL 00407320	
007C169F	< EB 0C	JMP SHORT 007C16AD	
007C16A1	< EB 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

007C1587 8D95 F0F0FFF LEA EDI,[EBP-210]	Unicode "SOFTWARE\Microsoft\Windows\CurrentVersion\NDE_"
007C158D B8 04172C00 MOV EAX,007C17A4	
007C1592 E8 AD6EFFFF CALL 007B8444	
007C1597 84C0 TEST AL,AL	
007C1599 0F84 E0000000 JZ 007C167F	llamada check tiempo
007C159F E8 207FC5FF CALL 004194C4	
007C15A4 83C4 F8 ADD ESP,-8	
007C15A7 DD1C24 FSTP QWORD PTR SS:[ESP]	
007C15AA 9B WAIT	
007C15AB FFB5 F4F0FFF PUSH DWORD PTR SS:[EBP-20C]	
007C15B1 FFB5 F0F0FFF PUSH DWORD PTR SS:[EBP-210]	
007C15B7 E8 C80CC9FF CALL 00452284	
007C15BC 83F8 1E CMP EAX,1E	compara el tiempo transcurrido
007C15BF 0F8D BA000000 JGE 007C167F	
007C15C5 8B85 FCF0FFF LEA EAX,[F8F-2141]	
004194C4 83C4 E8 ADD ESP,-18	llamada de check de tiempo "localtime"
004194C7 8D4424 08 LEA EAX,[ESP+8]	
004194CB 58 PUSH EAX	
004194CC E8 0B37FFFF CALL JMP.&kernel32.GetLocalTime	Jump to kernel32.GetLocalTime
004194D1 0FB74C24 0E MOVZX ECX,WORD PTR SS:[ESP+0E]	
004194D6 0FB75424 0A MOVZX EDI,WORD PTR SS:[ESP+0A]	
004194DB 0FB74424 08 MOVZX EAX,WORD PTR SS:[ESP+8]	
004194E0 E8 1BF0FFFF CALL 00419380	
004194E5 DD1C24 FSTP QWORD PTR SS:[ESP]	
004194E8 9B WAIT	
004194E9 DD0424 FLD QWORD PTR SS:[ESP]	
004194EC 83C4 18 ADD ESP,18	
004194EF C3 RETN	

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

007C1592 E8 AD6EFFFF CALL 007B8444	
007C1597 84C0 TEST AL,AL	
007C1599 0F84 E0000000 JZ 007C167F	si salta, no hay check de tiempo
007C159F E8 207FC5FF CALL 004194C4	llamada check tiempo
007C15A4 83C4 F8 ADD ESP,-8	
007C15A7 DD1C24 FSTP QWORD PTR SS:[ESP]	
007C15AA 9B WAIT	
007C15AB FFB5 F4F0FFF PUSH DWORD PTR SS:[EBP-20C]	
007C15B1 FFB5 F0F0FFF PUSH DWORD PTR SS:[EBP-210]	
007C15B7 E8 C80CC9FF CALL 00452284	
007C15BC 83F8 1E CMP EAX,1E	compara el tiempo transcurrido
007C15BF 0F8D BA000000 JGE 007C167F	
007C15C5 8B85 FCF0FFF LEA EAX,[F8F-2141]	

Luego quedo mas tranquilo que está registrado a la versión que quiera(mov numero de versión y parchado por si algún día 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

