

DESINFECCIÓN POR ROOTKIT + ROGUE

Tipo de infección: Falso antivirus + Rootkit

Nombre de los ejecutables instalados:

Nombre del virus	Nombre del proceso	Тіро
Malware Defense	Mdefense.exe	Rogue
Setdebugx	Settdebugx.exe	Malware
H8SRT	H8SRTovfuohojmb.dll	Rootkit
krl32mainweq	krl32mainweq.dll	TrojanDNS Changer
MEMSWEEP2	4.temp	Trojan/Backdoor

Acciones del virus:

- Desactivar toda protección instalada en el ordenador.
- Instalación de falso antivirus.
- Instalación de Rootkit.
- Instalación de Troyano camuflado por la acción del Rootkit

Lo ideal ante este tipo de casos sería:

- Cortar la conexión a internet lo antes posible para interrumpir que se descarguen ficheros a tu ordenador o al menos evitar que el atacante pueda seguir manipulando tu ordenador.
- No reiniciar el ordenador.
- Intentar NO conectar el ordenador comprometido a Internet para descargar las herramientas que te hagan falta, ten en cuenta que esta infección está activa incluso en modo seguro.
- Desactivar Restaurar Sistema.
- Eliminar los procesos creados por el virus en el Administrador de tareas.
- Comenzar a eliminar manualmente y con diferentes herramientas todo lo relacionado con el virus.

Herramientas para la eliminación de los diferentes virus instalados:

Nombre de la utilidad:	Enlace de descarga:
Ccleaner	http://www.ccleaner.com/download
RegSeeker	http://www.hoverdesk.net/freeware.htm
Gmer	http://www.gmer.net/
SpyDLLRemover	http://www.rootkitanalytics.com/tools/spy-dll-remover.php
Svchost Process Analizer	http://www.neuber.com/free/svchost-analyzer/
Malwarebytes Antimalware	http://www.malwarebytes.org/mbam.php
Spybot Search&Destroy	http://www.safer-networking.org/es/spybotsd/index.html
Dr.Web Anti-Virus	http://download.drweb.com/demoreg/
Hijackthis	http://free.antivirus.com/hijackthis/

Las herramientas "SpyDLLRemover" y "Svchost Process Analizer" se utilzarán solo para comprobar que estamos hablando de la misma infección, alguna variante del mismo o similar:

Análisis con SpyDLLRemover:

desec desec	J. K Z AND	delez	E S	er Pyware	s feo	m zhe s	รัฐระยาที			www.Root	kitAnalytics	.com Abo
Spy Scanner (2) Proc Start Scan	ess Viewer	ULL Tracer		ana an	ul reint	NA DAGA		Thre	eat Levels: nline	Dangerou DLL Pro	us Suspicio perties	us Need / Export
Name 🔺	Threat Inf	o	Compa	эпу	Description	n	Process ID	File Size	File Date	File Path		10,000
H8SRTovfuohojmb.dll	Check Onlin	ne						36 K	31-12-2009	\\?\globalr	oot\systemroot\s	ystem32\h8srto
ameacm.acm	Check Onlin	ле	http://	www.mp3dev	Lame MP3	codec engine		384 K	12-01-2004	c:\archivo:	s de programa\co	dec pack de elis
msdmo.dll	Check Onlin	ne						14 K	19-08-2004	c:\window	s\system32\msdn	no.dll
avizlib, dll	Check Onlin	ne						112 K	20-09-2000	c:\archivo:	s de programa\co	dec pack de elis
avimszh.dll	Check Onlin	ле						68 K	20-09-2000	c:\archivo:	s de programa\co	dec pack de elis
mcdvd_32.dll	Check Onlin	ne	MainCo	incept	MainConce	ept DV Codec	1000	277 K	15-04-2002	c:\archivo:	s de programa\co	dec pack de elis
arext.dll	Check Onlin	ne						123 K	21-07-2007	c:\archivo:	s de programa\wi	nrar\rarext.dll
UnlockerCOM.dll	Check Onlin	ne						8 K	07-09-2006	c:\archivo:	s de programa\un	locker\unlocker
hpzsnt08.dll	Check Onlin	ле	HP					180 K	11-03-2003	c:\window	s\system32\hpzsi	ht08.dll
						10						>
owing all the proce	esses havir	ng the select	ed DL	Т				Remo	ove DLL	Remove	DLL from ALL	Kill Proces
Process Name 🔺	PID	Company		Description		DLL Address	DLL Load	Memory	File Size	Date	File Path	
Explorer.EXE	1712	Microsoft Corp	oora	Explorador de W	indows	0x10000000	1	10,256 K	1,012 K	19-08-2004	C:\WINDOWS\	Explorer.EXE
svchost.exe	324	Microsoft Corp	oora	Generic Host Pro	cess for	0x10000000	1	956 K	14 K	19-08-2004	C:\WINDOWS\	system32\svcho
svchost.exe	2008	Microsoft Corp	oora	Generic Host Pro	cess for	0x10000000	1	784 K	14 K	19-08-2004	C:\WINDOWS\	system32\svchc
svchost.exe	1336	Microsoft Corp	oora	Generic Host Pro	cess for	0x10000000	1	1,648 K	14 K	19-08-2004	C:\WINDOWS\	system32\svchc
]svchost.exe	1256	Microsoft Corp	oora	Generic Host Pro	cess for	0x10000000	1	1,440 K	14 K	19-08-2004	C:\WINDOWS\	system32\svchc
svchost.exe	1204	Microsoft Corp	oora	Generic Host Pro	cess for	0x10000000	1	64,788 K	14 K	19-08-2004	C:\WINDOWS\	5ystem32\svcho
svchost.exe	1108	Microsoft Corp	oora	Generic Host Pro	cess for	0x10000000	1	1,752 K	14 K	19-08-2004	C:\WINDOWS\	system32\svcho
svchost.exe	1008	Microsoft Corp	oora	Generic Host Pro	cess for	0×00c70000	1	2,460 K	14 K	19-08-2004	C:\WINDOWS\	system32\svchc

Con esta herramienta podrás comprobar el archivo sospechoso, la fecha de creación y la ruta donde se aloja. Nos da la opción de eliminar el archivo infectado resaltado en la imagen en gris, pero corremos el riesgo que al eliminar "H8SRTovfuohojmb.dll" dañemos algunos de los procesos "Svchost" legitimos del sistema en los cuales se ha inyectado.

*** Si lo haces es bajo tu responsabilidad. Si no ha variado mucho el código del virus, siguiendo el tutorial queda desactivado, así que bajo mi punto de vista no tendría que ser eliminado con esta herramienta. *** Analisis con Svchost Process Analizer:

ollowing svchost pr	ocesses are run	ning on your computer:	1. 2000 0000 100		-
Process	ID	File	Group	Services	
svchost.exe	1108	< Acceso denegado, Run program as Administrato	< No Microsoft file >	0	
\Lambda svchost.exe	2008	< Acceso denegado, Run program as Administrato	< No Microsoft file >	0	
📕 svchost.exe	1336	C:\WINDOWS\system32\svchost.exe	LocalService	4	
📕 svchost.exe	1204	C:\WINDOWS\System32\svchost.exe	netsvos	28	
📕 svchost.exe	1008	C:\WINDOWS\system32\sychost.exe	DcomLaunch	2	
📕 svchost.exe	1256	C:\WINDOWS\system32\svchost.exe	NetworkService	1	- Î
📕 svchost.exe	324	C:\WINDOWS\system32\svchost.exe	imgsvc	1	
he selected proces	s contains the f	ollowing services:		1.5. 0.0000000	
Display Name		Service Name File		Status	
		Svchostanalyzer < Acceso denegado, Run program as Adn OK	ninistrator! >		

Comenzemos:

Una vez el ordenador infectado, no podremos hacer uso de ninguna opción en el escritorio. Solo mostrará acceso al falso antivirus y el resto del escritorio permanecerá inaccesible.

Presionaremos la secuencia de teclas (Ctrl+Alt+Supr) y para acceder al "Administrador de tareas", buscamos los siguientes procesos y los eliminamos:

- mdefense.exe
- settdebugx.exe

Son los dos únicos procesos "visibles" de la infección y forman parte del falso antivirus (Rogue), el resto permanece oculto por la acción del Rootkit.

Una vez terminados los procesos podremos observar que el falso antivirus desaparece y nos deja actuar sobre cualquier parte del escritorio y ejecutar algún que otro programa, aunque los procesos de las principales herramientas de desinfección están bloqueados.

Borrar la carpeta creada por "Malware Defense" en:

C:\Archivos de programa\Malware Defense

Eliminaremos las entradas creadas en el "MSConfig", así iremos borrando todos los restos: Inicio \rightarrow Ejecutar \rightarrow Escribir en la ventana: msconfig En la nueva ventana, navegaremos hasta la pestaña "Inicio" y desmarcan las dos entradas relacionadas con "mdefense.exe" y "settdebugx.exe". Ahora clickamos sobre Aplicar, Aceptar y en la nueva ventana que aparezca clickamos sobre: Salir sin reiniciar.

Configuración del sistema	
Debe reiniciar el equipo para que s	surtan efecto algunos cambios
efectuados por Configuración del	sistema.

A parte de desmarcar los casilleros pertencientes al virus, borrámos las entradas creadas en el Msconfig. Podemos utilizar Ccleaner o borrarlas manualmente desde el registro. Entrar al "Editor del registro": Inicio \rightarrow Ejecutar \rightarrow escribir regedit en la ventana y aceptar.

Busca y elimina las entradas relacionadas con "MDefense.exe" y "Settdebugx.exe" en las siguientes rutas:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Una vez delante del editor del registro pulsa las teclas (Ctrl+b) y aparecerá una pantalla de búsqueda, introduce los nombres de los procesos y borra todo lo relacionado con ellos. Rutas a borrar (eliminar la carpeta con todo el contenido) :

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\MSConfig\startupreg\Malware Defense

Nombre	Tipo	Datos
a)(Predeterminado)	REG_SZ	(valor no establecido)
a) command	REG_SZ	"C:\Archivos de programa\Malware Defense\mdefense.exe" -noscan
abhkey	REG_SZ	НКСИ
ad inimapping	REG_SZ	0
ablitem	REG_SZ	mdefense
abikey	REG_SZ	SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\MSConfig\startupreg\settdebugx.exe

Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
ab) command	REG_SZ	C:\DOCUME~1\Oscar\CONFIG~1\Temp\settdebugx.exe
abhkey	REG_SZ	НКСИ
ab) inimapping	REG_SZ	0
abitem	REG_SZ	settdebugx
abikey	REG_SZ	SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Una vez terminado de borrar todo lo relacionado a los procesos visibles, pasaremos Ccleaner al sistema de archivos y al registro, borrando todo lo que encuentre.

(Si lo tienes instalado se ejecutará con normalidad, no es bloqueado...)

Ahora necesitamos reiniciar el pc pero en "Modo a prueba de fallos", esto se hace para que el pc cargue solo los controladores y servicios básicos. Entraremos al "Msconfig", vamos hasta la pestaña "BOOT.INI" y marcamos el casillero "/SAFEBOOT", por defecto se activará la casilla "Mínimo". Click sobre Aplicar, Aceptar;

ieneral	SYSTEM.INI	WIN.INI	BOOT.INI	Servicios	Inicio	Herramientas		
boot loa imeout= default= operatii nulti(0)r	ader] =30 =multi(0)disk(0) ng systems] disk(0)rdisk(0)p	rdisk(0)par	tition(1)\WI	NDOWS ="Microsoft	Windows	: XP Professional" /noex	ecute=optin /fa	stdetect ,
•				III				Þ
Comp	robar todas la	s r <u>u</u> tas de i	nicio	Predetermi	nado	Subir] [Baja	31'
Opcion (SAF (NO (BO)		Mínimo Mínimo (int	© <u>R</u> ed ærfa <u>z</u> interad	⊚ Rep tiva)	paración	<u>T</u> iempo de espera	: 30 seg.	

Nos aparecerá una ventana donde nos dará la opción de reiniciar o no, ahora le decimos que SI queremos reiniciar y esperamos a que lo haga. Verás que carga Windows y nos muestra una ventana informativa donde nos dice que estamos ejecutando Windows en modo a prueba de fallos, aceptamos y esperamos que cargue el escritorio.

Ahora toca echar mano de algunas herramientas para poder eliminar el rootkit instalado en el sistema. El problema es que no podrás hacer uso de ninguna herramienta de desinfección a no ser que renombres el nombre del ejecutable SIN modificar su extensión (.exe). Una de las herramientas que mas utilizaremos es "Gmer antirootkit", pero si intentamos ejecutarla se nos dirá que no se puede por que se han modificado los permisos sobre la cuenta del administrador. El nombre del ejecutable del Gmer es "Gmer.exe", lo que haremos es renombrarlo como "er.exe" y ahora si se ejecutará;



Una vez ejecutado, hará un leve escaneo y nos mostrará la siguiente pantalla:

Туре	Name	Value	Sustem
Code Code Code Device Device AttachedD AttachedD AttachedD Service	82B26420 829BA648 82A147DE 829DA646 YFileSystem/Ntfs \Ntfs YFileSystem/Fastfat \Fat \Driver\Tcpip \Device\Tp \Driver\Tcpip \Device\Tcp \Driver\Tcpip \Device\Udp \Driver\Tcpip \Device\Bawlp C:\WINDOWS\system32\drivers\H8SRTgxwbmtjet.sys (*** hidde GMER WARNING !!!	ZwEnumerateKey ZwFlushInstructionCache IofCallDriver IofCompleteRequest 82B6C1F8 8281B1F8 epfwtdi.sys (ESET Personal Firewall T epfwtdi.sys (ESET Personal Firewall T epfwtdi.sys (ESET Personal Firewall T (SYSTEM) H8SRTd.sys	I Sections I Sections I IAT/EAT I Devices I Modules I Processes I Threads I Libraries I Services I Registry I Files
	GMER has found system modification, which might Dou you want to fully scan your system ?	t have been caused by ROOTKIT activity.	✓ C:\ ✓ ADS ✓ Show all Scan Copy

El mensaje de advertencia nos dice que Gmer ha encontrado una modificación en el sistema y podría ser causado por la acción de un Rootkit. Nos da la opción de realizar un escaneo completo del disco. De momento le decimos que NO, y eliminamos el servicio creado por el Rootkit, marcado en rojo :

Service → C:\WINDOWS\system32\drivers\H8SRTgxwbrntjet.sys → [***hidden***] → [SYSTEM] H8SRTd.sys

Clickamos con el derecho del ratón en el texto y aparecerá un desplegable, clickar sobre "Delete Service". Ahora SI haremos un escaneo completo, clickar sobre el botón "Scan" y dejarlo haciendo (dependiendo del procesador, memoria y cantidad de archivos tardará más o menos tiempo).

Una vez terminado nos mostrará en pantalla todo lo que haya encontrado y nos dará la opción de guardarlo en un log (esto puede ser útil, pues al presentarse en un foro con un problema les servirá de ayuda a solucionarlo).

Ya guardado el log del análisis, nos centramos en el Gmer y podrás comprobar que de todas las rutas donde se encuentran los rastros del rootkit, al clickar con el botón derecho del ratón para poder eliminarlo no deja elegir "ninguna" opción.



En la primera pantalla nada más iniciar Gmer, podrás ver que solo tenemos dos pestañas en el menú superior/izquierda. La primera pestaña "Rootkit/Malware" es donde haremos los escaneos en el sistema y la segunda "> > >" desplegará varias pestañas nuevas donde podremos ver/escanear también en el registro, sistema de archivos, módulos cargados, procesos en ejecución (con opción de terminar "x" proceso) y alguna cosa más que por ahora no tocaremos. Fijense que la pestaña para los análisis "Rootkit/Malware" ha quedado en sexto lugar después de clickar sobre "> > ".

Primero veremos unas capturas de las rutas y subcarpetas donde se alojan los diferentes archivos del Rootkit y luego miraremos la forma de eliminarlas:

** Justo debajo de las dos ventanas de datos, podrás ver las rutas completas donde está alojado :

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services\H8SRTd.sys









🖻 🦲 SOFTWARE		Name	Туре	Data	•	Event
🕀 🧰 Sivx		BB Combofix.exe	0			Export
🕀 🦲 ACE Compression Software		😼 daft.exe	0			Save
🕀 🦲 Adobe		download_mbam-setup.exe	0		3	
🗄 🛄 ahead		drwebbscd.exe	0			
🕀 🔜 Alcohol Sott		emergencyutil.exe	0		1	
		FAMEH32.exe	0			
		FCH32.exe	0			
		fixpolicies.exe	0			
E Classes		flash_disinfector.exe	0			
Elerits Elerits Elerits Elerits		fsaua.exe	0			
Elisoft		fsav32.exe	0			
ESET		iiii fsdfwd.exe	0			
🗄 🧰 Fraunhofer		fsgk32.exe	0			
🗄 🦲 Gemplus		fsgk32st.exe	0			
🕀 🧰 GNU		fsquidll.exe	0			
😟 🧰 Google		FSM32.EXE	0			
🖨 🧰 H8SRT		FSMA32.EXE	0			
- Connections		FSMB32.EXE	0			
- disallowed		fspc.exe	0			
injector		fsgh.exe	0			
		fssm32.exe	0			
Hewlett-Packard		fsus.exe	0			
	1	amer.exe	0		-1	
		1		0	C .	
	-					

En la ruta de la captura superior, podrás ver todos los ejecutables de las herramientas de desinfección que bloquea para hacer mejor su estancia en tu ordenador...

Ahora vamos hasta la pestaña "Registry":

rocesses Modules Services Files	Registry Rootkit/	'Malware 🛛 Autostai	rt CMD	_
🕽 My Computer	Name	Туре	Data	Export
				Save
				-
	▲ [• •	
IKEY_LOCAL_MACHINE				
				T Comment

Para navegar y poder modificar las diferentes claves del resgistro (ya que no nos deja eliminarlas), veremos que la pantalla se divide en dos secciones, en la ventana izquierda veremos las diferentes ramas del registro y al llegar a la ruta del archivo que deseamos eliminar y clickarle con el ratón, nos mostrará en la ventana derecha los valores del archivo. Esto es lo que tendremos que modificar, bien cambiándole la extensión al archivo o renombrándolo como valor "0".

En mi caso renombré las extensiones de los archivos.

Empezaremos modificando los valores del registro para inutilizar/hacer inservibles los ficheros creados por el Rootkit.

Navegar hasta:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services\H8SRTd.sys

Al clickar sobre la carpeta "modules" verás que en la ventana de la derecha muestra la ruta de unos cuantos archivos, haz click con el botón derecho del ratón sobre el primero y verás que se abre una pequeña ventanita que dice "Modify", clickale y se abrirá una nueva ventana donde tendrás que modificar el valor del archivo como hemos mencionado un poco más arriba.

De los tres casilleros de la ventana con datos, verás que solo deja modificar en el último, eso es lo que hay que modificar.

** En esta imagen ya están modificados los archivos, fíjate en la extensión de cada uno de ellos...

GMER 1.0.15.14972		- 🗆 ×
GMER 1.0.15.14972 Processes Modules Services Files R Flpydisk Flbydisk FlbMgr Fs_Rec Ftdisk Gpc H8SRTd.sys H8SRTd.sys HidServ HidServ HidServ HidUsb	egistry Rootkit/Malware Autostart CMD ata ?\globalroot\systemroot\system32\H8SRTpxurteoafw.dld ?\globalroot\systemroot\system32\H8SRTnqvnsyfrxl.dld ?\globalroot\systemroot\system32\H8SRTovfuohojmb.dld ?\globalroot\systemroot\system32\H8SRTtfmqibnmpxat	Export
Industry		
HKEY_LOCAL_MACHINE\SYSTEM\Controls	Set003\Services\H8SRTd.sys\modules	1
	OK	Cancel

Cuando termines de modificar las rutas, al volver hacia la ventana de la izquierda para buscar otra ruta a modificar, nos mostrará un pequeño aviso conforme hemos modificado ciertos valores de los ficheros, aceptamos y a por las siguientes rutas.

Tendrás que repetir los pasos de arriba en todas y cada una de las rutas expuestas a continuación, y si ves alguna ruta nueva que no esté en la imagen también tendrá que ser renombrada:

- * HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
- * HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services
- * HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services

Aquí unas cuantas capturas más de las rutas a modificar:

GMER 1.0.15.14972		- 🗆 ×
GMER 1.0.15.14972 Processes Modules Services Files Registry Rootkit/Ma Files Eventlog Files EventSystem Fastfat Files File	alware Autostart CMD T Data R 0 R \systemroot\system32\drivers_H8SRTgw000tjet.sy_ R 0x00000000 (0) R 0x00000000 (0)	Export
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services\H	3SRTd.sys	
	OK	Cancel



Una vez modificadas todas las rutas, aceptaremos los cambios realizados y haremos un nuevo escaneo en la pestaña <Rootkit/Malware>. Recuerda que primero realiza un breve escaneo y ya no tendría que mostrar el servicio que creaba y mostrado en rojo en el primer escaneo del Gmer.

Service → C:\WINDOWS\system32\drivers\H8SRTgxwbrntjet.sys → [***hidden***] → [SYSTEM] H8SRTd.sys

Hacemos un escaneo completo y cuando termine mostrara en pantalla lo que haya encontrado. Si modificaste las extensiones a las entradas creadas, mostrará la modificación en el log:

	Value 🔺	System
JSBFDO-2	82A601F8	G Sections
vice\LanmanDatagramReceiver	8286E1F8	I♥ Sections
vice\LanmanRedirector	8286E1F8	IAT/EAT
Control	82B6E1F8	✓ Devices
Scsi\a4n1i98j1	82A7C500	Modules
	8282E1F8	j∓ modules
	8285/1F8	Processe
ontrois et \services \sptd\Lrg@s1	771343423	✓ Threads
ontroiser \services \sptd\Lrg@s2	260007732	
ontrolSet/Services/sold/Cfa/0D79C293C1ED614		I Libraries
ontrolSet\Services\sptd\Cfg\0D79C293C1ED614	C:\Archivos de programa\Alcohol Soft\Alcohol 120\	Services
optrolSet\Services\sptd\Cfg\0D79C293C1ED614		Registru
ontrolSet\Services\sptd\Cfg\0D79C293C1ED614	0xD6 0x45 0xC9 0x02	it registly
ontrolSet\Services\sptd\Cfg\0D79C293C1ED614		I Files
ontrolSet\Services\sptd\Cfg\0D79C293C1ED614	0x20 0x01 0x00 0x00	10 CA
et003\Services\H8SRTd.sys@start	0	
et003\Services\H8SRTd.sys@type		
et003\Services\H8SRTd.sys@imagepath	\systemroot\system32\drivers_H8SRTgw000tjet.sy_	
et003\Services\H8SRTd.sys@group		
et003\Services\H8SRTd.sys\modules		
etUU3\Services\H85H1d.sys\modules@H85H1d	\\?\globalroot\systemroot\system32\drivers\H85H1gxwbrntjet.ss	1 '
etUU3/Services/H85H1d.sys/modules@H85H1c	\\/\dotside	ADS
etuus \Services \H85H d.sys \modules@H85H srcr w002\ Services \H85H d.sys \modules@h85H srcr	\\?\globalroot\systemroot\system32\H85H1tmqlbnmpxat \\?\alabakaat\outbanaat\outbana22\H85H1tmqlbnmpxat	Show all
etoos vservices vnoon i u. sys vnodules @nositsen	1121 glob alroot/ systemicot/ systemicot/ systemicot/ and microstrue did	
et003\Services\sotd\Cfa\0D79C293C1ED614184	TYP globalloonsystemioonsystemio2 (hosh i pxuiteoalw.ulu	I Scan
1		
]		Сору

Si las modificaste con valor "0", nos mostrará ese valor en vez de la ruta con la extensión modificada.

Ya terminadas las modificaciones, pasamos de nuevo Ccleaner borrando lo que encuentre en el sistema de archivos y en el registro.

Reiniciamos el pc sin modificar el cambio en el Msconfig, para que vuelva a iniciar en modo a prueba de fallos. Una vez cargue el escritorio ejecutamos Regseeker, y clickamos sobre <Clean the registry>, borramos todo lo relacionado con "H8SRT...".

Nos mostrara algunas rutas donde se alojan varios archivos, eliminamos las entradas, cerramos y volvemos a pasar Ccleaner borrando lo que encuentre.

RegSeeker				- 🗆 🗙
ReaSeeker	Find in registry	***		👌 Languages
Version 1.55	HKEY_CURRENT_USE	R		
Find in registry	HKEY_LOCAL_MACHI	INE \injector h8srtserf;h8	srtbbr	
 Startup entries 	HKEY_LOCAL_MACHI	INE 003\Services\ <mark>H8S</mark> RTd.sys		
📕 Histories				
🏂 Favorites				
扔 Tweaks				
🗳 Clean the Registry				
🛃 Backups				
🛃 Print				
🌀 About				
🗶 Quit RegSeeker				
F Backup before deletion	Select (1)	😽 Action	Total : 3	Stop
		0%		

Entramos al Msconfig y en la pestaña <BOOT.INI> dejamos marcada la entrada "/SAFEBOOT" pero clickamos sobre la opción "Red" (se desmarcará Mínimo), esto lo hacemos para que podamos tener acceso a internet y poder actualizar las bases de datos de las herramientas que a continuación utilizaremos. Una vez cambiado aceptamos y que reinicie...

Ahora instalamos "Malwarebytes Antimalware". Sin renombrar la extensión del programa, tendría que dejar instalarlo sin problemas. Antes de nada actualizar el programa...

Lo dejamos que haga un escaneo completo y nos arrojara la siguiente infección:

Malware	bytes' Anti-N	lalware					-	
	M	alwa	areb	ytes	Ant	f-)	Malwa	are
Escáner	Protección	Actualizar	Cuarentena	Registros	Lista a Ignor	ar	Preferencias	
	Resultado Aquí tiene la Cierre todos	s del Exame a lista de malwa los programas o interrumpan d	n are que Malware antes de elimina de forma inconor Elementos	bytes' Anti-Mal r ya que duran	ware ha encont te la eliminaciór	rado e n pued	en su sistema. le que algunos	
Troja	n.DNSChanger	File	C:\WINDOWS	\system32\krl3	2mainweq.dll	0	No action tak	 en.
Quitar lo	Seleccionad		Ignorar	Guard	lar Informe		Menú Principa	
					Comprar		Salir	

Eliminamos el archivo infectado y si podemos en modo seguro hacemos un escaneo con el antivirus que tengamos (dependiendo del antivirus puede ser que encuentre algún archivo infectado o no). Acabado el escaneo con antivirus si pudimos hacerlo, instalamos Spybot Search&Destroy y actualizamos también. Hacemos un escaneo completo y reparamos todas las entradas encontradas (no tengo captura de esto, pero eran tres o cuatro entradas, no más).

Entramos al editor del registro y eliminamos la carpeta siguiente (en el pie de foto pueden ver la ruta):

Archivo Edición Ver Favoritos Ayuda CurrentVersion Image: CurrentVersion Image	🎒 Editor del Registro			- 🗆 ×
CurrentVersion Nombre Tipo Datos	Archivo Edición Ver Favor	itos Ayuda		
App Manageme App Paths Applets Hearts Paint Regedit SysTray Tour Control Panel	CurrentVersion	Vombre	Tipo	Datos
	App Manageme App Paths Applets Hearts Paint SysTray Tour Control Panel	변(Predeterminado) IFindFlags 비LastKey IView	REG_SZ REG_DWORD REG_SZ REG_BINARY	(valor no establecido) 0x0000000e (14) Mi PC\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MEMSWEEP2 2c 00 00 00 00 00 00 00 01 00 00 00 ff

Cerramos el Regedit y volvemos a ejecutar la herramienta "Gmer" para eliminar del registro todo lo relacionado con las entradas creadas en la ruta "MEMSWEEP2".

Abierto el Gmer vamos a la pestaña Registry y modificamos el contenido de todas las entradas creadas, con valor "0" de la siguientes rutas:

- * HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
- * HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services
- * HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services

Aquí unas capturas de las entradas aun sin modificar;

in the state		Name	tkit/Malware	Autostart LMD	
 Idap Idap LicenseService LmHosts MEMSWEEP2 Security Messenger mirrorv3 mnmdd mnmsrvc 		Security	REG_BIN	01 00 14 80 90 00 00 0	Export
	240	<u></u>			

rocesses	Modules Se	ervices Files	Registry	Rootkit/Malware	Autostart CMD			
	ld ld l l l M M m m m m m m m	rtfdc ap censeService mHosts EMSWEEP2 essenger irrorv3 nmdd nmsrvc			Name DisplayName ErrorControl ImagePath Start Type	Type REG_SZ REG_DWORD REG_EXPAND_SZ REG_DWORD REG_DWORD	Data MEMSWEEP2 0x00000001 (1) \??\C:\WINDOWS\system32\4.tmp 0x00000003 (3) [MANUAL] 0x00000001 (1)	Export .
			autCautralC			10		

En esta captura puedes ver los valores ya modificados de la imagen superior:

🔳 (eivier										
Processes	Modules	Services	Files	Registry	Rootkit/Malwar	e Autostart CMD	1			
		Ibrtfdc			^	Name	Туре	Data		Evport
		Idap LicenseS) LmHosts MEMSWE Messenge mirrorv3	ervice EEP2 er		-	DisplayName BErrorControl ImagePath BE Start BE Type	REG_SZ REG_DWORD REG_EXPAND_SZ REG_DWORD REG_DWORD	0 0x00000000 (0) 0 0x00000000 (0) 0x00000000 (0)		Save
GMER	WARNING I GMER uses machine ret	II raw registr boot.	y read/	write acces	s. Please note the	at registry changes v ncelar	vill be visible by WIND(DWS API after	р ОК	Cancel

Aceptar los cambios realizados al registro.

Una vez que vuelvas a realizar un escaneo con Gmer la entrada "MEMSWEEP" no volverá a parecer. Cerramos el Gmer y realizamos una limpieza con Cleaner borrando los restos que encuentre.

Ya con los valores modificados haremos la última modificación para denegar los permisos creados sobre las cuentas de administrador del sistema en la rama del registro "LEGACY_MEMSWEEP2" pues no se puede eliminar, pero la dejaremos vacia por completo y sin permisos.

Abrimos el editor del registro (regedit). Una vez dentro pulsamos (ctrl+b) y buscamos la entrada creada "LEGACY_MEMSWEEP2".

Le hacemos un click con el botón derecho del raton y elegimos "Permisos", nos mostrará esta ventana:

SYSTEM		
	[0
armisos da SYSTEM	Agregar	ir Denegar
Control total		
Leer Permisos especiales		

Una vez en esta ventana, clickamos sobre el botón "Opciones avanzadas" y nos aparecerá la siguiente ventana de configuración de permisos:

Tipo		Permiso Control total	Hereda	ido de			Aplicar a
Permitir Permitir	SYSTEM Todos	Control total Leer	MACHI	NE\SYSTE NE\SYSTE	4\CurrentControlS(4\CurrentControlS)	et\Enum et\Enum	Esta clave y sus Esta clave y sus
Agreg	iar	Modificar		Quitar			
, Hereda con las	ar del objeto s entradas in	principal las er dicadas aquí c	ntradas d le forma	le permisos r explícita.	elativas a los objeti	os secund	arios. Incluirlas jun

Para modificar los permisos desmarcaremos la entrada enmarcada en color rojo en la foto superior, de forma que nos aparecerá una ventana informativa:

a ver mas muonarsi	n aabta parmiaaa aapaaialaa la	alaaaiana una antrada u	haas alia an Madiliaat
	n sobre permisos especiales, s	eleccione una entrada y	naga ciic en mouliicai.
ntradas de permisos:			
lipo Nombre	Permiso	Heredado de	Aplicar a
Denegar SYSTEM Denegar Todos	Control total	<no heredado=""></no>	Esta clave y sus subcl Esta clave y sus subcl
Permitir SYSTEM	Control total	MACHINE\SYS	Esta clave y sus subcl
Permitir Todos	Leer	MACHINE\SYS	Esta clave y sus subcl
Segu	uridad		
Agregar	Seleccionar esta opo	ción significa que las enti	radas de permisos primario
Heredar del ol	Que se refieren a los objeto.	objetos secundarios no	se aplicarán más a este
Reemplazar la	 Para copiar las entr este objeto desde el 	adas de permisos que se objeto principal, haga cli	e aplicaron previamente a ic en Copiar.
aqui y que se	 Para quitar las entra desde el objeto princi evolícitamente, baga 	adas de permisos que se sipal y guardar sólo aquel a clic en Quitar	aplicaron previamente llos permisos aquí definido:
Reemplazar la aquí y que se	este objeto desde el • Para quitar las entra desde el objeto princ	objeto principal, haga cl adas de permisos que se sipal y guardar sólo aque	ic en Copiar. aplicaron previamente llos permisos aquí defir

Clickamos sobre el botón "Quitar" y eliminamos las dos cuentas creadas que contienen las rutas con los archivos del MEMSWEEP2.

Aplicar y aceptar los cambios creados. aHora nos mostrará la siguiente ventana con el contenido completamente vacío:

Agregar	Quitar
Permitir	Denega
8	H
	Agregar

Una vez hecho todo lo expuesto podemos entrar al Msconfig y desmarcar la opción "/SAFEBOOT" para poder reiniciar en modo normal. Una vez en el escritorio de Windows nos aseguraremos de que no queden rastros realizando escaneos con tu antivirus preferido, Spybot, y Malwarebytes, por supuesto "actualizando las bases de firmas" antes de realizar los escaneos.

En caso que el pc tenga tiempo ya instalado el sistema operativo, sería conveniente hacer "<u>Desfragmentación</u>" al disco duro (ya que estamos liados). No se eliminaran datos, digamos serán ordenados y agrupados de forma que no queden espacios entre ellos . Es una tarea simple y eficaz para mantener tu disco ordenado:

Inicio \rightarrow Panel de control \rightarrow Herramientas administrativas \rightarrow Administración de equipos

Nos mostrará la siguiente ventana, en la etiqueta "Almacenamiento" clicka sobre el texto "Desfragmentador de discos" y listará los discos instalados. Haremos un click sobre la unidad (C:) y se activarán los botones para analizar el disco y comprobar si necesita ser desfragmentado o desfragmentar directamente. Esto dependerá como hemos dicho antes del tiempo que lleves con Windows instalado, la cantidad de archivos alojados o si has realizado alguna vez una desfragmentación. Puedes recibir el mensaje de que no se necesita desfragmentar el disco.



Espero les pueda ayudar en algo este tutorial pues aun siendo una infección diferente, los pasos a seguir para la desinfección pueden ser similares a los aquí expuestos.

Un saludo 😊

R32 – Usuario del foro de seguridad: http://www.infomalware.net/