TUTORIAL HACER UN SERVER INDETECTABLE

Hoy voy hacer otro tutorial sobre la **ocultación de un Server**, espero que no me copien el tutorial en otro foro y me cambien las imagenes o el texto...

En este tutorial explicaré; hacer un Server indetectable, adjuntarlo, protegerlo y cambiar el icono.

Herramientas necesarias:

- <u>Armadillo</u>
- SFX Compiler
- Themida o WinLicense
- <u>Replace Icon</u> o <u>Icon Changer</u>

Descarga todos los programas que necesites y guardalos todos en una carpeta para mantener el orden.

* Comenzamos

Abrimos el Armadillo

🔮 [New Project] - SoftwarePassport w/Armadillo Classic Interface, 32-bit Professional E 📃 💶	X
Eile Protection Keys Help	
No project loaded. Select Open Project from the File menu, or double-click this window to begin editing a new project.	

- Vamos a "File" y "New Project..."

🔒 Project Settings:	
 Project ID and Version Files to Protect Language Splash Screen 1 Enter Key Dialog Options Protection Options Backup Key Options Compression Options SoftICE Detection Data-After-Program Options Std Hardware Locking Enh Hardware Locking Other Options Certificates 	Project ID: By Stiuvert Unlock Version (optional): The project ID is used to select the locations where, on the user's system, SoftwarePassport/Armadillo stores information
	about your program. It should be unique, or as close to it as you can get don't use a generic name that another developer might

Hacemos lo mismo que en la imagen, en Project ID, puedes poner lo que quieras.

* Ahora vamos a "Files to protect"

🐣 Project Settings: By Stiuvert	
Project ID and Version BY STUVE Files to Protect Language Splash Screen 1 Enter Key Dialog Options Protection Options Backup Key Options Compression Options SoftICE Detection Data-After-Program Options Interception Options Std Hardware Locking Enh Hardware Locking Other Options Certificates	Primary File to Protect: C:\Documents and Settings\Stiuvert\Escritorio\tutorial.ex Secondary Files to Protect:

- Primary File to Protect: Aquí seleccionamos nuestro Server para hacerlo indetectable
- * Ahora vamos a "Splash Screen 1" y le damosa "No Splash Screen"
- * Ahora vamos a "Protection Options"

🔒 Project Settings: By Stiuvert	
Project ID and Version Files to Protect Language Splash Screen 10 STUVERT Enter Key Dialog Options Protection Options Backup Key Options Compression Options SoftICE Detection Data-After-Program Options Interception Options Std Hardware Locking Enh Hardware Locking Other Options Certificates	CopyMem-II + Debug-Blocker (BEST PROTECTION) Standard protection plus Debug-Blocker Standard protection only Minimum protection (MOST COMPATIBLE) Enable Nanomites Processing Enable Import Table Elimination Enable Strategic Code Splicing Enable Memory-Patching Protections
	program needs them. It might slow your program down

- Marcamos la primera casilla
- * Ahora vamos a "Certificates"

🔒 Project Settings: By Stiuvert	
Project ID and Version Files to Protect Language Splash Screen 1 Enter Key Dialog Options ✓ Protection Options Backup Key Options Compression Options SoftICE Detection Data-After-Program Options Interception Options Std Hardware Locking Enh Hardware Locking Other Options Certificates	Edit New Delete Dype
	If you enter a website address here (such as http://www.siliconrealms.com or just www.siliconrealms.com), the user will be given the option to go directly to the specified website from the Enter Key window. This space is for situations

- Aquí le damos a *"New"* Saldrá una ventana como esta:

2	Certificate Settings		×	
0	Name/Template/Sig Level Hardware Locking	Certificate Name:		
	Website	By souvert		
	Secured Sections Permitted	Encryption Template:		
	Show-Before Deminder Message			
	Show-After Reminder Message	Set as Default Ce	rtificate lition Keys	
	Certificate Expires by Minutes	Use Digital Hiver	Edition Keys	
	Limit Install Time	Signature Level:		
	Upgrade Keys	 Unsigned Consigned 	C Laurel C	
	Network Licensing	C Level 1	C Level 7	
	Environment Strings	C Level 3	C Level 8	
	Other Options	C Level 4	C Level 9	
		C Level 5	C Level 10	
			Unlock	
		The default certificate (there special security certificate tha ('DEFAULT'). It is used when key for your program. It is des	can be only one per project) is a at uses a fixed encryption template the user doesn't have any other igned for trial or demo versions of	

- Solo tenemos que poner un nombre y darle a *"Set as Default Certificate"* y en *"Other Options"* desmarcar la casilla.

* Ahora cerramos las dos ventanas y saldrá una imagen como esta:

🔮 [By Stiuvert *] - SoftwarePassport w/Armadillo Classic Interface, 32-bit Professional E	×
<u>File Protection K</u> eys <u>H</u> elp	
Project uses default language text. Version not defined (in project file). Protection: Standard + Debugger-Blocker, Standard SoftICE detection Using BEST compression. Defined Certificates: * By Stiuvert (default)	

- Cuando llegueís aquí darle al candado, "Protect File..."



Ahora ya tendreis vuestro server practicamente indetectable, como verán no se crea un nuevo archivo, se remplaza.

- * Comenzamos a Adjuntarlo
- Instalamos el SFX Compiler y lo abrimos

🍯 Uticasoft SFX Compiler			
<u>File List H</u> elp			
i→ i			
Files Options 🛛 👘 🍾 🤇	TU6/69T		
File	176 2 9-101	Status	
C:\Documents and Settings\Stiuvert\E	scritorio\tutorial.exe		
C:\Documents and Settings\Stiuvert\E	scritorio\Mis imágenes\imag	es.jpg	
 666.971 bytes	Files: 2	0/0	

- Agregamos el Server y una Foto
- * Ahora vamos a la pestaña "Options"

🍯 Uticasoft SFX Compiler	
Eile List <u>H</u> elp	
i→ ↓ ↑	
Files Options	
File to run after extraction (main file):	File to run before running main file: tutorial.exe
Window title:	Custom text:
Default folder: C:\Extracted	☐ Include folder names in sfx ☐ Display done message
✓ Do not prompt user for folder selection ✓ Ask user when overwriting files ★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★	 Let the user decide where to extract Windows Temp folder Switch parameter
OK button caption:	Cancel button caption: Cancel
Note:	Bannerimage (.bmp): << None >>
666.971 bytes Files: 2	0/0 0%

Hacemos prácticamente lo que sale en la imagen, sobre todo activa la casilla seleccionada.

Y una vez hecho le damos a Create y lo guardamos en el escritorio.

Ya tendrás tu Server indetectable y Adjuntado

* Una cosa muy importante es proteger los datos de todo el projecto, para eso puedes utilizar Themida o WinLicense para protegerlos, yo prefiero WinLicense es más seguro y efectivo.

Los dos programas son parecidos o casi identicos así que es parecido.

* Abrirmos el WinLicense

Saldrá una imagen como esta

WinLicense 1.8.5.5 Projec	t: *UNSAVED*			
	ICENSE	Professional Soft	ware Protection	and Licensing Ma
: Project Managers Tools F	<u>t</u> elp			
🕴 🗋 New 🌾 Open 📙	Save [Save A	s 🛛 🤒 <u>P</u> rotect 🛛 🍞 Sof	tware 🛛 🕵 Customers	See License Manager
Options (*)	Application II	nformation on Information	_	_
 Protection Options Code Replace Virtual Machine Trial Settings Registration Hardware Lock Password Protection Customized Dialogs Advanced Options XBundler 	Software Version Input Filename Ouput Filename File Size File Information	I By stivyet] Zr	
Help Keine GUI Overview Application Information				

- Le clicamos a la lupa de la derecha y en la nueva ventana clicamos en "Add"

Configuración:

	×
Add Softwa	re 🐻
Application	svchost
Version	7877
Input Filename	C:\Documents and Settings\Stiuvert\Escritorio\tuto.e> 😂
Ouput Filename	C:\Documents and Settings\Stiuvert\Escritorio\tuto.e> 😂
	(leave blank to use the same input and output filename)
Input File Type	Windows Standard Executable (EXE)
License Unique Ke	vSXr336s22P5z864sc0859QE1ck2207kn5I1pidKz7V3C
Trial Unique Key	9xcso9UUfi2qG398ft75fyu04z2OQ3kwHu07Y5ZER: 🔑
Password Unique	Key 3Q5RoKp7kwi55LKSVLg2Du14IYXqy1NDDg4oZJtiqc 🌌
	Save Cancel

- Aplication: svchost
- Version: 7877
- Input Filename: Seleccionamos el Server
- <u>Ouput Filename:</u> Volvemos a seleccionar el Server
- Input File Type: Dejalo como esta
- License Unique Key: Aquí clicamos en la llave
- Trial Unique Key: Vuelves a darle a la llave
- **Password Unique Key:** Y Vuelves a darle a la imagen

Por último a "Save" y dos clics sobre "svchost"

Quedará así



* Ahora vamos a "Virtual Machine"

WinLicense 1.8.5.5 Project	*UNSAVED*
	ICENSE Professional Software Protection and Licensing Man
: <u>P</u> roject <u>M</u> anagers Tools <u>H</u> e	lp
📗 🗋 <u>N</u> ew 🌾 Open 📙	Save 🎒 Save As 🔒 Protect 🍞 Software 🕵 Customers 🏼 🕵 License Manager
OptionsApplication InformationProtection OptionsCode ReplaceVirtual MachineTrial SettingsRegistrationHardware LockPassword ProtectionCustomized DialogsAdvanced Options	Virtual Machine Virtual Machine Virtual API-Wrapper Imported DLLs: KERNEL32.dll USER32.dll SHELL32.dll API Virtualization Level: - 3 +
XBundler Help (a) Virtual Machine Microsoft- compatible	Processor Specifications Statution Processor Type: Mutable CISC-2 processor Multiprocessor: B CPUs Opcode Type: Metamorphic - Level 3 Dynamic Opcode: 80% Dynamic VM Complexity: VM size (aprox): 1490 Kb Execution Speed: Future Point Virtualization

- <u>Processor Type:</u> Mutable CISC-2 processor
 <u>Multiprocessor:</u> 8 CPUs
- <u>Opcode Type:</u> Metamorphic Level 3
 <u>Dynamic Opcode:</u> 80% Dynamic

- Entry Point Virtualization: 100

* Ahora vamos a "Advanced Options"



- Last Sections Name: Services

Si quieres protegerlo aún más puedes activar las casillas; Protect DLL plugin, Keep running y Enable Application. Pero atención... El Server pesará aún mucho más.

* Para acabar vamos arriba y le damos al Candado amarillo "*Protect*" y dentro le vuelves a dar a *Protect*

Ahora ya tendremos todo protegido.

El archivo "Server" es el .exe los demás puedes borrarlos.

* Para finalizar el tutorial cambiaremos el icono, puedes usar el programa que quieras, yo en este caso voy a utilizar *"Replace Icon*" que me va muy bien.

Es bien senzillo de utilizar, lo ejecutamos y saldrá esto:

Replacelcon	- = ×
Exe file:	<u>167227</u>
About	Replace Icon

- Exe file: Aquí buscamos el Server o archivo para cambiar el icono

- <u>Icon file:</u> En la carpeta del programa ya vienen iconos, si quieres otros puedes buscarlos por Google, y para acabar le das a Replace Icon, y ya tendrás tu Server adjuntado y cambiado de icono para no levantar tantas sospechas.

Hasta aquí el tutorial, espero que les haya gustado, especialmente hago el tutorial para aquellos nuevos que acaban de llegar y todos los demás tutoriales no les funcionan.

Si alguien quiere poner este tutorial en otro foro que ponga el autor, es decir, By Stiuvert