

UT01: Adopción de pautas de seguridad informática – Amenazas 2A

Nombre: Francisco Jesús García – Uceda Díaz - Albo
Curso: 2º ASIR.

Índice

- Antimalware: MalwareBytes.....	2
o Archivos analizados.....	4
o Uso CPU.....	4
o Opciones Avanzadas.....	5
o Tiempo de escaneo.....	8
o Vulnerabilidades y virus encontrados y desinfectados.....	8
- Antimalware: Spybot - Search & Destroy.....	9
o Archivos analizados.....	13
o Uso CPU.....	14
o Opciones Avanzadas.....	14
o Tiempo de escaneo.....	17
o Vulnerabilidades y virus encontrados y desinfectados.....	18
Conclusión.....	18

Instala al menos dos aplicaciones antimalware en modo local y realiza su comprobación en el PC para compararlos. Anota en dicha documentación de comparación: (Número archivos analizados, % Ocupación de CPU en ejecución, opciones avanzadas de escaneo, tiempo de escaneo, vulnerabilidades y malware encontrado y desinfectados).

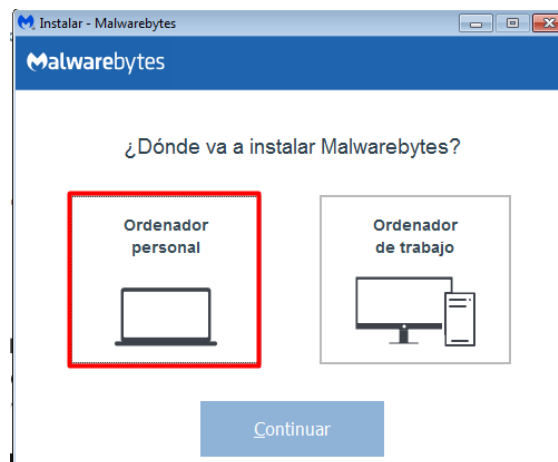
- Antimalware: MalwareBytes.

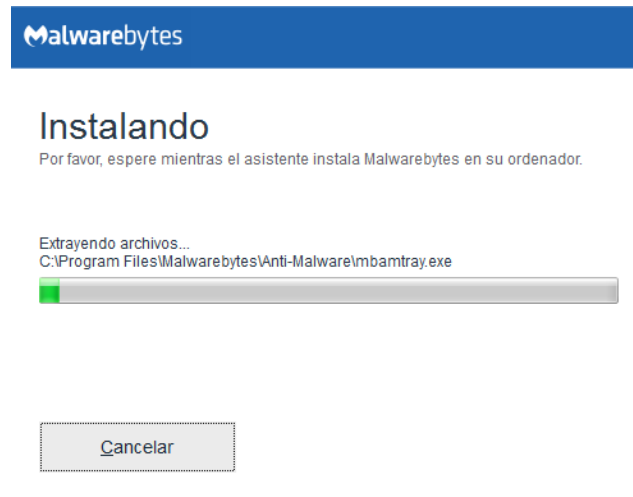
Malwarebytes Anti-Malware es un software anti-malware para Microsoft Windows, macOS y Android que detecta y elimina el malware. Fabricado por Malwarebytes Corporation, se lanzó por primera vez en enero de 2006. [Más info.](#)

Su instalación es sencilla, vamos a la web oficial a descargarlo, [Link.](#)



Una vez descargado lo ejecutamos e instalamos.

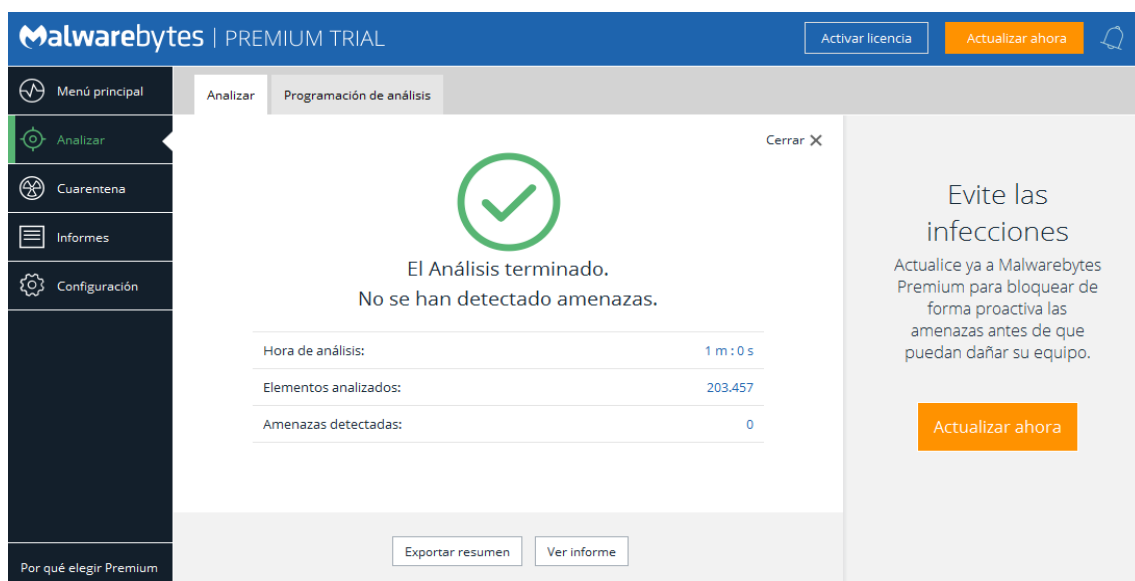




Una vez instalado lo ejecutamos, tendremos una prueba de 14 días. Pulsaremos en *Análizar ahora* para comenzar el análisis.

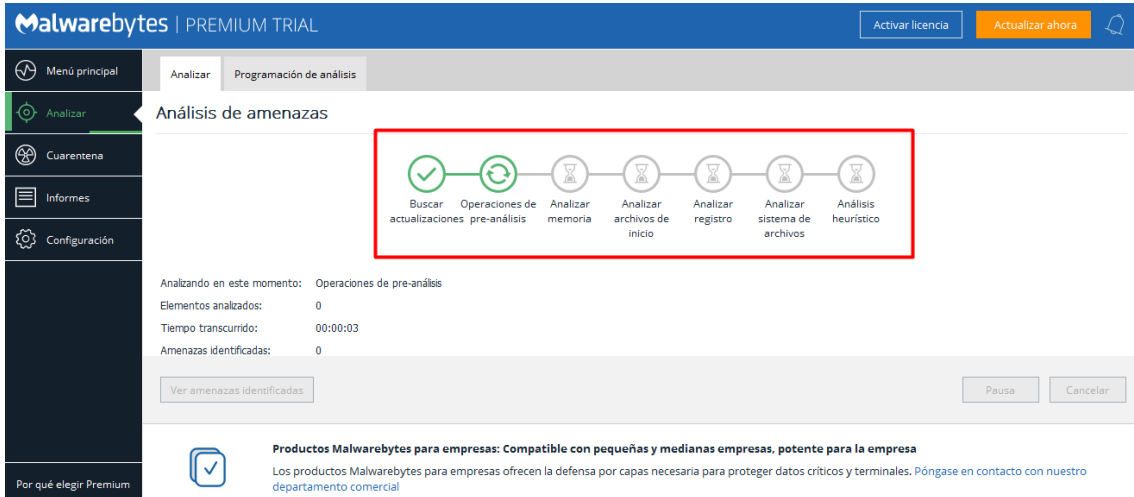


El análisis lo hará rápidamente.

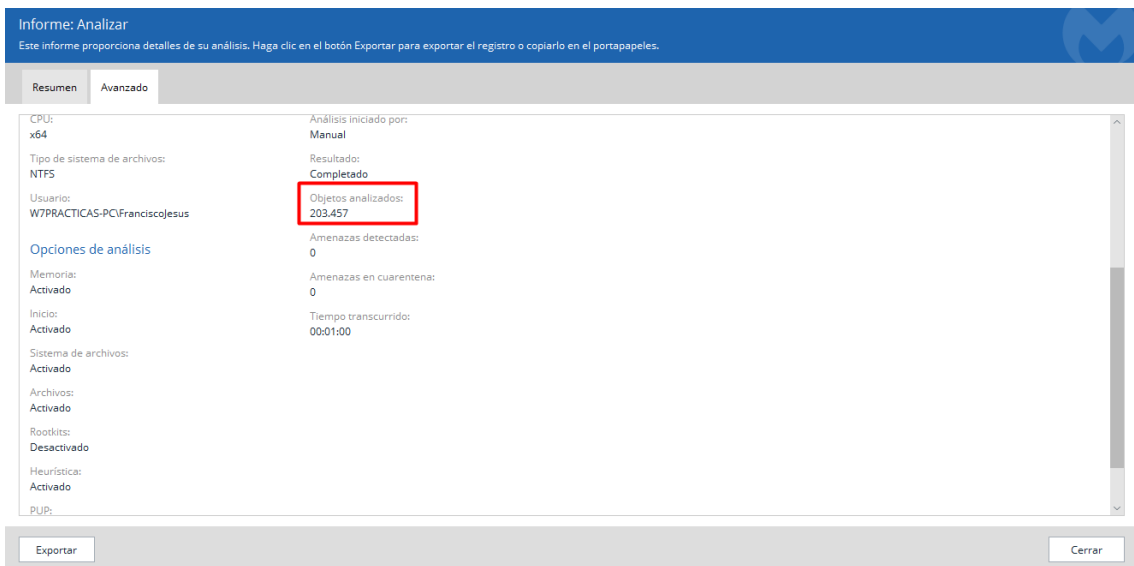


- Archivos analizados.

El programa analiza más archivos que el antivirus, podemos ver en el análisis los archivos que analiza.

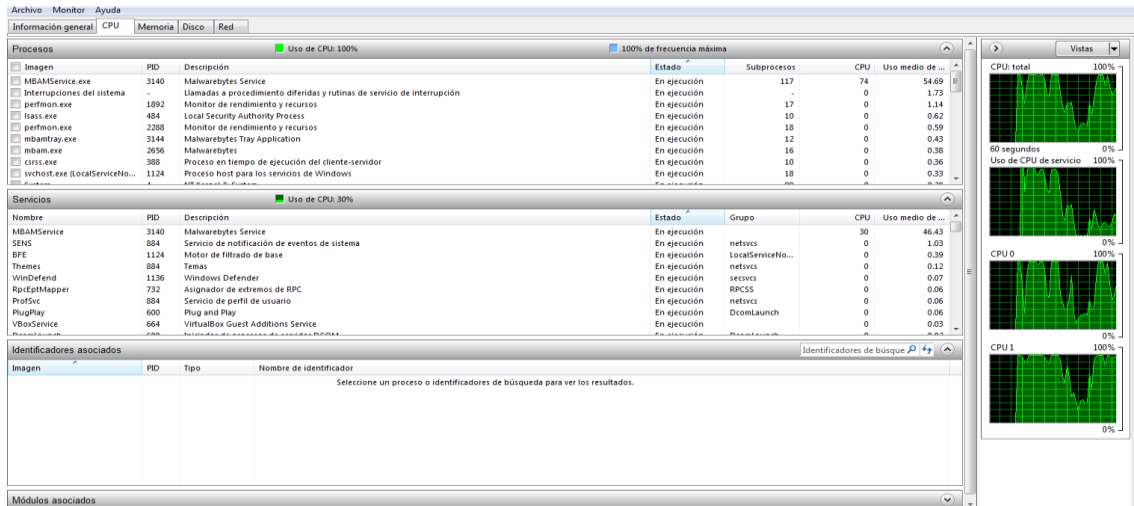


En total se analizaron 203.457 archivos.



- Uso CPU.

El uso que hace de la CPU es realmente grande (90% - 100%), pero esto no quiere decir que sea malo, ya que cuando abrimos una pestaña o navegamos baja el porcentaje del uso del programa, siempre usa los 4 núcleos del ordenador por lo cual hace pensar que el programa está totalmente optimizado para usar todos los núcleos libres, algo que me sorprende bastante y es muy positivo ya que no todos lo hacen.



○ Opciones Avanzadas.

Prácticamente apenas tenemos opciones avanzadas ya que son la mayoría de pago. Tenemos protección en tiempo real en la versión de prueba disponible.

Malwarebytes | PREMIUM TRIAL

Activar licencia Actualizar ahora

Menú principal

Analizar Cuarentena Informes Configuración

¡Fantástico!
Está protegido.

Su versión de prueba Premium finaliza en 13 días
Actualizar a la versión Premium

Analizar ahora

Por qué elegir Premium

FUNCIÓN PREMIUM: Caduca en 13 días.

Protección en tiempo real

Todas las capas de protección en tiempo real están activadas.

Protección web: Activada

Protección contra exploits: Activada

Protección contra malware: Activada

Protección contra ransomware: Activada

Detecciones de la protección en tiempo real: 0

Estado del análisis

Último análisis: Hace 3 minutos

Próximo análisis: 7/10/19 2:48

Detecciones de análisis: 0

Sistema

Actualizaciones: Actual

Podremos escoger entre tres tipos de análisis.

Malwarebytes | PREMIUM TRIAL

Activar licencia Actualizar ahora

Menú principal

Tipos de análisis Programación de análisis

Analizar

Cuarentena Informes Configuración

Por qué elegir Premium

Seleccionar un método de análisis

Análisis de amenazas

Nuestro análisis más exhaustivo. Analiza todos los lugares donde los malwares se suelen ocultar, incluyendo Memoria, Inicio, Registro y objetos del Sistema de archivos. Recomendado como análisis diario.

Recomendado

Análisis personalizado

Le permite personalizar dónde y qué desea analizar. Las modificaciones incluyen la elección de qué objetos deben analizarse (Memoria, Inicio y Registro). Permite personalizar el tratamiento de programas (PUP) y modificaciones (PUM) potencialmente no deseados.

Análisis rápido

Comprueba rápidamente los objetos de memoria y de inicio para detectar amenazas de malware activas. Si no se encuentra nada, le recomendamos que ejecute un análisis de amenazas para una detección más completa.

Iniciar análisis

En las opciones tendremos cosas interesantes como actualizaciones, seguridad, exclusiones, programación de análisis...

Malwarebytes | PREMIUM TRIAL Activar licencia Actualizar ahora

Menú principal | Aplicación | Protección | Programación de análisis | Exclusiones | Detalles de la cuenta | Acerca de

Actualizaciones de aplicaciones Restaurar valores predeterminados

Descargar e instalar automáticamente actualizaciones de componentes de aplicaciones

- Activada
- Notificarme cuando estén disponibles actualizaciones de la versión completa Activada
- Instalar actualizaciones de aplicación

Notificaciones Mostrar notificaciones de Malwarebytes en la bandeja del sistema de Windows

- Activada
- Cerrar notificaciones tras:
- Ver notificaciones cuando los ajustes de protección en tiempo real estén desactivados Activada

Modo de juego Ocultar notificaciones cuando las aplicaciones seleccionadas se muestran a pantalla completa

Recomendado si utilizar juegos, ver películas y realizar presentaciones

Habilitar automáticamente el Modo de juego cuando se detecte una aplicación seleccionada Activada

Impacto de los análisis en el sistema

- Los análisis manuales tienen alta prioridad y terminarán más deprisa
- Reducir la prioridad de los análisis manuales para mejorar la multitarea

Menús contextuales de Windows

Por qué elegir Premium

Malwarebytes | PREMIUM TRIAL Activar licencia Actualizar ahora

Menú principal | Aplicación | Protección | Programación de análisis | Exclusiones | Detalles de la cuenta | Acerca de

Protección en tiempo real Restaurar valores predeterminados

Protección web: Evita conexiones a sitios web maliciosos o comprometidos Activada

Protección contra exploits: Evita exploits de vulnerabilidades y ataques de día cero Activada

Protección contra malware: Evita infecciones por malware Activada

Protección contra ransomware: Evita que ransomware cifre sus archivos Activada

Opciones de análisis

Análisis en busca de rootkits Desactivada

Análisis dentro de los archivos Activada

Utilizar la detección de anomalías sin firmas para una mayor protección Activada

Protección contra amenazas potenciales

Programas potencialmente no deseados (PUP)

Modificaciones potencialmente no deseadas (PUM)

Por qué elegir Premium

Malwarebytes | PREMIUM TRIAL Activar licencia Actualizar ahora

Menú principal | Aplicación | Protección | Programación de análisis | Exclusiones | Detalles de la cuenta | Acerca de

Gestione la lista de elementos que se excluirán de la detección.

<input type="checkbox"/>	Exclusión	Tipo de exclusión
--------------------------	-----------	-------------------

Por qué elegir Premium

Podemos programar análisis.

Malwarebytes | PREMIUM TRIAL

Activar licencia Actualizar ahora

Menú principal Aplicación Protección **Programación de análisis** Exclusiones Detalles de la cuenta Acerca de

Análisis

Cuarentena

Informes

Configuración

Por qué elegir Premium

Gestione cuándo y cómo los análisis programados se ejecutan en su sistema.

<input checked="" type="checkbox"/>	Tipo	Inicio	Frecuencia	Si no existe
<input checked="" type="checkbox"/>	Normal	7/10/19 2:48:45	Se repite una vez cada 1 día	Ejecutar de nuevo dentro de 23 horas después de la última ej...

Añadir análisis programado

Cree y edite análisis programados automatizados para Malwarebytes.

Tarea programada

Tipo de operación:

Fecha de inicio: Hora de inicio:

Frecuencia y ajustes

Programar frecuencia: Recurrencia:

Buscar actualizaciones antes de analizar

Avanzado

ACEPTAR Cancelar

Agregar Editar Borrar

Malwarebytes | PREMIUM TRIAL

Activar licencia Actualizar ahora

Menú principal Aplicación Protección **Programación de análisis** Exclusiones Detalles de la cuenta Acerca de

Análisis

Cuarentena

Informes

Configuración

Por qué elegir Premium

Gestione cuándo y cómo los análisis programados se ejecutan en su sistema.

<input checked="" type="checkbox"/>	Tipo	Inicio	Frecuencia	Si no existe
<input checked="" type="checkbox"/>	Normal	6/10/19 22:12:38	Se repite una vez cada 1 día	Ejecutar de nuevo dentro de 23 horas después de la última ej...
<input type="checkbox"/>	Normal	7/10/19 2:48:45	Se repite una vez cada 1 día	Ejecutar de nuevo dentro de 23 horas después de la última ej...

En *Cuarentena* podremos ver los archivos en cuarentena, en este caso no tenemos ninguno ya que no se detectó nada en el sistema.

Malwarebytes | PREMIUM TRIAL

Activar licencia Actualizar ahora

Menú principal **Cuarentena**

Análisis

Cuarentena

Informes

Configuración

Por qué elegir Premium

Malwarebytes ha puesto estos elementos en cuarentena. Ellos no representan ningún peligro cuando están en cuarentena. Puede restaurar o eliminar estos elementos. Los elementos eliminados de la cuarentena se eliminarán de forma permanente de su equipo.

<input type="checkbox"/>	Nombre	Fecha	Tipo	Ubicación
--------------------------	--------	-------	------	-----------

Restaurar Borrar

- Tiempo de escaneo.

El tiempo de escaneo ha sido muy pero que muy rápido, entiendo que es gracias a la optimización que tiene con los núcleos y porque busca cosas en concreto. En total tardo 1 minuto.

The screenshot shows the 'Informe: Analizar' interface. At the top, there is a blue header with the text 'Informe: Analizar' and a sub-header 'Este informe proporciona detalles de su análisis. Haga clic en el botón Exportar para exportar el registro o copiarlo en el portapapeles.' Below the header, there are two tabs: 'Resumen' (selected) and 'Avanzado'. The main content area is divided into two columns. The left column is titled 'Información del sistema' and contains the following details: SO: Windows 7, CPU: x64, Tipo de sistema de archivos: NTFS, Usuario: W7PRACTICAS-PC\Franciscojesus, Opciones de análisis: Memoria: Activado, Inicio: Activado, Sistema de archivos: Activado, Archivos: Activado, Rootkits: Desactivado. The right column is titled 'Resumen del análisis' and contains: Tipo de análisis: Amenaza, Análisis iniciado por: Manual, Resultado: Completado, Objetos analizados: 203.457, Amenazas detectadas: 0, Amenazas en cuarentena: 0, and Tiempo transcurrido: 00:01:00. The 'Tiempo transcurrido' value is highlighted with a red rectangular box.

- Vulnerabilidades y virus encontrados y desinfectados.

No se encontró ninguna amenaza ni vulnerabilidad.

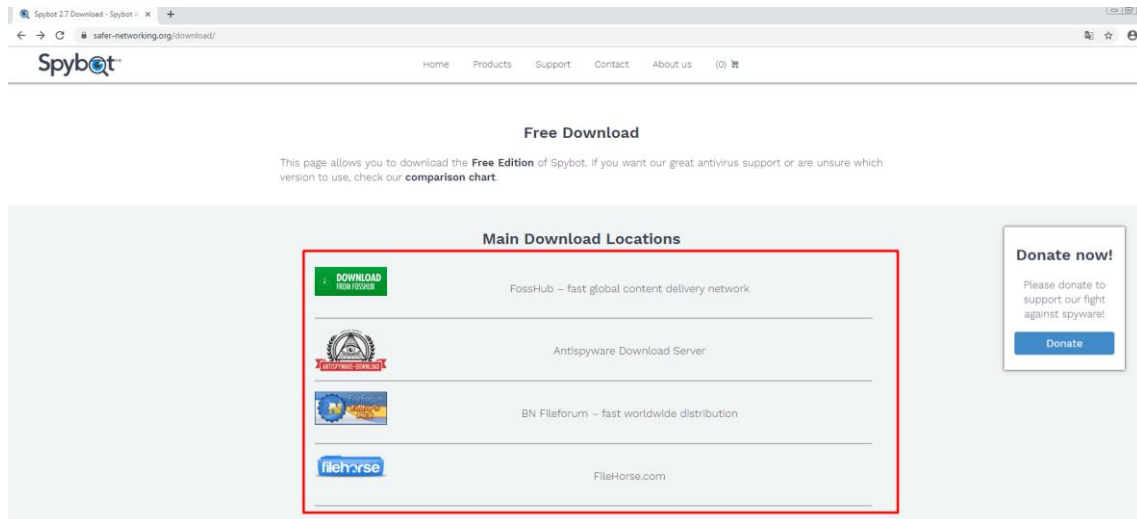
This screenshot is similar to the one above, showing the 'Informe: Analizar' interface. The 'Resumen' tab is selected. The 'Resumen del análisis' section on the right shows: Tipo de análisis: Amenaza, Análisis iniciado por: Manual, Resultado: Completado, Objetos analizados: 203.457, Amenazas detectadas: 0, Amenazas en cuarentena: 0, and Tiempo transcurrido: 00:01:00. In this version, the 'Amenazas detectadas: 0' and 'Amenazas en cuarentena: 0' lines are highlighted with a red rectangular box. At the bottom of the interface, there are two buttons: 'Exportar' on the left and 'Cerrar' on the right.

- Antimalware: Spybot - Search & Destroy

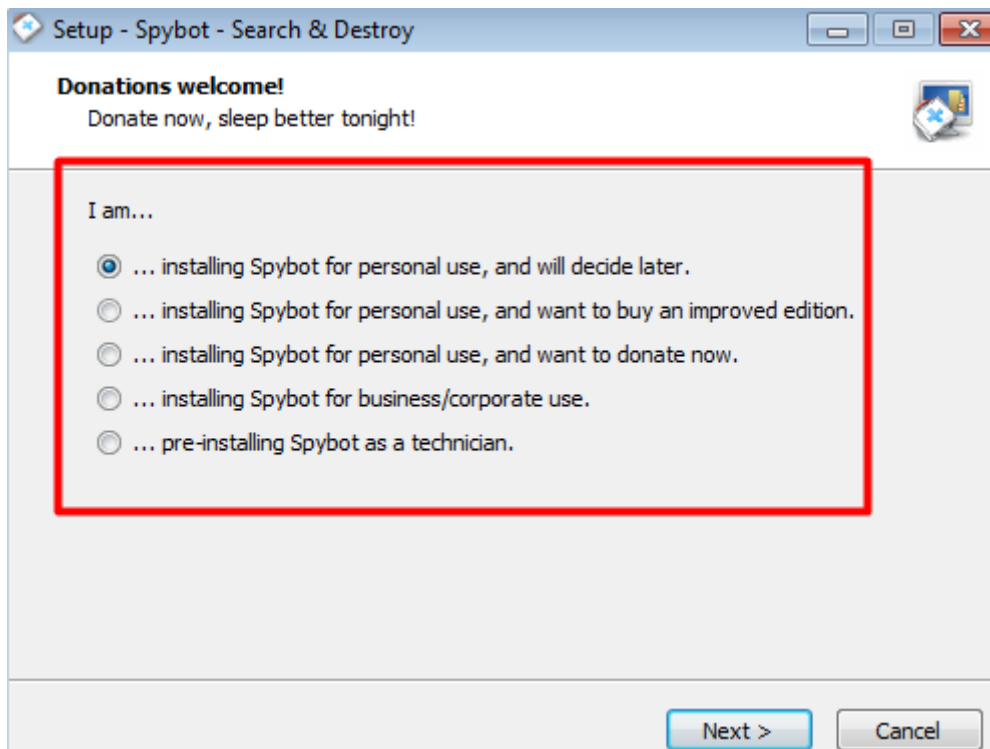
Spybot-Search & Destroy es un programa que elimina malware, spyware y adware. Trabaja desde Microsoft Windows 95 en adelante. Como la mayoría de los buscadores de malware, Spybot explora el disco duro o la memoria RAM de la computadora en busca de software malicioso.

[Wikipedia](#)

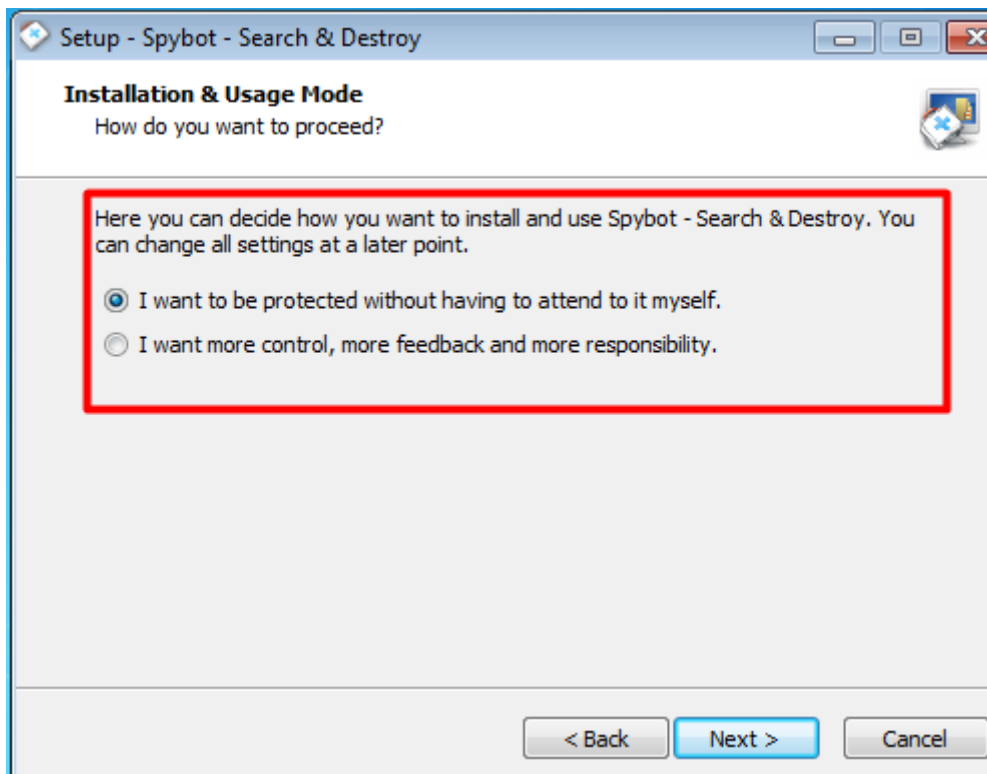
Su instalación es sencilla, podremos descargarlo desde [aquí](#).



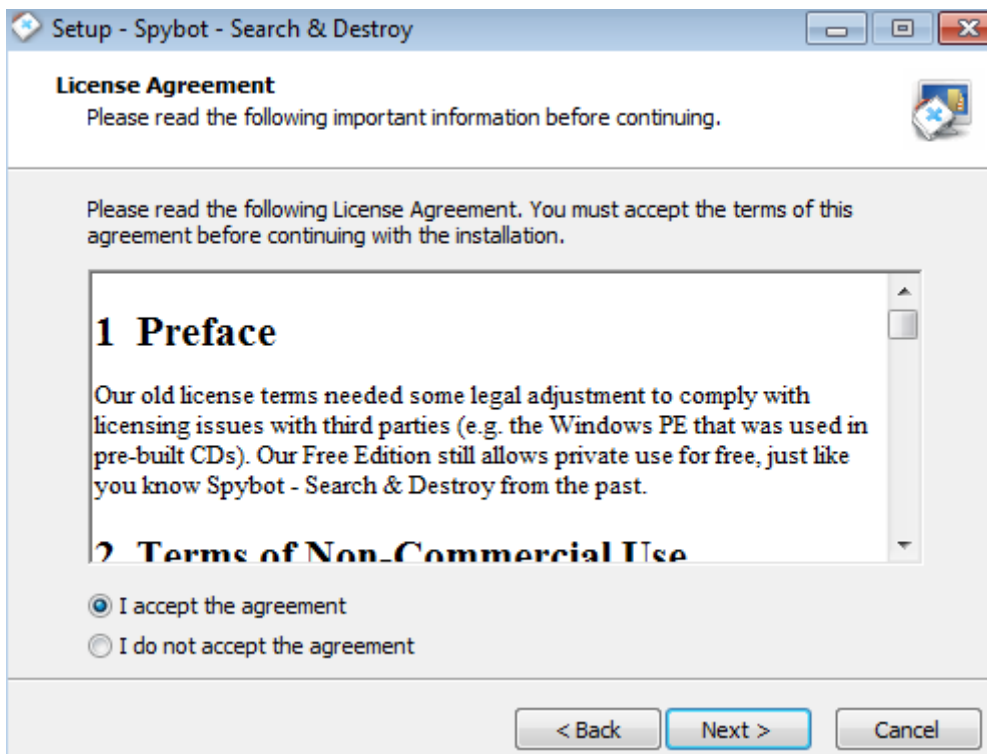
Una vez descargado lo ejecutamos y empezamos a instalarlo.



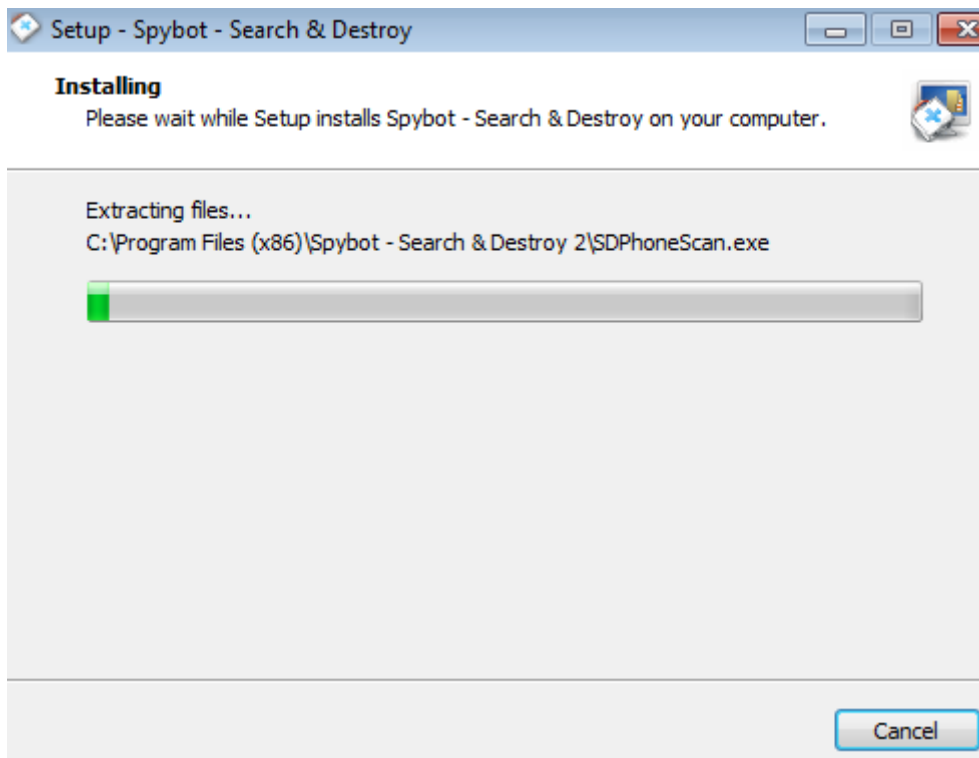
Dejamos la primera opción y pulsamos en *Next*.



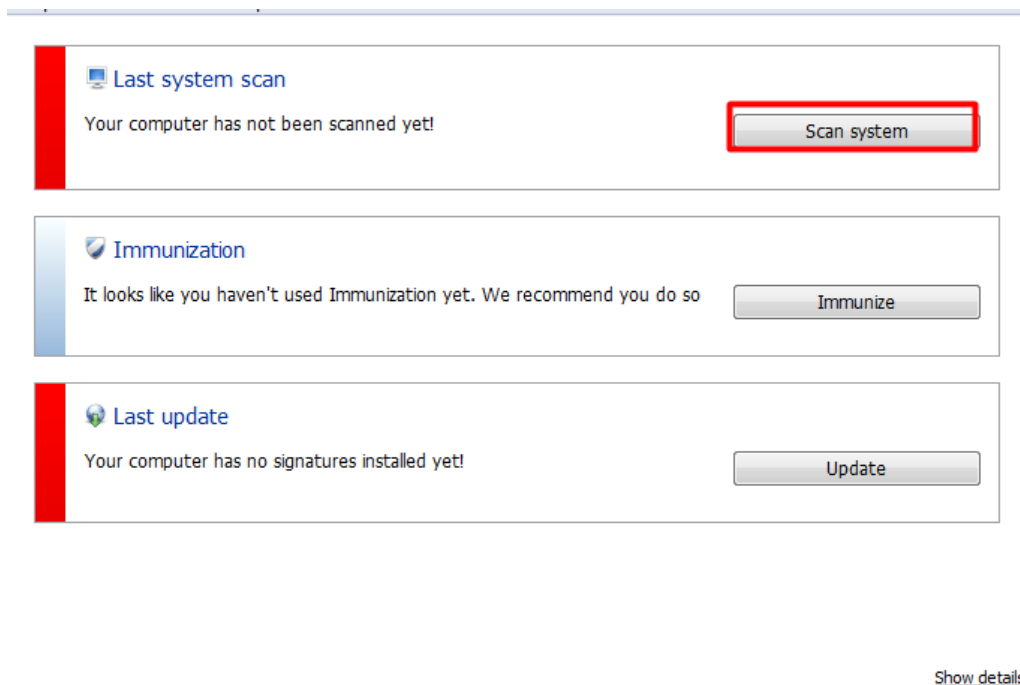
Aceptamos los términos y condiciones.



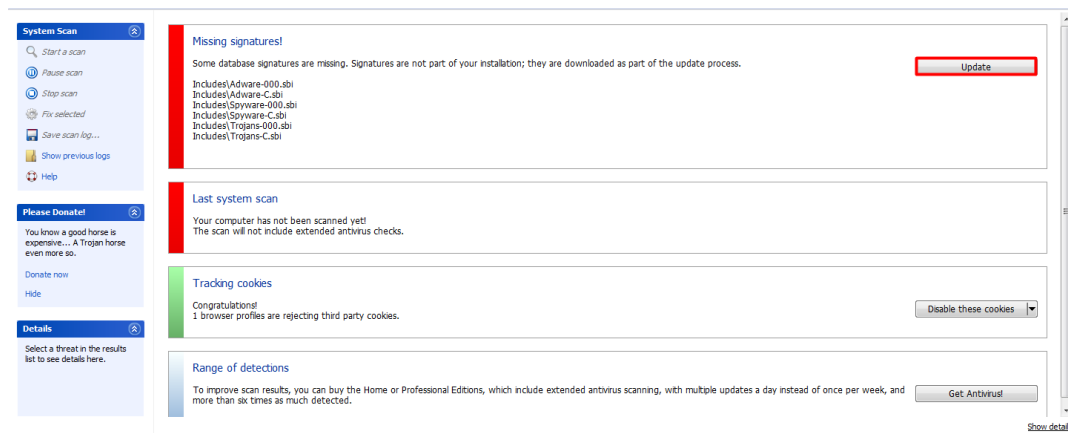
Esperamos a que se instale.



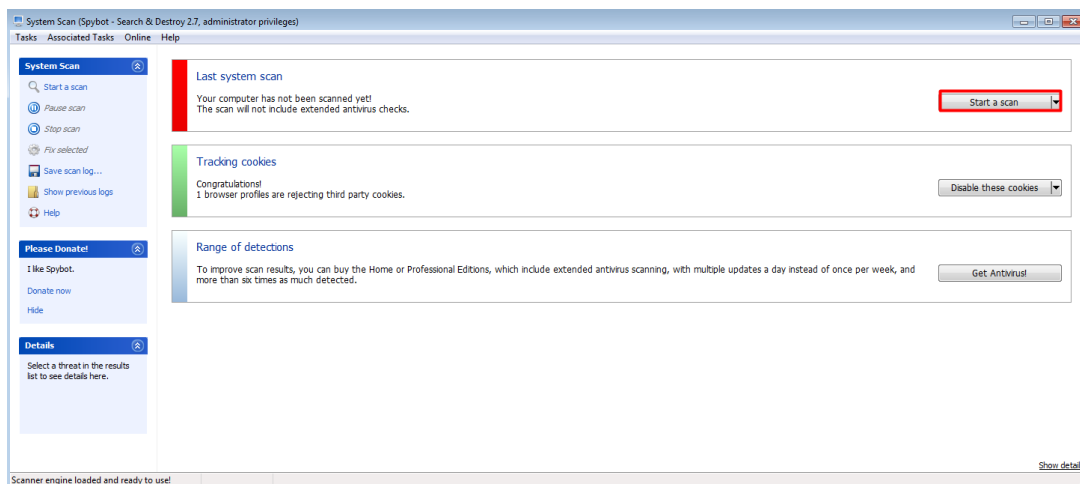
Una vez instalado lo ejecutamos. Se nos abrirá la siguiente ventana y pulsaremos en <<Scan System>> para empezar un escaneo.



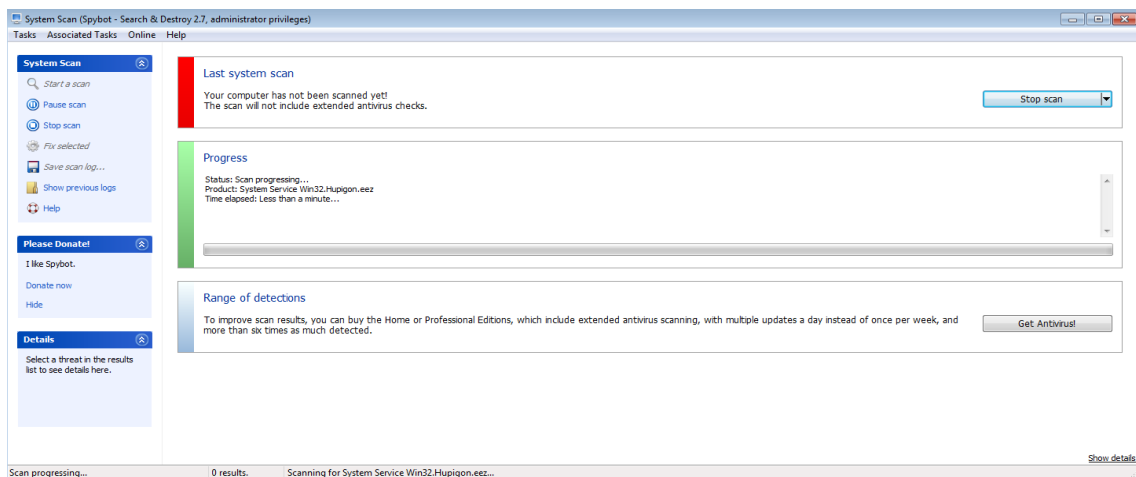
Puede que tengamos que actualizar la base de datos.



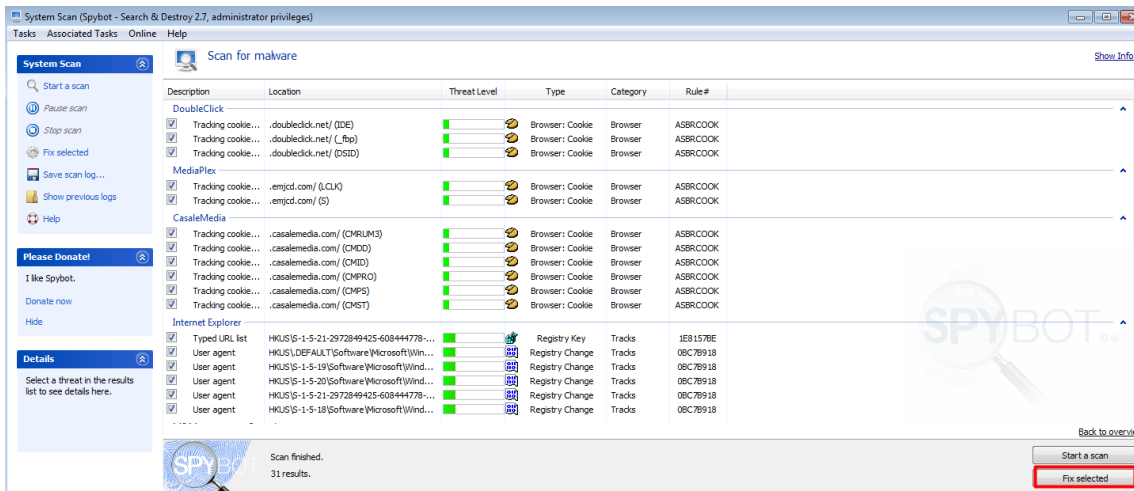
Una vez realizado esto podemos empezar el escaneo.



Esperaremos a que se realice el escaneo.

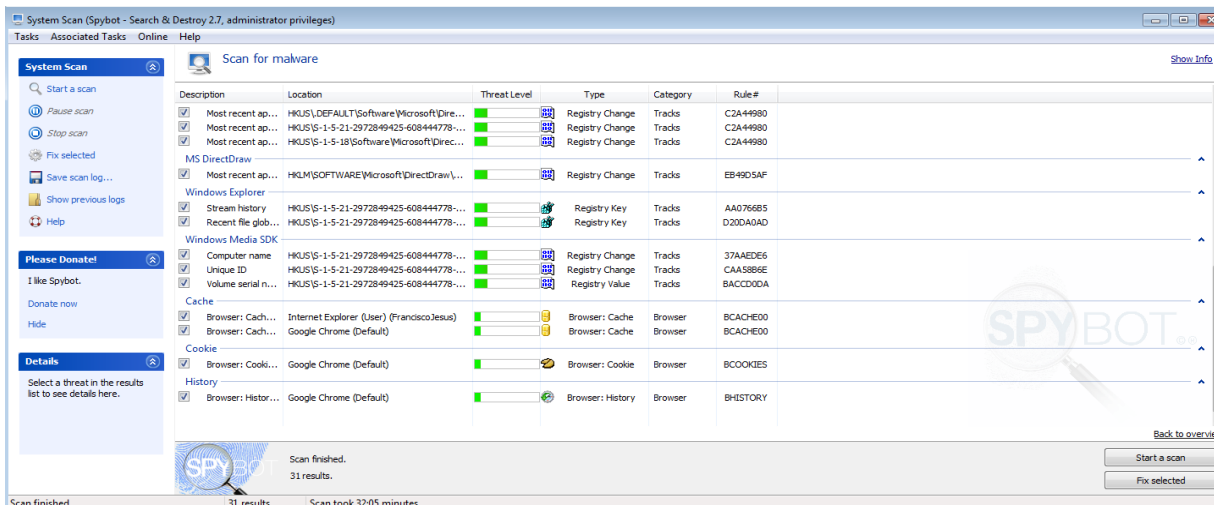
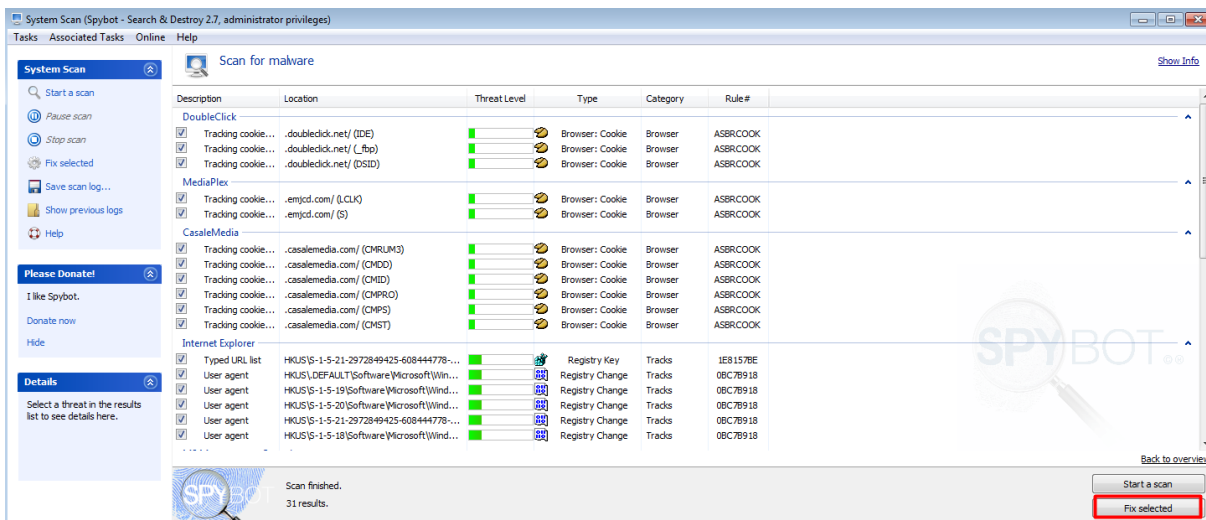


Daremos a <<Fix Selected>> para finalizar, podemos ver que encontró 31 resultados que no son graves.



o Archivos analizados.

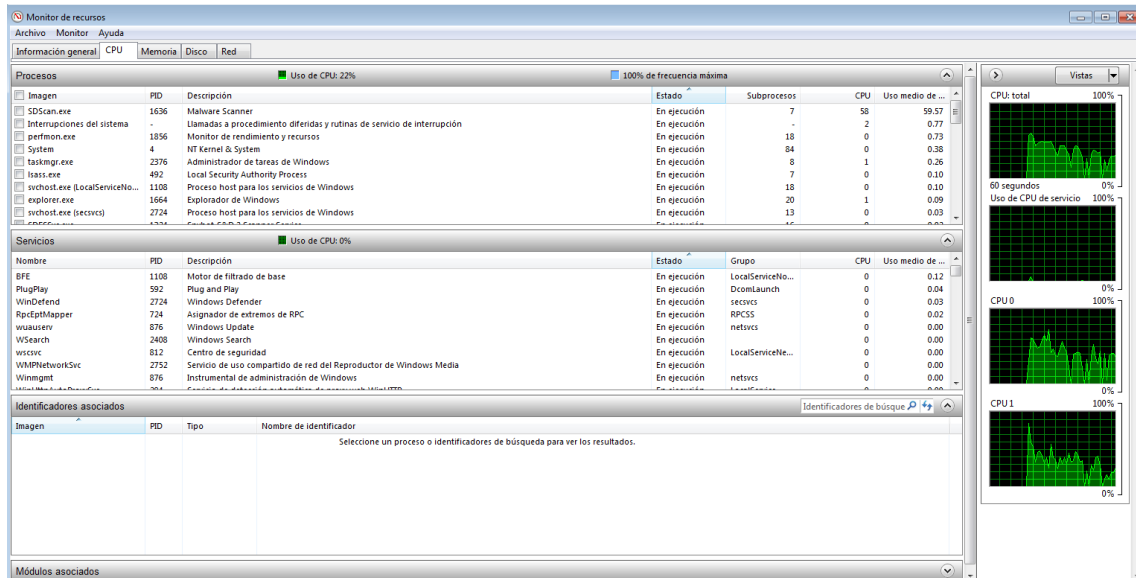
Cuando finalice podemos ver que analizo muchos archivos (registro, historial, cookies, caché...)



No nos indica el total de archivos analizados.

- Uso CPU.

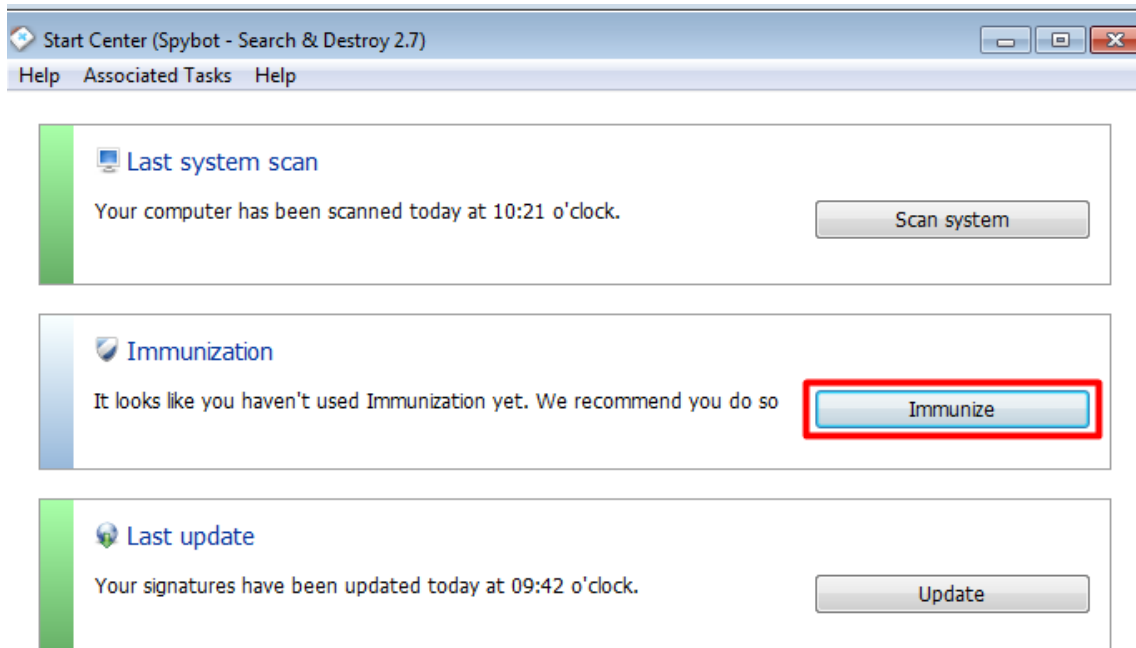
El uso que hace del procesador no es mucho, aunque por lo que se puede ver en la gráfica no usa los 4 al mismo tiempo como MalwareBytes. En total de media ocupo un 20 – 40% de uso de procesador.



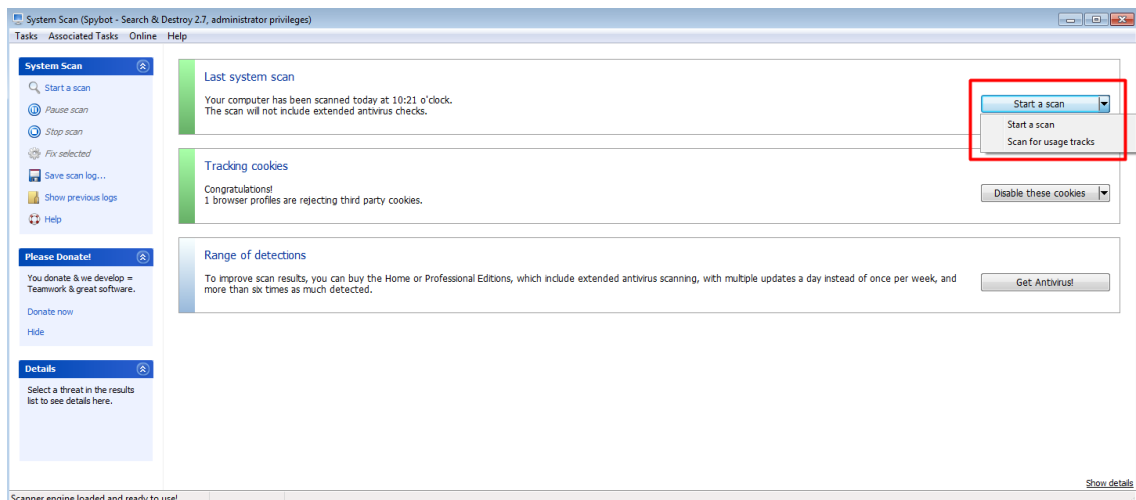
- Opciones Avanzadas.

El programa no cuenta con muchas opciones avanzadas, las más destacadas son:

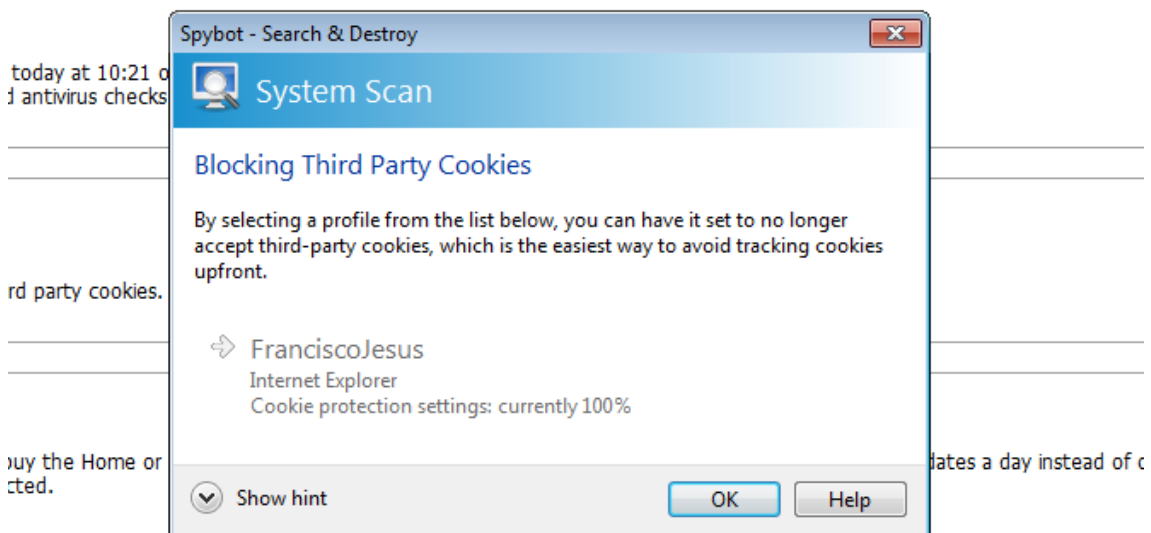
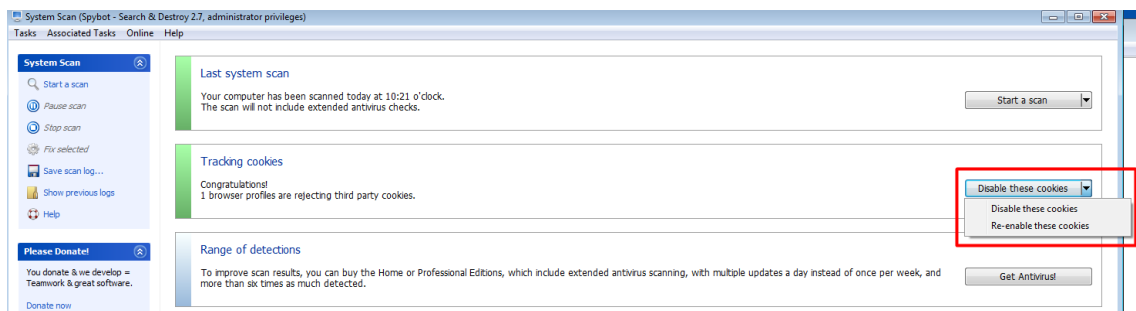
Immunitization, actúa como un antivirus para proteger también de los virus en tiempo real cuando navegas.



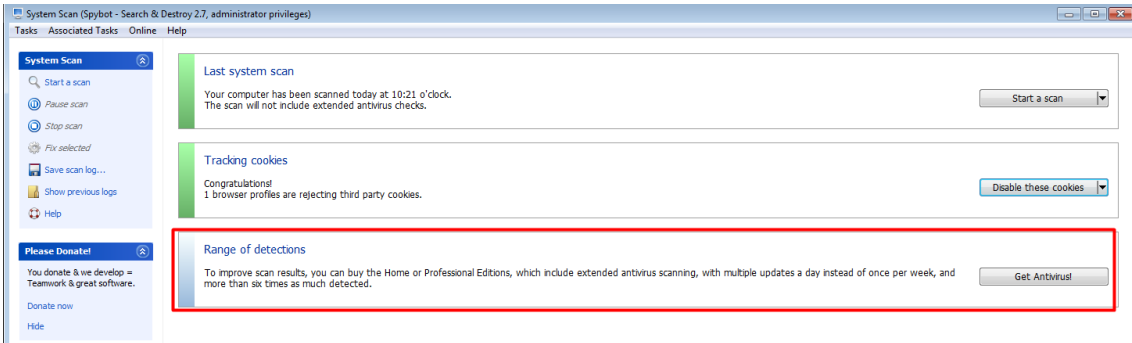
Los escaneos no se pueden hacer avanzados o customizados.



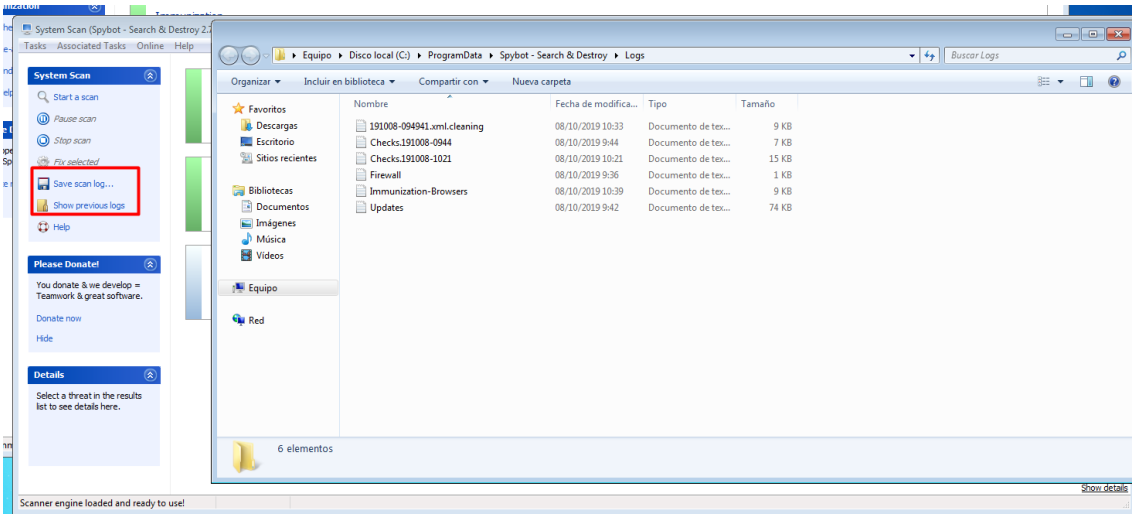
Podemos desactivar o eliminar las cookies, al mismo tiempo, podremos volverlos a activar.



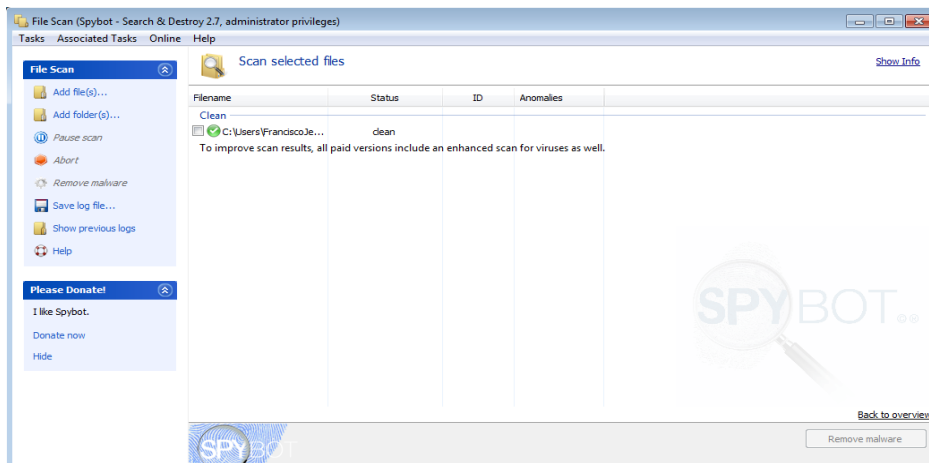
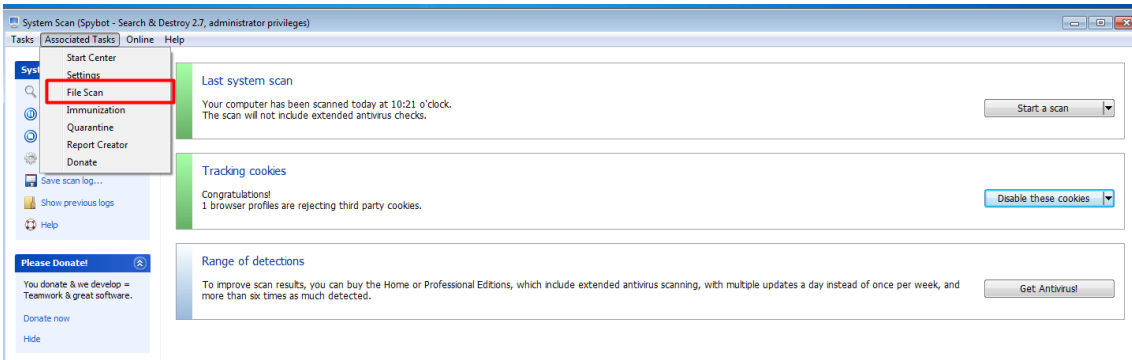
También tendremos la opción de acompañarlo con su antivirus, el cual es de pago.



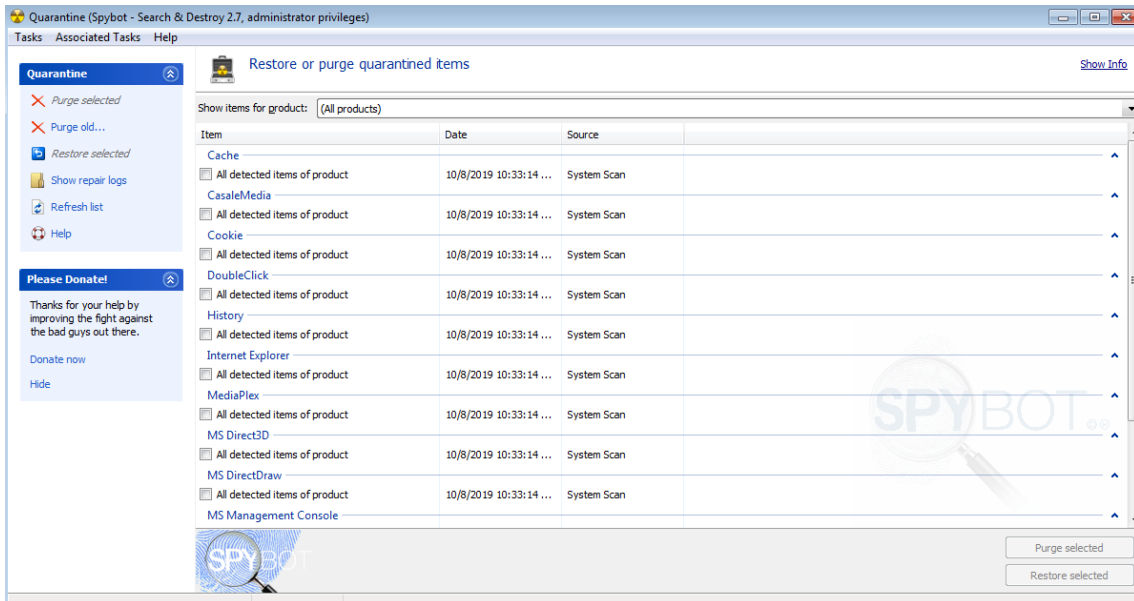
Podremos mostrar los *logs* antiguos y exportarlos.



Podemos analizar archivos individualmente o ver la cuarentena.

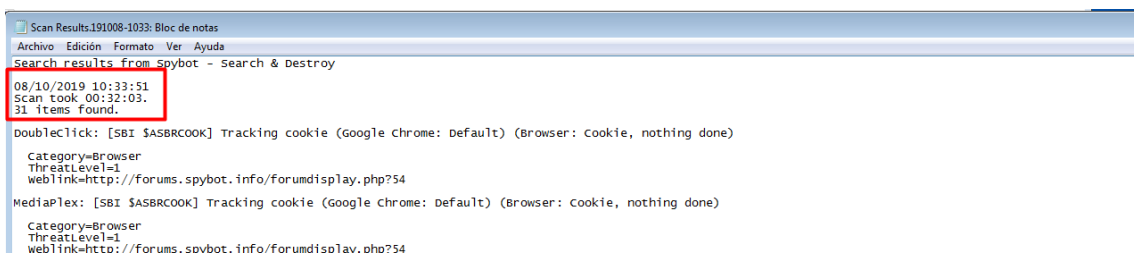
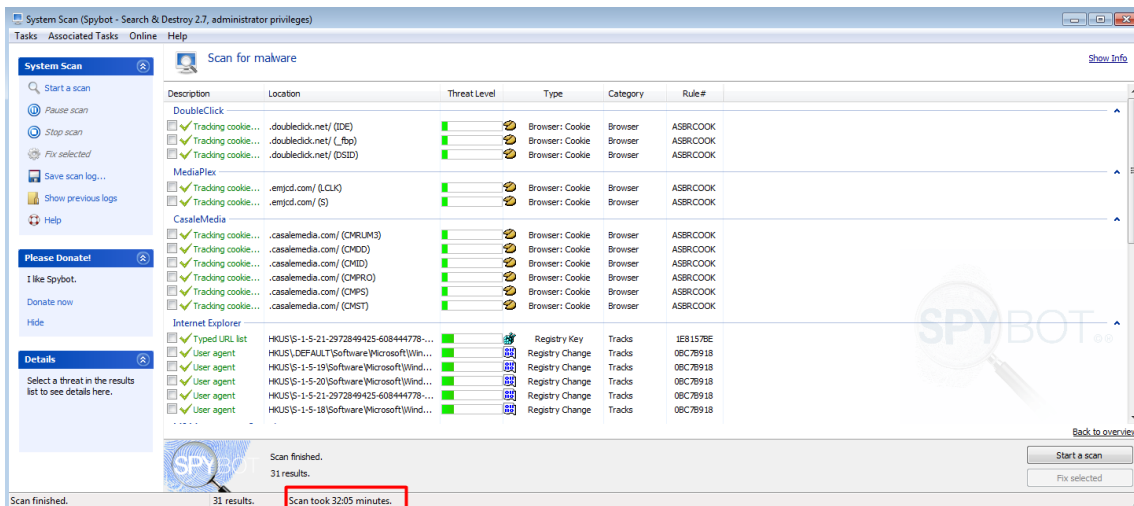


Cuarentena



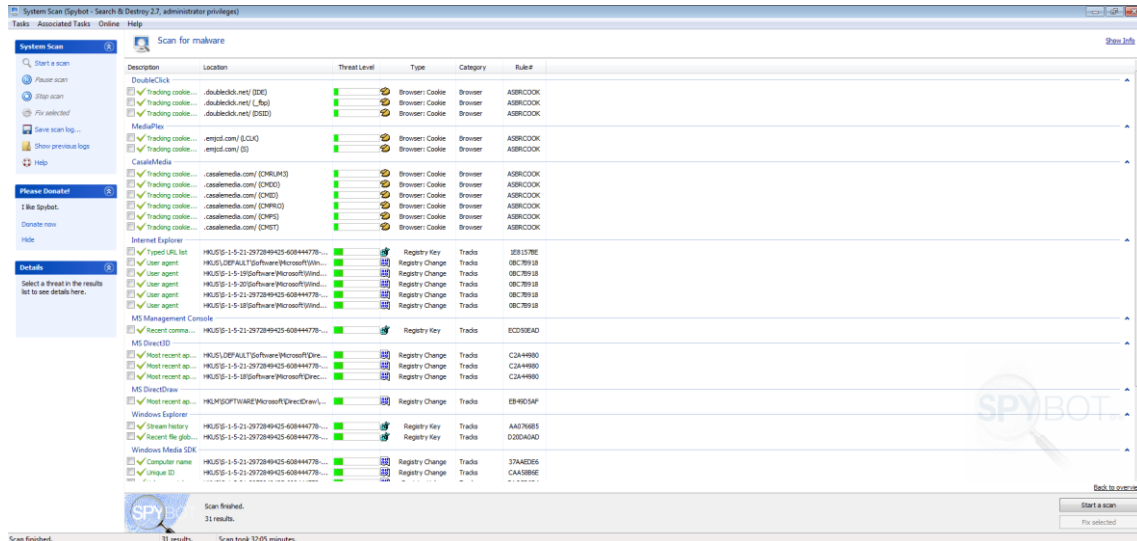
- Tiempo de escaneo.

El escaneo duro bastante más tiempo que Malware Bytes sin saber cuántos archivos ha escaneado, en total fue 32 minutos con 5 segundos.



- Vulnerabilidades y virus encontrados y desinfectados.

No había virus ni vulnerabilidades, únicamente elimino las cookies, historial y algunos archivos del registro que parecían estar obsoletos.



Como vemos no es un programa muy avanzado, pero es de código libre y gratis, un punto muy a favor.

Conclusión

En esta práctica hemos comparado dos antimalware el cuál uno era una versión de pago y otra “gratuita” con algunas opciones de pago. Claramente la mejor ha sido la de pago por todas las opciones y eficacia que tiene, SpyBot no ha estado mal al ser un programa muy ligero y gratis, pero es verdad que en comparación con Malware Bytes flojea mucho como es lógico. Las dos son buenas opciones ya que SpyBot se actualiza constantemente y cumple su función correctamente.