Detección y eliminación de Malware

Manual básico



10/02/2010 www.stopmalware.net Albert López

1. Introducción

Este manual está destinado a todas aquellas personas que quieran por ellas mismas llevar un control de seguridad básico en sus ordenadores donde aprenderán a utilizar algunas herramientas sencillas y prácticas para detectar y eliminar posible malware alojado en un ordenador.

Se mostrará el uso de software que nos ayudará a realizar la detección generalmente de virus o gusanos y servicios gratuitos que nos permitirán analizar posibles muestras.

El manual está pensado para gente que tiene conocimientos básicos de informática ya que para el seguimiento de este no está de más conocer ligeramente las rutas y carpetas de un sistema, conocer lo que es el administrador de tareas o el mismo registro de Windows.

Con este manual el usuario será capaz de:

- Conocer algunas herramientas básicas y gratuitas para la detección de archivos sospechosos.
- Localizar archivos sospechosos y eliminarlos.
- Aprenderá más sobre el sistema operativo Windows y su funcionamiento.
- Aprenderá el funcionamiento de los virus y gusanos más comunes.
- Aumentar la seguridad de su entorno de trabajo así como una actitud activa frente a posibles amenazas.

Cabe destacar, que este manual simplemente es una puerta introductoria al análisis y detección de malware, el caso de malware que utilizaremos para realizar los ejemplo de este tutorial es específico, eso quiere decir que las características del malware analizado es propio de éste y el lector debe ser capaz después de interpretar con los métodos utilizados de forma más general otros virus o gusanos ya que casa uno de ellos tiene características distintas como nombre, rutas, procesos o claves en el registro entre otros.

Un virus o gusano, no deja de ser un programa como cualquier otro con unas acciones determinadas, así que no se debe tener ningún miedo a ellos. Lo único que se debe tener es precaución y uso del sentido común ya que hoy día gran parte de las infecciones son por culpa de los propios usuarios que no toman las medidas suficientes o simplemente son engañados mediante distintos métodos para ejecutar archivos.

2. Funcionamiento de un virus o troyano.

Antes de poder hacer un análisis de un ordenador hace falta saber a lo que realmente le tenemos de hacer frente. La idea es que con este breve apartado el usuario tenga una idea de las diferentes acciones básicas que realiza todo tipo de malware.

Supondremos que el malware a analizar se ejecutará en un sistema, con el objetivo de permanecer en él el máximo tiempo posible, la finalidad de esto pueden ser muchas, aunque en ese aspecto no entraremos ya que si no se deberían especificar un gran número de casos y lo que interesa es conocer el funcionamiento básico de este.

Por lo general, el malware tiene tres acciones indispensables para asegurar su integridad en un sistema, estas son la de ejecutarse, copiarse y auto ejecutarse en cada inicio del sistema.

Una vez ejecutado, su función de copiarse es indispensable y generalmente existen diferentes rutas que los programadores de malware suelen utilizar. El uso repetido de estas rutas quizá es la falta de imaginación de estos, yo personalmente la desconozco pero el patrón se repite y eso hace que sea mucho más fácil de intuir la posible existencia de malware. Las rutas típicas donde se copia el malware son las siguientes (no por eso las únicas).

- C:\
- C:\Windows\
- C:\Windows\System32

El segundo paso, una vez ejecutado y copiado un malware creará una clave en el registro de Windows. El registro de Windows no deja de ser un software que tiene el propio Windows donde residirá una gran información sobre el sistema así como gran parte de la configuración de este.

El registro se divide en distintas claves y subclaves, a nosotros solo nos interesa conocer donde se copian los archivos que se auto ejecutan en cada inicio. Para acceder al registro de Windows, simplemente deberán ir a INICIO y presionar en EJECUTAR, allí escriben "regedit" y al apretar se les abrirá el registro de Windows y verán las distintas claves y subclaves que lo conforman.

Para que un ejecutable se auto-inicie con el sistema operativo creará una clave en las siguientes rutas:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ RunOnce



Si buscan la clave y subclaves mencionadas deberían de poder ver los programas que se ejecutan al iniciar Windows, seguramente muchos los reconocerán como puede ser el antivirus que tengan o por ejemplo el propio Messenger muy utilizado. En caso de tener un virus, éste creará una clave y subclave en esa ruta.

Por otro lado, aparte de copiarse, ejecutarse y asegurar su auto inicio el virus abrirá un proceso en el sistema donde nos dará a entender que está ejecutándose.

Para poder visualizar los procesos activos en un sistema, utilizaremos el administrador de sistema o también conocido como taskmanager. Para ejecutar el taskmanager solo deberemos presionar las teclas CNTRL+ALT+SUPR donde se abrirá una pequeña pantalla con una pestaña con los procesos en ejecución.

El administrador de tareas, tiene una función que es la de cerrar procesos que estén ejecutándose, es decir, los procesos que aparecen se pueden cerrar, esto nos será de utilidad posteriormente para eliminar los ejecutables del malware que podamos encontrar. Hay programas que realizan la misma función que el taskmanager pero con éste ya tendremos suficiente.

	Administrador de	tareas de W	/indow	'S				— 🗆 <mark>—</mark> X	
Ar	hivo Onciones	Ver Avu	da						-
	chive operates								
A	plicaciones Proces	os Servicios	Ren	dimiento Fu	nciones de red Us	suarios			
	Nombre de im	Nombre	CPU	Memoria	Descripción			^	
	ALSMON.exe	Media	00	5.580 KB	ALSMON				
	ashDisp.exe *32	Media	00	1.160 KB	avast! se				
	atiedxx.exe		00	2.816 KB					
	BluetoothHea	Media	00	1.080 KB	Bluetooth				
	BTStackServe	Media	00	8.208 KB	Bluetooth				
	BTTray.exe	Media	00	6.980 KB	Bluetooth				
	CCC.exe	Media	00	15.196 KB	Catalyst			=	
	CLMLSvc.exe	Media	00	1.988 KB	CyberLink				
	CorelIOMonit	Media	00	1.916 KB	Corel File				
	csrss.exe		00	2.680 KB					
	DVDAgent.ex	Media	00	396 KB	HP DVDS				
	dwm.exe	Media	00	18.924 KB	Administr				
	explorer.exe	Media	00	30.492 KB	Explorado				
	firefox.exe *32	Media	00	87.936 KB	Firefox				
	hpdocstart.ex	Media	00	964 KB	HP Envy				
	HpqToaster.e	Media	00	2.064 KB	HpqToast				
	HPWAMain.exe	Media	00	11.836 KB	HP Wirele				
	hpwuschd2.e	Media	00	1.068 KB	hpwuSch				
	IAAnotif.exe	Media	00	2.576 KB	Event Mo				
	jucheck.exe	Media	00	5.720 KB	Java(TM)				
	jusched.exe	Media	00	2.968 KB	Java(TM)				
	jusched.exe *32	Media	00	3.192 KB	Java(TM)				
	MOM.exe	Media	00	4.936 KB	Catalyst				
	msnmsgr.exe	Media	00	5.096 KB	Windows				
	QLBCTRL.exe	Media	00	3.160 KB	Quick Lau		 	*	
	Mostrar proces	sos de todos l	os usua	arios			(Finalizar proceso	
Pro	cesos: 84 U	lso de CPU: (0%	Memo	ria física: 39%				

Simplemente eligiendo con un click el proceso a cerrar y luego presionando a "Finalizar proceso" lo podremos cerrar.

Es importante, entender el porqué hace falta cerrar un proceso, la explicación es sencilla y es porque el propio sistema no nos permite eliminar un archivo ejecutándose con un proceso abierto. Cada ejecutable tendrá su propio proceso.

En caso de querer eliminar un archivo con su proceso abierto, el sistema nos mostrará el siguiente mensaje.

Error a	l borrar un archivo o carpeta 🛛 🛛 🔀
8	No se puede eliminar meet the fockers(2)(2): Está siendo usado por otra persona o programa.
	Cierre todos los programas que puedan estar utilizando este archivo e inténtelo de nuevo.
	Aceptar

En caso por ejemplo de Windows 7, nos mostrará directamente un mensaje advirtiendo que no se puede borrar porque el archivo esta ejecutándose.

3. Analizando nuestro sistema.

Ahora, después de la breve descripción del funcionamiento de un malware común y el uso de dos de los elementos más importantes como el taskmanager y el registro de Windows, ya puede como usuario analizar el sistema.

Para ello utilizaremos una herramienta muy sencilla y practica que nos generará un resumen en un archivo de texto sobre los procesos y archivos que se ejecutan en el sistema. Posteriormente utilizaremos una herramienta online para analizar el log generado, aunque con un poco de experiencia y conocimiento cuando se adquiere más experiencia es sencillo simplemente con el log localizar malware.

La herramienta se llama hijackthis, es gratuita y la podrán encontrar en el siguiente enlace:

• <u>http://free.antivirus.com/hijackthis/</u>

Una vez descargada la ejecutan y tendrá el siguiente aspecto.

Trend Micro HijackThis - vz.	J.Z	لكانكا
elow are the results of the HijackThis so	an. Be careful what you delete with the	he 'Fix
necked' button. Scan results do not det	ermine whether an item is bad or not.	The
est thing to do is to Analyze this and s	low the log file to knowledgeable folks	3.
R0 - HKCU\Software\Microsoft\Inter	net Explorer \Main,Start Page = http://	/www.toshibadirect.com/dpdstart
R1 - HKLM\Software\Microsoft\Interr	net Explorer Main, Default_Page_URL =	= http://go.microsoft.com/fwlink/?Link
R1 - HKLM\Software \Microsoft\Interr	net Explorer Main, Default_Search_URI	L = http://go.microsoft.com/fwlink/?Lir
R1 - HKLM\Software \Microsoft \Interr	net Explorer Main,Search Page = http:	://go.microsoft.com/fwlink/?LinkId=54
R0 - HKLM\Software \Microsoft \Interr	het Explorer Main,Start Page = http://	/go.microsoft.com/fwlink/?LinkId=691!
R1 - HKCU\Software \Microsoft \Inter	net Connection Wizard,ShellNext = htt	tp://windowsupdate.microsoft.com/
02 - BHO: (no name) - {7E853D72-6	26A-48EC-A868-BA8D5E23E045} - (no	o file)
] O4 - HKLM\\Run: [igfxtray] C:\WIN	DOWS\system32\jgfxtray.exe	1
] O4 - HKLM\ \Run: [igfxhkcmd] C:\W	INDOWS\system32\hkcmd.exe	
04 - HKLM\ Run: [igfxpers] C:\WIN	IDOWS\system32\jgfxpers.exe	
04 - HKLM\ Run: [ehTray] C:\WIND	OOWS\ehome\ehtray.exe	2.5
04 - HKLM\ Run: [THotkey] C: Pro	gram Files\Toshiba\Toshiba Applet\tho	itkey.exe
04 - HKLM\ Run: [LtMoh] C: Progra	am Files (tmoh (Ltmoh.exe	
O4 - HKLM \ (Run: [AGRSMMSG] AGE	RSMMSG.exe	Lara a
04 - HKLM\ (Run: [Intel/eroConfig]	C: Program Files (Intel Wireless bin /2	CtgSvc.exe
04 - HKLM Run: [IntelWireless] C	: Program Files (Intel (Wireless (Bin (ffm))	ewrk.exe /tf Intel PROSet/Wireless
04 - HKLM \ Run: [MSKDetectorExe	C: Program Files McAfee Spamkiller	MSKDetct.exe /uninstall
104 - HKCU), Kun: [TOSCDSPD] C: [VINDOWS lowstom 22) stemps over	scaspa.exe
04 - HKCU ((kun: [cumon.exe] C: (WINDOWS (system 52 (ctimon.exe	WIS SMR Client VI 01/fab ava
08 - Extra context menu item: E8vn	art to Microsoft Excel - res: //C-\PPOG	PA at MICPOS 200 ffce 12 EVEL EVEL
09 - Extra button: Research - (9278	0825-18CC-41C8-898E-3C9C571A826	533 - C \PROGRAM 1MICROS 2)Office
Scan & fix stuff		Other stuff
find a second	AnalyzeThis	
Scan Fix checked	Upload to TrendSecure	Info Config

Simplemente deberán seleccionar un análisis del sistema con la opción de crear un log. Esto generará un archivo de texto el que guardaremos en nuestro ordenador para posteriormente analizarlo.

Una vez tengamos el log, simplemente utilizaremos uno de los servicios gratuitos online que permite hacer una lectura de éste y mostrarnos las claves correctas o que pueden ser intrusivas. Hay veces que una clave la muestra como no segura aunque puede ser que no esté en la base de datos y por eso no la reconoce, no quiere decir que todo lo que no indica como seguro deba ser un malware.

Para realizar el análisis de estos archivos podremos utilizar los siguientes servicios online gratuitos.

- <u>www.hijackthis.de</u>
- <u>http://hjt.networktechs.com/</u>

El uso de estos servicios es muy sencillo, simplemente suban el archivo de texto o copien el contenido en la pantalla que hay en la web, una vez hecho tendrán unos resultados parecidos a la siguiente imagen.



Como pueden ver en la imagen, toda la lista aparece con una marca verde, eso quiere decir que los procesos y archivos son correctos, en caso de aparecer con una aspa amarilla es que son desconocidos y en el caso de que tengan una aspa roja es que lo más probable es que sea algún tipo de malware.

En caso de localizar archivos maliciosos, simplemente con lo explicado anteriormente cerraremos los procesos que tengan abierto, eliminaremos los archivos y seguidamente las claves del registro.

4. Análisis, detección y eliminación real.

La mejor forma de aprender algo es con la práctica, pero puestos a que en este caso no se puede hacer una práctica muy real, se realizará el análisis de un sistema que previamente ya he detectado un malware, pero quiero que vayan viendo los pasos que voy siguiendo y sobre todo como utilizo los conceptos explicados hasta esta parte del manual para que luego mediante esta pauta puedan hacer sus análisis.

Como usuario que quiere realizar el análisis a un posible ordenador infectado, primero de todo utilizaré el hijackthis, para poder generar el log y posteriormente realizar un análisis online. Una vez abierto generarémos el log que tendrá el siguiente aspecto:

Logfile of Trend Micro HijackThis v2.0.2 Scan saved at 12:50:53, on 10/2/2010 Platform: Windows XP SP2 (WinNT 5.01.2600) MSIE: Internet Explorer v7.00 (7.00.6000.16608) Boot mode: Normal

Running processes: C:\WINDOWS\System32\smss.exe C:\WINDOWS\system32\winlogon.exe C:\WINDOWS\system32\services.exe C:\WINDOWS\system32\lsass.exe C:\WINDOWS\system32\svchost.exe C:\WINDOWS\System32\svohost.exe C:\Archivos de programa\Archivos comunes\Symantec Shared\ccSvcHst.exe C:\WINDOWS\Explorer.EXE C:\Archivos de programa\Archivos comunes\Symantec Shared\ccProxy.exe C:\Archivos de programa\Lavasoft\Ad-Aware 2007\aawservice.exe C:\WINDOWS\system32\spoolsv.exe C:\Archivos de programa\Google\Common\Google Updater\GoogleUpdaterService.exe C:\Archivos de programa\Keyboard & Mouse Driver\KMWDSrv.exe C:\WINDOWS\system32\nvsvc32.exe C:\WINDOWS\RTHDCPL.EXE C:\WINDOWS\system32\RUNDLL32.EXE C:\Archivos de programa\Archivos comunes\Symantec Shared\ccApp.exe C:\Archivos de programa\Keyboard & Mouse Driver\StartAutorun.exe C:\WINDOWS\system32\ctfmon.exe C:\Archivos de programa\Google\Google Updater\GoogleUpdater.exe C:\Archivos de programa\Keyboard & Mouse Driver\KMConfig.exe C:\Archivos de programa\Keyboard & Mouse Driver\KMProcess.exe C:\WINDOWS\system32\wuauclt.exe C:\Archivos de programa\Internet Explorer\iexplore.exe C:\Documents and Settings\Juan José\Escritorio\HiJackThis.exe C:\ARCHIV~1\Symantec\LIVEUP~1\LUCOMS~1.EXE

R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page = google.es R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL = <u>http://go.microsoft.com/fwlink/?LinkId=69157</u>

R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Search_URL = http://go.microsoft.com/fwlink/?LinkId=54896 R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Page = http://go.microsoft.com/fwlink/?LinkId=54896 R0 - HKLM\Software\Microsoft\Internet Explorer\Main,Start Page = http://go.microsoft.com/fwlink/?LinkId=69157 R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName = Vínculos O2 - BHO: Aplicación auxiliar de vínculos de Adobe PDF Reader - {06849E9F-C8D7-4D59-B87D-784B7D6BE0B3} - C:\Archivos de programa\Archivos comunes\Adobe\Acrobat\ActiveX\AcroIEHelper.dll O2 - BHO: (no name) - {1E8A6170-7264-4D0F-BEAE-D42A53123C75} - C:\Archivos de programa\Archivos comunes\Symantec Shared\coShared\Browser\1.5\NppBho.dll O2 - BHO: Spybot-S&D IE Protection - {53707962-6F74-2D53-2644-206D7942484F} -C:\ARCHIV~1\SPYBOT~1\SDHelper.dll O2 - BHO: (no name) - {7E853D72-626A-48EC-A868-BA8D5E23E045} - (no file) O2 - BHO: Google Toolbar Helper - {AA58ED58-01DD-4d91-8333-CF10577473F7} c:\archivos de programa\google\googletoolbar1.dll O2 - BHO: Google Toolbar Notifier BHO - {AF69DE43-7D58-4638-B6FA-CE66B5AD205D} -C:\Archivos de programa\Google\GoogleToolbarNotifier\2.1.1119.1736\swg.dll O3 - Toolbar: Mostrar la Barra de herramientas de Norton - {90222687-F593-4738-B738-FBEE9C7B26DF} - C:\Archivos de programa\Archivos comunes\Symantec Shared\coShared\Browser\1.5\UIBHO.dll O3 - Toolbar: & Google - {2318C2B1-4965-11d4-9B18-009027A5CD4F} - c:\archivos de programa\google\googletoolbar1.dll O4 - HKLM\..\Run: [NvCpIDaemon] RUNDLL32.EXE C:\WINDOWS\system32\NvCpl.dll,NvStartup O4 - HKLM\..\Run: [nwiz] nwiz.exe /install O4 - HKLM\..\Run: [SkyTel] SkyTel.EXE O4 - HKLM\..\Run: [RTHDCPL] RTHDCPL.EXE O4 - HKLM\..\Run: [Soundman] svohost.EXE O4 - HKLM\..\Run: [NvMediaCenter] RUNDLL32.EXE C:\WINDOWS\system32\NvMcTray.dll,NvTaskbarInit O4 - HKLM\..\Run: [ccApp] "C:\Archivos de programa\Archivos comunes\Symantec Shared\ccApp.exe" O4 - HKLM\..\Run: [Symantec PIF AlertEng] "C:\Archivos de programa\Archivos comunes\Symantec Shared\PIF\{B8E1DD85-8582-4c61-B58F-2F227FCA9A08}\PIFSvc.exe" /a /m "C:\Archivos de programa\Archivos comunes\Symantec Shared\PIF\{B8E1DD85-8582-4c61-B58F-2F227FCA9A08}\AlertEng.dll" O4 - HKLM\..\Run: [KMCONFIG] C:\Archivos de programa\Keyboard & Mouse Driver\StartAutorun.exe KMConfig.exe O4 - HKCU\..\Run: [CTFMON.EXE] C:\WINDOWS\system32\ctfmon.exe O4 - HKUS\S-1-5-19\..\Run: [CTFMON.EXE] C:\WINDOWS\system32\CTFMON.EXE (User 'SERVICIO LOCAL') O4 - HKUS\S-1-5-20\..\Run: [CTFMON.EXE] C:\WINDOWS\system32\CTFMON.EXE (User 'Servicio de red') O4 - HKUS\S-1-5-18\..\Run: [CTFMON.EXE] C:\WINDOWS\system32\CTFMON.EXE (User 'SYSTEM') O4 - HKUS\.DEFAULT\..\Run: [CTFMON.EXE] C:\WINDOWS\system32\CTFMON.EXE (User 'Default user') O4 - Global Startup: Google Updater.Ink = C:\Archivos de programa\Google\Google Updater\GoogleUpdater.exe O6 - HKCU\Software\Policies\Microsoft\Internet Explorer\Control Panel present O6 - HKLM\Software\Policies\Microsoft\Internet Explorer\Control Panel present

O9 - Extra button: (no name) - {DFB852A3-47F8-48C4-A200-58CAB36FD2A2} -C:\ARCHIV~1\SPYBOT~1\SDHelper.dll O9 - Extra 'Tools' menuitem: Spybot - Search & Destroy Configuration - {DFB852A3-47F8-48C4-A200-58CAB36FD2A2} - C:\ARCHIV~1\SPYBOT~1\SDHelper.dll O9 - Extra button: (no name) - {e2e2dd38-d088-4134-82b7-f2ba38496583} -C:\WINDOWS\Network Diagnostic\xpnetdiag.exe O9 - Extra 'Tools' menuitem: @xpsp3res.dll,-20001 - {e2e2dd38-d088-4134-82b7f2ba38496583} - C:\WINDOWS\Network Diagnostic\xpnetdiag.exe O9 - Extra button: Messenger - {FB5F1910-F110-11d2-BB9E-00C04F795683} - C:\Archivos de programa\Messenger\msmsgs.exe O9 - Extra 'Tools' menuitem: Windows Messenger - {FB5F1910-F110-11d2-BB9E-00C04F795683} - C:\Archivos de programa\Messenger\msmsgs.exe O16 - DPF: {D27CDB6E-AE6D-11CF-96B8-444553540000} (Shockwave Flash Object) http://fpdownload2.macromedia.com/get/shockwave/cabs/flash/swflash.cab O17 - HKLM\System\CCS\Services\Tcpip\..\{0BF242E0-B11F-49C6-9892-81B7FD307C52}: NameServer = 80.58.61.250,80.58.61.254 O17 - HKLM\System\CS1\Services\Tcpip\..\{0BF242E0-B11F-49C6-9892-81B7FD307C52}: NameServer = 80.58.61.250,80.58.61.254 O20 - Winlogon Notify: !SASWinLogon - C:\Archivos de programa\SUPERAntiSpyware\SASWINLO.dll O23 - Service: Ad-Aware 2007 Service (aawservice) - Lavasoft - C:\Archivos de programa\Lavasoft\Ad-Aware 2007\aawservice.exe O23 - Service: Symantec Event Manager (ccEvtMgr) - Symantec Corporation - C:\Archivos de programa\Archivos comunes\Symantec Shared\ccSvcHst.exe O23 - Service: Symantec Network Proxy (ccProxy) - Symantec Corporation - C:\Archivos de programa\Archivos comunes\Symantec Shared\ccProxy.exe O23 - Service: Symantec Settings Manager (ccSetMgr) - Symantec Corporation - C:\Archivos de programa\Archivos comunes\Symantec Shared\ccSvcHst.exe O23 - Service: Symantec Lic NetConnect service (CLTNetCnService) - Symantec Corporation -C:\Archivos de programa\Archivos comunes\Symantec Shared\ccSvcHst.exe O23 - Service: COM Host (comHost) - Symantec Corporation - C:\Archivos de programa\Archivos comunes\Symantec Shared\VAScanner\comHost.exe O23 - Service: Google Updater Service (gusvc) - Google - C:\Archivos de programa\Google\Common\Google Updater\GoogleUpdaterService.exe O23 - Service: Keyboard And Mouse Communication Service (KMWDSERVICE) -UASSOFT.COM - C:\Archivos de programa\Keyboard & Mouse Driver\KMWDSrv.exe O23 - Service: LiveUpdate - Symantec Corporation -C:\ARCHIV~1\Symantec\LIVEUP~1\LUCOMS~1.EXE O23 - Service: LiveUpdate Notice Service Ex (LiveUpdate Notice Ex) - Symantec Corporation -C:\Archivos de programa\Archivos comunes\Symantec Shared\ccSvcHst.exe O23 - Service: LiveUpdate Notice Service - Symantec Corporation - C:\Archivos de programa\Archivos comunes\Symantec Shared\PIF\{B8E1DD85-8582-4c61-B58F-2F227FCA9A08}\PIFSvc.exe O23 - Service: NVIDIA Display Driver Service (NVSvc) - NVIDIA Corporation -C:\WINDOWS\system32\nvsvc32.exe O23 - Service: Symantec Core LC - Unknown owner - C:\Archivos de programa\Archivos comunes\Symantec Shared\CCPD-LC\symIcsvc.exe

End of file - 7812 bytes

Una vez tengamos nuestro log, abriremos el navegador e iremos a una de las páginas anteriormente recomendadas para analizarlo. En la página nos aparecerá con una aspa roja las dos entradas que se han indicado en rojo, eso quiere decir que la entrada del registro y el fichero puede ser algún tipo de malware y yo como usuario soy consciente de que no tengo ningún software legítimo con ese nombre procederé a su borrado.

Resumiendo, el archivo sospechoso es el siguiente y tiene la siguiente clave para auto ejecutarse en el inicio del sistema.

C:\WINDOWS\System32\svohost.exe

O4 - HKLM\..\Run: [Soundman] svohost.EXE

Una vez tengamos clara la lista de posible malware, procederemos a su eliminación. Para ello, es importante tener claro lo explicado en los primeros puntos, ya que si no empezarán los problemas. Para la eliminación seguiremos el siguiente orden.

- Cerrar el proceso o procesos del ejecutable o ejecutables.
- Eliminar la clave o claves del registro de Windows.
- Eliminar el archivo o archivos.
- Reiniciar el ordenador y comprobar.

Primero de todo, cerraremos el proceso creado por el virus, para ello presionamos CNTRL+ALT+SUPR y vamos a la pestaña de "procesos" del administrador de tareas.

Administrador Archivo Opcion	r de nes	tareas de W Ver Ayu	/indow da	IS					x
Aplicaciones Pro	oceso	os Servicios	Ren	dimiento F	unciones de red	Usuarios			
									_
Nombre de im		Nombre	CPU	Memoria	Descripción				*
jusched.exe *	*32	Media	00	2.792 K	B Java(TM)				
MOM.exe		Media	00	4.008 Ki	B Catalyst				
msnmsgr.exe		Media	00	36.228 Ki	B Windows				
QLBCTRL.exe	·	Media	00	2.480 Ki	B Quick Lau				
qttask.exe *3	32	Media	00	1.220 Ki	B QuickTime				
sidebar.exe		Media	00	7.128 Ki	B Gadgets				
SmartMenu.e	xe	Media	00	5.656 Ki	B SmartMenu				
splwow64.exe	e	Media	00	2.432 Ki	B Print driv				
sttray64.exe		Media	00	8.208 Ki	B IDT PC A				
svohost.exe .		Media	00	1.720 Ki	B svohost				Ξ
SynTPEnh.ex	e	Media	00	5.540 K	B Synaptics				
SynTPHelper.		Media	00	2.220 Ki	B Synaptics				
taskeng.exe		Media	00	2.780 K	B Motor de				
taskhost.exe		Media	00	4.144 Ki	B Proceso d				
taskmgr.exe		Media	00	4.164 Ki	B Administr				-
🛞 Mostrar pr	roces	os de todos l	los usu:	arios				Finalizar proce	so
Procesos: 86	U	so de CPU: (0%	Mem	oria física: 39%				

Para finalizarlo, simplemente haciendo un click sobre el nombre del proceso y luego a "Finalizar proceso" se cerrará el proceso y tendremos vía libre para borrar el archivo sin problemas.

Para los curiosos, hay otra forma de eliminar archivos y es en el llamado "Modo seguro" pero en este caso no le daremos importancia. Si quiere saber más sobre este modo simplemente utilizando google se puede obtener información.

Ahora el siguiente paso es localizar el archivo y eliminarlo, para ello la ruta donde se ubica recordemos que es:

							x
Equipo	 Disco local (C:) 	:) ▶ Windows ▶ System32 ▶	_	Buscar Syster	n32	_	Q
Organizar 🔻 🖬 Abr	rir Nueva carp	peta					0
 ★ Favoritos ↓ Descargas ■ Escritorio ③ Sitios recientes ○ Bibliotecas ○ Documentos ○ Imágenes ↓ Música 	Nombre svchost svohost syproxy sxs.dll sxshare sxssrv.d sxsstore	Abrir Ejecutar como administrador Solucionar problemas de comp Escanear svohost.exe Add to archive Add to archive Add to "svohost.rar" Compress and email Compress and email	Fecha de modifica 14/07/2009 3:39 vatibilidad	Tipo Aplicación Extensión de la apl Extensión de la apl	Tamaño 27 KB 61 KB 512 KB 74 KB 570 KB 42 KB 31 KB 27 KB		^
 ➡ Vídeos ➡ Grupo en el hogar ➡ Equipo 	SyncCe SyncCe Syncen SyncHc SyncHc	Anclar a la barra de tareas Anclar al menú Inicio Restaurar versiones anteriores Enviar a	•	Aplicación Extensión de la apl Extensión de la apl Aplicación Extensión de la apl Extensión de la apl	35 KB 2.210 KB 93 KB 43 KB 13 KB 417 KB		-
Svohost Fe Aplicación	echa de modifica Tamañ	Cortar Copiar Crear acceso directo	1	D 22:48	11110		
		Eliminar					
		Cambiar nombre					
		Propiedades					

C:\WINDOWS\System32\svohost.exe

En éste caso cabe destacar un detalle, si se fijan en la captura, el archivo que hay justamente arriba de nuestro archivo malicioso tiene un nombre muy similar. Esto lo hacen muchos virus o troyanos para pasar inadvertidos o sea más difícil de detectarlos.

Por otra parte, comentar que existe un tipo de malware llamados rootkits (google para más información) que aprovechan procesos del sistema para auto ejecutarse. Este tipo de malware, su detección es algo más compleja que requeriría de otro manual y software para ser detectado.

Por último, para dejar el ordenador limpio es importante eliminar la clave del registro, en caso de no hacerlo no pasará absolutamente nada, pero para

mantener nuestro ordenador y el registro de Windows más limpio se recomienda hacer el borrado.

Para ello, podemos utilizar algún tipo de software que nos permita limpiar el registro de claves innecesarias, en este caso contamos con una herramienta llamada CCleaner, la podrán descargar del siguiente enlace.

- Piriform CCleaner CCleaner.com MS Windows XP SP2 Intel Pentium D CPU 3.00GHz, 2.0GB RAM, ATI FireGL V3100 Windows Applications ✓ Internet Explorer C:\WINDOWS\MiniDump\Mini072507-01.dmp 100.00KB ~ ~ C: WINDOWS MiniDump Mini080307-01.dmp 64.00KB Temporary Internet Files C:\WINDOWS\system32\wbem\Logs\FrameWork.log 180 bytes Cleane Cookies C:\WINDOWS\system32\wbem\Logs\wbemprox.log 42.73KB C:\WINDOWS\system32\wbem\Logs\wbemprox.log 2.58KB History C: \WINDOWS \system 32 \wbem \Logs \wmiadap.log 2.02KB Recently Typed URLs C:\WINDOWS\system32\wbem\Logs\wmiprov.log 6.00KB Delete Index.dat files C:\WINDOWS\system32\wbem\Logs\wbemess.lo_64.10KB Last Download Location C:\WINDOWS\0.log 0 bytes Autocomplete Form History C:\WINDOWS\EventSystem.log 966 bytes Windows Explorer C:\WINDOWS\setupact.log 75 bytes C:\WINDOWS\setupapi.log 36.50KB Recent Documents C:\WINDOWS\setuperr.log 0 bytes C:\WINDOWS\Freecorder Toolbar Setup Log.txt 6.60KB Run (in Start Menu) Tools Search Autocomplete C:\WINDOWS\Debug\Dfsr00001.log 0.68MB ✓ Other Explorer MRUs C:\WINDOWS\Debug\UserMode\userenv.log 0.29MB - 🗸 System < > Empty Recycle Bin Temporary Files Options Analyze Run Cleaner Clinboard Online Help Check for updates...
- http://www.ccleaner.com/

No obstante, frente a la alternativa de utilizar CCleaner u otro programa similar, como solamente hay una clave en el registro a eliminar, se puede proceder a la eliminación de forma manual mediante el registro de Windows, ya que su localización no es complicada.

Para ello vamos a inicio y en la pestaña de ejecutar o en buscar, según sistema operativo escribímos regedit. Al aceptar se nos abrirá el registro de Windows.

Programas (1)	
P Ver más resultados	
regedit ×	Apagar 🕨

En el registro de Windows, simplemente se deberá localizar la siguiente clave y borrarla.

PhotoPropertyHandler Nombre Tipo Datos PnPSysprep Policies (Predeterminado) REG_SZ (valor no establecido) PropertySystem PropertySystem SanatMenu REG_SZ C:\Program Files(\k86)\Intel\Intel Matrix Storage M Reliability SanatMenu REG_SZ C:\Program Files(\k86)\Intel\JuveltPackard\HP MediaSmar Reliability SunJavaUpdateS REG_SZ C:\Program Files(\k96)\Synaptics(\k97)PTPS\ynTPEnh.exe RunOnce SysTrayApp REG_EXPAND_SZ C:\Program Files\UDVWDM\sttray64.exe Shell Extensions Soundman REG_SZ C:\WINDOWS\System32\svohost.exe StideBySide SideBySide SMDEn REG_SZ C:\WINDOWS\System32\svohost.exe	or del Registro o Edición Ver Favoritos Aj	yuda			
StructuredQuery	vo Edición Ver Favoritos At vo Edición Ver Favoritos At vo PhotoPropertyHandler PhotoPropertyHandler PhotoPropertyHandler vo PnPSysprep Policies vo Policies PreviewHandlers vo PreviewHandlers PreviewHandlers vo Reliability PreviewHandlers vo Reliability PreviewHandlers vo RenameFiles PreviewHandlers vo Shell Extensions Policites vo Shell Extensions Policites vo Shell ServiceObjectDela Sidebar vo SMDEn Policites vo SMUEn Policites vo SMI Policites	yuda Nombre (Predeterminado) (a) JAAnotif (b) SantMenu (c) SynJavaUpdateS (c) SynJavaUpdateS (c) SynJavaUpdateS (c) SynJavaUpdateS (c) SynJavaUpdateS (c) SynJavaUpdateS (c) SynJavaUpdateS (c) SynJavaUpdateS	Tipo REG_SZ REG_SZ REG_SZ REG_SZ REG_EXPAND_SZ REG_EXPAND_SZ REG_SZ	Datos (valor no establecido) C:\Program Files (x86)\Intel\Intel Matrix Storage M C:\Program Files\Hewlett-Packard\HP MediaSmar "C:\Program Files\USynaptics\SynTPShh.exe C:\Program Files\USynaptics\SynTPShh.exe C:\Program Files\UT\WDN\Sttray64.exe C:\WINDOWS\System32\svohost.exe	

O4 - HKLM\..\Run: [Soundman] svohost.EXE

Visto con más detalle, fijémonos que aparece la clave del posible malware.

RenameFiles	ab SynTPEnh	REG_EXPAND_SZ	%ProgramFiles%\Synaptics\SynTP\SynTPEnh.exe
Run	ab SysTrayApp	REG_EXPAND_SZ	C:\Program Files\IDT\WDM\sttray64.exe
RunOnce	ab Soundman	REG_SZ	C:\WINDOWS\System32\svohost.exe

Si se clicka con el botón derecho encima, nos dará varias posibilidades, simplemente seleccionamos eliminar para borrar la clave.

ab SynTPl ab SysTray	Enh yApp	REG_EXPAND_SZ REG_EXPAND_SZ	%ProgramFiles%\Synaptics\SynTP\SynTPEnh.exe C:\Program Files\IDT\WDM\sttray64.exe
ab Sound	man Modi Caml	REG SZ	C:\WINDOWS\System32\svohost.exe
	Elimi Caml	nar biar nombre	

Una vez llegados a este punto, aparentemente el malware estará eliminado del equipo, felicidades!

De todas formas, es muy importante asegurar que no queda ningún indicio de este, para ello reiniciaremos el ordenador y comprobaremos que no existen los archivos maliciosos y las rutas del registro de Windows.

A veces ocurre, que al reiniciar vuelven a aparecer los archivos y claves del registro de Windows, en este caso suele pasar que hay más de un ejecutable del malware activo en el ordenador y al reiniciar vuelve a crear las copias.

En caso de que en el log del hijackthis no aparezca nada más que nos pueda hacer sospechar, podría darse el caso de que el malware tuviera función de rootkit, es decir que se ejecutara bajo un proceso de un archivo del sistema por ejemplo y no se haya detectado.

5. Consideraciones

Como se ha especificado al principio de este manual, el principal problema al producirse infecciones es el usuario, por otra parte el sistema puede tener agujeros de seguridad ya sea mediante sistema operativo o por navegador de internet por ejemplo que permiten la infección.

En este apartado solo quiero poner algunas pautas claves para evitar infecciones.

- Actualiza periódicamente tu software, sobre todo cada día el software de seguridad de tu ordenador.
- Los antivirus, aunque estén actualizados, no protegen al 100% un sistema, pero ayudan en la mayor parte a eliminar malware o scripts maliciosos.
- Nunca descargues archivos adjuntos de emails, incluso a veces de personas conocidas. Mucho malware es capaz de auto enviar emails con correos de conocidos adjuntándose. Se detectan muchas veces porque no son del idioma del país que se reside.
- El software que descargues, ten por costumbre hacerlo de la página de su autor o autores, hay mucha software que no es lo que parece o simplemente viene manipulado.
- Nunca aceptes archivos ejecutables de desconocidos o conocidos por el Messenger, en este último caso si te parece raro el ejecutable o no tenías una conversación consúltale antes de descargar y ejecutar.
- Cuidado con las páginas de videos, ya que a veces muchas son falsas y obligan a los usuarios a descargar falsos códec.
- Evita usar una cuenta de administrador en un ordenador, crea un segundo usuario al principal y usa ese.
- Utiliza un buen firewall, en caso de colarse algún tipo de malware que conecte a otro ordenador o servidor puede éste cortar la transmisión.

6. Enlaces de interés.

http://www.stopmalware.net/ http://www.inteco.es/ http://www.infomalware.net http://foro.elhacker.net http://www.hispasec.com/ http://www.sinfocol.org/

7. Licencia.



Reconocimiento - NoComercial (by-nc): Se permite la generación de obras derivadas siempre que no se haga un uso comercial. Tampoco se puede utilizar la obra original con finalidades comerciales.