

¿Los Antivirus realmente nos protegen?



By 4n0nym0us

Eliminando un Spy de nuestro sistema

Este documento está creado didácticamente para no solo mostrar las vulnerabilidades de 39 de los mejores antivirus del mercado, si no también para enseñar de una forma clara y entendible como encontrar y eliminar algunos tipos de malwares de nuestro sistema.

Bueno hace un par de días un compañero de trabajo me vino alarmado con su PC ya que este de repente empezaba a tener una conexión demasiado lenta al conectarse a Internet y el equipo en sí, además le consumía un 90% de la memoria disponible.

Estaba casi de claro que le entro un virus, lo cual lo primero que hice fue mirar el administrador en busca de algún proceso extraño...

Me llamo la atención el encontrarme con un **lsass.exe** con su nombre de usuario cargado en memoria, ya que el original se carga de sistema...

Rápidamente fui a consola he hice un **netstat -b** para ver los procesos y sus conexiones, impresionantemente había un montón de incesantes intentos de conexión desde dicho proceso al mismo rango de IP únicamente se le sumaba uno a la última cifra... parecía estar hecho para petar mi red...

G:\Documents and Settings\diego>netstat -b

Conexiones activas

Proto	Dirección local	Dirección remota	Estado	PID
TCP	casa-nwskzwe6z:2132	94.58.15.185:22	SYN_SENT	1836
[lsass.exe]				
TCP	casa-nwskzwe6z:2133	94.58.15.186:22	SYN_SENT	1836
[lsass.exe]				
TCP	casa-nwskzwe6z:2134	94.58.15.187:22	SYN_SENT	1836
[lsass.exe]				
TCP	casa-nwskzwe6z:2135	94.58.15.188:22	SYN_SENT	1836
[lsass.exe]				
TCP	casa-nwskzwe6z:2136	94.58.15.189:22	SYN_SENT	1836
[lsass.exe]				
TCP	casa-nwskzwe6z:2137	94.58.15.190:22	SYN_SENT	1836
[lsass.exe]				
TCP	casa-nwskzwe6z:2138	94.58.15.191:22	SYN_SENT	1836
[lsass.exe]				
TCP	casa-nwskzwe6z:2139	94.58.15.192:22	SYN_SENT	1836
[lsass.exe]				
TCP	casa-nwskzwe6z:2140	94.58.15.193:22	SYN_SENT	1836
[lsass.exe]				
TCP	casa-nwskzwe6z:2141	94.58.15.194:22	SYN_SENT	1836
[lsass.exe]				
TCP	casa-nwskzwe6z:1041	lusten.si:31091	ESTABLISHED	1836
[lsass.exe]				
TCP	casa-nwskzwe6z:5152	localhost:1775	CLOSE_WAIT	1700
[jqs.exe]				

Archivo Opciones Ver Apagar Ayuda

Aplicaciones Procesos Rendimiento Funciones de red Us

Nombre de imagen	PID	Nombre de usuario
dfrgnfss.exe	1328	diego
explorer.exe	1336	diego
GoogleToolbarNot...	724	diego
hpwu5chd2.exe	1712	diego
jqs.exe	1700	SYSTEM
lsass.exe	620	SYSTEM
lsass.exe	1836	diego
mmc.exe	474	diego
mspaint.exe	3156	diego
nvsvc32.exe	1884	SYSTEM
Proceso inactivo d...	0	SYSTEM
realsched.exe	2980	diego
rundll32.exe	1760	diego
services.exe	608	SYSTEM
smss.exe	480	SYSTEM
spoolsv.exe	1144	SYSTEM
svchost.exe	224	SYSTEM
svchost.exe	776	SYSTEM
svrhnst.exe	824	Servicio de red

Mostrar procesos de todos los usuarios

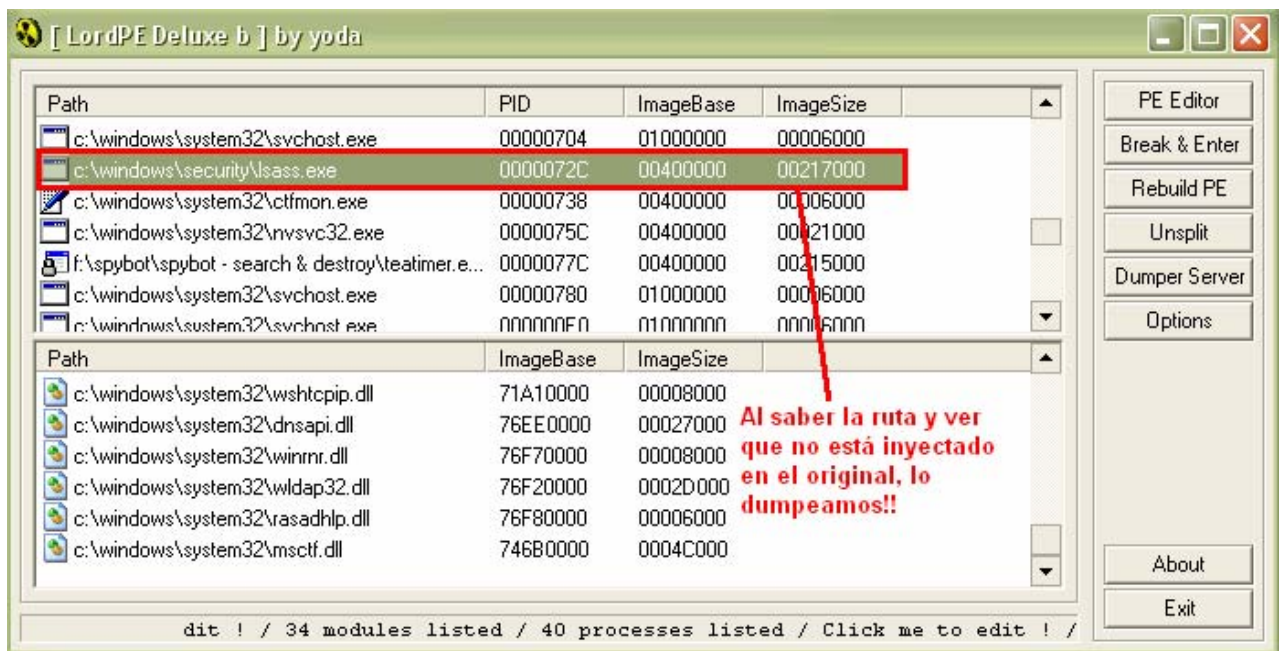
Procesos: 40 Uso de CPU: 20% Carga de transacción

El verdadero lsass.exe es un ejecutable de SYSTEM, además de tener un PID más bajo y no hace conexiones como este =)

Abrí mi querido **LordPE** para buscar el **PID**, este en Hexadecimal ahora por si estaba inyectado en el verdadero **lsass.exe** y escondía la ruta original...

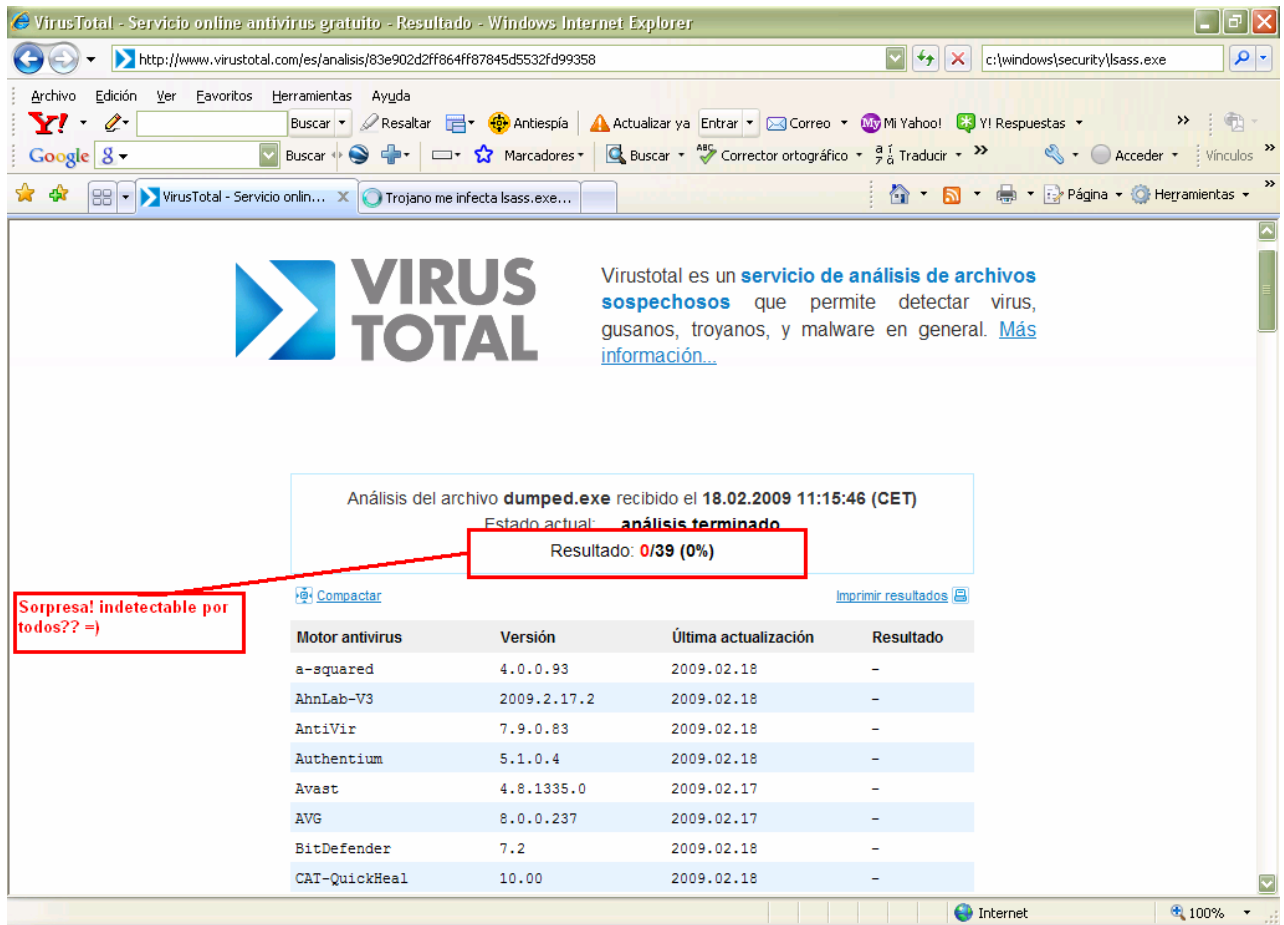
1836 = 72C

Nos dirigimos a este **PID** desde el **LordPe** y nos encontramos con que la ruta del falso **lsass.exe** es otra totalmente distinta de la original, ya que el de Microsoft se aloja de forma predeterminada en la carpeta **“C:/Windows/System32”** y este misteriosamente lo hacia en **“C:/Windows/Security”**:



Pinchamos con el botón derecho y hacemos un **Dump Full** para copiar el archivo que funciona en memoria y tenerlo más a mano...

Una vez dumpeado se guarda en el escritorio y fue enviado a un Scanner Online con **39 Antivirus**, veamos el resultado del Scanner...



The screenshot shows the VirusTotal website interface in Internet Explorer. The browser's address bar displays the URL: <http://www.virustotal.com/es/analisis/83e902d2ff864ff87845d5532fd99358>. The page title is "VirusTotal - Servicio online antivirus gratuito - Resultado - Windows Internet Explorer".

The main content area features the VirusTotal logo and a description: "Virustotal es un **servicio de análisis de archivos sospechosos** que permite detectar virus, gusanos, troyanos, y malware en general. [Más información...](#)".

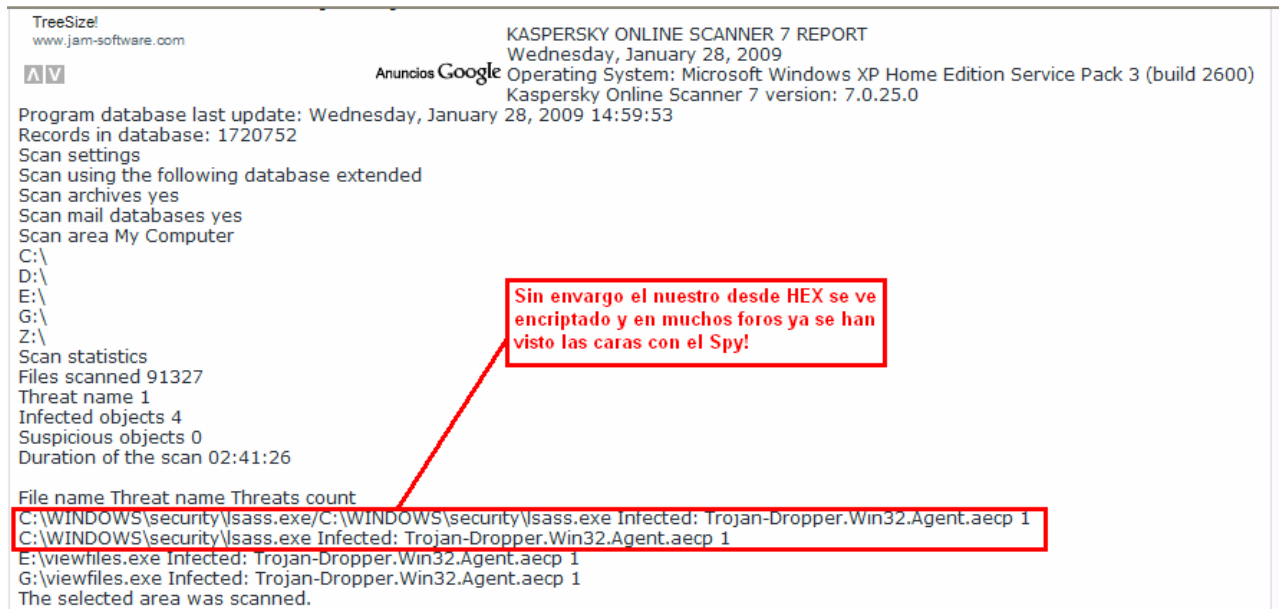
The analysis details for the file **dumped.exe** are shown, received on **18.02.2009 11:15:46 (CET)**. The current status is **análisis terminado** (analysis finished) and the result is **Resultado: 0/39 (0%)**. A red box highlights this result, with a red arrow pointing to a note: "Sorpresa! indetectable por todos?? =)".

Below the analysis details is a table listing the antivirus engines used for scanning:

Motor antivirus	Versión	Última actualización	Resultado
a-squared	4.0.0.93	2009.02.18	-
AhnLab-V3	2009.2.17.2	2009.02.18	-
AntiVir	7.9.0.83	2009.02.18	-
Authentium	5.1.0.4	2009.02.18	-
Avast	4.8.1335.0	2009.02.17	-
AVG	8.0.0.237	2009.02.17	-
BitDefender	7.2	2009.02.18	-
CAT-QuickHeal	10.00	2009.02.18	-

Algo no cuadra, es seguro que este archivo está infectado y los Scanners no nos alarman... sigamos con la investigación.

Bueno lo siguiente que hice fue poner la ruta de “C:/Windows/Security/lsass.exe”, y bien encontré mucha información sobre varios foros que alarmaban de un muy posible malware escondido en esa carpeta, aunque en estos los antivirus si lo detectaban...



TreeSize!
www.jam-software.com

KASPERSKY ONLINE SCANNER 7 REPORT
Wednesday, January 28, 2009
Operating System: Microsoft Windows XP Home Edition Service Pack 3 (build 2600)
Kaspersky Online Scanner 7 version: 7.0.25.0

Program database last update: Wednesday, January 28, 2009 14:59:53
Records in database: 1720752
Scan settings
Scan using the following database extended
Scan archives yes
Scan mail databases yes
Scan area My Computer
C:\
D:\
E:\
G:\
Z:\

Scan statistics
Files scanned 91327
Threat name 1
Infected objects 4
Suspicious objects 0
Duration of the scan 02:41:26

File name Threat name Threats count

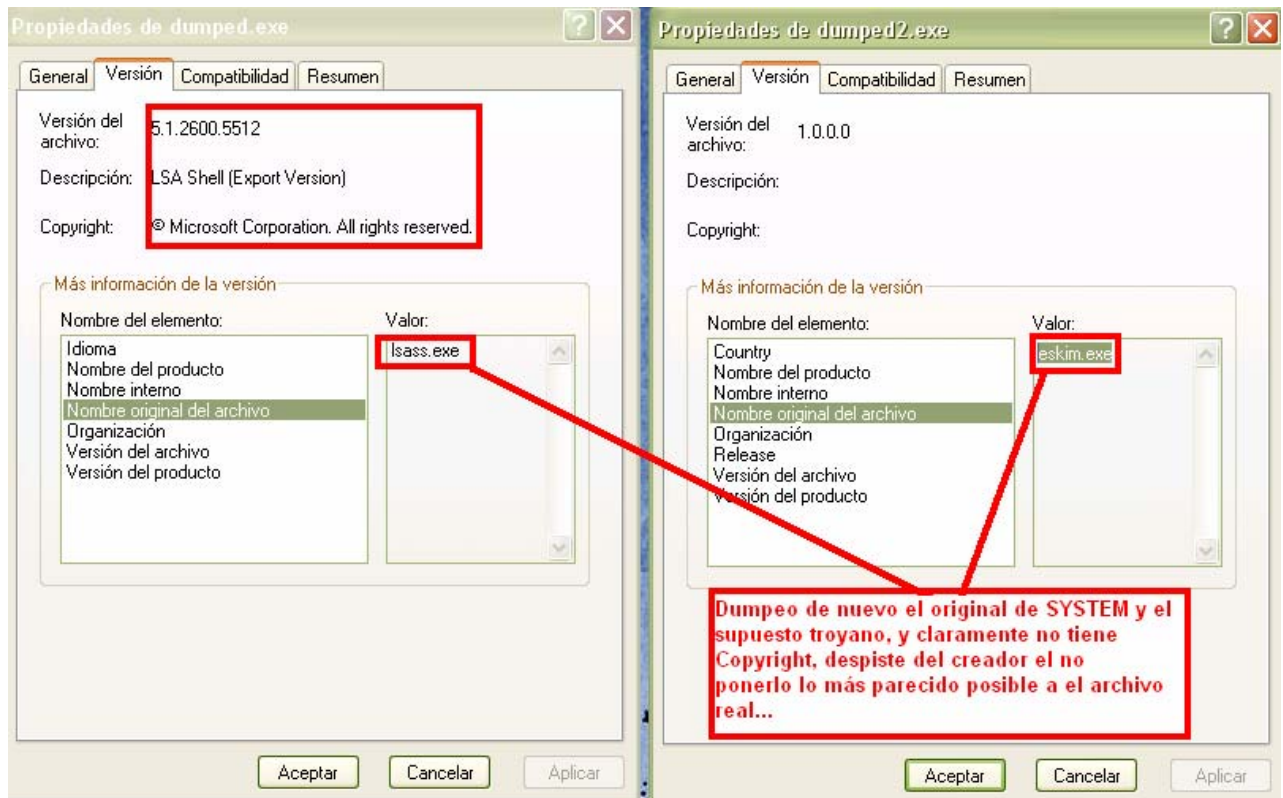
C:\WINDOWS\security\lsass.exe	C:\WINDOWS\security\lsass.exe	Infected: Trojan-Dropper.Win32.Agent.aecp 1
C:\WINDOWS\security\lsass.exe		Infected: Trojan-Dropper.Win32.Agent.aecp 1
E:\viewfiles.exe		Infected: Trojan-Dropper.Win32.Agent.aecp 1
G:\viewfiles.exe		Infected: Trojan-Dropper.Win32.Agent.aecp 1

The selected area was scanned.

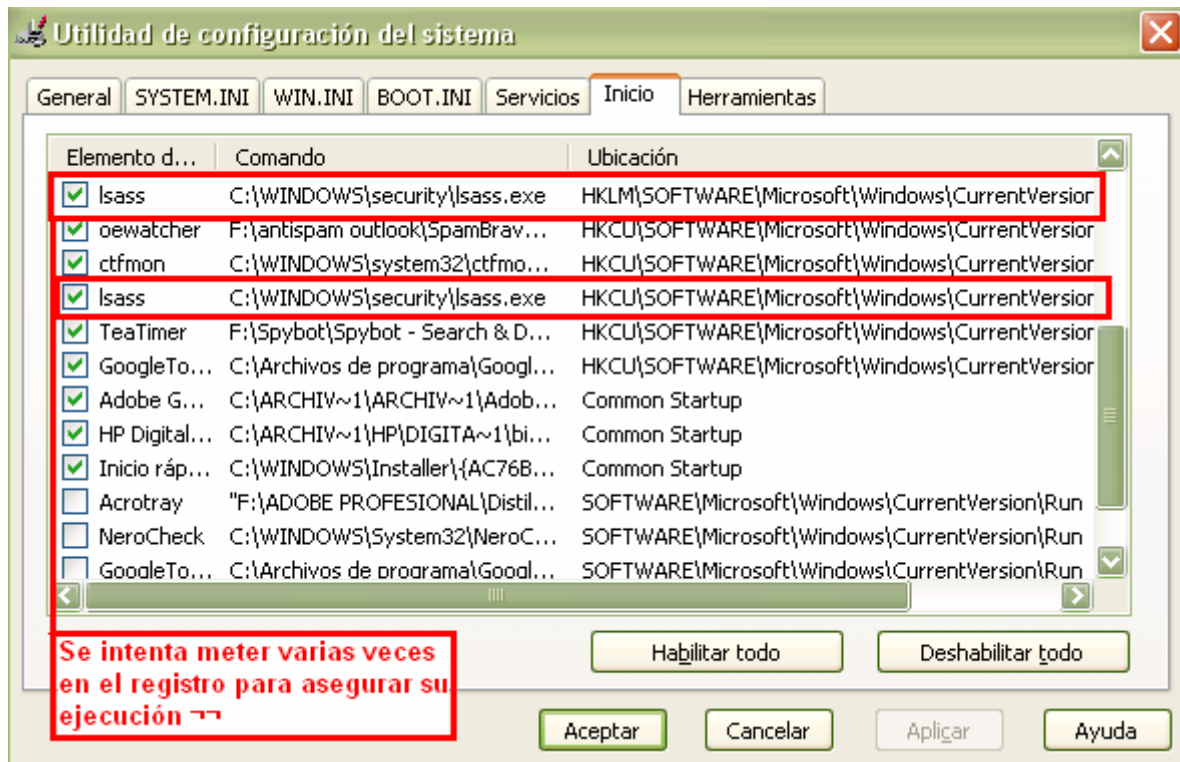
Sin envargo el nuestro desde HEX se ve encriptado y en muchos foros ya se han visto las caras con el Spy!

Desde Hexadecimal el archivo parecía totalmente encriptado así que supuse que era muy posible que fuera este el motivo de ninguna alarma.

Me dispuse a dumppear ahora los dos archivos el **lsass** de la carpeta original y el sospechoso, claramente como se ve en la imagen tenían claras diferencias en sus versiones, en peso y código...



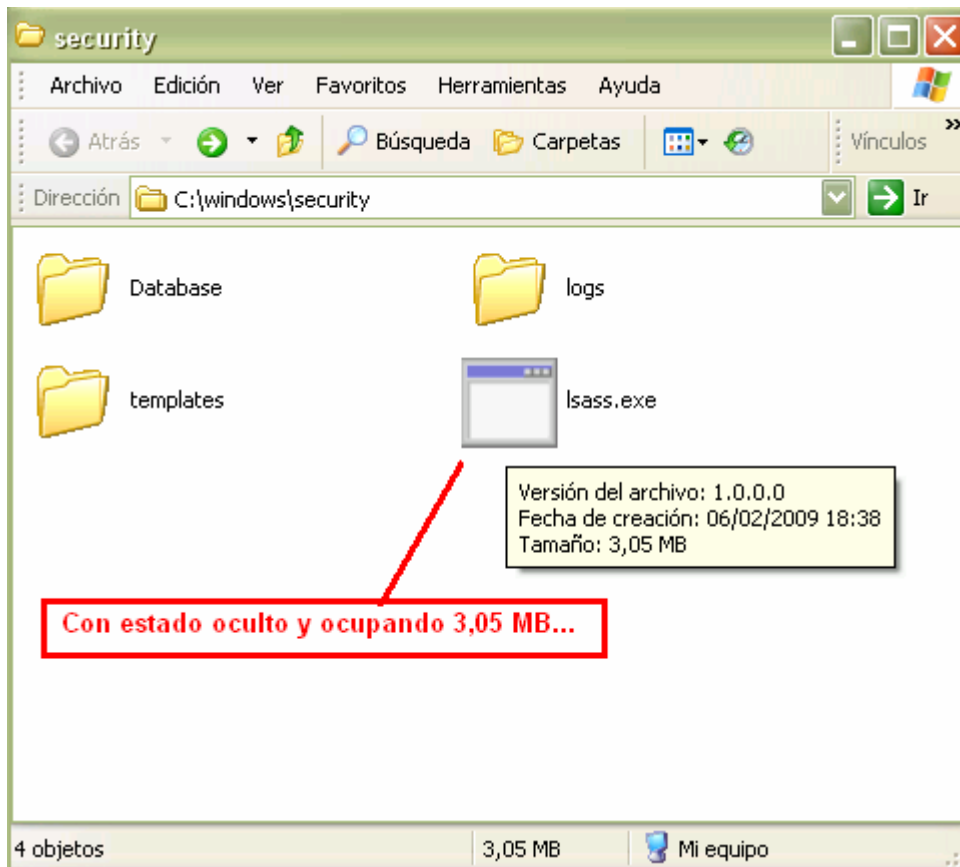
Después de salir de tantas dudas ante si en realidad era un malware me parecía bueno ver de que forma se lanzaba en el sistema para iniciarse automáticamente, así que me dirigí a **msconfig** desde ejecutar:



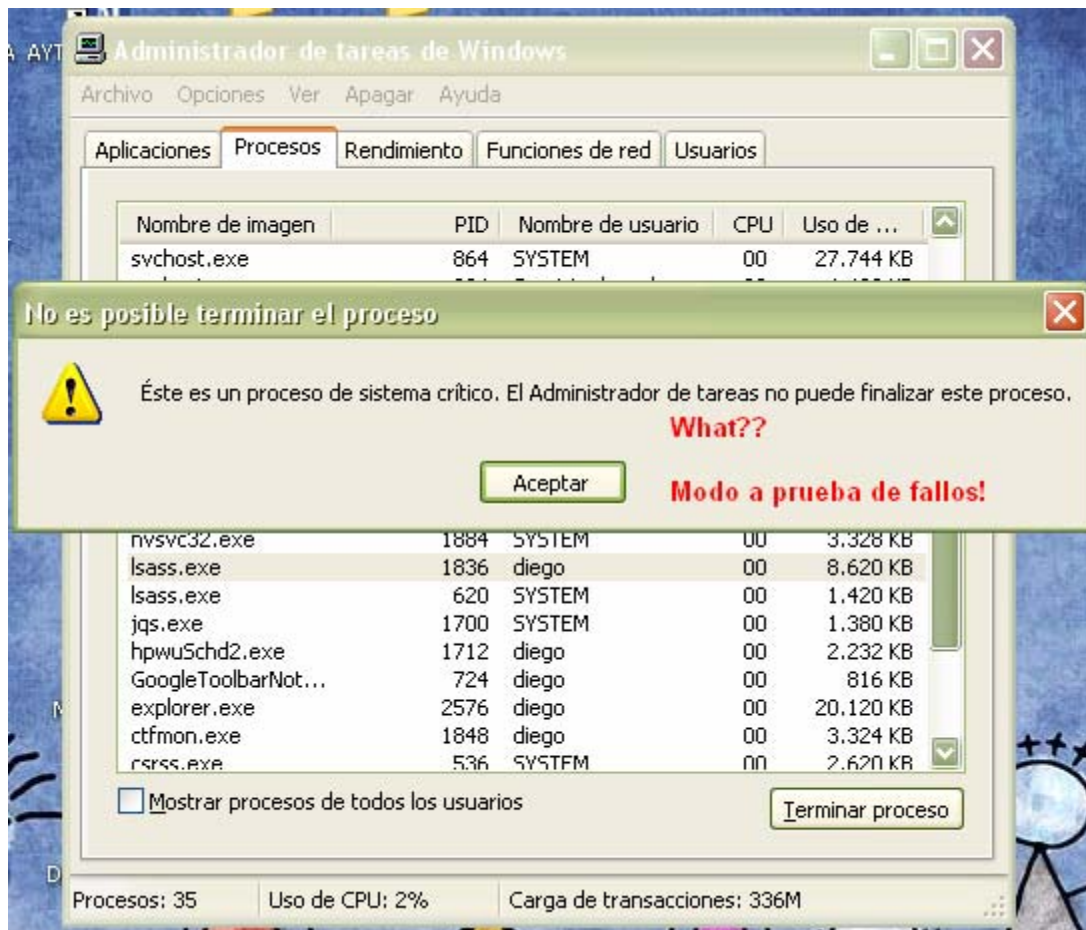
Claramente se veía incluso en el nombre de la entrada que lo intentaba varias veces para asegurarse que el archivo se ejecutaría...

Ahora ya si me decidí entrar en la misteriosa carpeta para identificar de manera visual a mi contrincante xD!!

Observando el archivo vemos que está de forma oculta de solo lectura y pesa 3,05MB, algo bastante raro para ser este archivo el de sistema...



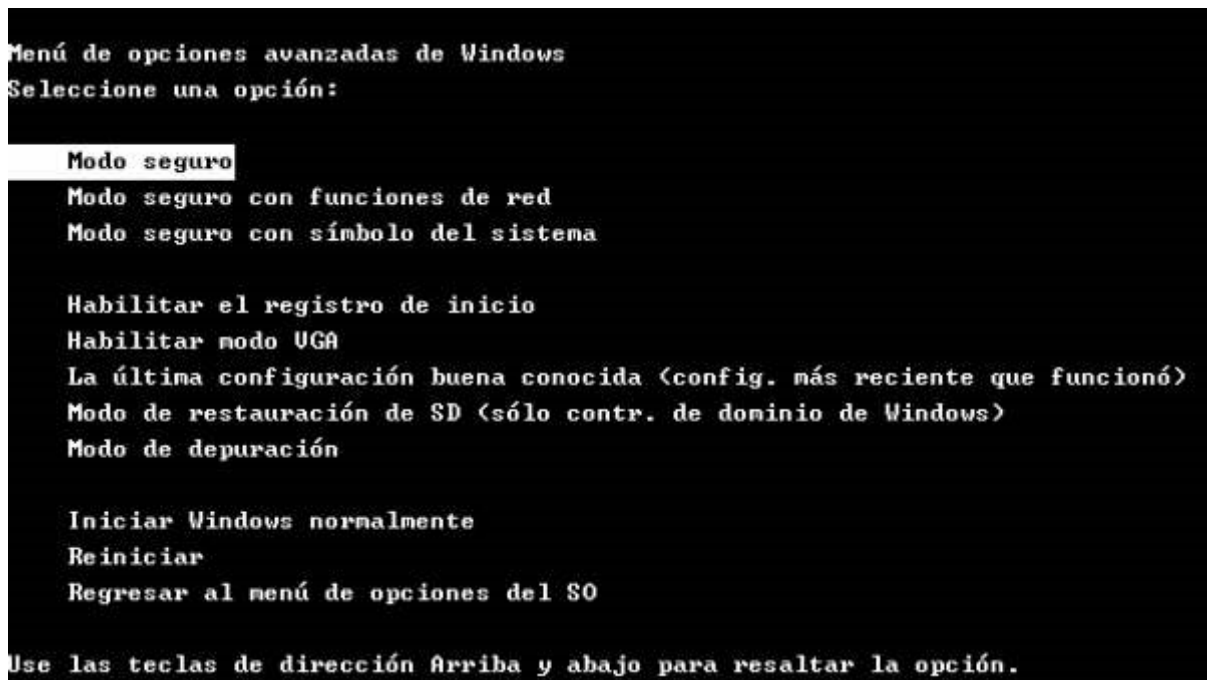
Con un “**Contrl + Alt + Supr**” saco el administrador de tareas para eliminar el proceso de manera fácil y poder eliminarlo manualmente, pero me salta para mi información que es un proceso critico! ¿¿??



Lo cual corriendo a modo a prueba de fallos para que no se ejecute con el inicio y poder eliminarlo fácilmente.

Nos disponemos a reiniciar la máquina.

Presionando **F8** antes de la iniciación del sistema para entrar al **Modo seguro**:



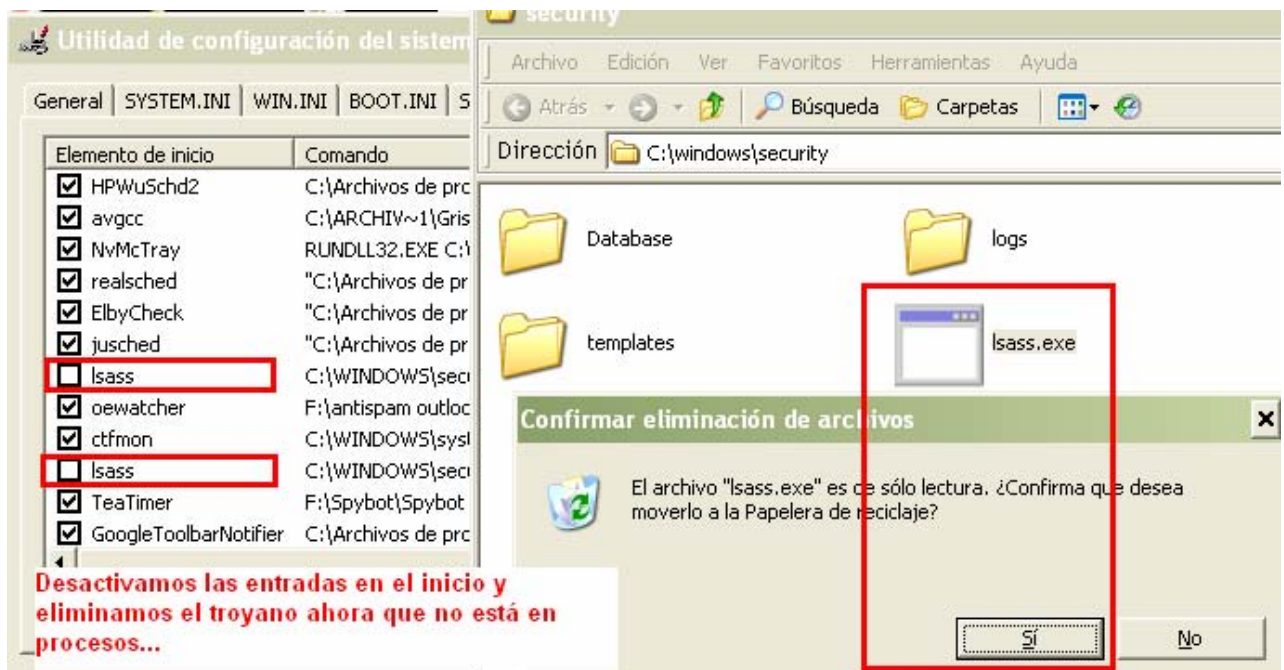
Una vez dentro del sistema saca de nuevo el **LordPE** para contemplar que proceso **lsass.exe** es el que se está ejecutando:

Task Manager window showing the 'PROCESOS' tab. The process list is as follows:

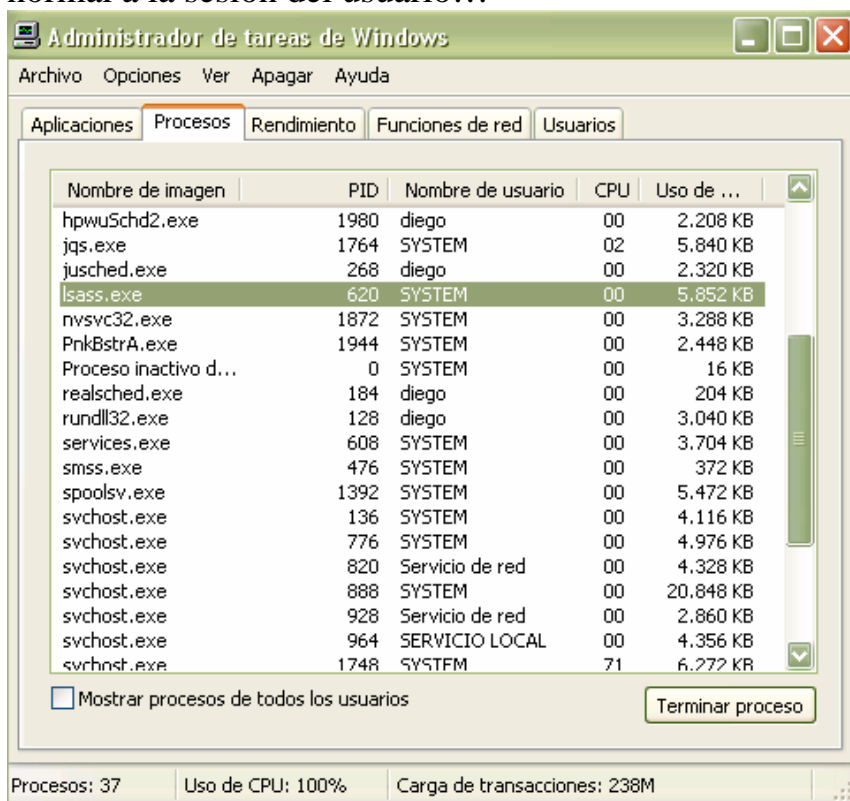
Nombre de imagen	PID	Nombre de usuario	CPU	Uso de m...
taskmgr.exe	1220		04	3,768 KB
LordPE.EXE	1208		00	4,076 KB
WinRAR.exe	1176		00	488 KB
explorer.exe	824		02	24,236 KB
svchost.exe	552		00	9,048 KB
svchost.exe	508		00	3,928 KB
svchost.exe	448		00	3,332 KB
lsass.exe	292		00	4,928 KB
services.exe	280		00	3,172 KB
winlogon.exe	236		00	992 KB
csrss.exe	212		02	3,308 KB
smss.exe	160		00	372 KB
System	4		00	208 KB
Proceso inactivo d...	0	SYSTEM	92	16 KB

A red box highlights the **lsass.exe** process. Below the task manager, a red box contains the text: **Desde aquí ya no está en ejecución el troyano, empezaremos con su eliminación...**

Viendo que el que corre es el original y el otro permanece dormido, vuelvo a las claves de registro y a eliminar el archivo de la carpeta **Security**:



Una vez acabado con este nos disponemos a reiniciar el sistema y entrar en modo normal a la sesión del usuario...



Una vez vueltos al sistema en modo normal vemos que el Isass.exe ha desaparecido, y el funcionamiento del equipo ahora es más rápido =>

Como se ve en la imagen anterior el **lsass.exe** que está corriendo ahora es el de sistema.

Volvemos a consola para ver si con un **netstat -b** si muestras las anteriores conexiones:

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\diego>netstat -b

Conexiones activas

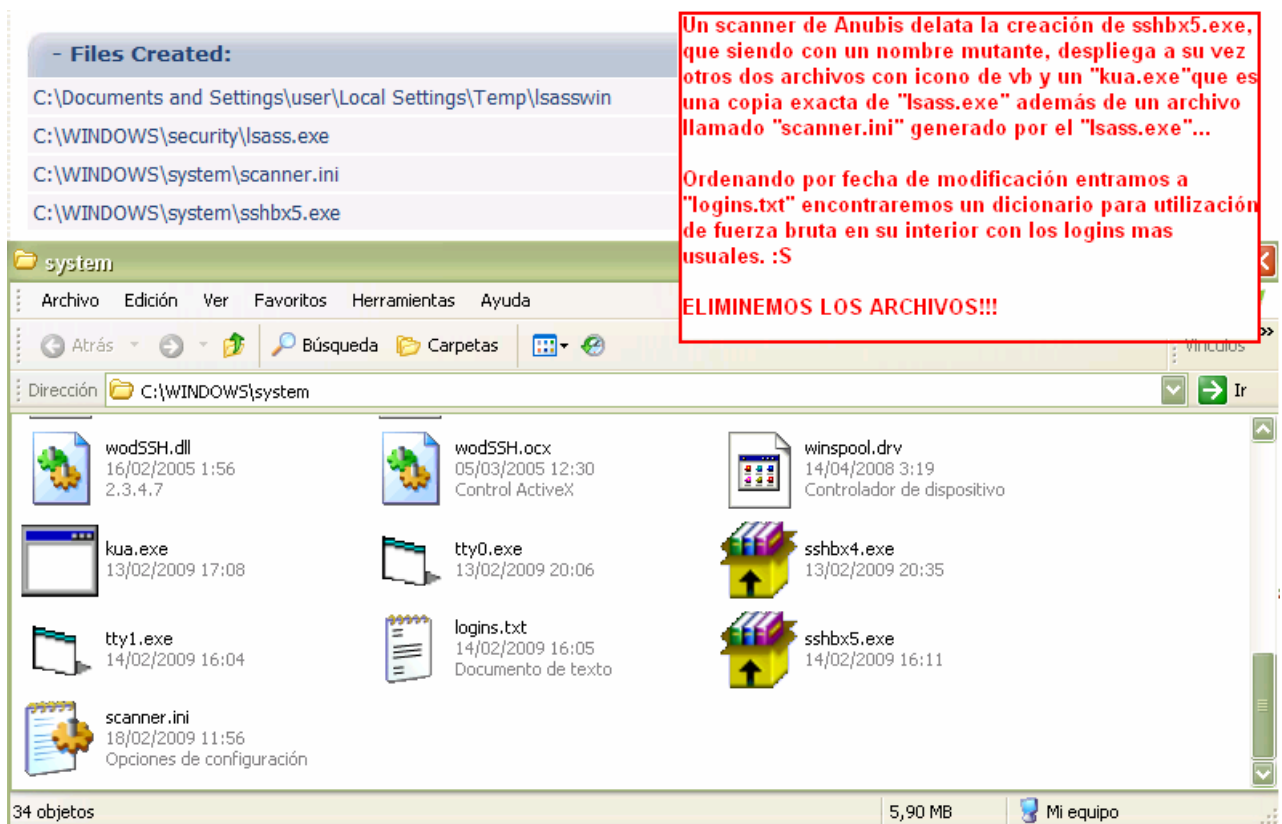
Proto  Dirección local      Dirección remota      Estado                PID
TCP    casa-nwskzew6z:1034  localhost:5152        FIN_WAIT_2            3220
[Sistema]

TCP    casa-nwskzew6z:5152  localhost:1034        CLOSE_WAIT             1764
[jqs.exe]

C:\Documents and Settings\diego>

Y las conexiones a la IP anterior desde el troyano se
perdieron... ya está eliminado totalmente!!!! =)
```

Intrigado por saber que tipo de malware era envié un Scanner del archivo infectado a Anubis el cual me mostró lo siguiente:



De todos estos archivos el que más me llamo la atención fue el **logins.txt**, ¿Para que quiere un archivo plagado de palabras?

Bien recopilemos información:

Las IP conectadas eran iguales, únicamente variaba su último número de orden siempre seguido, el puerto de conexión utilizado era el **22**, siendo este el de serie para las conexiones desde el protocolo **SSH**, además de crear dos archivos aleatorios llamados "**Sshbx?.exe**", tenemos un "**logins.txt**" con una burrada de palabras para ataques de diccionarios como **Admin Admin.- Root Root - User User...**

Mi conclusión clara es que nos encontramos con un **Robot**, el controlador nos usa de máquina **Zombie** para realizar ataques fortuitos por "**Ssh**" a todas las direcciones de IP que se encuentre por su paso por ataque de diccionario, cuando una de estas sea acertada se le enviará todo a nuestro pequeño delincuente...

Bueno acabando dejando la indagación ante tanta confusión me despido y termino eliminando los archivos y las claves de registro para que no haya más problemas...

Activado	Clave	Programa	Archivo
Si	HKCU:Run	ctfmon.exe	C:\WINDOWS\system32\ctfmon.exe
Si	HKCU:Run	SnowbotSD.TeaTimer	F:\Snowbot\Snowbot - Search & Destroy\TeaTimer.
No			rograma\Google\Google Toolbar
Si			soft\AVG7\avgcc.exe /STARTL
Si			ograma\Archivos comunes\Re
Si			ograma\Java\jre6\bin\jushec
Si			Health\HelpCtr\Binaries\MSCor
Si			SIONAL\Distillr\Acrotray.exe"
No			ograma\Elaborate Bytes\Clone
No			ograma\HP\HP Software Updat
No	HKLM:Run	hpztsb10	C:\WINDOWS\System32\spool\drivers\w32x86\
No	HKLM:Run	NeroCheck	C:\WINDOWS\System32\NeroCheck.exe
No	HKLM:Run	NvCpl	RUNDLL32.EXE C:\WINDOWS\System32\NvCpl.c
No	HKLM:Run	NvMcTray	RUNDLL32.EXE C:\WINDOWS\System32\NvMcTr
No	HKLM:Run	lsass	C:\WINDOWS\security\lsass.exe
No	Startup Common	Adobe Gamma.lnk	C:\ARCHIV~1\ARCHIV~1\Adobe\CALIBR~1\AD
No	Startup Common	Director de aplicaciones de escritorio Corel 8.LNK	F:\Corel\Suite8\Programs\DAD8.EXE
No			A~1\bin\hpqtra08.exe
No			{AC76BA86-1034-4700-

CCleaner

¿Esto borrará permanentemente la entrada para el programa del Menú Inicio.

¿Está seguro que quiere hacer esto?

Aceptar Cancelar

Para no dejar rastros en registro eliminemos la entrada con CCleaner

Espero que al menos les haya sido tan entretenido como a mí y de su agrado.

Un Saludo =)

By 4n0nym0us

Para indetectables.net

MSN: 4n0nym0us@Professionalhackers.gov