



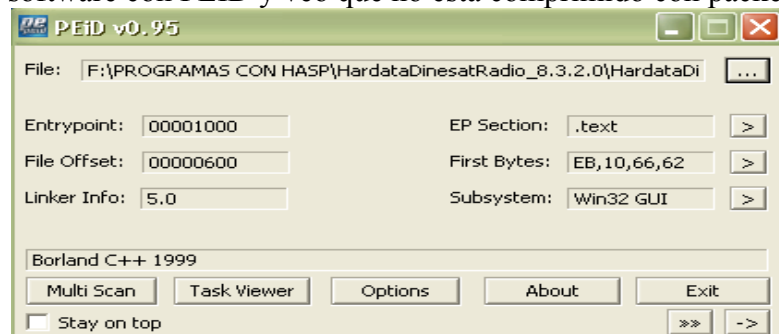
Tute escrito por Master X

Programa:	Hardata Dinesat Radio 8.3.2.0
Descripción:	Códigos
Dificultad:	Baja
Herramientas:	OllyDbg v.1.10, PeID v0.93, RDG packer detector.
Objetivos:	Hacer que acepte Nuestra Licencia Y nuestro Código

Bien este es mi primer tute espero ser entendible, en particular fue el primer moustro que yo le metí mano aun teniendo pocos conocimientos, y a mi gran amigo “LSL De España” te dedico este tute hermano saludos...!!!

Bueno hablándoles un poco de este software, es un automatizador que está en el mercado mundial con una buena demanda en radios del mundo... muy bueno por cierto aun que les faltan muchas mejoras... por ahora es el que está mandando en el mercado de los automatizadores...

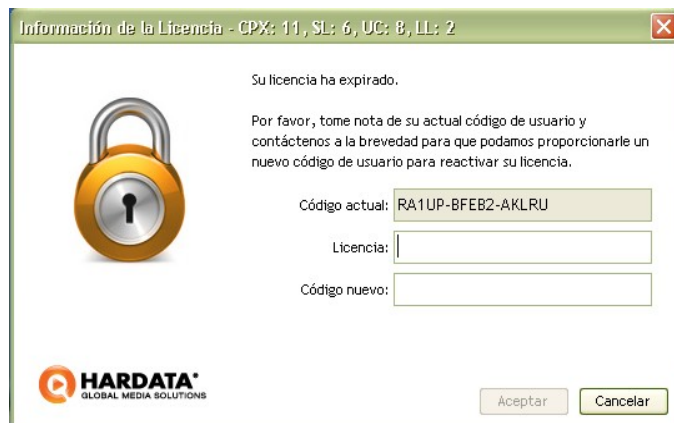
Reviso el software con PEID y veo que no esta comprimido con packer alguno



Bien una vez instalado nos vamos a el icono. Ejecutamos y siguiente cuadro que nos aparecerá. Solicitándonos el cual esta valorado en 500 \$ aproximadamente a la versión NET es la mas costosa desde el punto de vista que ellos lo como yo trabaje en una radio local aprendí a usarlo y me gusto sus funciones en particular la radio donde labore tienen la versión XP. Fue la mas barata que pudieron adquirir.



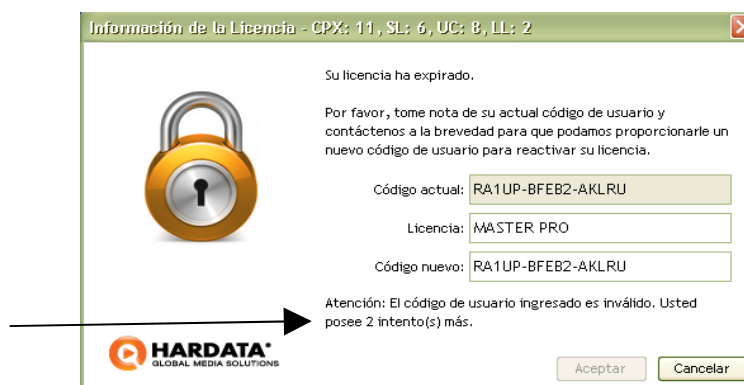
veremos el código la que pondré la tienen. Bien



Un pequeño recuento de este software... ellos tienen tres versiones la cuales son XP, PRO, NET... bien la XP no permite agregar mas emisoras para controlar remotamente o local, la PRO permite agregar las emisoras que deseen a controlar y activan las funciones para enviar y recibir materiales desde internet. NET es full ya que permite Enviar y recibir desde internet a un server del dinesat la cual por ahora no poseo información ya que no se prestan a pasarme una dumper para revisarlo y ver que es lo que esconde este software.

Bien manos a la obra

Veamos colocándole el mismo código que el mismo genera y colocándole nuestro número de licencia cualquiera.



Te dan Solo tres Intentos despues de eso al colocar codigos erroneos te llama una aplicación llamada HDAUX.exe por cierto demasiado ladillosa...

Diciendote que usted a sobre pasado los intentos necesarios. De continuar con este caso puede llegar a invalidarse el producto en la pc.

Bla bla puro drama... bueno metamos nuestro software en olly... un punto muy importante que note y que desde alli podemos tener como guia es que cuando el programa te solicita el codigo te muestra arriba.



Bien buscamos en olly el CPX. Botón derecho search for > all referenced text strings

0049BC96	PUSH 0049BD18	ASCII "CPK: "
0049BCA8	PUSH 0049BD28	ASCII ", "
0049BCBB	PUSH 0049BD28	ASCII ", "
0049BCCB	PUSH 0049BD28	ASCII ", "
0049BD18	ASCII "CPK: ",0	
0049BD28	ASCII " ",0	
0049BE6A	MOV EAX,0049BF6C	ASCII "+OFKHPERH8hLe041GGpGQ7jiUbgGjj8x"
0049BF6C	ASCII "+OFKHPERH8hLe041"	
0049BF7C	ASCII "GGpGQ7jiUbgGjj8x"	
0049BF8C	ASCII 0	
0049BFF3	MOV EDX,0049C168	ASCII "\\Hardata"
0049C168	ASCII "\\Hardata",0	
0049C343	MOV EAX,0049C3D0	ASCII "Zfp1xQJo-1HKer0K5sru-S4sNc8p2Z1zRU5"
0049C352	MOV EAX,0049C464	ASCII "CP3230G04wQ5TcsiETDC0eH8bZkpaByGU1g"
0049C3D0	ASCII "Zfp1xQJo-1HKer0K"	
0049C3E0	ASCII "5sru-S4sNc8p2Z1z"	

Esto es como guía que nos sirve nos vamos un poco mas arriba buscando esta dirección

0049B996	- 8B4D F4	MOV ECX,DWORD PTR SS:[EBP-C]	
0049B999	- 8B55 F8	MOV EDX,DWORD PTR SS:[EBP-8]	
0049B99C	- E8 6B000100	CALL @Hducutils@HDUCCheckNextUC\$qqr17Sy:	
0049B9A1	- 837D EC 00	CMP DWORD PTR SS:[EBP-14],0	
0049B9A5	- 74 0A	JE SHORT 0049B9B1	
0049B9A7	- E8 08B00E00	CALL 005869B4	
0049B9AC	- E9 A1000000	JMP 0049B952	
0049B9B1	- 8B45 F4	MOV EAX,DWORD PTR SS:[EBP-C]	
0049B9B4	- E8 33C80000	CALL @Hdslicutils@HDSLicWriteLicNumber\$	
0049B9B9	- 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	

Bien colocamos breakpoint en esas tres direcciones y damos run f9

0049BF85	- 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
0049BF88	- F640 20 10	TEST BYTE PTR DS:[EAX+20],10	
0049BF8C	- 0F85 73010000	JNZ 0049C135	
0049BFC2	- 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
0049BFC5	- E8 B2260000	CALL @Hdcomplexprotocolformunit@THDComp:	
0049BFCA	- 84C0	TEST AL,AL	
0049BFCC	- 75 66	JNZ SHORT 0049C034	
0049BFCE	- 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
0049BFD1	- 8A80 24040000	MOV AL,BYTE PTR DS:[EAX+424]	
0049BFD7	- 50	PUSH EAX	
0049BFD8	- 8D55 F4	LEA EDX,DWORD PTR SS:[EBP-C]	
0049BFD8	- B8 23000000	MOV EAX,23	
0049BFE0	- E8 FBFC0000	CALL @Hducutils@GetSpecialFolderPath\$qqr	
0049BFE5	- 8B45 F4	MOV EAX,DWORD PTR SS:[EBP-C]	
0049BFE8	- 8D55 F8	LEA EDX,DWORD PTR SS:[EBP-8]	
0049BFEB	- E8 44140E00	CALL 0057D434	
0049BFF0	- 8D45 F8	LEA EAX,DWORD PTR SS:[EBP-8]	
0049BFF3	- BA 68C14900	MOV EDX,0049C168	ASCII "\\Hardata"
0049BFF8	- E8 DBB00E00	CALL 005870D8	
0049BFFD	- 8B45 F8	MOV EAX,DWORD PTR SS:[EBP-8]	

El software va a crear una carpeta llamada Hardata en la siguiente dirección de nuestra PC sin consultarnos allí en esta carpeta va a guardar información de nuestra PC, la fecha el año y la hora en la que estamos que mas adelante explicare el porque dice que expiro. E programa crea la carpeta en esta dirección

Documents and Settings\\All Users\\Datos de programa

Seguimos de hecho por ahora esto no nos interesa nuestro objetivo es que acepte nuestro código. Allí en la imagen ven un JNZ no salta claro esta creando la carpeta. Seguimos con f9 run...

0049B999	- 8B55 F8	MOV EDX,DWORD PTR SS:[EBP-8]	
0049B99C	- E8 6B000100	CALL @Hducutils@HDUCCheckNextUC\$qqr17Sy:	
0049B9A1	- 837D EC 00	CMP DWORD PTR SS:[EBP-14],0	
0049B9A5	- 74 0A	JE SHORT 0049B9B1	
0049B9A7	- E8 08B00E00	CALL 005869B4	
0049B9AC	- E9 A1000000	JMP 0049B952	
0049B9B1	- 8B45 F4	MOV EAX,DWORD PTR SS:[EBP-C]	

OLLY se detuvo. Cambiamos

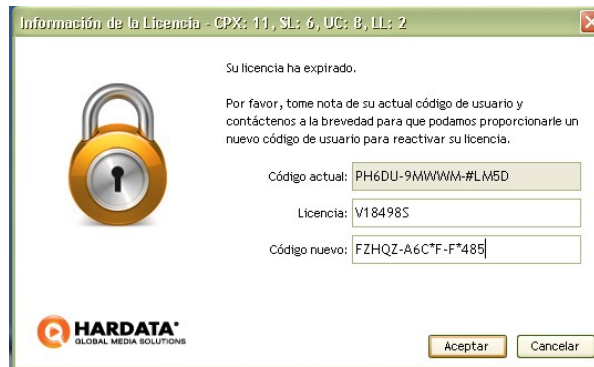
0049B9A1 . 837D EC 00 CMP DWORD PTR SS:[EBP-14],0

0049B9A5 . 74 0A JE SHORT 0049B9B1

0049B9A1 . 837D EC 00 CMP DWORD PTR SS:[EBP-14],1

0049B9A5 . 74 0A JMP SHORT 0049B9B1

Y continuamos con run F9 ya nos aparece el cuadro solicitando la licencia agregamos nuestra licencia cualquiera y le damos aceptar



Olly se detiene aquí vemos que tiene un salto que no se da y que ay -0B negativa los cuales no aceptara la licencia y se nos cerrara la cual obligamos la siguiente dirección a saltar

0049CDD1 | . /0F84 3D020000 JE 0049D014

0049CDD1 | . /0F84 3D020000 JMP 0049D014

0049CDC8	-	E8 3BE90000	CALL @Hducutils@HDUCCheckLicense\$qr17S
0049CDCD	-	837D F4 00	CMP DWORD PTR SS:[EBP-C],0
0049CDD1	~	0F84 3D020000	JE 0049D014
0049CDD7	-	837D F4 F5	CMP DWORD PTR SS:[EBP-C],-0B
0049CDD8	-	74 0A	JE SHORT 0049CDE7
0049CDDD	-	837D F4 FB	CMP DWORD PTR SS:[EBP-C],-5
0049CDE1	~	0F85 FD010000	JNZ 0049CFE4
0049CDE7	>	8D45 90	LEA EAX,DWORD PTR SS:[EBP-70]

Le damos run y agarro nuestra licencia pero no cantemos victoria el software esconde muchos secretos ALLI NOS DICE QUE ESTA EN XP jeje descubrí que cerrando el software y volviéndolo abrir me dice que esta activado en NET. Nos logeamos en usuarios



La clave predeterminada de fabrica es **superman** Bien nos vamos a



Bien por ahora el software funciona de pelos obvio que cada 60 minutos o 120 minutos el hará una comprobación de licencia

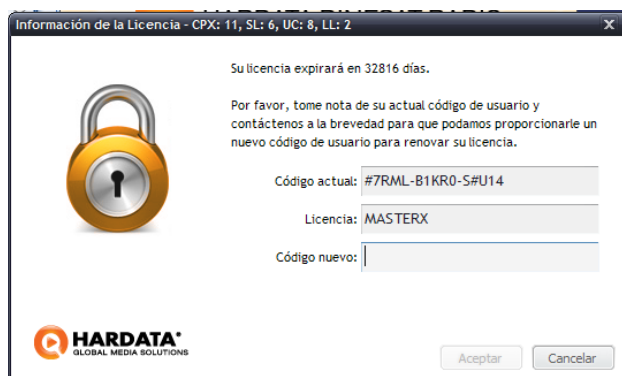


jejeje bueno esta es una licencia que me facilito mi amigo personal. Se la enviaron por un año jejeje pero yo no estoy conforme con esto y quiero mas... ósea que diga mas días en vencerse.

Entonces luego de buscar y buscar y dejarlo por un tiempo y luego seguir y estudiando las calls y los ret logre dar con un punto muy importante jejeje licencias vencidas ahora son vigentes y licencias nuevas jejeje bienvenidas

004AB93A	- 64:8920	MOV DWORD PTR FS:[EAX],ESP	EPL 00200246 <NO,NB,E,BE
004AB93D	- 66:B9 0100	MOV CX,1	ST0 empty 0.0
004AB941	- 66:BA 0100	MOV DX,1	ST1 empty 0.0
004AB945	- 66:B8 DA07	MOV AX,7DA	ST2 empty 0.0
004AB949	- E8 EA370D00	CALL 0057F138	ST3 empty 0.0
004AB94E	- DD1B	FSTP QWORD PTR DS:[EBX]	ST4 empty 0.0
004AB950	- 9B	WAIT	ST5 empty 0.0
004AB951	- C706 FFFFFFFF	MOV DWORD PTR DS:[ESI],-1	ST6 empty 7.205759403792
			ST7 empty 6.075161636560

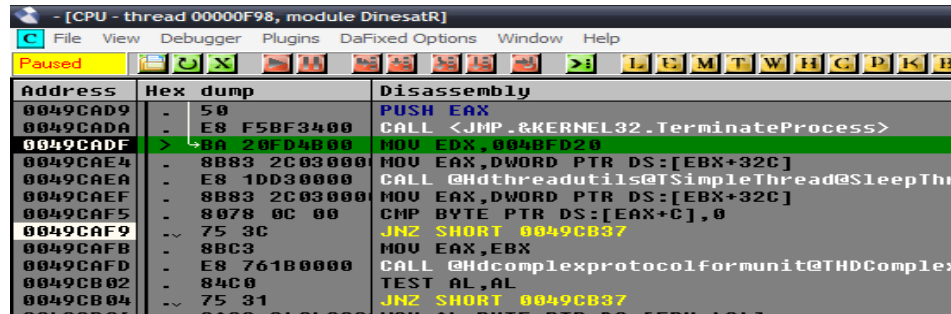
7DA HEX CONVERTIDO EN DECIMALES ES 2010. Claro con razón el software te dice que la licencia vence... entonces como yo quiero que se venza en el en el 2100 abro mi calculadora de Windows y le pongo 2100 en decimales y luego lo paso a hexadecimales para que me de 833 y cambio el MOV AX, 7DA POR EL MOV AX,833 YYY....



Y ahora mi licencia es de 32816 días restantes jeje
Muy bien para evitar que se cierre a los 83 minutos aproximadamente le colocamos un salto EN LA DIGUIENTE DIRECCION 0049CAF9

POR EN LA DIRECCION 0049CADF esta MOV EDX, 004BFD20

Que transformado en decimales da $4980000 / 1000 = 4890 / 60 = 83$ minutos esto es un cronometro que el tiene de comprobación de licencia y si no salta nos lanza un mensaje y se nos cierra entonces la dirección 0049CAF9 JNZ obligarla con un salto JMP.



Address	Hex	dump	Disassembly
0049CAD9	-	50	PUSH EAX
0049CADA	-	E8 F5BF3400	CALL <JMP.&KERNEL32.TerminateProcess>
0049CADE	>	8B 20FD4000	MOV EDX, 004BFD20
0049CAE4	-	8B83 2C030000	MOV EAX, DWORD PTR DS:[EBX+32C]
0049CAEA	-	E8 1DD30000	CALL @Hdthreadutils@SimpleThread@SleepTh
0049CAEF	-	8B83 2C030000	MOV EAX, DWORD PTR DS:[EBX+32C]
0049CAF5	-	8078 0C 00	CMP BYTE PTR DS:[EAX+C], 0
0049CAF9	-	75 3C	JNZ SHORT 0049CB37
0049CAFB	-	8BC3	MOV EAX, EBX
0049CAFD	-	E8 761B0000	CALL @Hdcomplexprotocolformunit@THDComple
0049CB02	-	84C0	TEST AL, AL
0049CB04	-	75 31	JNZ SHORT 0049CB37
0049CB06	-	8083 24030000	MOV AL, BYTE PTR DS:[EBX+424]

Objetivo cumplido gracias a mi querido amigo LSL por tu ayuda... al principio fue crakeado pero sin licencias y yo por curiosidad lo quería con licencia logrando mi objetivo... ahora voy a ver si se le puede hacer un keygen seria calidad hacerlo si alguien se propone puede lograrlo y creo que así funcionaria ya que el toma información de la BIOS y de todo el sistema en general y de allí es que genera un código para posteriormente enviarlo al departamento de códigos y ellos te generen uno nuevo ya activado... todo es cuestión de proponerse y se lograr saludos a todos y espero ser entendible en mi primer tute que por cierto lo tengo desde hace tiempo pero por problemas de tiempo no logre hacerlo para compartirlo con todos ustedes. En fin si se me pasa algo los que tienen conocimientos pueden arreglarlo muy cómodamente o preguntarme ok saludos.

MASTERX “ QUE DIVERTIDO ES CRAKEAR” ;)