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

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

Índice

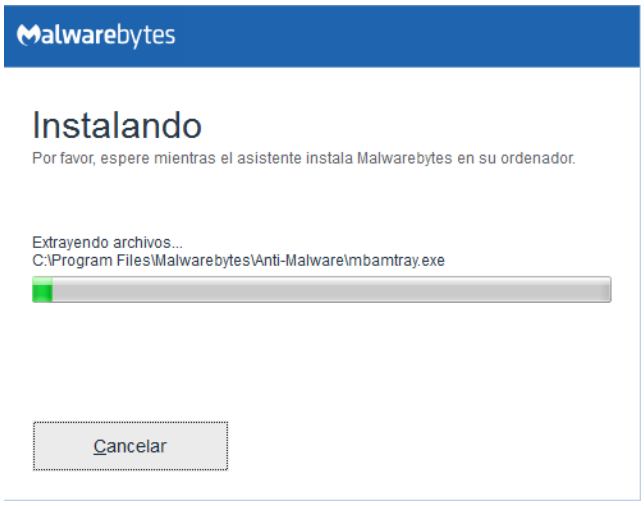
Instala al menos dos aplicaciones antimalware en modo local y realiza su comprobación en el PC para compararlos. Anota en dicha documentación de comparación: (Número archivos analizados, % Ocupación de CPU en ejecución, opciones avanzadas de escaneo, tiempo de escaneo, vulnerabilidades y malware encontrado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

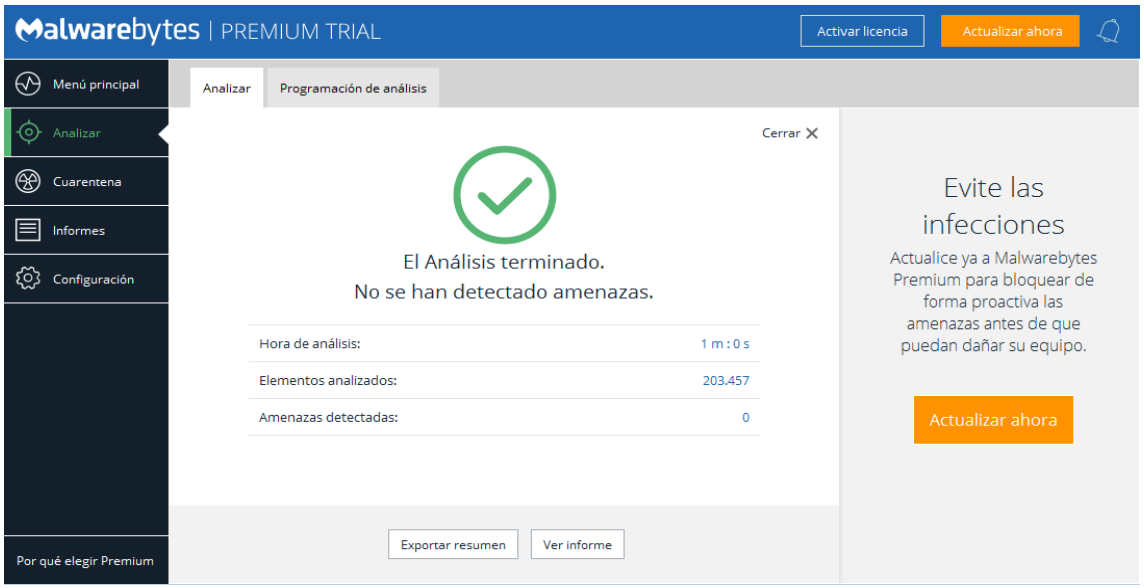
Su instalación es sencilla, vamos a la web oficial a descargarlo, Link.

Una vez descargado lo ejecutamos e instalamos.



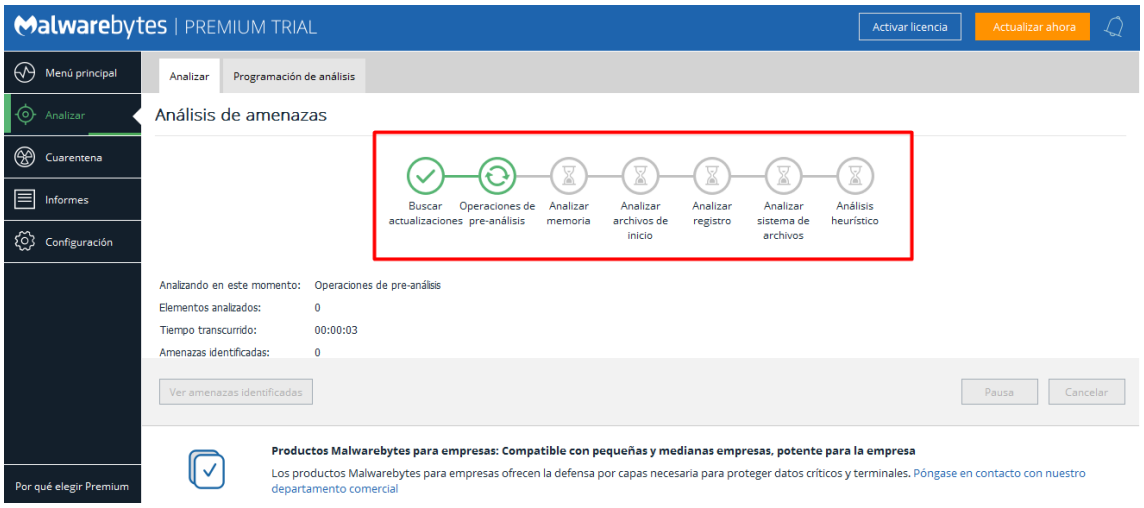
Una vez instalado lo ejecutamos, tendremos una prueba de 14 días. Pulsaremos en *Análizar ahora* para comenzar el análisis.

El análisis lo hará rápidamente.

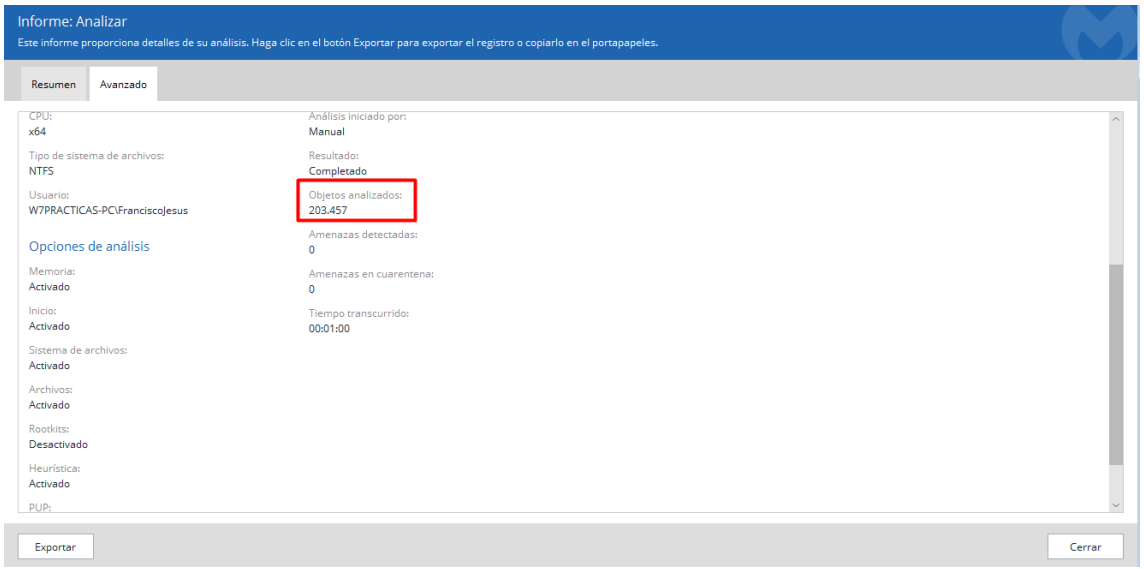


- Archivos analizados.

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

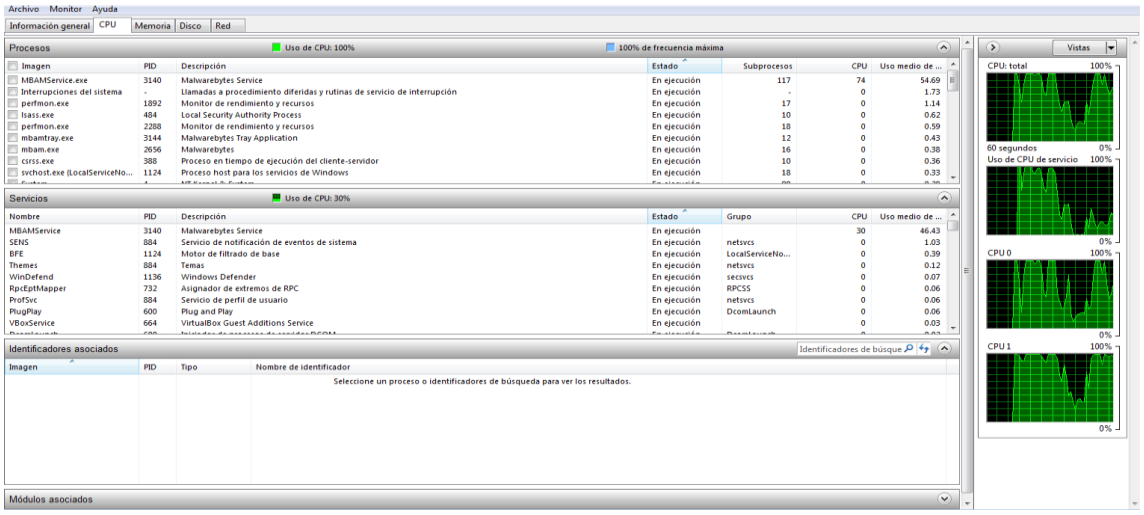


En total se analizaron 203.457 archivos.



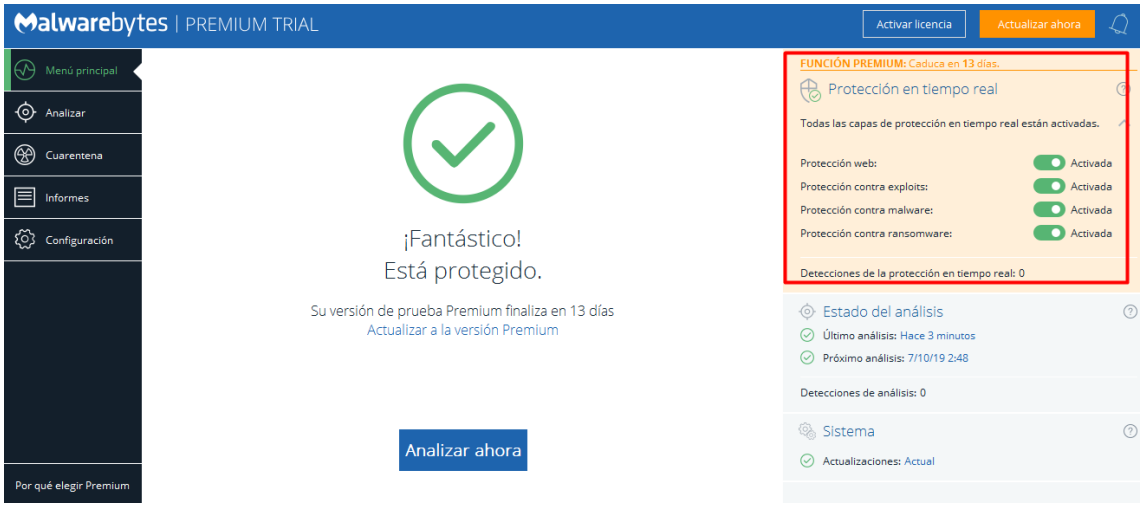
- Uso CPU.

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.

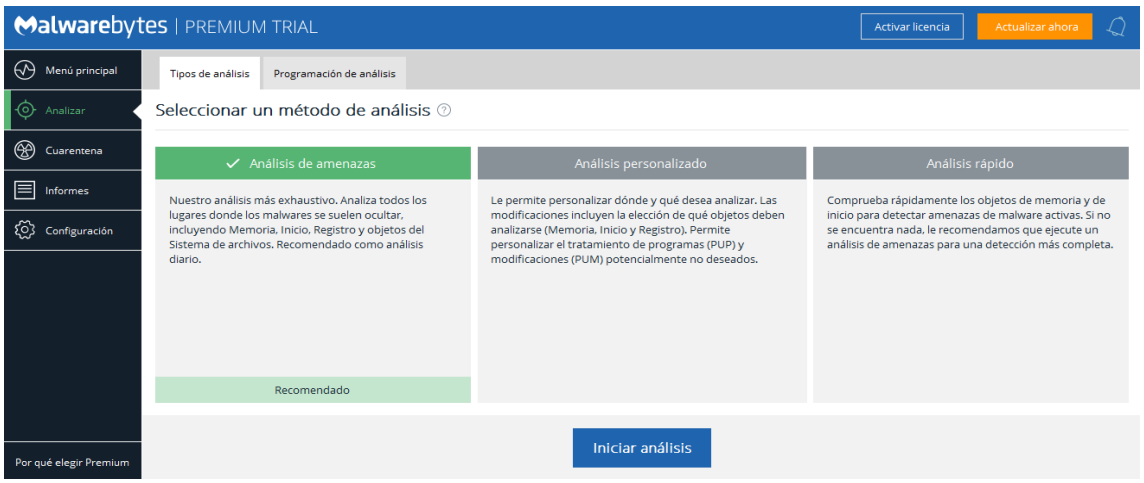


- Opciones Avanzadas.

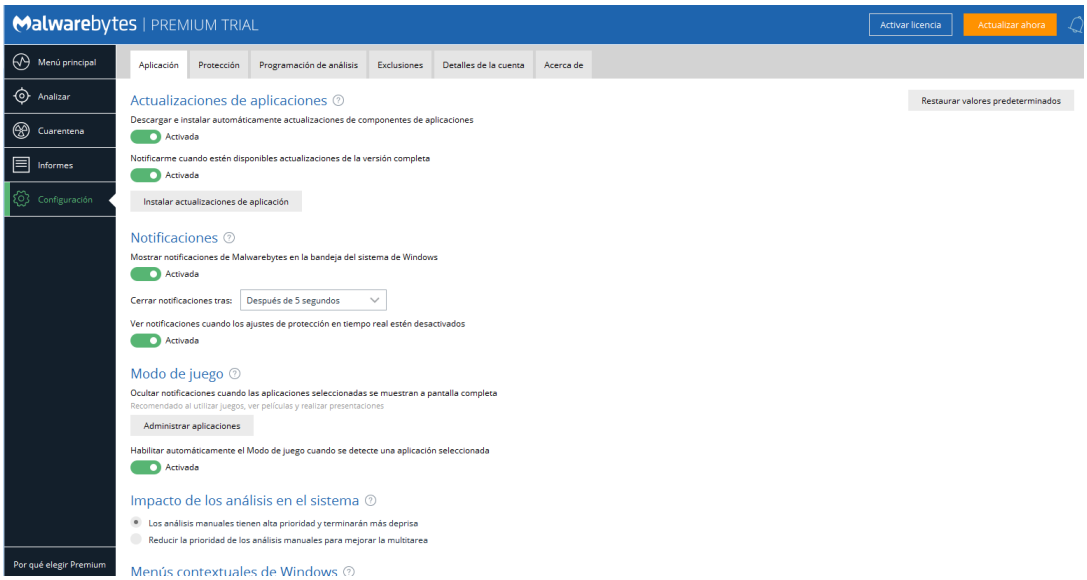
Prácticamente apenas tenemos opciones avanzadas ya que son la mayoría de pago. Tenemos protección en tiempo real en la versión de prueba disponible.

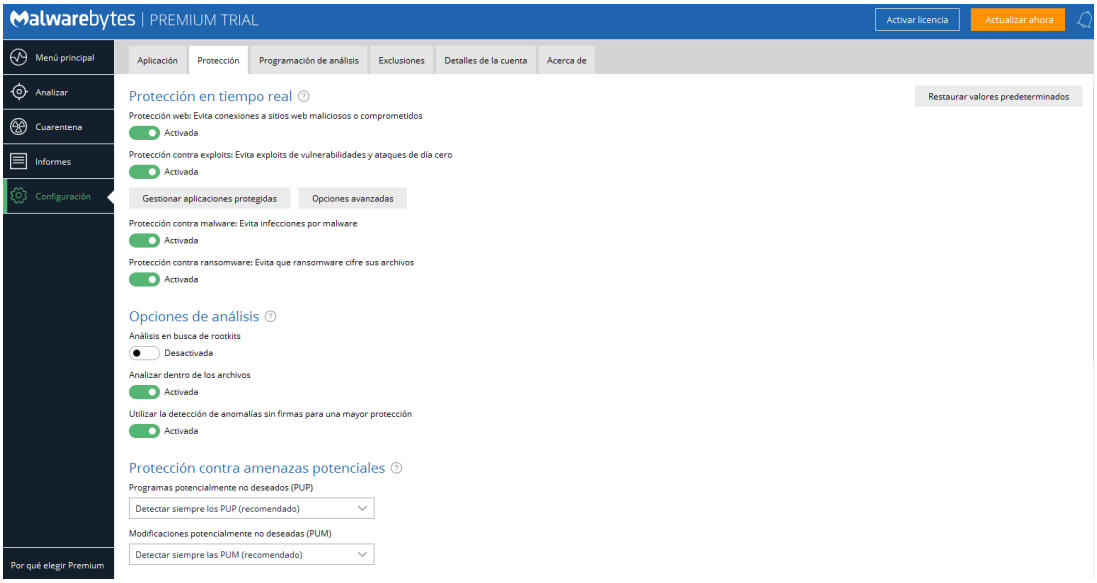


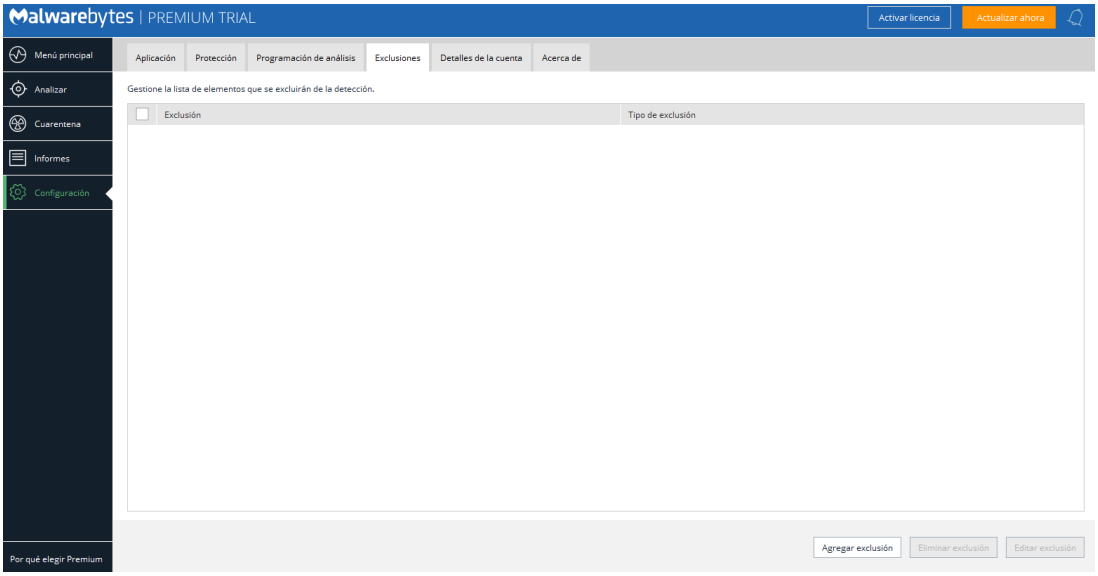
Podremos escoger entre tres tipos de análisis.



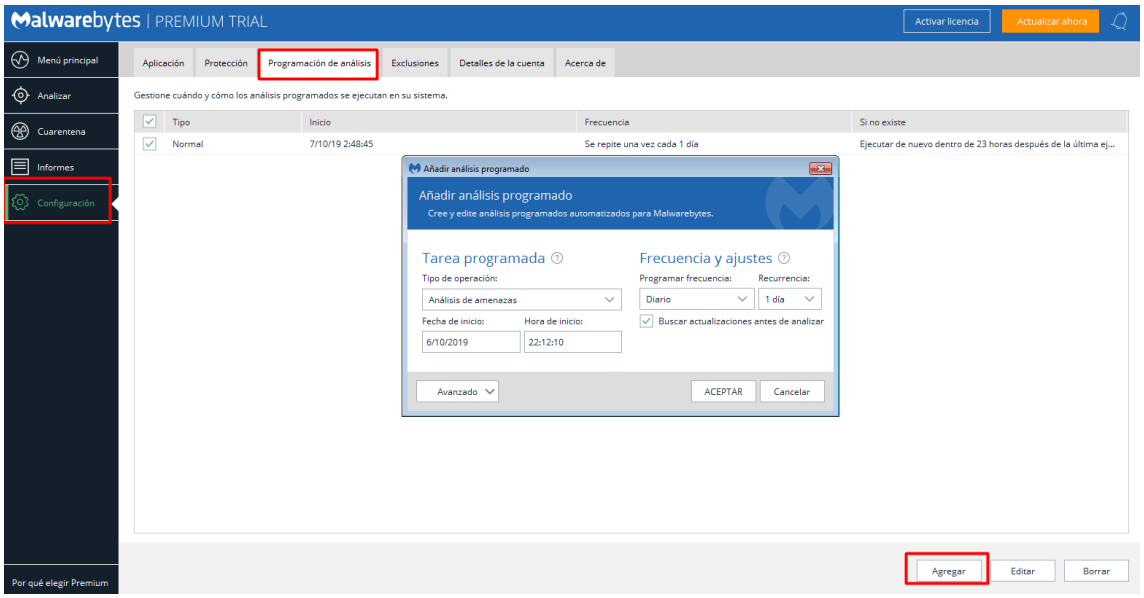
En las opciones tendremos cosas interesantes como actualizaciones, seguridad, exclusiones, programación de análisis…

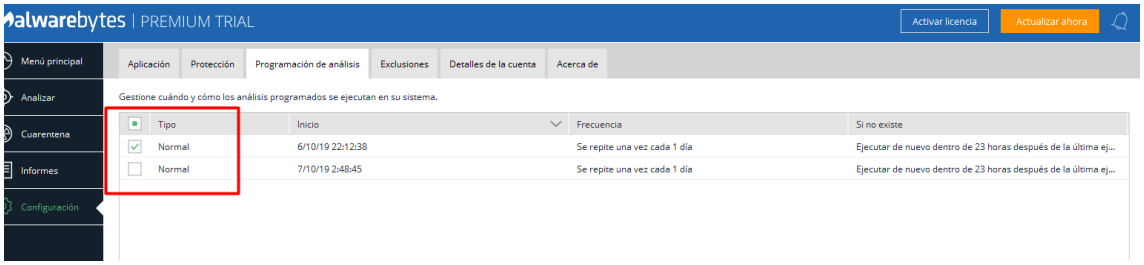




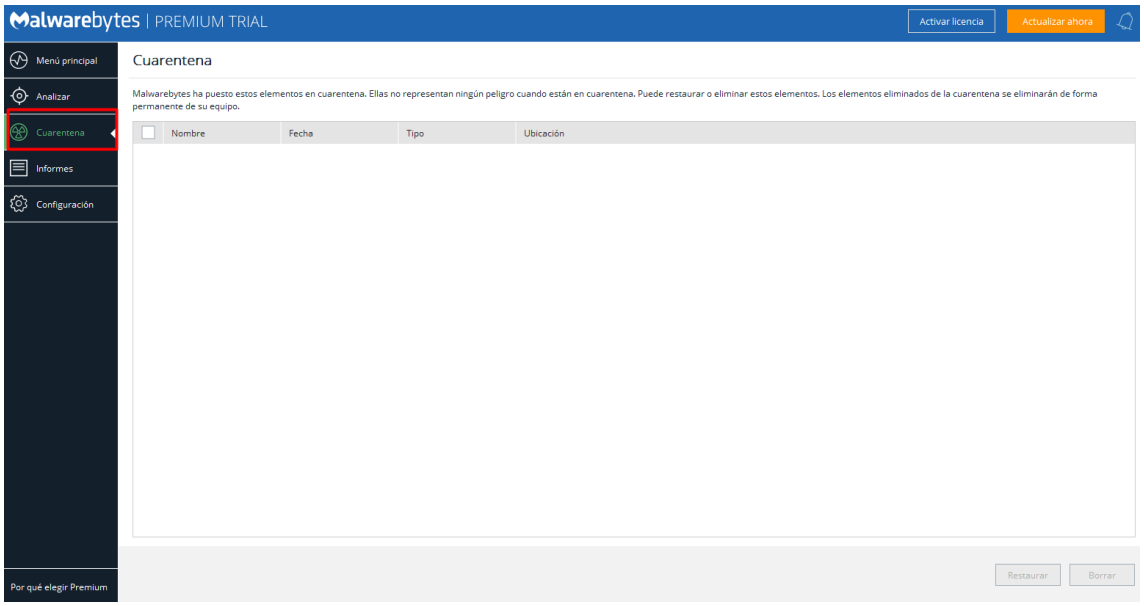


Podemos programar análisis.



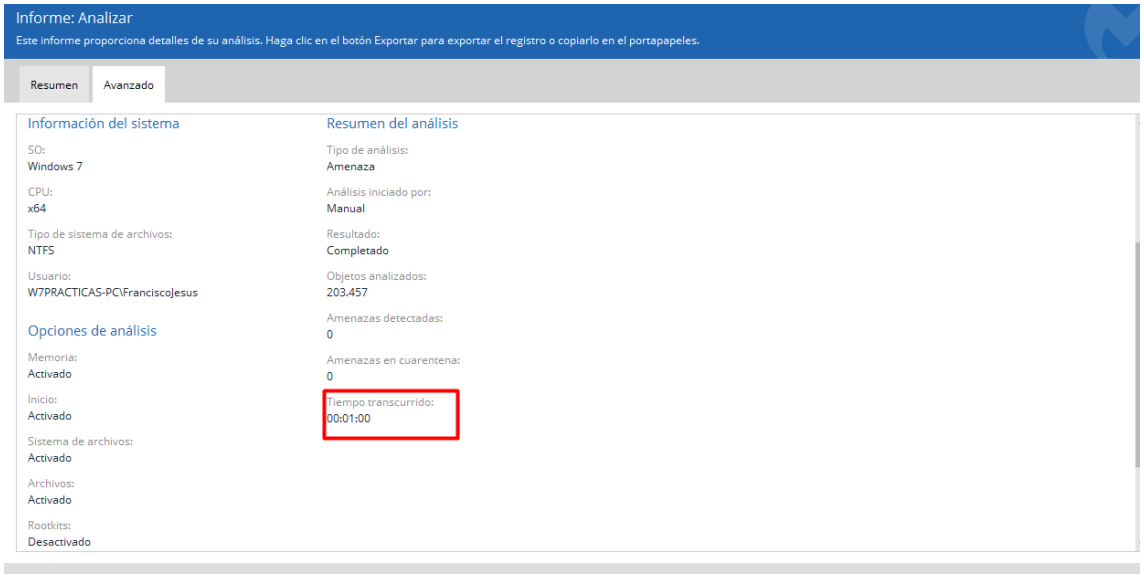


En *Cuarentena* podremos ver los archivos en cuarentena, en este caso no tenemos ninguno ya que no se detectó nada en el sistema.



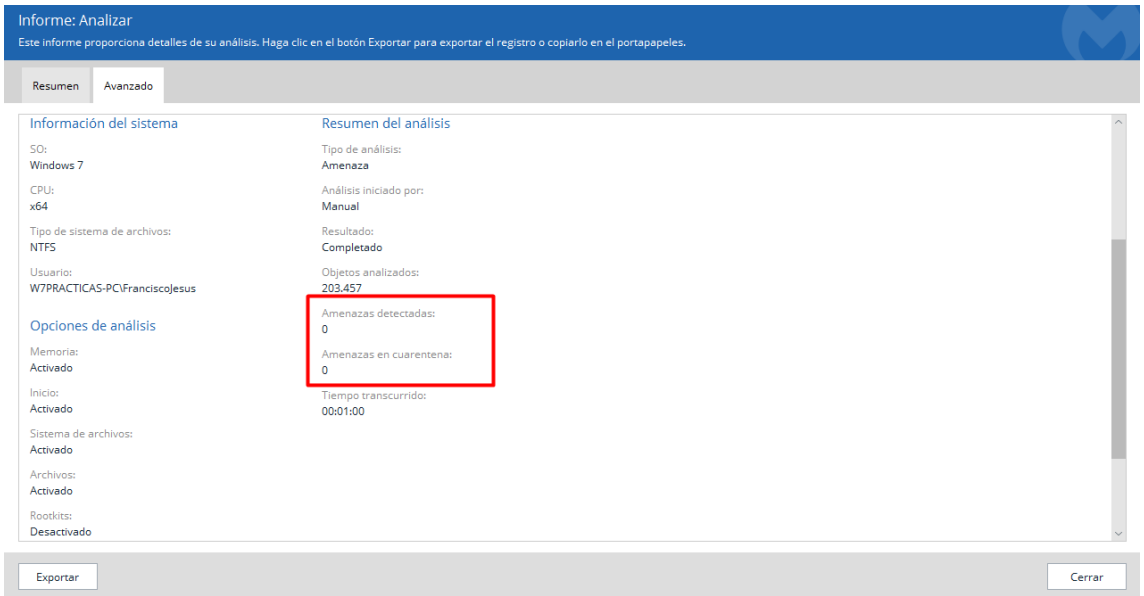
- Tiempo de escaneo.

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.



- Vulnerabilidades y virus encontrados y desinfectados.

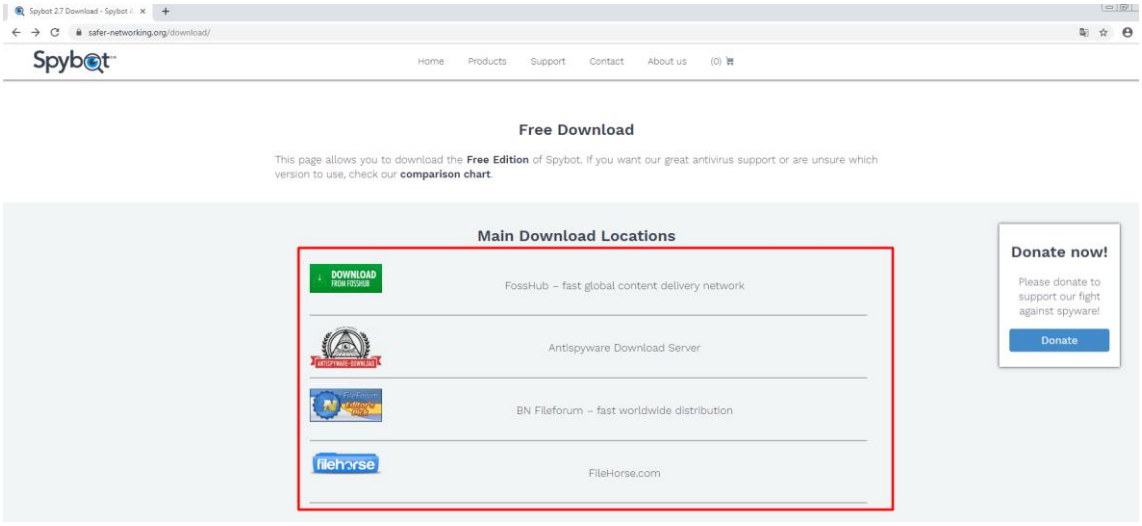
No se encontró ninguna amenaza ni vulnerabilidad.



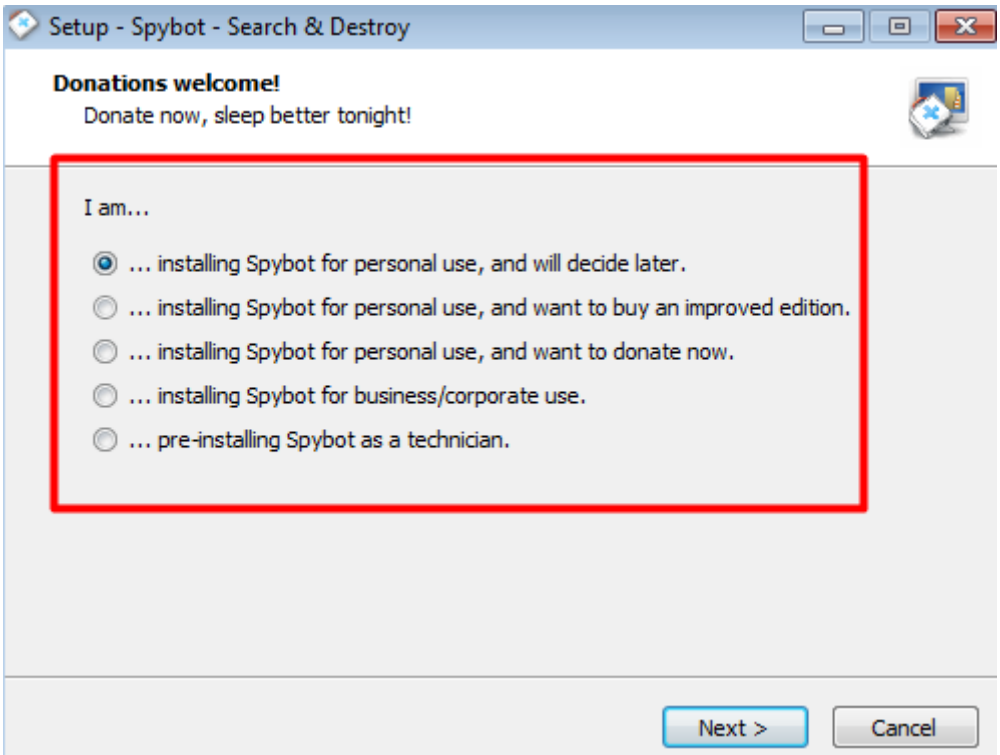
- Antimalware: Spybot - Search & Destroy

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

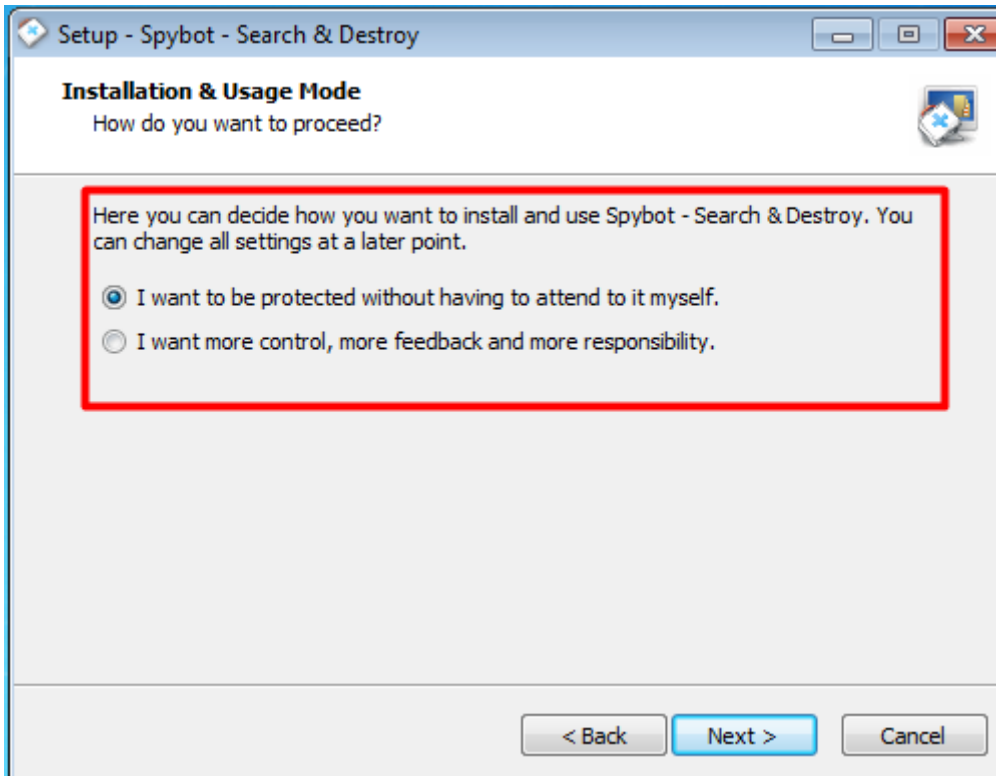
Su instalación es sencilla, podremos descargarlo desde aquí.



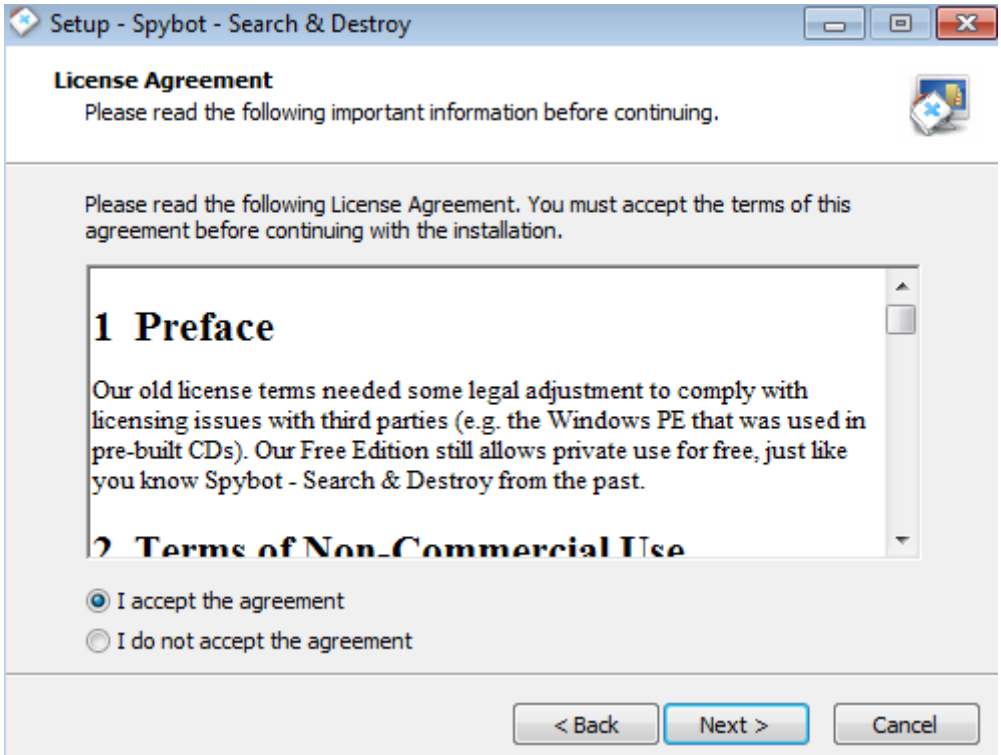
Una vez descargado lo ejecutamos y empezamos a instalarlo.



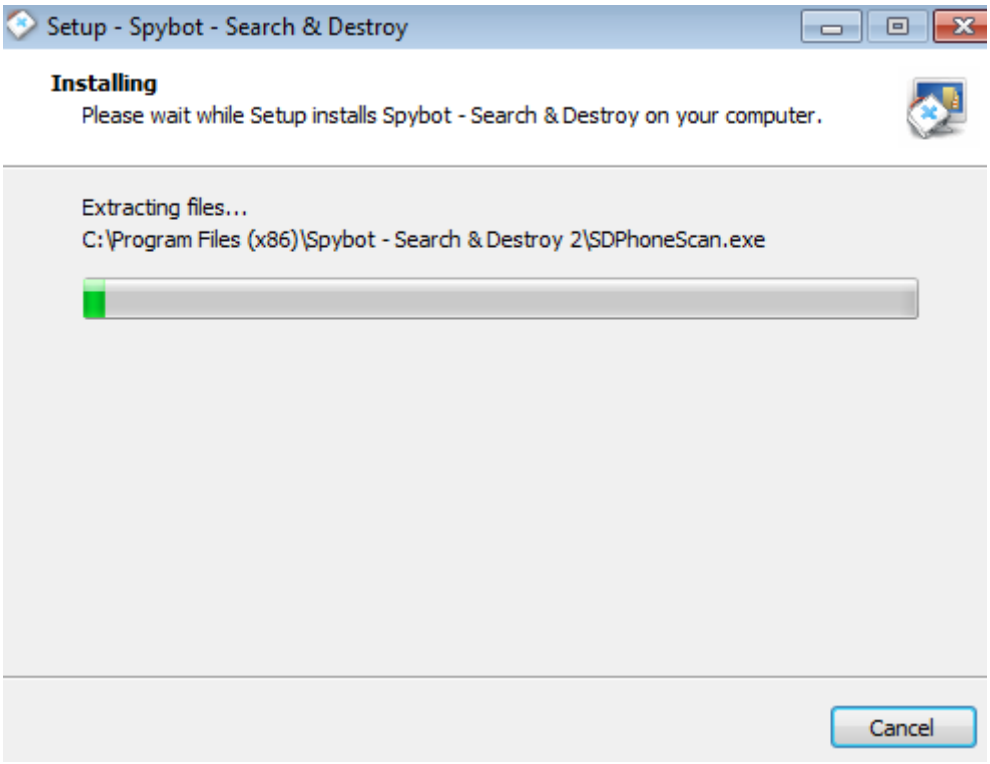
Dejamos la primera opción y pulsamos en *Next.*



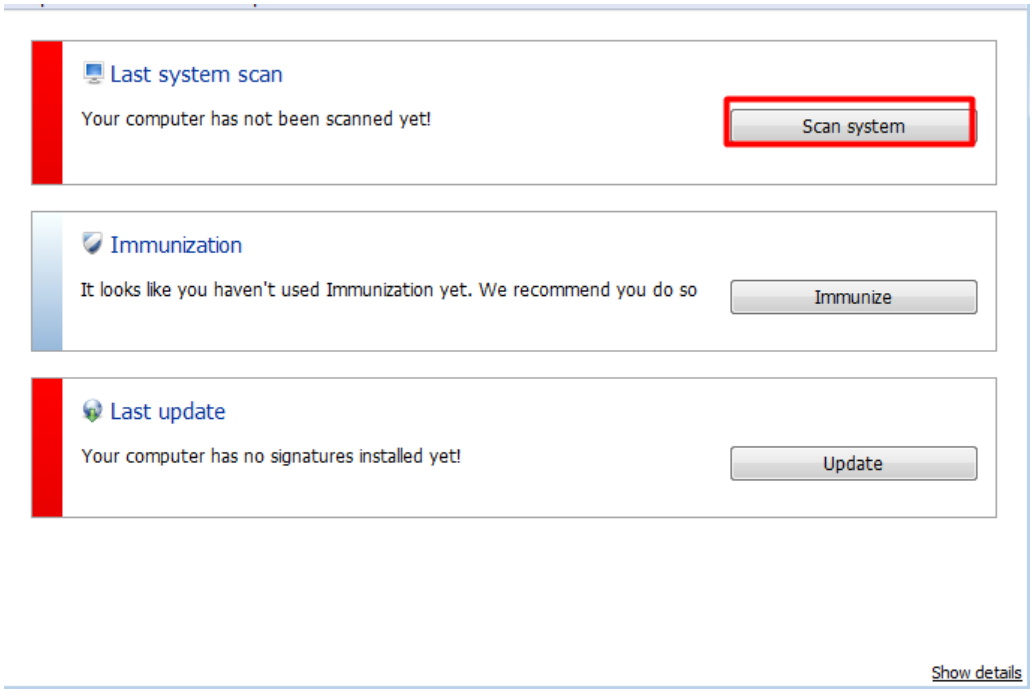
Aceptamos los términos y condiciones.



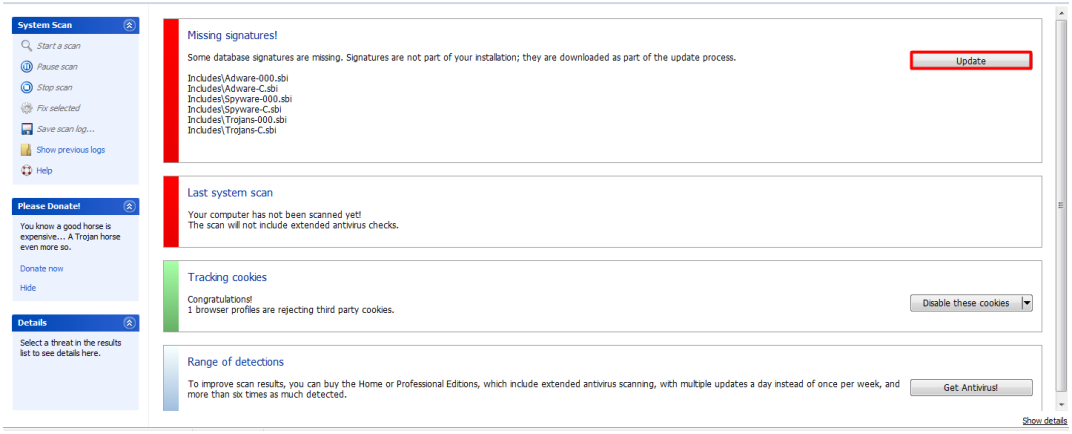
Esperamos a que se instale.



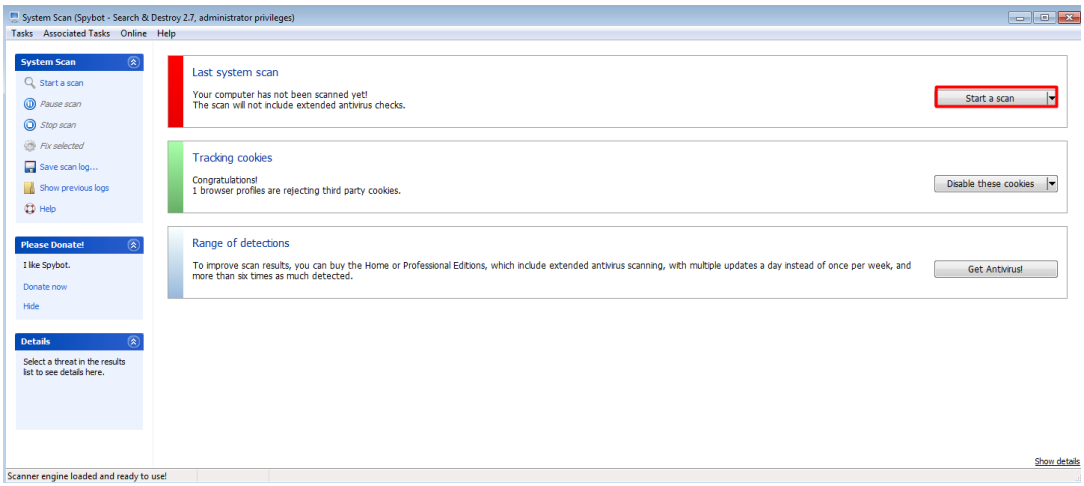
Una vez instalado lo ejecutamos. Se nos abrirá la siguiente ventana y pulsaremos en <<*Scan System*>> para empezar un escaneo.



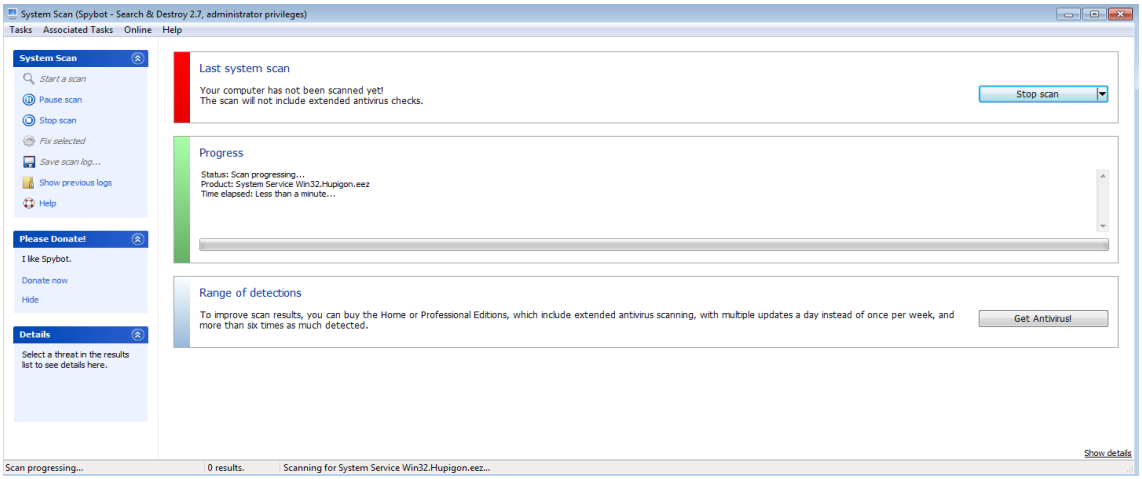
Puede que tengamos que actualizar la base de datos.



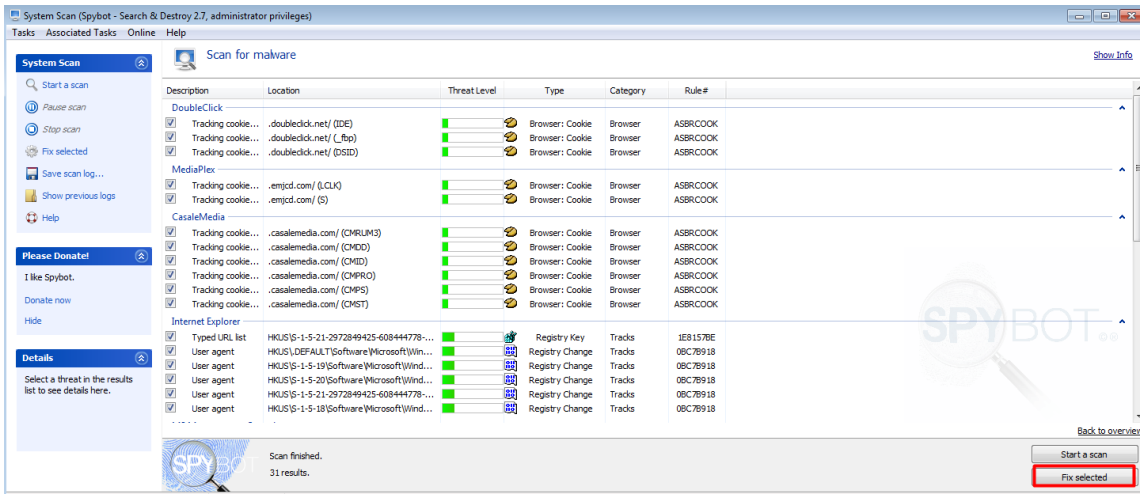
Una vez realizado esto podemos empezar el escaneo.



Esperaremos a que se realice el escaneo.

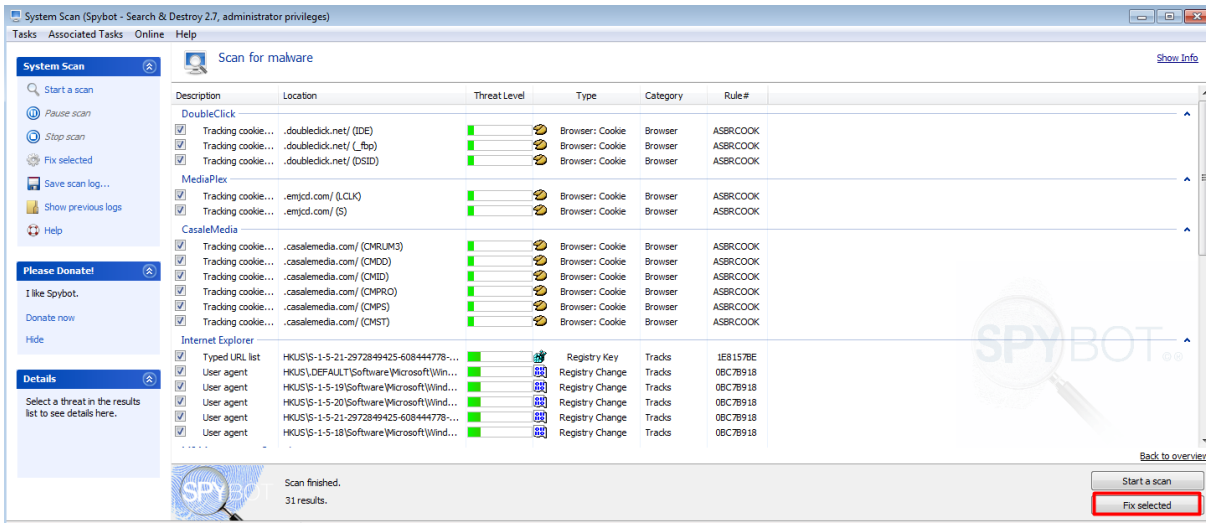


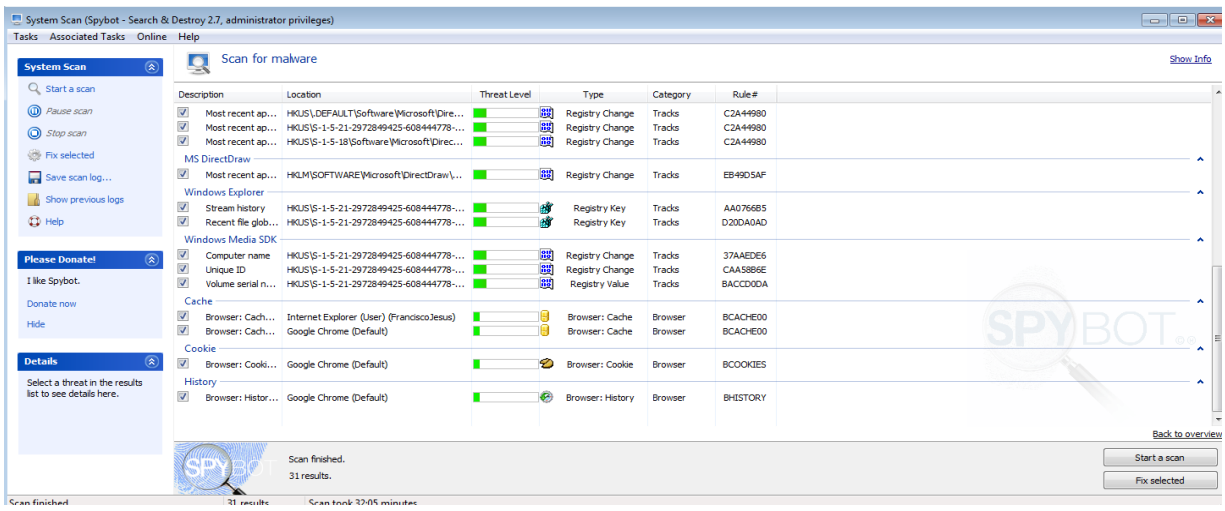
Daremos a *<<Fix Selected>>* para finalizar, podemos ver que encontró 31 resultados que no son graves.



- Archivos analizados.

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

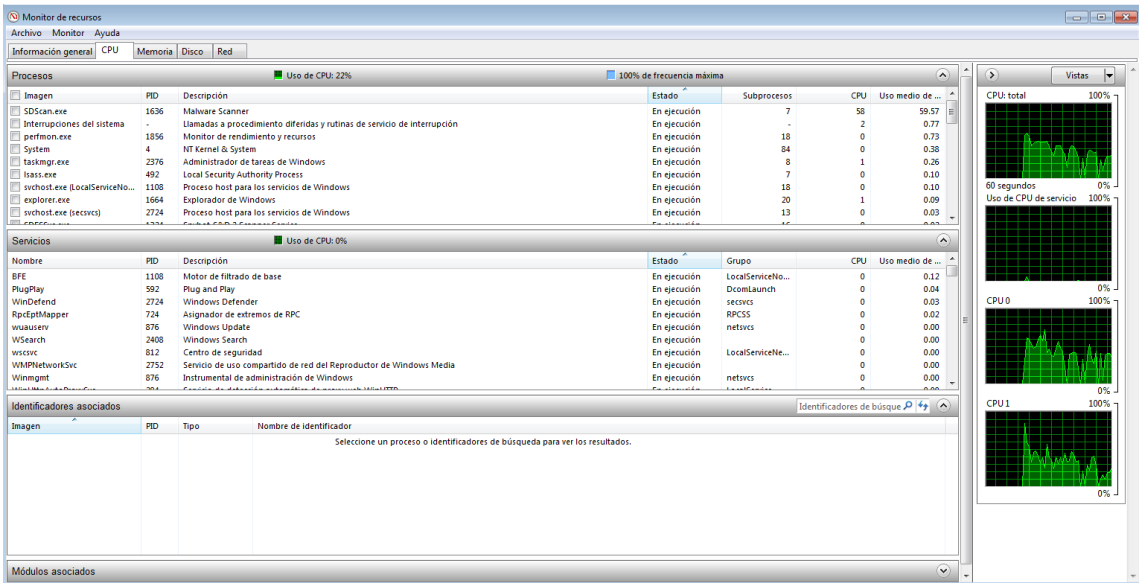




No nos indica el total de archivos analizados.

- Uso CPU.

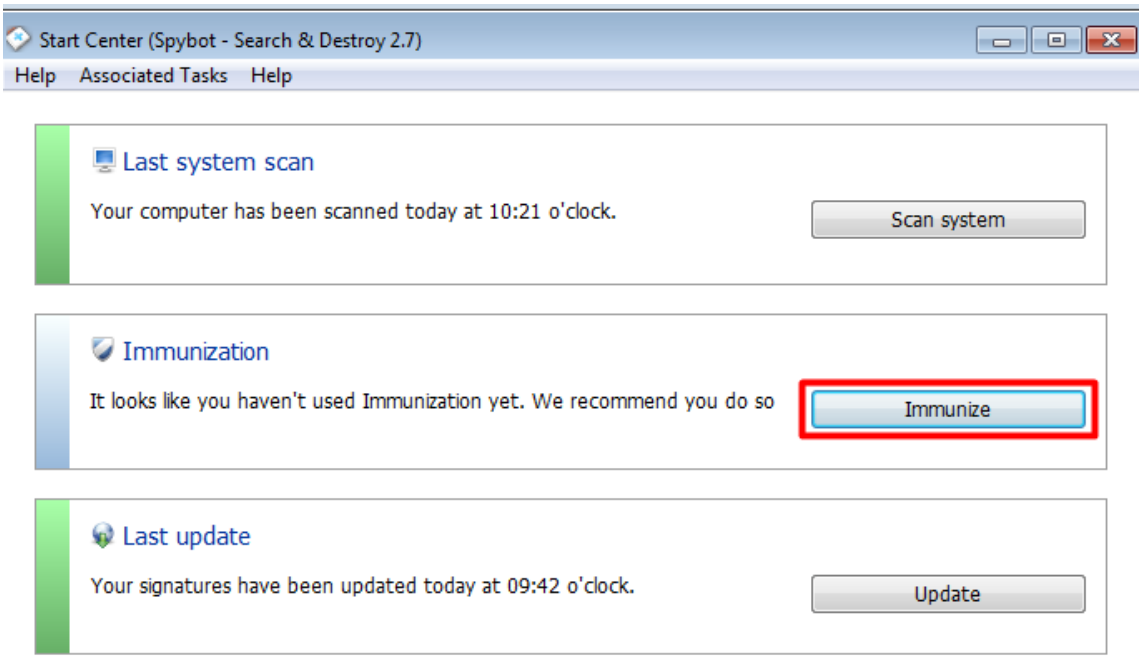
El uso que hace del procesador no es mucho, aunque por lo que se puede ver en la gráfica no usa los 4 al mismo tiempo como MalwareBytes. En total de media ocupo un 20 – 40% de uso de procesador.



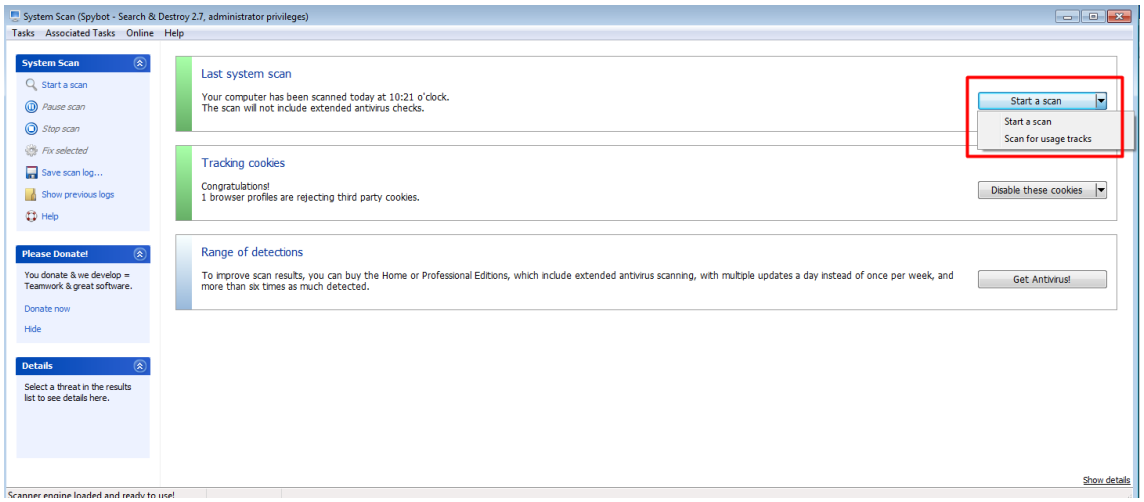
- Opciones Avanzadas.

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

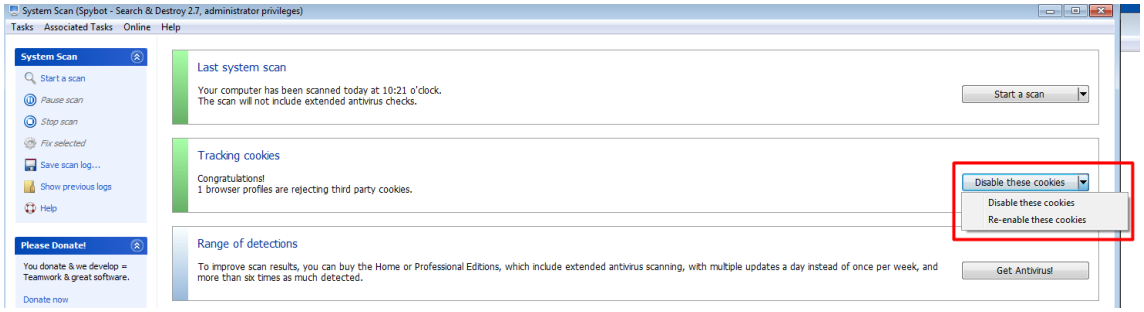
Inmunization, actúa como un antivirus para proteger también de los virus en tiempo real cuando navegas.

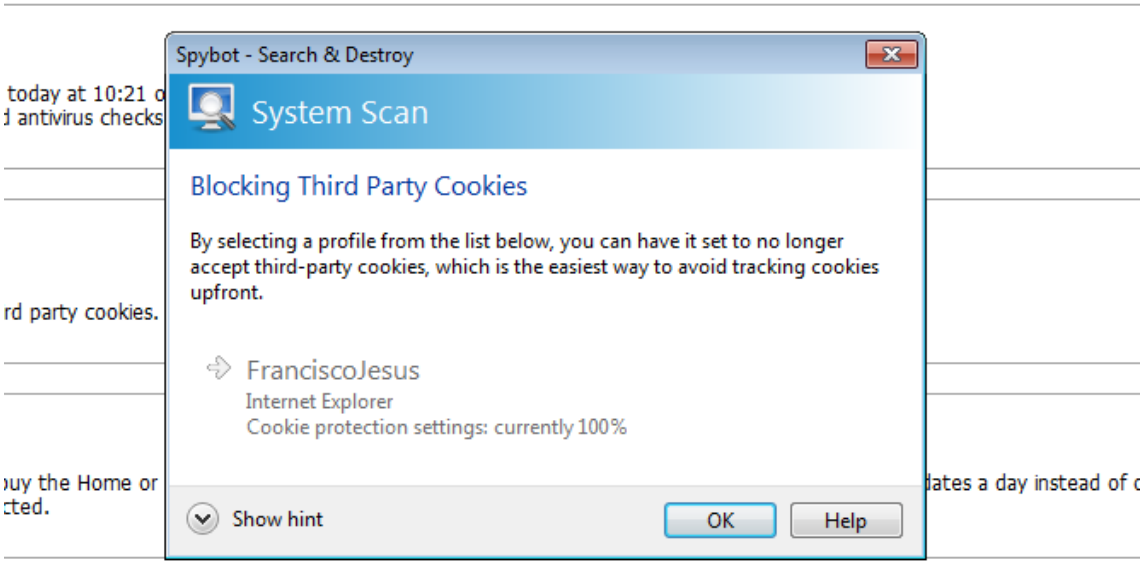


Los escaneos no se pueden hacer avanzados o customizados.

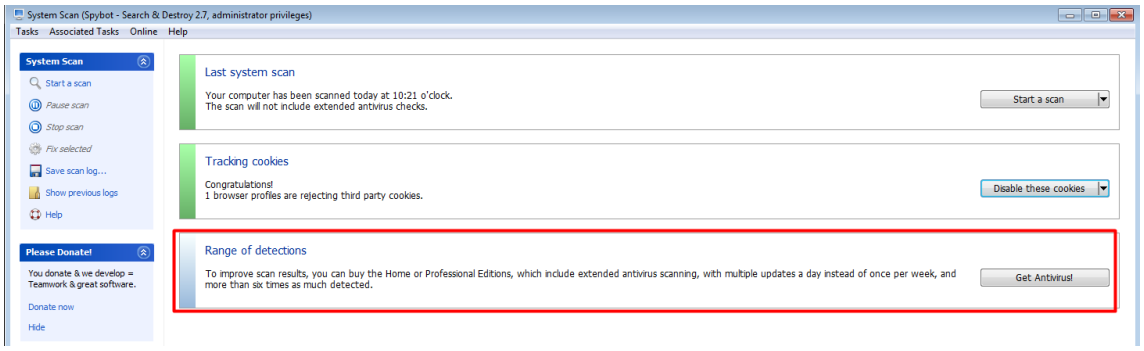


Podemos desactivar o eliminar las cookies, al mismo tiempo, podremos volverlos a activar.

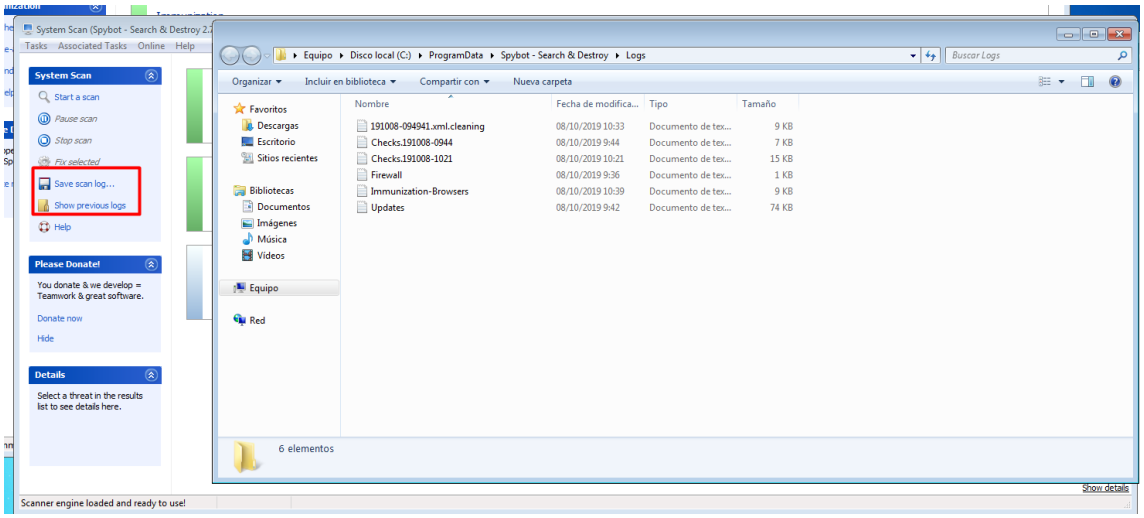




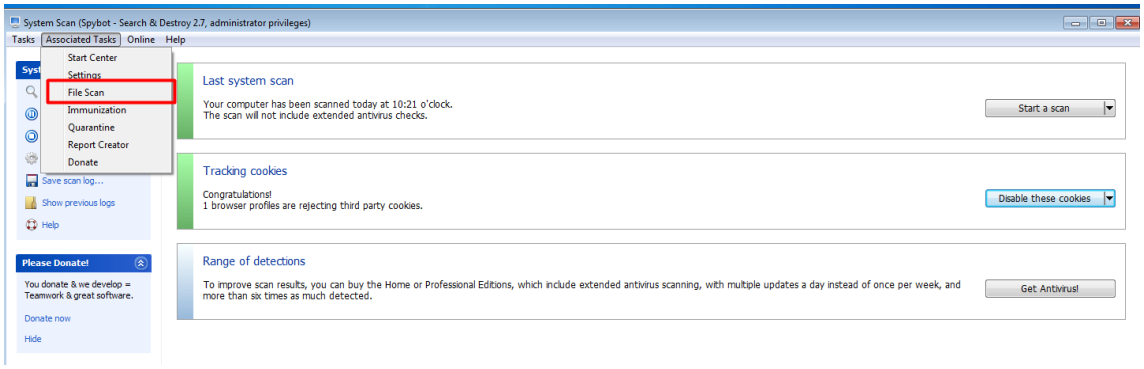
También tendremos la opción de acompañarlo con su antivirus, el cual es de pago.

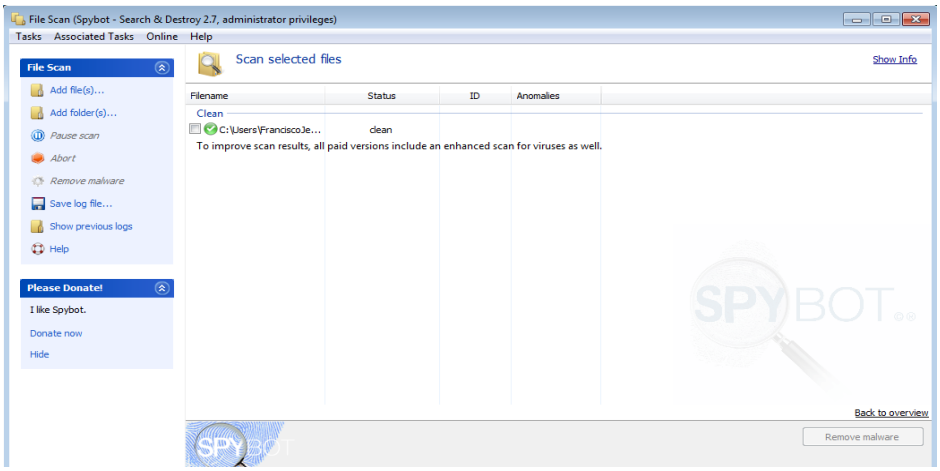


Podremos mostrar los *logs* antiguos y exportarlos.

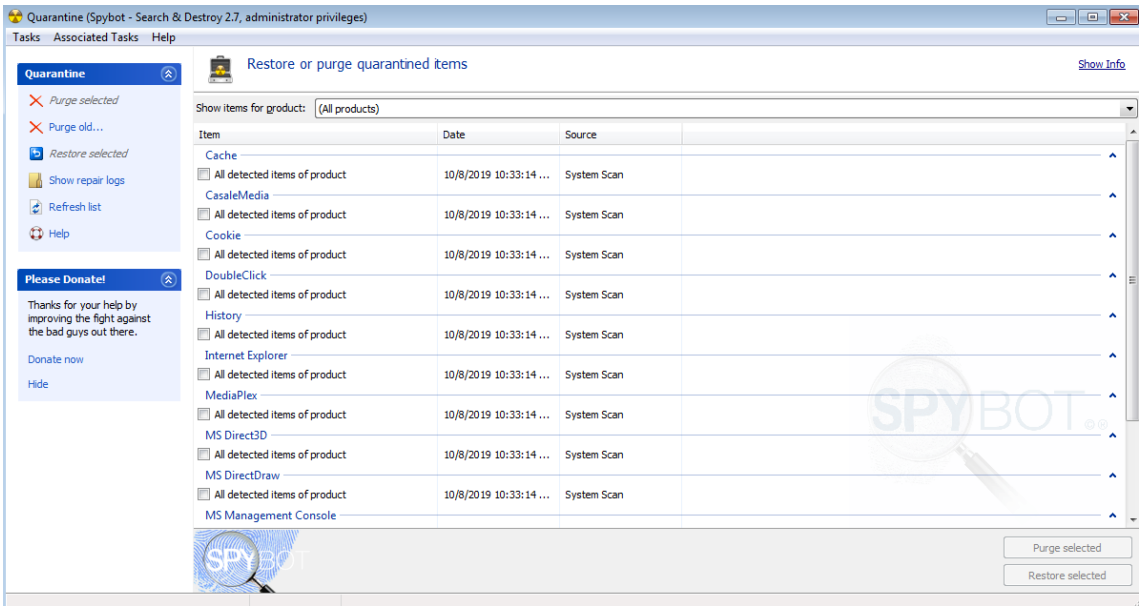


Podemos analizar archivos individualmente o ver la cuarentena.



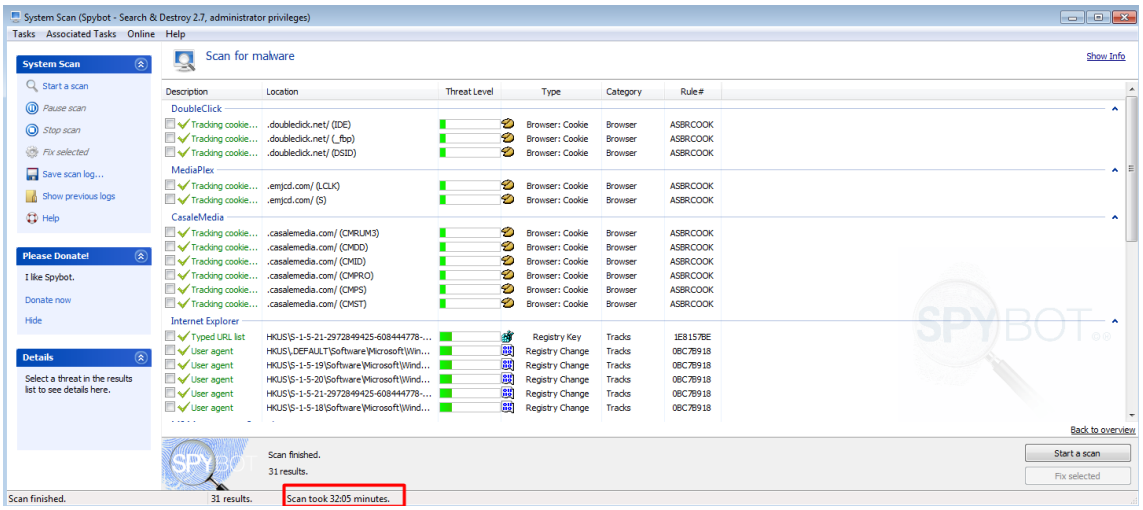


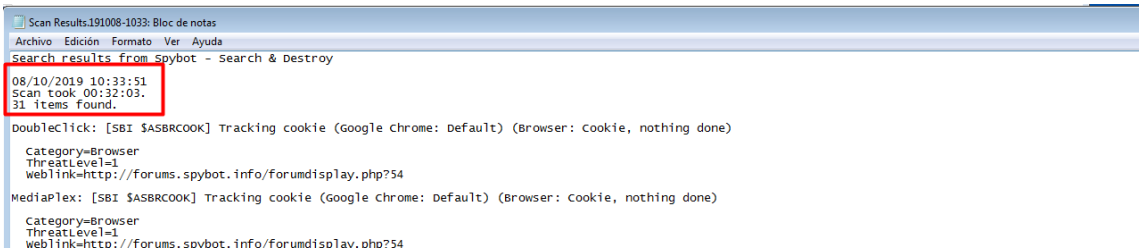
Cuarentena



- Tiempo de escaneo.

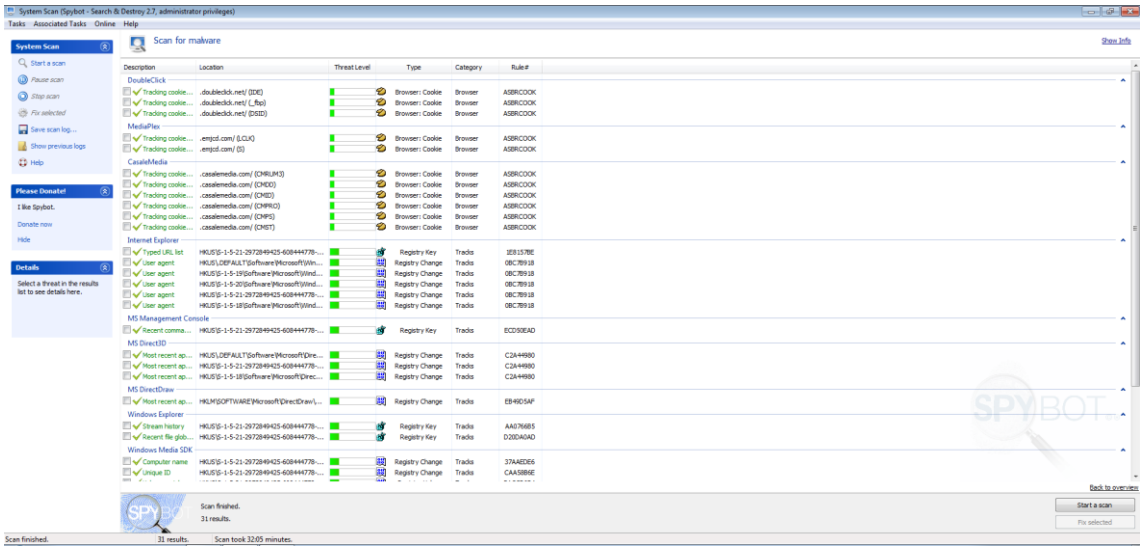
El escaneo duro bastante más tiempo que Malware Bytes sin saber cuántos archivos ha escaneado, en total fue 32 minutos con 5 segundos.





- 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, algo que es normal, 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.