



ACDSEE 19

Depurando el programa antes visto

Este pequeño tutorial expondrá lugares vulnerables de una aplicación muy bien cuidada

Apuromafo CLS
23/12/2015

Contenido

Introducción: 2

Conociendo al Programa: 3

Conclusión: 8

Introducción:

Hola hoy revisando el tutorial de BitmanMB, hablaba de una aplicación que había cambiado un serial, entonces me propuse lo mismo pero en una versión de a poco mayor.

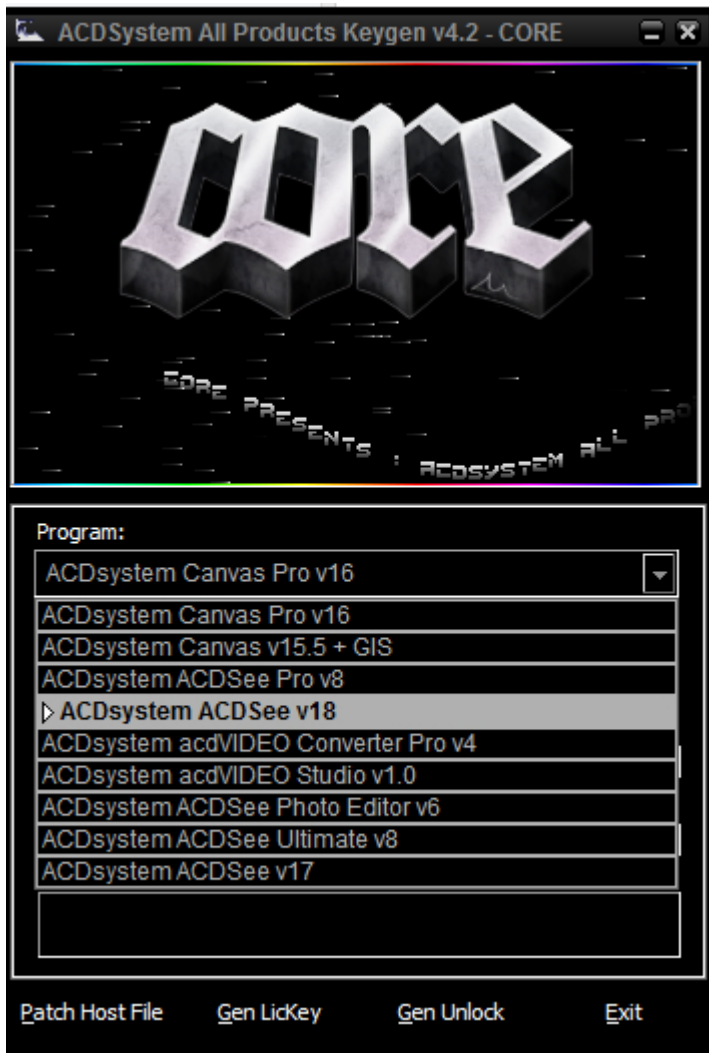
Busca la simplicidad en el desorden. Busca la armonía en la discordia. En el corazón de la dificultad se encuentra la oportunidad. Albert Einstein

Programa	ACDSEE v 19
Compañía	Copyright ©2015 ACD Systems International Inc. All rights reserved.
Descarga	http://dl.acdsystems.com/acdsee/en/acdsee.exe
Tamaño	Setup: 87 mb / Programa:26.5 mb
Víctima	ACDSee19.exe
Versión del Programa	19.1.0.419
Herramientas	Ollydbg, keygen v18 team Core
Packer/protector	Ninguno
Utilidad	Visor de Imágenes
Entorno	Windows 8.1 x64
Compilador	Visual C/c++
Objetivos	Parchar cuanto se pueda.
Tutorial por	Apuromafo CLS
Fecha	23 Diciembre 2015

El programa es Trial, este escrito va dedicado a un joven que recién comienza a escribir tutoriales, ya complementarás este cuando puedas ☺

Conociendo al Programa:

Lo más básico es ver si hay versiones crackeadas o keygen, encontré la versión 18 con un keygen en intercambiosvirtuales

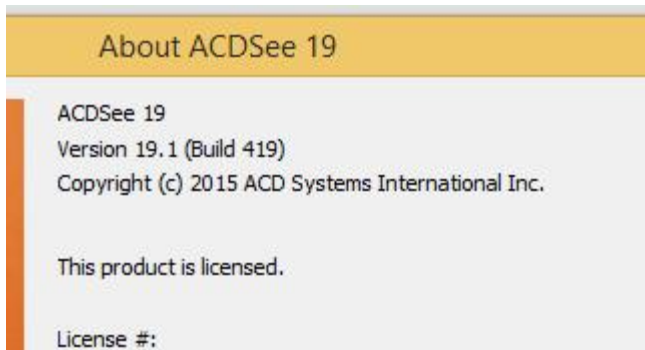


Solo para ayuda guardé un serial y llega el momento de probar en el ollydbg

Inválida, probando otras seriales también inválidas...

00611726	FF15 D668C01	CALL DWORD PTR DS:[&fnc120u.#296]	nfc120u.#296	
00611727	8D45 E8	LEA EAX,DWORD PTR SS:[EBP-18]		
00611728	C645 FC 03	MOV BYTE PTR SS:[EBP-4],3		
00611729	58	PUSH EAX		
00611734	8BCF	MOV ECX,EDI		
00611735	FF15 95C0100	CALL ACDSes19.00620F00		
00611736	8BF8	MOV ESI,ERX		
00611737	E8 734B0000	PUSH 4B73		
00611742	8D4D E4	LEA ECX,DWORD PTR SS:[EBP-1C]		
00611745	C645 FC 04	MOV BYTE PTR SS:[EBP-4],4		
00611749	FF15 D668C01	CALL DWORD PTR DS:[&fnc120u.#286]	nfc120u.#286	
0061174F	C645 FC 05	MOV BYTE PTR SS:[EBP-4],5		
00611752	FF30	PUSH DWORD PTR DS[ERX]		
00611753	C645 EC	LEA EAX,DWORD PTR SS:[EBP-14]		
00611754	58	PUSH EAX		
00611758	FF15 D668C01	CALL DWORD PTR DS:[&fnc120u.#4772]	nfc120u.#4772	
00611761	85C4 05	MOV EBP,05		
00611764	C645 FC 04	MOV BYTE PTR SS:[EBP-4],4		
00611765	8D4D E4	LEA ECX,DWORD PTR SS:[EBP-1C]		
00611768	FF15 D468C01	CALL DWORD PTR DS:[&fnc120u.#1042]	nfc120u.#1495	
00611771	8D4D E3	LEA ECX,DWORD PTR SS:[EBP-18]		
00611774	C645 FC 03	MOV BYTE PTR SS:[EBP-4],3		
00611778	FF15 D468C01	CALL DWORD PTR DS:[&fnc120u.#1042]	nfc120u.#1495	
0061177E	8D45 E4	LEA EAX,DWORD PTR SS:[EBP-1C]		
00611781	8BCF	MOV ECX,EDI		
00611783	58	PUSH EAX		
00611794	E8 47C0100	CALL ACDSes19.00620F00		
00611797	84 4B	PUSH 4B		
00611798	C645 FC 06	MOV BYTE PTR SS:[EBP-4],6		
0061179F	FF30	PUSH DWORD PTR DS[ERX]		
006117A1	FF75 EC	PUSH DWORD PTR SS:[EBP-14]		
006117A4	FF77 20	PUSH DWORD PTR DS[EDI+20]	apphelp.749126F8	
006117A7	FF15 F519C01	CALL DWORD PTR DS:[&USER32.SendMessageBowl]		
006117A8	8D4D E4	LEA ECX,DWORD PTR SS:[EBP-1C]		
006117A9	C645 FC 03	MOV BYTE PTR SS:[EBP-4],3		
006117B4	FF15 D468C01	CALL DWORD PTR DS:[&fnc120u.#1042]	nfc120u.#1495	
006117B8	8BCF	MOV ECX,EDI		
006117C0	FF15 D667C01	CALL DWORD PTR DS:[&fnc120u.#13404]	nfc120u.#13404	
006117C2	85C4 05	MOV EBP,05		
006117C3	8BCF	MOV ECX,EDI		
006117C4	8BCF	MOV ECX,EDI		
006117C5	8BCF	MOV ECX,EDI		
006117C6	8BCF	MOV ECX,EDI		
006117C7	8BCF	MOV ECX,EDI		
006117C8	8BCF	MOV ECX,EDI		
006117C9	8BCF	MOV ECX,EDI		
006117CA	8BCF	MOV ECX,EDI		
006117CB	8BCF	MOV ECX,EDI		
006117CC	8BCF	MOV ECX,EDI		
006117CD	8BCF	MOV ECX,EDI		
006117CE	8BCF	MOV ECX,EDI		
006117CF	8BCF	MOV ECX,EDI		
006117D0	8BCF	MOV ECX,EDI		
006117D1	8BCF	MOV ECX,EDI		
006117D2	8BCF	MOV ECX,EDI		
006117D3	8BCF	MOV ECX,EDI		
006117D4	8BCF	MOV ECX,EDI		
006117D5	8BCF	MOV ECX,EDI		
006117D6	8BCF	MOV ECX,EDI		
006117D7	8BCF	MOV ECX,EDI		
006117D8	8BCF	MOV ECX,EDI		
006117D9	8BCF	MOV ECX,EDI		
006117DA	8BCF	MOV ECX,EDI		
006117DB	8BCF	MOV ECX,EDI		
006117DC	8BCF	MOV ECX,EDI		
006117DD	8BCF	MOV ECX,EDI		
006117DE	8BCF	MOV ECX,EDI		
006117DF	8BCF	MOV ECX,EDI		
006117E0	8BCF	MOV ECX,EDI		
006117E1	8BCF	MOV ECX,EDI		
006117E2	8BCF	MOV ECX,EDI		
006117E3	8BCF	MOV ECX,EDI		
006117E4	8BCF	MOV ECX,EDI		
006117E5	8BCF	MOV ECX,EDI		
006117E6	8BCF	MOV ECX,EDI		
006117E7	8BCF	MOV ECX,EDI		
006117E8	8BCF	MOV ECX,EDI		
006117E9	8BCF	MOV ECX,EDI		
006117EA	8BCF	MOV ECX,EDI		
006117EB	8BCF	MOV ECX,EDI		
006117EC	8BCF	MOV ECX,EDI		
006117ED	8BCF	MOV ECX,EDI		
006117EE	8BCF	MOV ECX,EDI		
006117EF	8BCF	MOV ECX,EDI		
006117F0	8BCF	MOV ECX,EDI		
006117F1	8BCF	MOV ECX,EDI		
006117F2	8BCF	MOV ECX,EDI		
006117F3	8BCF	MOV ECX,EDI		
006117F4	8BCF	MOV ECX,EDI		
006117F5	8BCF	MOV ECX,EDI		
006117F6	8BCF	MOV ECX,EDI		
006117F7	8BCF	MOV ECX,EDI		
006117F8	8BCF	MOV ECX,EDI		
006117F9	8BCF	MOV ECX,EDI		
006117FA	8BCF	MOV ECX,EDI		
006117FB	8BCF	MOV ECX,EDI		
006117FC	8BCF	MOV ECX,EDI		
006117FD	8BCF	MOV ECX,EDI		
006117FE	8BCF	MOV ECX,EDI		
006117FF	8BCF	MOV ECX,EDI		
00611800	8BCF	MOV ECX,EDI		
00611801	8BCF	MOV ECX,EDI		
00611802	8BCF	MOV ECX,EDI		
00611803	8BCF	MOV ECX,EDI		
00611804	8BCF	MOV ECX,EDI		
00611805	8BCF	MOV ECX,EDI		
00611806	8BCF	MOV ECX,EDI		
00611807	8BCF	MOV ECX,EDI		
00611808	8BCF	MOV ECX,EDI		
00611809	8BCF	MOV ECX,EDI		
0061180A	8BCF	MOV ECX,EDI		
0061180B	8BCF	MOV ECX,EDI		
0061180C	8BCF	MOV ECX,EDI		
0061180D	8BCF	MOV ECX,EDI		
0061180E	8BCF	MOV ECX,EDI		
0061180F	8BCF	MOV ECX,EDI		
00611810	8BCF	MOV ECX,EDI		
00611811	8BCF	MOV ECX,EDI		
00611812	8BCF	MOV ECX,EDI		
00611813	8BCF	MOV ECX,EDI		
00611814	8BCF	MOV ECX,EDI		
00611815	8BCF	MOV ECX,EDI		
00611816	8BCF	MOV ECX,EDI		
00611817	8BCF	MOV ECX,EDI		
00611818	8BCF	MOV ECX,EDI		
00611819	8BCF	MOV ECX,EDI		
0061181A	8BCF	MOV ECX,EDI		
0061181B	8BCF	MOV ECX,EDI		
0061181C	8BCF	MOV ECX,EDI		
0061181D	8BCF	MOV ECX,EDI		
0061181E	8BCF	MOV ECX,EDI		
0061181F	8BCF	MOV ECX,EDI		
00611820	8BCF	MOV ECX,EDI		
00611821	8BCF	MOV ECX,EDI		
00611822	8BCF	MOV ECX,EDI		
00611823	8BCF	MOV ECX,EDI		
00611824	8BCF	MOV ECX,EDI		
00611825	8BCF	MOV ECX,EDI		
00611826	8BCF	MOV ECX,EDI		
00611827	8BCF	MOV ECX,EDI		
00611828	8BCF	MOV ECX,EDI		
00611829	8BCF	MOV ECX,EDI		
0061182A	8BCF	MOV ECX,EDI		
0061182B	8BCF	MOV ECX,EDI		
0061182C	8BCF	MOV ECX,EDI		
0061182D	8BCF	MOV ECX,EDI		
0061182E	8BCF	MOV ECX,EDI		
0061182F	8BCF	MOV ECX,EDI		
00611830	8BCF	MOV ECX,EDI		
00611831	8BCF	MOV ECX,EDI		
00611832	8BCF	MOV ECX,EDI		
00611833	8BCF	MOV ECX,EDI		
00611834	8BCF	MOV ECX,EDI		
00611835	8BCF	MOV ECX,EDI		
00611836	8BCF	MOV ECX,EDI		
00611837	8BCF	MOV ECX,EDI		
00611838	8BCF	MOV ECX,EDI		
00611839	8BCF	MOV ECX,EDI		
0061183A	8BCF	MOV ECX,EDI		
0061183B	8BCF	MOV ECX,EDI		
0061183C	8BCF	MOV ECX,EDI		
0061183D	8BCF	MOV ECX,EDI		
0061183E	8BCF	MOV ECX,EDI		
0061183F	8BCF	MOV ECX,EDI		
00611840	8BCF	MOV ECX,EDI		
00611841	8BCF	MOV ECX,EDI		
00611842	8BCF	MOV ECX,EDI		
00611843	8BCF	MOV ECX,EDI		
00611844	8BCF	MOV ECX,EDI		
00611845	8BCF	MOV ECX,EDI		
00611846	8BCF	MOV ECX,EDI		
00611847	8BCF	MOV ECX,EDI		
00611848	8BCF	MOV ECX,EDI		
00611849	8BCF	MOV ECX,EDI		
0061184A	8BCF	MOV ECX,EDI		
0061184B	8BCF	MOV ECX,EDI		
0061184C	8BCF	MOV ECX,EDI		
0061184D	8BCF	MOV ECX,EDI		
0061184E	8BCF	MOV ECX,EDI		
0061184F	8BCF	MOV ECX,EDI		
00611850	8BCF	MOV ECX,EDI		
00611851	8BCF	MOV ECX,EDI		
00611852	8BCF	MOV ECX,EDI		
00611853	8BCF	MOV ECX,EDI		
00611854	8BCF	MOV ECX,EDI		
00611855	8BCF	MOV ECX,EDI		
00611856	8BCF	MOV ECX,EDI		
00611857	8BCF	MOV ECX,EDI		
00611858	8BCF	MOV ECX,EDI		
00611859	8BCF	MOV ECX,EDI		
0061185A	8BCF	MOV ECX,EDI		
0061185B	8BCF	MOV ECX,EDI		
0061185C	8BCF	MOV ECX,EDI		
0061185D	8BCF	MOV ECX,EDI		
0061185E	8BCF	MOV ECX,EDI		
0061185F	8BCF	MOV ECX,EDI		
00611860	8BCF	MOV ECX,EDI		
00611861	8BCF	MOV ECX,EDI		
00611862	8BCF	MOV ECX,EDI		
00611863	8BCF	MOV ECX,EDI		
00611864	8BCF	MOV ECX,EDI		
00611865	8BCF	MOV ECX,EDI		
00611866	8BCF	MOV ECX,EDI		
00611867	8BCF	MOV ECX,EDI		
00611868	8BCF	MOV ECX,EDI		
00611869	8BCF	MOV ECX,EDI		
0061186A	8BCF	MOV ECX,EDI		
0061186B	8BCF	MOV ECX,EDI		
0061186C	8BCF	MOV ECX,EDI		
0061186D	8BCF	MOV ECX,EDI		
0061186E	8BCF	MOV ECX,EDI		
0061186F	8BCF	MOV ECX,EDI		
00611870	8BCF	MOV ECX,EDI		
00611871	8BCF	MOV ECX,EDI		
00611872	8BCF	MOV ECX,EDI		
00611873	8BCF	MOV ECX,EDI		
00611874	8BCF	MOV ECX,EDI		
00611875	8BCF	MOV ECX,EDI		
00611876	8BCF	MOV ECX,EDI		
00611877	8BCF	MOV ECX,EDI		
00611878	8BCF	MOV ECX,EDI		
00611879	8BCF	MOV ECX,EDI		
0061187A	8BCF	MOV ECX,EDI		
0061187B	8BCF	MOV ECX,EDI		
0061187C	8BCF	MOV ECX,EDI		
0061187D	8BCF	MOV ECX,EDI		
0061187E	8BCF	MOV ECX,EDI		
0061187F	8BCF	MOV ECX,EDI		
00611880	8BCF	MOV ECX,EDI		
00611881	8BCF	MOV ECX,EDI		
00611882	8BCF	MOV ECX,EDI		
00611883	8BCF	MOV ECX,EDI		
00611884	8BCF	MOV ECX,EDI		
00611885	8BCF	MOV ECX,EDI		
00611886	8BCF	MOV ECX,EDI		
00611887	8BCF	MOV ECX,EDI		
00611888	8BCF	MOV ECX,EDI		
00611889	8BCF	MOV ECX,EDI		
0061188A	8BCF	MOV ECX,EDI		
0061188B	8BCF	MOV ECX,EDI		
0061188C	8BCF	MOV ECX,EDI		
0061188D	8BCF	MOV ECX,EDI		
0061188E	8BCF	MOV ECX,EDI		
0061188F	8BCF	MOV ECX,EDI		
00611890	8BCF	MOV ECX,EDI		
00611891	8BCF	MOV ECX,EDI		
00611892	8BCF	MOV ECX,EDI		
00611893	8BCF	MOV ECX,EDI		
00611894	8BCF	MOV ECX,EDI		
00611895	8BCF	MOV ECX,EDI		
00611896	8BCF	MOV ECX,EDI		
00611897	8BCF	MOV ECX,EDI		
00611898	8BCF	MOV ECX,EDI		
00611899	8BCF	MOV ECX,EDI		
0061189A	8BCF	MOV ECX,EDI		
0061189B	8BCF	MOV ECX,EDI		
0061189C	8BCF	MOV ECX,EDI		
0061189D	8BCF	MOV ECX,EDI		
0061189E	8BCF	MOV ECX,EDI		
0061189F	8BCF	MOV ECX,EDI		
006118A0	8BCF	MOV ECX,EDI		
006118A1	8BCF	MOV ECX,EDI		
006118A2	8BCF	MOV ECX,EDI		
006118A3	8BCF	MOV ECX,EDI		
006118A4	8BCF	MOV ECX,EDI		
006118A5	8BCF	MOV ECX,EDI		
006118A6	8BCF	MOV ECX,EDI		
006118A7	8BCF	MOV ECX,EDI		
006118A8	8BCF	MOV ECX,EDI		
006118A9	8BCF	MOV ECX,EDI		
006118AA	8BCF	MOV ECX,EDI		
006118AB	8BCF	MOV ECX,EDI		
006118AC	8BCF	MOV ECX,EDI		
006118AD	8BCF	MOV ECX,EDI		
006118AE	8BCF	MOV ECX,EDI		
006118AF	8BCF	MOV ECX,EDI		
00611				

y en about muestra que está Licenciado:



Por otro lado tiene lista negra o Blacklist, cualquier nombre de la lista invalidará el registro

00448258	PUSH	ACDSee19.01901H14	ASCII	"Error 200"
00448386	PUSH	ACDSee19.018FFB8C	ASCII	"Unlock code is invalid."
004483DD	PUSH	ACDSee19.01901A0C	ASCII	"\$TEAM"
004483F0	PUSH	ACDSee19.01901A04	ASCII	"\$BEAN"
00448403	PUSH	ACDSee19.019019FC	ASCII	"\$TEAM"
00448416	PUSH	ACDSee19.019019F4	ASCII	"\$BEAN"
00448431	PUSH	ACDSee19.019019EC	ASCII	"\$TITETA"
00448446	PUSH	ACDSee19.019019E4	ASCII	"\$NICOLE"
0044845B	PUSH	ACDSee19.019019DC	ASCII	"\$RUTHFR"
00448470	PUSH	ACDSee19.019019D4	ASCII	"\$LIRANI"
00448485	PUSH	ACDSee19.019019C8	ASCII	"\$NEISTEMHT"
0044849A	PUSH	ACDSee19.019019C0	ASCII	"\$VESSDA"
004484AF	PUSH	ACDSee19.019019B8	ASCII	"\$JOHNEK"
004484C4	PUSH	ACDSee19.019019B0	ASCII	"\$SIKORS"
004484D9	PUSH	ACDSee19.018BDA9C	ASCII	"\$UNIQUE"
004484EE	PUSH	ACDSee19.019019A8	ASCII	"\$HIKEWA"
00448503	PUSH	ACDSee19.019019A0	ASCII	"\$fywhl"
00448518	PUSH	ACDSee19.01901998	ASCII	"\$GATECI"
0044852D	PUSH	ACDSee19.01901990	ASCII	"\$SALDANA"
00448542	PUSH	ACDSee19.01901988	ASCII	"\$UESLA"
00448557	PUSH	ACDSee19.01901980	ASCII	"\$HARISK"
0044856C	PUSH	ACDSee19.01901978	ASCII	"\$PARMI"
00448581	PUSH	ACDSee19.01901970	ASCII	"\$SHIL"
00448596	PUSH	ACDSee19.01901968	ASCII	"\$CLSTICK"
004485AB	PUSH	ACDSee19.01901960	ASCII	"\$SETUNO"
004485C0	PUSH	ACDSee19.01901958	ASCII	"\$GRUP0I"
004485D5	PUSH	ACDSee19.0190194C	ASCII	"\$BioImage"
004485EA	PUSH	ACDSee19.01901944	ASCII	"\$JEFFRE"
00448603	PUSH	ACDSee19.0190193C	ASCII	"\$m3Z2p"
00448616	PUSH	ACDSee19.01901934	ASCII	"\$V7BE"
00448629	PUSH	ACDSee19.0190192C	ASCII	"\$op07"
0044863C	PUSH	ACDSee19.01901934	ASCII	"\$V7BE"
0044864F	PUSH	ACDSee19.01901924	ASCII	"\$0gXc"
00448662	PUSH	ACDSee19.0190191C	ASCII	"\$Dzf7"
00448675	PUSH	ACDSee19.01901914	ASCII	"\$7E3X"
00448688	PUSH	ACDSee19.0190190C	ASCII	"\$c0xN"
0044869B	PUSH	ACDSee19.01901904	ASCII	"\$taqf"
004486AE	PUSH	ACDSee19.019018FC	ASCII	"\$B7on"
004486C1	PUSH	ACDSee19.019018F4	ASCII	"\$ucsR"
004486D4	PUSH	ACDSee19.019018EC	ASCII	"\$o08H"
004486E3	PUSH	ACDSee19.019018E4	ASCII	"\$6p6N"
004486F2	PUSH	ACDSee19.019018DC	ASCII	"\$GEx4"
00448701	PUSH	ACDSee19.019018D4	ASCII	"\$F03m"
00448710	PUSH	ACDSee19.019018CC	ASCII	"\$6zUn"
0044871F	PUSH	ACDSee19.019018C4	ASCII	"\$zhxE"
0044872E	PUSH	ACDSee19.019018BC	ASCII	"\$p6s7"
0044873D	PUSH	ACDSee19.019018B4	ASCII	"\$k3qB"
0044874C	PUSH	ACDSee19.019018AC	ASCII	"\$Mg2o"
00448768	PUSH	ACDSee19.01901890	ASCII	"This code has been revoked!"
0044877F	PUSH	ACDSee19.01901874	ASCII	"This code has been revoked!"
00448789	PUSH	ACDSee19.01901854	ASCII	"0W5sb2NrIgtleSBpoyBpbnZhbGk"
004487B0	PUSH	ACDSee19.01900838	ASCII	"02hpb6thdCBtb2Z0d2FyZSwgSW5jLg=="
004487CF	PUSH	ACDSee19.01901848	ASCII	"U0hF00s="
0044880F	PUSH	ACDSee19.01901824	ASCII	"Unlock code is invalid. (reason=11)"
004488F6	PUSH	ACDSee19.01901818	ASCII	"required"
00448910	PUSH	ACDSee19.01901810	ASCII	"regCode"
0044899A	PUSH	ACDSee19.01901804	ASCII	"Error 201"
004489C2	PUSH	ACDSee19.019017F4	ASCII	"requiresPerm"
004489F6	PUSH	ACDSee19.019017E4	ASCII	"%02d%02d%04d"
00448A08	PUSH	ACDSee19.019017C8	ASCII	"re-parsing expire date..."
00448A20	PUSH	ACDSee19.019017B8	ASCII	"%02d%02d%02d"
00448A57	PUSH	ACDSee19.01900910	ASCII	"%d/%d/%d"
00448A6F	PUSH	ACDSee19.019017A8	ASCII	"TempExpireDate"

Luego veo en el panel que pide además una registración offline pide una activación, pruebo denuevo el mismo método (abro keygen, pego mi validación y vemos donde valida:

00629319	FFD3	CALL EBX	
0062931B	8B35 3C6A0C01	MOV ESI,DWORD PTR DS:[&mfc120u.#4843>]	mfc120u.#4843
00629321	50	PUSH EAX	
00629322	FFD6	CALL ESI	
00629324	8B80 CC000000	MOV EAX,DWORD PTR DS:[EAX+CC]	
0062932A	8B00	MOV EAX,DWORD PTR DS:[EAX]	
0062932C	8B00	MOV EAX,DWORD PTR DS:[EAX]	
0062932E	8B00	MOV ECX,DWORD PTR DS:[EAX]	
00629330	85C9	TEST ECX,ECX	
00629332	✓0F84 A6010000	JE ACDSee19.006294DE	
00629338	8D45 F0	LEA EAX,DWORD PTR SS:[EBP-10]	
0062933B	50	PUSH EAX	
0062933C	E8 3F050100	CALL ACDSee19.00639880	
00629341	84C0	TEST AL,AL	
00629343	✓0F84 95010000	JE ACDSee19.006294DE	fuerzo que no salte
00629349	FF77 20	PUSH DWORD PTR DS:[EDI+20]	
0062934C	FFD3	CALL EBX	
0062934E	50	PUSH EAX	
0062934F	FFD6	CALL ESI	
00629351	8A80 DC000000	MOV AL,BYTE PTR DS:[EAX+DC]	
00629357	84C0	TEST AL,AL	
00629359	✓0F85 AB000000	JNZ ACDSee19.0062940A	
0062935F	FF77 20	PUSH DWORD PTR DS:[EDI+20]	
00629362	FFD3	CALL EBX	
00629364	50	PUSH EAX	
00629365	FFD6	CALL ESI	
00629367	8BC8	MOV ECX,EAX	
00629369	E8 12D3FDFF	CALL ACDSee19.00606680	
0062936E	84C0	TEST AL,AL	
00629370	✓0F85 94000000	JNZ ACDSee19.0062940A	
00629376	8D45 E8	LEA EAX,DWORD PTR SS:[EBP-18]	
00629379	8BCF	MOV ECX,EDI	
0062937B	50	PUSH EAX	
0062937C	E8 4F4C0000	CALL ACDSee19.0062DFD0	
00629381	8BF0	MOV ESI,EAX	
00629383	68 DD4B0000	PUSH 4BDD	
00629388	8D4D EC	LEA ECX,DWORD PTR SS:[EBP-14]	
0062938A	C645 FC 03	MOV BYTE PTR SS:[EBP-41] 3	

Program:

ACDsystem ACDSee v18

Language:

English

License Key:

MD6DHH-S4TYHU-EYPAMH-APBZXU-R8ELOB-AVOG94-RCUSS7

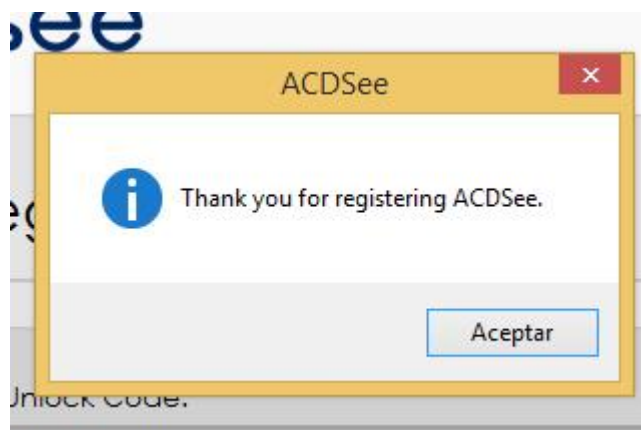
Request Code:

5789RL-FYQMDHMK-LK6C9ARQ-TRXMYBSX-NTYT4ESW-Q47ZFHJ6

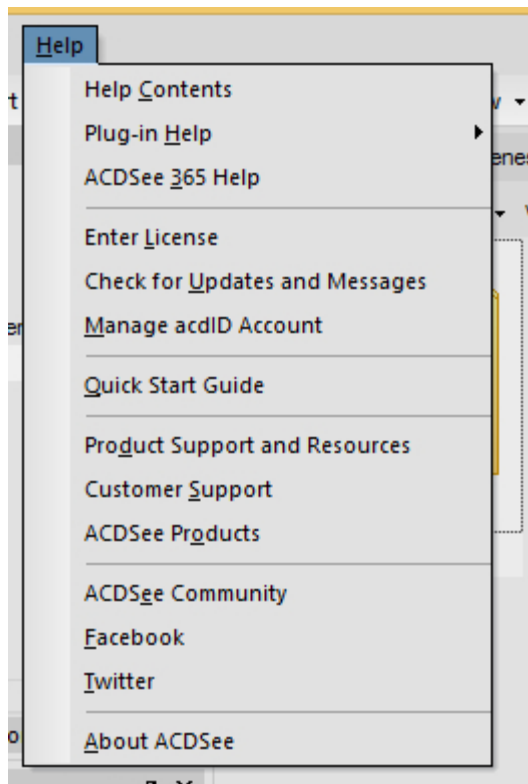
Application Unlock Code:

WV54P-ZTJGTXHN-UYJQR539-LGJFQ2GB-M7KC8HFL-M26UACNV-X4W2R2WB-JHPGD6WS-TTHP696P-XWS8PGZU

Y con el salto forzado tenemos:



Al reiniciar vemos la diferencia que ahora no pide registro offline:



Conclusión:

Si fuera por resumir el escrito, tenemos un programa que ha aumentado la complejidad de algoritmos con el tiempo, pero con los mismos errores del pasado, guarda el serial y muestra registrado sin volver a validar como lo hace cuando te registras con solo 1 salto, buena muestra que debe tener algo más escondido que no somos capaces de ver a simple vista, hay muchas versiones de ACDSEE, este es la inglesa, espero se motiven a revisar de otro tipo de idioma, bueno espero sirva de comienzo, saludos a la lista Apuromafo CLS

