



BY ANTRAX ANTRAX@E-RØØT.NET



Bueno, ahora llega la parte en la que comenzaremos la configuración del troyano que queramos utilizar.

Es bueno tener un tipo de idea de los troyanos existentes, de cuales son los que más se utilizan, etc.

En mi opinión personal, el mejor es el Bifrost. Siempre es bueno tener la ultima versión. En el caso del Bifrost es la 1.2.1D que es la versión privada pero que ya es publica.

Tambien existen otros muy buenos como lo son el Poison Ivy, Spy-Net, Nuclear RAT, y otros.

Es bueno saber primero que nada lo que deseamos hacer con la pc que queramos infectar, para tener una idea de lo que vamos a hacer con el troyano.

Como por ejemplo hay troyanos como el Nuclear RAT que tiene la opción de explorar los discos que están en una Red LAN.

Pasare a explicar como se configura alguno de los troyanos mas conocidos en la red.

Comenzare por el Bifrost.



Bueno, lo que debemos hacer es abrir el cliente de el Bifrost. Para esta demostración utilizare la versión 1.2.1D.



Abrimos el cliente, que es el que esta en rojo.

La carpeta Computers es en donde se almacenaran los archivos que descarguemos de la pc que hayamos infectado, y el server es el que les enseñare a editar para que lo envíen a quien quieran infectar.

Terms An	d Condit	ions	EULA
----------	----------	------	------

Bifrost v1.2 DISCLAIMER THIS DISCLAIMER REPRESENTS A CONTRACT BETWEEN YOU AND CHASENET. AFTER READING, YOU WILL BE ASKED TO ACCEPT THIS AGREEMENT AND CONTINUE TO USE THE SOFTWARE, OR, IF YOU DO NOT WISH TO ACCEPT THIS AGREEMENT, TO EXIT, IN WHICH CASE YOU WILL NOT BE ABLE TO USE, INSTALL OR OPERATE THE SOFTWARE. BY USING THIS SOFTWARE YOU ACCEPT ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT. Ξ This disclaimer is a legal agreement between you (henceforth referred to as "the User") and ChaseNET, regarding the software application Bifrost (henceforth referred to as "the Software") which you have downloaded, or otherwise obtained through other resources or media such as CD-ROMs, floppy disks, or through a network in object code form or other related services. By accessing, downloading, storing, loading, installing, executing, displaying, copying the Software into the memory of a computer or otherwise benefiting from using the functionality of the Software in accordance with the documentation, you agree to be bound by the terms of this agreement. If you do not agree to the terms and conditions of this Agreement, ChaseNET is unwilling to grant usage of the Software to you. In such event, you may not Operate or use the Software in any way. BY CLICKING THE "LAGREE" BUTTON IT IS INTERPRETED AS A SYMBOL OF YOUR SIGNATURE AND YOU ARE THEREBY CONSENTING TO BE BOUND BY THIS AGREEMENT AND AGREE THAT IT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT. CLICK THE EXIT BUTTON REMOVE THE SOFTWARE FROM YOUR COMPUTER. By running this Software, you are consenting to be bound by this agreement. Upon termination of this agreement you will no longer be authorized to operate or use the Software in any way. The Software will not run on your computer unless or until you accept the terms of this agreement. ANTRAX Proprietary Ownership Rights. You agree that the Software and any associated ideas, methods of operation, documentation and other information contained in the Software, are intellectual properties of ChaseNET. You acknowledge that the source code for the Software is proprietary to ChaseNET. You agree not to modify, adapt, translate, reverse engineer, decompile, disassemble or otherwise attempt to discover the source code of the Software. You may not remove any proprietary notices or labels on the Software. 2. Usage. ChaseNET grants you permission to store, load, install and execute the specified version of the Software on an unlimited number of computers, workstations, personal digital assistants, mobile phones, hand-held devices, or other electronic devices for which the software was designed provided you are in compliance with the terms and conditions set out in this agreement. By accepting this agreement, you agree not to use the Software to: I Agree I Decline Do not show this in the future.

La primera vez que abrimos el troyano aparecerá esto, tildamos el cuadrito en donde dice "Do not show this in the future" para que no vuelva a aparecer y hacemos click en I Agree.

Seguido a esto, se abrirá el cliente.

🔄 Bifro	🔄 Bifrost v1.2d 🛛 0 users connected 💦 🗖 🔀									
Assigne	d Name	IP	Comput	er/User Name	Ver	. с	Е	ldle	Ping	Active Window
A	NTR	AX								
•				III						•
Options	Builder	About	Update	Upload Extensi	on Lister	ing on	port 8	31,80,80	080	

Damos click en Options como muestra la imagen.

Settings 🔀
Ports (0 for not in use): 81 80 8080 Password: ANTRAX Name of extension after upload: addons.dat
 Try to forward port with UPnP Msn style notification Check password for incoming connections Compress file transfer Method to determine flag Use computer country settings Use keyboard language
File manager File manager Image: Delete thumbnails when closing file manager Image: DK Image: DK

Aquí solo ponemos los puertos que tengamos abiertos en nuestro Router. En caso de no tenerlos deberas buscar en google como abrirlo o pidiendo ayuda en algún foro.

En el password deben poner alguna contraseña que deseen.

Una vez completado todo esto, dar click en OK.

🔄 Bifrost v1.2d 🛛 0 users connected 💦 🗖 🗖 🔀										
Assigne	d Name	IP	Compu	ter/User Name	Ver	C	Е	ldle	Ping	Active Window
	A1	NTRZ	X							
•				III						>
Options	Builder	About	Update	Upload Extension	Listening	; on j	oort 8	31,80,80	080	

Ahora vamos al botón Builder para editar el servidor.

Builder	
Connection Installation Stealth	
Connection 5	Connect Through Socks 4
	Enable connection through proxy Port:
Dynamic DNS/IP : w300.no-ip.info 1	Dynamic DNS/IP : 1080
2 Add dns/IP	Add dns/IP Port
Delete w300.no-ip.info	Delete
Bassword: ANTRAX	
4Port: 81	
	ANTRAX
Up	
Down	
Export Import server.exe	Build Cancel

Seguir los pasos en orden para evitar equivocarse.

1) Escribir la no-ip que crearon para ustedes

2) Click en Add para que aparezca en la lista como muestra la imagen

3) Escribir la misma password que escribieron en la configuración del cliente

- 4) Escribir el mismo puerto que escribieron en el cliente. Solo escribir el primero
- 5) Click en la pestaña Installation

Builder	×
Connection Installation Steelth	
File Installation	Extension
Filename when installed: server.exe	Include extension pack addons.dat
Directory to instatio: wind	- Keylogge
C Program files directory	✓ Offline keylogger logg.dat
• System directory 2	Exclude Shift and Ctrl
C Windows directory	Exclude Backspace
Autostart	_ Injection
Autostart at reboot Random Key	6
Registry start key: {64762713-9857-75F3-166A-	Process name: msnmsgr.exe
Mutex name: 3 wind	7 Assigned name: Victima
Registry key: 4 wind 8	Persistant server
ANTRAX	
Export Import server.exe	Build Cancel

- 1) Escribimos un nombre para que el server se oculte en dicho directorio.
- 2) Tildamos en que parte del sistema queremos que se oculte el server. En este caso puse la carpeta de System
- 3) En mutex name se lo cambiamos por alguno que pase desapercibido.
- 4) Lo mismo que en el 3
- 5) Activamos el Offline Keylogger
- 6) Activamos la opción para que se inyecte en algún proceso.
- 7) Si quieren le pueden poner algún nombre al server para cuando infecten a alguien sepan diferenciarla.
- Activamos esta opción que es fundamental para que no se pierdan las victimas cuando se reinicia la pc
- 9) Pasamos a la siguiente y ultima pestaña de configuración.

Builder	
Connection Installation Stealth	
Connection Installation Stealth Stealth Mode Visible mode Cautious mode Agressive mode Agressive mode Agressive mode Server File Stealth Set attribute hidden Set attribute hidden Set older file date Melt server Melt server	 Delayed Connection No delay Delay to next reboot Delay 0 Days, 0 Hours, 0 Min Rootkit ✓ Hide Process
Export Import server.exe	Build Cancel

Aquí es todo un poco mas personalizado. Esto trata de cuando queremos que comience a actuar el servidor, de que modo queremos que actue, etc

Yo tilde esas opciones por que son las que mas me gustan. En especial Hide Process para ocultar el proceso en el cual se inyecto el servidor.

Una vez hecho todo esto, le damos click en Build y saldrá algo como esto:

Abrir	_	_	_		-	-		2 🗵
Buscar en:	🚚 dinno			•	G	9.	•	
Documentos recientes	📕 Compute 🎒 Bifrost.e: 🌒 server.e:	rs xe xe						
Escritorio	AN	TRAX						
() Mis documentos								
Mi PC								
	Nombre:	server.exe					-	Abrir
Mis sitios de red	Tipo:	All Files (*.*)					•	Cancelar

Seleccionamos el Server.exe y damos click en Abrir.

Si muestra un cartel como el siguiente, es por que todo salió bien



Si aparece algún tipo de error, es por que debes quitar el antivirus o desactivarlo.

Una vez hecho esto, ya tendremos el servidor listo para enviarlo.





Para este manual usare la versión privada mas reciente del Poison Ivy.

Abrimos el cliente, y veremos algo como lo siguiente:

🧏 Po	Reison Ivy								
ID	WAN	LAN	Computer	User Name	Acc.T	OS	CPU	RAM	
	ANTRAX								
•								•	
Version	2.1.4 Connection	s/Build/Settings/	(Stats (About /			Port: 81	Connec	tions: 0	

Ahora nos dirijimos a Settings para configurar el cliente.

🧏 Poison Ivy	
Settings	
	81 1 ANTRAX 60 ANTRAX
I Enable Caching	3 🔹 Window name Time stamp Key name
Close to system tray	Minimize to system tray
☑ Balloontip notification	✓ Autosave passwords
Enable docking	Prompt for password on new connection English ▼ 1000 ms ▼ Save
Version 2.1.4 Connections Build	Settings/Stats/About/ Port: 81 Connections: 0

Para la configuración de el cliente es muy fácil al igual que la del Bifrost. 1) Escribimos el puerto que tengamos abierto y una password.

2) Damos click en Save

3) Pasamos a Build para configurar el servidor

🧏 Poison Ivy	
New Server	
Connection	
DNS/Port: w300.no-ip.info:81,	Add 1
ID: Victima 2	
Password: ANTRAX 3	
Socks4	
DNS/Port:	Add
✓ Startup	
Active-X Key: {1F878833-1B24-2304-0706-08	30 Random
Installation	
Filename: srv.exe 4	
Copy file to:	
5 💿 System Folder ANTRA	X
O Windows Folder	
Custom:	
□ Melt	
⊠ Keylogger 6	
	Build
Version 2.1.4 Connections Build Settings (Stats /	About Port: 81 Connections: 0

- 1) Damos click en Add y ponemos nuestra no-ip seguida de nuestro puerto abierto.
- 2) Si quieren pueden ponerle un nombre especifico para que diferencien a la pc que infecten
- 3) Escriban la misma password que escribieron en el cliente
- 4) Pueden darle un nombre al servidor
- 5) Eligen en donde quieren que se instale el server, en este caso en System
- 6) Activamos el keylogger y si quieren pueden activar en Melt para que el servidor se derrita o desaparezca al ser ejecutado
- 7) Si quieren pueden ponerle un icono
- 8) Por ultimo click en Build

Guardar como		2 🛛
Guardar en:	III PI 2.1.4 (private)	-
Documentos recientes	<mark>↓</mark> Download <mark>↓</mark> Images ♥ PI 2.1.4.exe	
Escritorio		
Mis documentos	x	
Mi PC	Nombre: server.exe	Guardar
Mis sitios de red	Tipo: Executables (*.exe)	Cancelar

Escribimos el nombre, en este caso Server.exe. Atencion! No olvidar la extensión *.exe por que es fundamental! Lo que pueden cambiar es el nombre y ponerle el que quieran.

Una vez hecho click en Guardar, tendrán el server creado y listo para ser utilizado.



Este troyano es el mas reciente, pero lamentablemente el creador no seguirá con el proyecto.

De todas formas es un excelente troyano y a continuación mostrare como se configura. Esta es la ultima versión 1.8.

Abrimos el cliente:



Al abrirlo, verán algo como esto:



Son dos opciones de cómo quieren enviar los plugins.

Recomiendo por comodidad dejar la opción que esta puesta y darle a OK

Esto los llevara directamente al cliente:

🥝 Spy-Net [RA	🕘 Spy-Net [RAT] 1.8 Servidores online: 0 📃 🗌 🔀								
Identificação	WAN IP / LAN IP	Computador/Usuário	Sistema Operacional	Memória R	Versão	C F	Primeira Execu	Ρ	
ANT	RAX								
								-	
•	۰ III >								
Opções Novo	Opções Novo Info. Atualizar Enviar Plugin IV Enviar plugin ao conectar Aguardando conexões nas portas: 81 0 0								

No se asusten, el creador es portugués, ahora les enseño a como pasarlo a español.

Damos click en el botón marcado en rojo, que supuestamente dice Opciones.



- 1) Click en Idioma
- 2) Seleccionan Español.ini
- 3) Click en Salvar

Listo, ya lo tenemos en español, ahora será mas fácil trabajarlo.

🧿 Spy-Net [R	🖉 Spy-Net [RAT] 1.8 Servidores online: 0 📃 🗖 🔀								
Identificación	IP WAN 7 LAN IP	Ordenador / usuario	Sistema Operativo	RAM	Versión	С	Ρ	Primera ejecución	Ρ
A	NTRAX								
•		III							•
Opciones Nuev	o Info. Actualiza	ar Enviar Plugin 🗹 Envi	ar plugin al conectarse	Esperando	conexione	s en l	los p	uertos: 81 0 0	

Vamos nuevamente a opciones. Para configurar el cliente.

Ventana de Opciones			×
Opciones	Conexión]
Onexión	Contraseña de la cone:	xión	
	ANTRAX		🗌 Ocultar Contraseña
 Notificación 			
Oldioma	Puertos de conexión	81	80 8080
Ť			
Columnas visibles	ANTEAV		Guardar Salir
L	ANTRAA		

Ponemos una contraseña que queramos, y escribimos los puertos que tengamos abiertos en nuestro Router.

Una vez hecho vamos a Guardar.

🙆 Spy-Net [RAT] 1.8 Servidores online: 0 📃 🗖 🔀								
Identificación	IP WAN 7 LAN IP	Ordenador / usuario	Sistema Operativo	RAM	Versión	С	P Primera ejecución	Р
ZN	TDAV							
	INAN							
•	< W							
Opciones Nuevo	Info. Actualiza	r Enviar Plugin 🗹 Envia	ar plugin al conectarse	Esperando	conexiones	s en lo	s puertos: 81 80 8080	

Ahora vamos a Nuevo para crear el servidor.

Crear nuevo server		×
Configuración	Opciones básicas w300.no-ip.info	Identificación:
Arranque	w300.no-ip.info	Vîtima Contraseña para la conexión
O Maquinas virtuales	ANTRAX	ANTRAX Mostrar la contra:
OMostrar mensajes OLista Negra		Puerto de conexión 81 Pausa entre conexiones
O Descripción general		2 Segundos
En este ámbito, se encuentran opciones y una breve descrip	toda la información necesaria para crear el servidor. F ción de la opción seleccionada aparecerá aquí.	Pase el ratón sobre una serie de

Lo que debemos hacer aquí, es agregar nuestra no-ip en la lista.

Si quieren en donde dice Victima pueden cambiarle el nombre para identificar a la pc a la cual infectaran

En la contraseña, deben poner la misma que en la configuración del cliente.

Y por ultimo ponen el puerto que tengan abierto, recuerda que debe ser el primero que colocaste en el cliente.

Pasamos a la segunda opción:

Crear nuevo server	_	×
Configuración	Instalación del servidor	
Opciones básicas	Instalar el servidor	
 Instalación del servido 	Directorio de instalación	Nombre del archivo
○ Arranque	Sistema 👻	Aplicación (*. exe)
🔿 Añadir archivo	wind	wind
◯ Maquinas virtuales		
Opciones extra		ANTRAX
◯ Mostrar mensajes		
🔿 Lista Negra		
O Descripción general		
◯ Crear servidor		
Establecer la dirección IP, puer	to de conexión, la contraseña y la pa	ausa entre intentos de conexión.

Aca es en donde se instalara el servidor en la pc que infectamos. En este caso se instalara con el nombre en una carpeta que se llama wind dentro de system, y el server se llamara wind.exe

Pasamos a la siguiente

Configuración Opciones básicas Instalación del servidc Arranque Afadia arabita	Arranque MKEY_LOCAL_ wind	_MACHINE\SOFTVVARE\Microsoft\\Vindows\CurrentVersio	n∖Run
Maquinas virtuales Opciones extra Mostrar mensajes		NT_USER\Software\Microsoft\Windows\CurrentVersion\R TRAX	un
U Lista Negra			
O Lista Negra	Active Setup	{T5TBB77L-4678-0MKC-421Q-14416031DYU6}	+
Descripción general Crear servidor	Active Setup	{T5TBB77L-4678-0MKC-421Q-14416031DYU6} Spy-Net	+

Aca es la información que le damos al server para que se guarde en el inicio de la pc. En otras palabras queda guardado en el registro para que el servidor arranque junto cuando se enciende la pc.

Ahora pasamos a la opción Maquinas Virtuales.

Crear nuevo server	
Configuración Opciones básicas Instalación del servidc Arranque Añadir archivo Maquinas virtuales Opciones extra Mostrar mensajes Lista Negra Descripción general Crear servidor	Maquinas virtuales Lucha Virtual PC Lucha VMWare Lucha VirtualBox Trate de evitar los siguientes métodos: 01 - Sandboxie 02 - ThreatExpert 03 - Anubis Anutreax 04 - CVVSandbox 05 - JoeBox 06 - Norman Sandbox

En este ámbito, se encuentran toda la información necesaria para crear el servidor. Pase el ratón sobre una serie de opciones y una breve descripción de la opción seleccionada aparecerá aquí. Aquí personalmente tildo todo, esto es para evitar ser descubiertos. En caso de que el server sea analizado, no puedan encontrarle nada malo.

Crear nuevo server		×
Configuración Opciones básicas Instalación del servidc Arranque Añadir archivo Maquinas virtuales Opciones extra Mostrar mensajes Lista Negra Descripción general Crear servidor	Opciones extra Keylogger ▼Keylogger Activo Eliminar [Retroceso]	Nombre del archivo: logs.dat
	 Cambiar la fecha de creación de archivos 2 Ocultar archivos 3 Eliminar en inicio 	
	 ✓ Persistencia 4 ✓ Inyectar en el explorador predeterminado o en el Pro Mutex: 	iexplore.exe 5 wind 6
En este ámbito, se encuentran t opciones y una breve descripci	oda la información necesaria para crear el servidor. Pase ón de la opción seleccionada aparecerá aquí.	el ratón sobre una serie de

- 1) Activamos el Keylogger
- 2) Cambiamos la fecha de los archivos para evitar ser descubiertos
- 3) Ocultamos los archivos para evitar ser visualizados
- 4) Agregamos la persistencia para que no se pierda la conexión cuando reinicia la pc
- 5) Inyectamos el servidor en el proceso que deseen
- 6) Cambiamos el nombre del mutex por alguno que confunda

Por ultimo vamos a la ultima opción para crear el servidor

Crear nuevo server				_	\mathbf{X}
Configuración	-Crear servidor				
Configuración Opciones básicas Instalación del servidc Arranque Añadir archivo Maquinas virtuales Opciones extra Mostrar mensajes Lista Negra Descripción general Crear servidor En este ámbito, se encuentran opciones y una breve description	Crear servidor Guardar archivo con Server-ANTRAX Ejecutar un servid Comprimir servido Comprimir servido Oncluir el plugin (au Utilice el icono	no: dor en el Modo Vi pr con UPX umenta el tamaño Lista de los ico avp.ico Default.ico excel.ico icq.ico msnmes.ico photoshop.ico	Extensión de Aplicación (* sible o del servidor) onos	archivo: *. exe) ANTR Pase el ratón so	Crear servidor bre una serie de
En este ámbito, se encuentran opciones y una breve descripe	toda la información ne ción de la opción selec	cesaria para cre cionada aparece	ar el servidor. rá aquí.	Pase el ratón so	bre una serie de
opciones y una breve descrip	ción de la opción selec	cionada aparece	rá aquí.		

Tildamos la opción marcada en rojo. Si quieren también pueden modificarle el icono.

Damos click en crear servidor

Si muestra el siguiente cartel, salió todo bien

Inform	nation 🔀
0	Servidor creado. Se guardo en: F:\Nueva carpeta (3)\pack troyanos\Spy-Net [RAT] v1.8\Server-ANTRAX.exe ANTRAX OK

Sino les aparece, saquen el antivirus o desactívenlo, pero es recomendado desinstalarlo.

NUCLEAR RAT

Este es otro famosísimo troyano, tiene opción de explorar la Red LAN, es por eso que este viejo troyano se ha hecho famoso. Tambien es de conexión hibrida. Esto quiere decir que puede ser de conexión directa e inversa.

Les mostrare como se configura a continuación:



Abrimos el cliente, y tendremos algo como esto.

🛠 Nuclear RAT 2.1.0 by caesar2k					
Spy Controls Managers Extras Quick Men	u Languages About				
IP:Port Connect ?	💫 Connection Manager	💡 Create Server	Share Serv	/er 🧇	Check new version
Log	Connections				
[16:45:03] Nuclear RAT client initialized	Socket IP	Com	puter Name	OS	Server Name
[16:45:03] Listening on port 12345					
ANTRAX					
-					
Open Windows					
Connected at					
Online servers 0					
Connected Time Open port 12345					
Outgoing Traffic OB					
Incoming Traffic OB Average Speed OB/s					
Ping Countdown 13	4				
					, , , , , , , , , , , , , , , , , , ,

Así se ve el cliente

Aquí no se configura el cliente. Asique pasaremos a la configuración del server.

Vamos a la opción del foquito que dice: "Create Server"

Create Serv	er			×		
Connections	Installation	Options	Message B	ł		
Reverse Con	nection Dire	ect Connec	tion			
IP via URL (o	ptional)			?		
IP or DNS to	connect			?		
w300.no-ip.	info					
Port	Port ?					
81	81					
Connect retry interval ?						
1						
Provided URL is a redirection service						
Server Type: R	everse Conn	ection				

Aquí ponemos la no-ip de nosotros y el puerto que tengamos abierto. El resto de las opciones son opcionales.

Aclaro que esto es para la configuración de conexión Inversa!

Luego presionamos las flechitas, hasta llegar a Build

Guardar como		_	_	_						2 🔀
Guardar en:	🚚 NR2.1.0				•	G	ø	Þ	•	
Documentos recientes	📕 Language 📕 Plugins 🔇 client.exe	s								
Escritorio										
J Mis documentos	ANT	RAX								
Mi PC										
	Nombre:	server.exe							-	Guardar
Mis sitios de red	Tipo:	Executables	s (*.exe,*.pif	,*.bat,*.com,*	*.scr)				•	Cancelar

Como muestra la imagen, escribimos el nombre del server, el que deseen y con la extensión *.exe, y le damos a guardar.

Y ya estaría listo el servidor para enviar.

LITTLE WITCH

Bueno, este es un troyano Argentino. Solo Funciona en redes LAN Al abrir el cliente, nos encontraremos con lo siguiente:



Cargara la interfaz, y nos mostrara el cliente



Este troyano es de conexión directa, asique debemos poner la IP de la PC a la cual infectamos.

En este caso puse 127.0.0.1 ya que infectare mi propia PC.

Una vez enviado el server, el cual viene con el cliente ya creado que se ve de la siguiente manera:



Una vez enviado el server y ejecutado, vamos nuevamente al cliente, y damos click en conectar, que se encuentra en la esquina inferior derecha.



Como verán, dice: Conectados con "127.0.0.1" Esto quiere decir que ya estamos conectados correctamente con la PC que infectamos.

Las opciones las tienen en el menú de arriba y a la derecha en donde dice: Broma, Config, Otros...



Bueno, este es un troyano muy conocido y muy viejo.

Aquí les traigo la versión 5 de este troyano, que fue editado desde el source por VozR.

Les dejo un pantallazo de cómo se ve:



Bueno, lo primero que haremos será ponerlo en ingles, por que sino no se entiende nada…

Seguido a esto, vamos a Editor, que es en donde se creara el server. Al hacerle click, veremos algo como lo siguiente:



Como pueden ver a la derecha, nos da para poner el DNS - IP, ahí es en donde ponemos la IP o la NO-IP, En Conection Port, el puerto que tengamos abieto. En User Name, ponemos el nombre con el que identificaremos a la victima. Y por ultimo pueden cambiar el icono si quieren para ocultar un poco el server. Luego de haber configurado todo eso, le damos a Save, y se abrirá una ventana para gurdar el server.

Una vez creado, si todo esta correcto, veremos un cartel asi:



Y tendremos el server Creado:



Al ejecutarlo, si todo es correcto, se conectara al cliente:

tur	-koja	n. V	
English 💽	🏸 Editor 🛛 🕢 Settings 🚺	About 🧼 Order Po	rt: 81 🔊 Stop
 accessories remote de webcam s audio stre settings mana manage keyb extra communication manage files commands server propertion system inform contact us local tools 	sktop treaming ager oard on ties nation	TRAX turkojan TURKOJAN Fw Client 2008 - 20	n 5.0.1
Connection ID :	IP Address :	Computer Name :	OS :
	127.0.0.1/127.0.0.1	DINNO	WinXP
Ready			ANTRAX nicknamed user is online

Las opciones las tienen en el panel de la izquierda.

BIOHAZARD - JUMPER



Menu							
Nombre	Usuario	IP/DNS	V	Pais	S.0		
BY	ANTRAX						
BioHazard 3	2 Edición Privada	🔆 OVíctimas co	onectadas				

Es de interfaz sencilla, opciones básicas, es cryptable, estable y mas indetectable que el resto por haber sido privado y poco usado por la gente.

JUMPER 3.2

🦉 Jump	er Trojan 3.2 -							
Menu	Menu							
Nombre	Usuario	IP/DNS	V	Pais	S.0			
	BY ANT	RAX						
	Jumpe	er Troian 3.2 Project O plataforma espe	ere					
\Box	<u>5</u>	5 033	33	/				

JUMPER 3.7



JUMPER 4

🗿 Jumper	Remote Adminis	tration Tool Troj	an 4.0 - CRACKE	D BY ANTRAX ww	w.e-r00t.net COD	ED By Margera		- 🗆 ×
Nombre	Usuario	IP/DNS	v	Pais	S.0		Estatidisticas de conexion	
			_					
							-	
😕 Registrado	c0m4dr3j4@hotma	il.es / 2008	a 0 victimas	conectadas		1		

Bueno, este troyano fue privado hasta que lo hice publico por razones que no voy a decir.

Para poder usar estos troyanos privados es necesario crackearlos o editarlos.

Para Crackearlo o Editarlo, necesitaremos un Editor Hexadecimal. Yo aconsejo utilizar el Hex WorkShop, que es el que utilizo siempre y el que utilizare en este tutorial. Primero que nada abrimos la carpeta contenedora del server Seleccionamos



Seleccionamos con el otro botón al Server, en este caso es el Server ANTRAX.exe y presionamos en la opción "Hex Edit with Hex Workshop v5".

BioHazard 3.2.exe Experied remove and the second se	Control ActiveX 137 KB	conection.wav	Control ActiveX 76 KB
MSCOMCTL.OCX Control ActiveX 1,057 KB	MSWINSCK.OCX Control ActiveX 107 KB	server (mod).BAK Archivo BAK 128 KB	Server ANTRAX.exe Abrir Ejecutar <u>c</u> omo
			Hex Edit with Hex Workshop v5
			Añadir a Server Antraz rar
			Añadir a "Server ANTRAX.rar" v enviar por email
			Anclar al m <u>e</u> nú Inicio
			En⊻iar a
			Cortar
			<u>C</u> opiar
			Crear acce <u>s</u> o directo
			Eliminar
			Cambiar nom <u>b</u> re
			Propiedadaa

Una vez seleccionada, se abrirá el Editor Hexadecimal con todos los Offsets. La imagen se ve un poco pequeña, pero esta seleccionada la opción que tiene un 10 (decimal).

H Hex Workshop - [Server ANTRAX.exe]	
🕅 Eile Edit Disk Options Tools Window Help	
😂 🗃 🖶 🎒 🕺 🖻 🛍 그 오드 🔖 💥 💷 🛅 🛅 🖪 🖇 L Q F D 👿 🕀 🔲	$\leftarrow \leftarrow \rightarrow \rightarrow$
(≒ ~ « » /	× * •
00000000 4D5A 9000 0300 0000 0400 0000 FFFF 0000 B800 0000 0000	4000 0000 0000 0000 0000 MZ
00000036 0000 0000 0000 0000 0000 0000	B800 0000 0E1F BA0E 00B4 09CD
00000072 21B8 014C CD21 5468 6973 2070 726F 6772 616D 2063 616E 6E6F	7420 6265 2072 756E 2069 6E20 L. This program cannot be run in
00000108 444F 5320 6D6F 6465 2E0D 0D0A 2400 0000 0000 0000 B712 07D	F373 6988 F373 6988 F373 6988 DOS modeŞsisisi.
00000144 1A6C 6488 F2/3 6988 5269 6368 F3/3 6988 0000 0000 0000 0000	5000 0501 0501 0600 0050 0100 DF L \ H
00000252 0100 0000 0400 0000 0000 0000 000 000 0	
	E4E5 0100 2800 0000 0010 0200
00000324 D008 0000 0000 0000 0000 0000 0000 000	0000 0000 0000 0000 0000
00000396 2000 0000 0010 0000 E400 0000 0000 0000 0	
00000432 2E/4 65/8 /400 0000 FUD/ 0100 0010 0000 00E0 0100 0010 0000	0000 0000 0000 0000 0000 .text
	0000 0000 0000 0000 0000aata
00000540 0000 0000 0000 0000 4000 0040 ECCE 3840 1000 0000 0000	0000 0000 4D53 5642 564D 3630
00000576 2E44 4C4C 0000 0000 0000 0000 0000 0000 0	0000 0000 0000 0000 0000 .DLL
00000612 0000 0000 0000 0000 0000 0000 0	0000 0000 0000 0000 0000
Server ANT	
Seffset: 0 [0x0000000]	I I Compare Results
887 Signed Byte 77	
16807 Signed Short 23117	
168IT Unsigned Short 23117	
328/T Signed Long 9460301	
Stational Cong 9460301	
SYBIT Unsigned Quad 12894362189	
328IT Float 1.3256705e-038	
8181 Double 6.3706614e-314	
U \Data Inspector / Structure Viewer /	□ \ Compare \ Checksum \ Find \ Bookmarks \ Output /
кеаду	jottset: U jvalue: 23117 1310/2 bytes jOVR MOD READ
🖉 🙀 😻 💉 BioHazard 🤝 Hexadecimal 📙 Hex Workshop - D	
	E 🖸 🔞 🖉
1. Martin 1997	Sábado

Seguido a esto presionamos "CTRL + F5" y nos aparecerá un cartel, que sirve para Buscar un Offset. En el cartel que aparecerá para la búsqueda. Y debemos seleccionar las opciones como muestra la imagen:

Find	
Criteria By ANTRAX	[
Iype: Text String	
⊻alue: no-ip	•
Hex: 6E00 6F00 2D00 6900 7000	
Options Find All Instances Match Case ASCII String	Direction C Up C Down
 Unicode String Either 	
Aceptar Cancelar	Apli <u>c</u> ar

Una vez escrito esto y seleccionada las opciones correspondientes, presionamos Aceptar, y nos enviara al Offset que aparece la NO-IP.

Hex Workshop - [Server ANTRAX.exe]		
🖾 🔃 Edit Disk Options Tools Window Help		
Image: Weak open Ctrl+N Image: Weak open Ctrl+O Image: Weak open B L Image: Weak open Image: Weak open <th image:="" td="" weak<=""><td>$\leftarrow \leftrightarrow \rightarrow \rightarrow]$</td></th>	<td>$\leftarrow \leftrightarrow \rightarrow \rightarrow]$</td>	$\leftarrow \leftrightarrow \rightarrow \rightarrow]$
J Ave Ctrl+S		
C Save As F DOFF E000 0000 0C00 0000 636C 6F73 6573 6F63	6865 7400 A073 4000 9880 4000@closesockets@@. 💽	
C Insert File D 4100 0000 0000 0000 0000 0000 0000 0000 526 6350 526 6367 7465 0465 Save Selection 15 6D6F 7465 486F 7374 4950 0000 0000 426F 6361 Import 15 6361 6248 827744 100 1000 426F 6361 C Export 10 0000 527 486 724 4000 426F 6361	02FF E068 A480 4000 B8F0 1040	
C Page Setup 53 636B 0000 0000 436F 6565 6563 7400 4263 6563 6664 6665 7460 6665 7461 0000 0000 6655 7456 6573 7400 0000 0000 6656 6664 4661 7461 0000 0000 6655 7456 6573 7400 0000 0000 555 6664 436F 6270 6655 7456 6573 7400 0000 0000 655 6664 436F 6270 6656 7456 6070 0000 6656 7456 6670 6000 0000 6656 7456 0000 0000 6656 7456 0000 0000 6656 7456 00000 0000	0000 0000 5365 6E64 4461 7461 CloseSckConnect.BindSendData 0 4C69 7374 656E 0000 4163 6365 4461 7461 4172 7269 7661 6C00 ptConnectionReguestDataArrival. 5365 6E64 5072 6F67 7265 7373 ErrorSendCompleteSendProgress	
C 1 Server ANTRAX.exe 0 0000 2E00 2E2E 542E 552E 4E2E 4F2E 2D2E 492E	50 <u>00</u> 2E00 6E00 4F00 2D00 6900(
Exet 0 6E00 6600 6F00 0000 794F AB33 9966 CF11 C 5x0t 00 5400 6900 6000 6500 7200 2600 6500 7300 6500 00033372 0000 0000 1800 0000 7300 7000 7200 2600 6500 7300 6400 00033408 1A00 0000 7A00 6500 6500 6200 6100 6500 7200 6200 2600 6500 7200 6200 2600 6500 6500 7200 6200 2600 6500 <td>B70C 00AA 0060 dags 1800 0000 bin.f. y0.3.f. 0000 0000 0000 0000 0000 T.e.a.T.i.m.e.re.x.e. </td>	B70C 00AA 0060 dags 1800 0000 bin.f. y0.3.f. 0000 0000 0000 0000 0000 T.e.a.T.i.m.e.re.x.e.	
00033624 6800 6500 7900 6000 6700 6700 6500 7200 2800 7400 7800) 7400 0000 0B00 0000 0800 0808 k.e.y.l.o.g.g.e.rt.x.t	
Server ANT		
offset: 33289 [0x00008209]	I instances of 'no-ip' found in Server ANTRAX.exe	
##T Signed Byte 0 ##T Signed Byte 0 ##W Signed Shott 11776 ##W Linsigned Shott 11776 ##W Linsigned Shott 11776 ##W Linsigned Shott 11776 ##W Linsigned Long 1845505536 ##W Linsigned Long 1845505536 ##W Linsigned Long 1845505536 ##W Linsigned Long 1845505236	Address Length 33292 10	
Witt Insigned Quad 3242713779342945792 3248 Float 9,917423e4027 Witt Duble 6,3026655e-092 Witt Duble 0,2026655e-092	Compare) Cherkrum) Find (Bookmarke) Outruit (
Save the active document	Offset: 33289 Value: 11776 131072 buter OVD MOD DEAD	
	prise, 3229 prade, 11778 131072 bytes pork problecter	
Contraction of the state of the	i ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	

En donde esta el 3, es en donde aparece el resultado de nuestra Busqueda. Hacemos Click en el, y nos llevara al Offset.

En donde esta el 1, es en donde esta la búsqueda respectiva.

En donde esta el 2, es lo que tenemos que modificar.

Para modificarlo, como muestra la imagen, debe ir nuestra no-ip separada por puntos.

Por ejemplo: p.e.p.i.t.o...n.o.-.i.p...i.n.f.o

En donde están los tres puntos, quiere decir que el punto del medio es un punto que en verdad es. En este caso, la no-ip es: pepito.no-ip.info.

Seguido a esto, presionamos Archivo>Guardar como muestra el numero 4.

Esto es todo. Aunque en algunas ocaciones, cuando buscamos la no-ip no aparece… en estos casos hacemos lo siguiente.

Abrimos el server con el editor. Y en vez de presionar "CTRL + F", presionamos "CTRL + G" esto es para buscar un Offset.

Goto	_ = ×
<u>0</u> ffset: 00033300	From Where <u>Beginning of File</u> Current <u>P</u> osition
Go Cancel Help Use F5 to jump to next position or SI	○ End of File (back from) hift+F5 to jump to previous position

En Offset, escribimos "00033300" que es en donde se encuentra la no-ip que debemos cambiar. Y presionamos en GO.

Y esto nos llevara al Offset de la no-ip y por ultimo lo modificamos. Como enseñe mas arriba.

Con esto el servidor queda listo para que conecte con el cliente. Tambien existe un editor de server para el jumper 4 Es muy fácil usarlo:



1 - Ponemos nuestra no-ip

2 - En Stub ponemos el server

3 - En File Out guardamos el server editado. Con la extensión *.exe

Y por ultimo en Generate

Con eso tendremos listo el server editado.