GUIAS DE SEGURIDAD UJA

Software malicioso (*malware*)

Servicio de Informática
Vicerrectorado de Tecnologías de la Información
y la Comunicación y Universidad Digital
Universidad de Jaén

Edición: **enero 2018**

Contenidos

1. ¿Qué es el malware?

El término *malware* (también conocido como software malicioso o software malintencionado) hace referencia a todo tipo de programas diseñados específicamente para dañar un ordenador o una red o para obtener algún tipo de beneficio o hacer mal uso del mismo.

El malware en muchos casos se instala en nuestro ordenador sin nuestro conocimiento, generalmente a través de descargas o enlaces de carácter engañoso que simulan ser contenido en el que podríamos estar interesados. Una vez que el malware se ha instalado en el ordenador, las personas que tienen el control en muchas ocasiones pueden intentar acceder a nuestra información personal. A veces registran nuestras pulsaciones de teclas (*keylogging*) o controlan la actividad de nuestro equipo, pudiendo forzarlo a visitar determinados sitios web, enviar correos electrónicos o realizar otras acciones sin nuestro conocimiento. Los efectos del malware pueden ser tan inofensivos como una pequeña molestia o tan graves como un robo de identidad, con todo el perjuicio que ello nos puede causar.

Los síntomas más habituales de que nuestro equipo ha sido infectado con algún tipo de *malware* son diversos:

- Aparición de barras de elementos adicionales en nuestro navegador web sin que nosotros las hayamos instalado conscientemente.
- Nuestra página de inicio cambia sin que nosotros lo indiquemos. Si la sustituimos por la correcta, vuelve a cambiar automáticamente.
- Cuando navegamos por Internet, determinadas páginas son redirigidas automáticamente a otras de dudoso contenido (pornografía, hacking, juegos on-line, páginas de acceso mediante pago...). La lista desplegable que indica los elementos más visitados se elimina y los elementos se cambian por enlaces a páginas web cuyo contenido se encuentra entre los citados anteriormente.
- El equipo se ralentiza y se cargan iconos desconocidos en la barra de Windows.

En esta guía veremos con detalle en qué consiste el malware, así como las medidas de prevención, análisis y eliminación que podemos poner en práctica.

2. Tipos de malware y técnicas de infección más comunes

Los ejemplos de malware más habituales suelen ser los siguientes:

- **Virus:** es un tipo de malware cuya finalidad es la de alterar el funcionamiento normal de nuestro equipo, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados y pueden destruir de manera intencionada datos almacenados en un ordenador, aunque en otros casos son más inofensivos y solo se caracterizan por ser molestos.
- **Gusanos (*worms*):** similares a los virus, los gusanos son programas informáticos malintencionados que se replican automáticamente, usando una red

informática para enviar copias de sí mismos a otros ordenadores de la red, pudiendo causar un enorme efecto en muy poco tiempo.

- **Troyanos:** son programas destructivos que se hace pasar por una aplicación legítima e inofensiva. En teoría, este software parece realizar la función deseada por el usuario, pero por detrás y sin el conocimiento del usuario, roba información, daña el sistema o abre una puerta trasera para poder entrar al equipo de forma remota sin ser detectado.

- **Software espía (*spyware*):** es un software malintencionado que extrae información sobre los usuarios sin su conocimiento. Sus objetivos son muy determinados: básicamente el envío de datos del sistema donde están instalados y la apertura de puertas para el acceso al PC desde Internet. En muchos casos, quien accede puede ser una empresa de publicidad de Internet. Todas estas acciones, como en la mayoría de los casos de malware, son llevadas a cabo sin el conocimiento del usuario.

  Aunque tiene cierta similitud con los troyanos, el *spyware* generalmente no representa un peligro de manipulación ajena del sistema, ni suele causar daños a nuestro ordenador por parte de terceros. Sus efectos son, simple y llanamente, la violación de nuestros derechos de confidencialidad de nuestros datos y una navegación más lenta

- **Software publicitario (*adware*):** cualquier paquete de software que reproduce, muestra o descarga anuncios en nuestro ordenador de forma automática y sin nuestro consentimiento.

- **Rogue software y Ransomware:** Los programas "rogue" hacen creer al usuario que su ordenador está infectada por algún tipo de virus u otro tipo de software malicioso, esto induce al usuario a pagar por un software inútil o a instalar un software malicioso que supuestamente elimina las infecciones y que el usuario realmente no necesita, puesto que no está infectado.

  Los programas de tipo ransomware, también llamados criptovirus o secuestradores, son programas que cifran los archivos importantes para el usuario, haciéndolos inaccesibles, y piden que se pague un rescate para poder recibir la contraseña que permite recuperar esos archivos.

- **Rootkits.** Son conjuntos de programas que modifican el sistema operativo de nuestro PC para permitir que el malware permanezca oculto al usuario. Por ejemplo, los rootkits evitan que un proceso malicioso sea visible en la lista de procesos del sistema o que sus ficheros sean visibles en el explorador de archivos. Este tipo de modificaciones consiguen ocultar cualquier indicio de que el ordenador está infectado por un malware.

- **BHO (*Browser Helper Objects*):** son otro tipo de pequeños programas que pueden cambiar el funcionamiento habitual de nuestro navegador con fines diversos, en la mayoría de los casos, no deseados por el usuario. Los BHO son programas asociados al navegador Internet Explorer de Microsoft (plugins), que extienden sus funcionalidades. Ejemplos de BHO son barras adicionales que se añaden al navegador.

  Un BHO no tiene por qué ser malicioso, pero sí que se puede usar en muchas ocasiones con fines maliciosos. El *spyware* y los denominados "secuestradores de navegador" a menudo se instalan en forma de BHO. Un BHO puede acceder a

cada dirección web que visitamos y nos puede redirigir a visitar páginas no solicitadas (sexo, publicidad...). Los secuestradores de navegador (*browser hijackers*) son pequeños programas o entradas en el registro de Windows que cambia las páginas de inicio y búsqueda del navegador Internet Explorer de Microsoft. Si nuestro navegador arranca con una página desconocida, empieza a abrir ventanas con paginas web de contenido "dudoso" y efectos similares, probablemente en nuestro equipo se haya instalado un secuestrador de navegador. Los secuestradores a menudo se instalan aprovechando agujeros de seguridad.

2.1. ¿Cómo llega el malware hasta nuestro PC?

La respuesta es simple: lo introducimos nosotros mismos, aunque en la mayoría de los casos sin tener conocimiento. En unos casos, el malware viene acompañando a programas de tipo *shareware* y *freeware*, especialmente en aquellos programas que incorporan publicidad. Estos programas suelen ser una oferta tentadora para multitud de usuarios, ya que en muchos casos se trata de programas útiles y en ocasiones, los mejores de su categoría. Cuando instalamos uno de estos programas, al mismo tiempo introducimos en nuestro sistema los archivos ocultos incluidos en forma de malware y que en muchos casos revelarán nuestros datos a empresas muy interesadas en ellos o permitirán el acceso remoto de forma oculta a nuestro equipo.

Existen gran variedad de formas por las que el malware puede llegar a un ordenador:

- **Explotando una vulnerabilidad:** cualquier programa del ordenador puede tener una vulnerabilidad o agujero de seguridad que puede ser aprovechada para introducir programas maliciosos. Todos los programas instalados en el equipo: sistemas operativos (Windows, Linux, MacOS, etc), navegadores web (Internet Explorer, Firefox, Opera, Chrome, etc), clientes de correo electrónico (Outlook, Thunderbird, etc) o cualquier otra aplicación son susceptibles a tener alguna vulnerabilidad que puede ser aprovechada por un atacante para introducir programas maliciosos. Para prevenir infecciones por esta vía, se recomienda tener siempre actualizado el software en nuestro equipo.

- **Ingeniería social:** Las técnicas de ingeniería social apremian al usuario a que realice determinada acción. La ingeniería social se utiliza sobre todo en correos de phishing, informando de una falsa noticia de gran impacto, o amenazando al usuario de diversas formas. Tanto para los correos de phishing como para el resto de mensajes con contenido generado con ingeniería social, lo más importante es no hacer caso de ellos.

- **A través de un archivo malicioso:** esta es la forma que tienen gran cantidad de troyanos de llegar al equipo. El archivo malicioso puede llegar como adjunto de un mensaje, por redes P2P, como enlace a un fichero que se encuentre en Internet, a través de carpetas compartidas en las que el gusano haya dejado una copia de sí mismo, etc. La mejor forma de prevenir la infección es analizar con un buen antivirus actualizado todos los archivos antes de ejecutarlos, además de no descargar archivos de fuentes que no sean fiables.

- **Dispositivos extraíbles (ej: llaves USB):** muchos gusanos suelen dejar copias de sí mismos en dispositivos extraíbles para que automáticamente, cuando el dispositivo se conecte a un ordenador, ejecutarse e infectar el nuevo equipo. La

mejor forma de evitar quedarse infectados de esta manera, es deshabilitar el autoarranque de los dispositivos que se conecten al ordenador.

3. Cómo combatir el malware. Medidas prácticas

1. **Actualiza tu sistema operativo** con todos los parches más recientes y activa las actualizaciones automáticas si es posible.

2. **Instala periódicamente todas las actualizaciones del navegador.** Actualmente, la mayoría de navegadores se actualizan de forma automática y transparente a la última versión. No obstante, se recomienda comprobar si hay actualizaciones pendientes. La mayoría de navegadores además muestran un mensaje de advertencia si el usuario intenta acceder a un sitio web sospechoso de contener malware. Presta mucha atención a estas advertencias. Ten en cuenta que el malware también puede incluirse en los complementos del navegador, así que te recomendamos que instales únicamente extensiones en las que confíes.

3. **Sé muy cuidadoso al hacer clic en un enlace o descargar un archivo.** Al hacer clic en enlaces desconocidos, puedes exponer tu ordenador a software y sitios web malintencionados. Este software suele contener programas que analizan tu ordenador o realizan un seguimiento de las teclas que pulsas, incluidas tus contraseñas. Para proteger tu ordenador, descarga únicamente archivos de fuentes en las que confíes. Ten cuidado cuando accedas a sitios desconocidos. Si no estás seguro, sal del sitio y busca información sobre el software que se te pide que instales.

4. **Desconfía de cualquier elemento de un correo electrónico que parezca sospechoso.** Incluso los correos electrónicos de las personas que conoces pueden contener archivos adjuntos o enlaces malintencionados si se han comprometido sus cuentas. Ten cuidado al hacer clic en los enlaces incluidos en un correo electrónico. Es recomendable visitar los sitios web introduciendo la dirección directamente en el navegador.

5. **No abras archivos si no conoces su extensión** o si recibes advertencias o mensajes del navegador web que no te resulten familiares.

6. Algunos programas incluyen malware u otro software de carácter engañoso como parte de su proceso de instalación. **Al instalar software, presta especial atención a los mensajes que aparezcan y lee la letra pequeña.** También es recomendable buscar información sobre cualquier software desconocido antes de iniciar el proceso de instalación. Si sospechas que el software pueda ser malicioso, cancela la instalación de forma inmediata.

7. **Ten mucha precaución con las unidades USB.** Tus amigos, familiares o compañeros de trabajo pueden darte una unidad USB (un pendrive o un disco duro externo) con archivos infectados sin su conocimiento. Siempre ten la precaución de analizar la unidad externa con un buen software antivirus antes de abrir los archivos.

8. **No te fíes de las ventanas emergentes que te piden que descargues software.** Normalmente, estos pop-ups te harán creer que se ha infectado tu ordenador y

te pedirán que descargues software para protegerte frente a amenazas (rogue software). Cierra la ventana y asegúrate de no hacer clic en ninguna zona de la ventana emergente.

9. **Ten cuidado con la descarga de ficheros desde redes P2P** (BitTorrent y similares). Este tipo de servicios apenas controla la existencia de software malintencionado, por lo que debes tener cuidado si descargas un archivo a través de ellos. El software malintencionado se puede hacer pasar por un programa, un disco, una película o cualquier elemento conocido.

10. **Elimina el malware lo antes posible.** Existe una serie de programas que te pueden resultar útiles y que explicamos con detalle en la siguiente sección.

4. Herramientas anti-malware específicas

La forma más practica de detectar y eliminar el malware pasa por el uso de herramientas específicas. Actualmente, la gran mayoría de productos antivirus incluyen funcionalidades de detección y limpieza de malware. No obstante, son las herramientas específicas las que mejores resultados suelen ofrecer, sobre todo con determinados tipos de malware difícil de detectar. En esta guía se ofrece una guía rápida de una de las herramientas más usadas: Malwarebytes Antimalware.

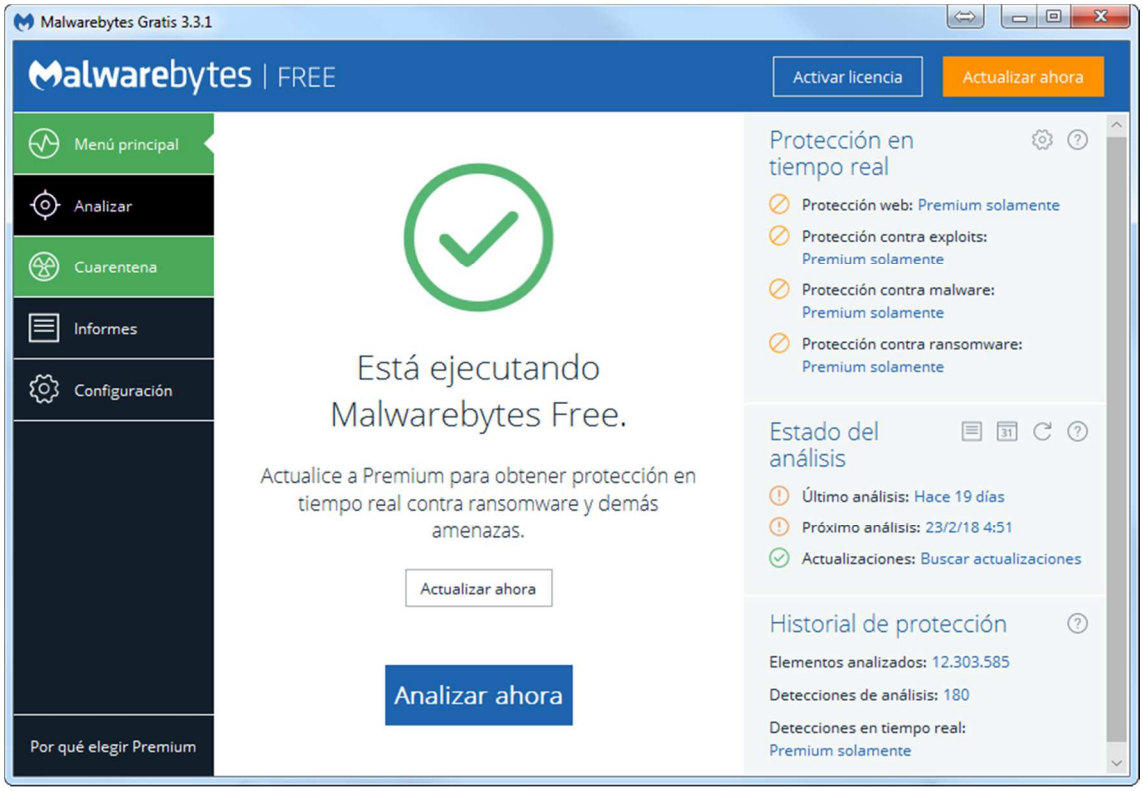
4.1. Malwarebytes Antimalware

Malwarebytes Antimalware es una excelente utilidad gratuita que busca, detecta y elimina todo tipo de malware. Está diseñado con las más sofisticadas técnicas antimalware que le permiten detectar y eliminar los programas maliciosos más comunes y peligrosos que incluso los más conocidos antivirus no son capaces de detectar.

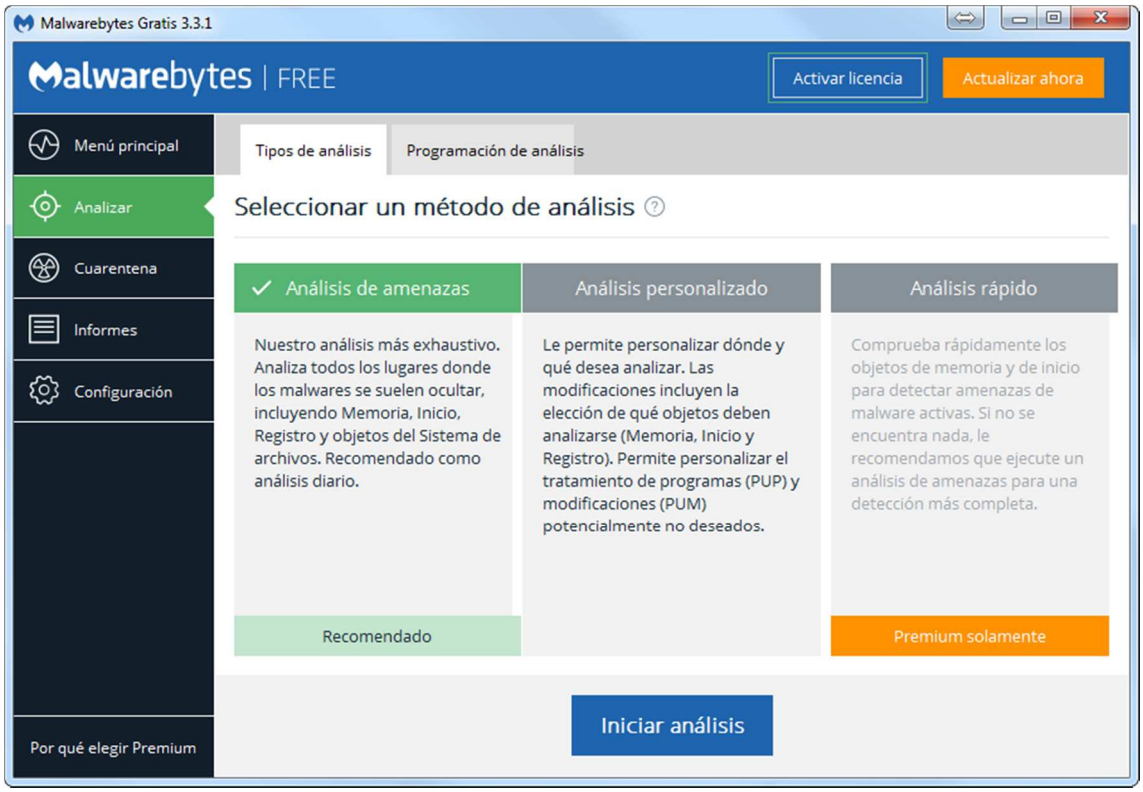
Podemos descargar la última versión del programa desde su web (hay una versión gratuita y otra de pago). Está disponible para diferentes sistemas operativos (Windows, MacOS X, Android…) y se puede descargar desde:

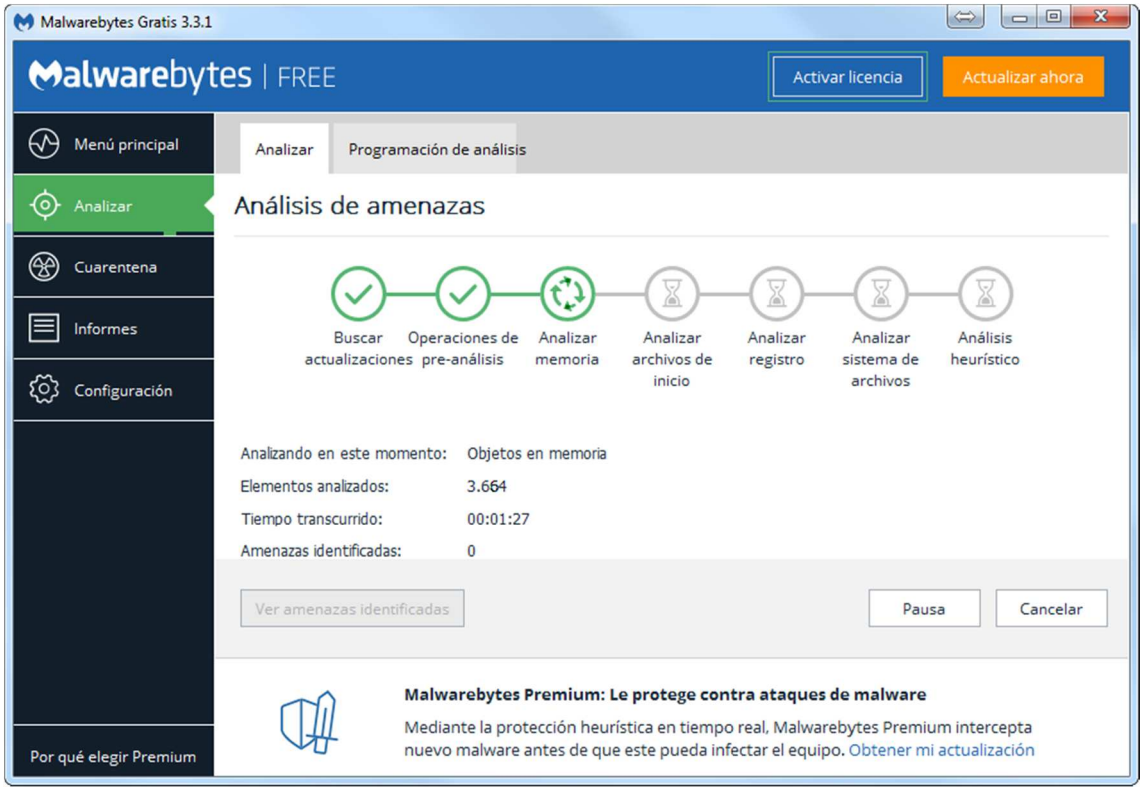
https://es.malwarebytes.com/mwb-download/

Una vez tengamos el programa, pasaremos a instalarlo. Basta con seguir el asistente de instalación paso a paso. Cuando la instalación finalice, ejecutaremos el programa y aparecerá la ventana principal:

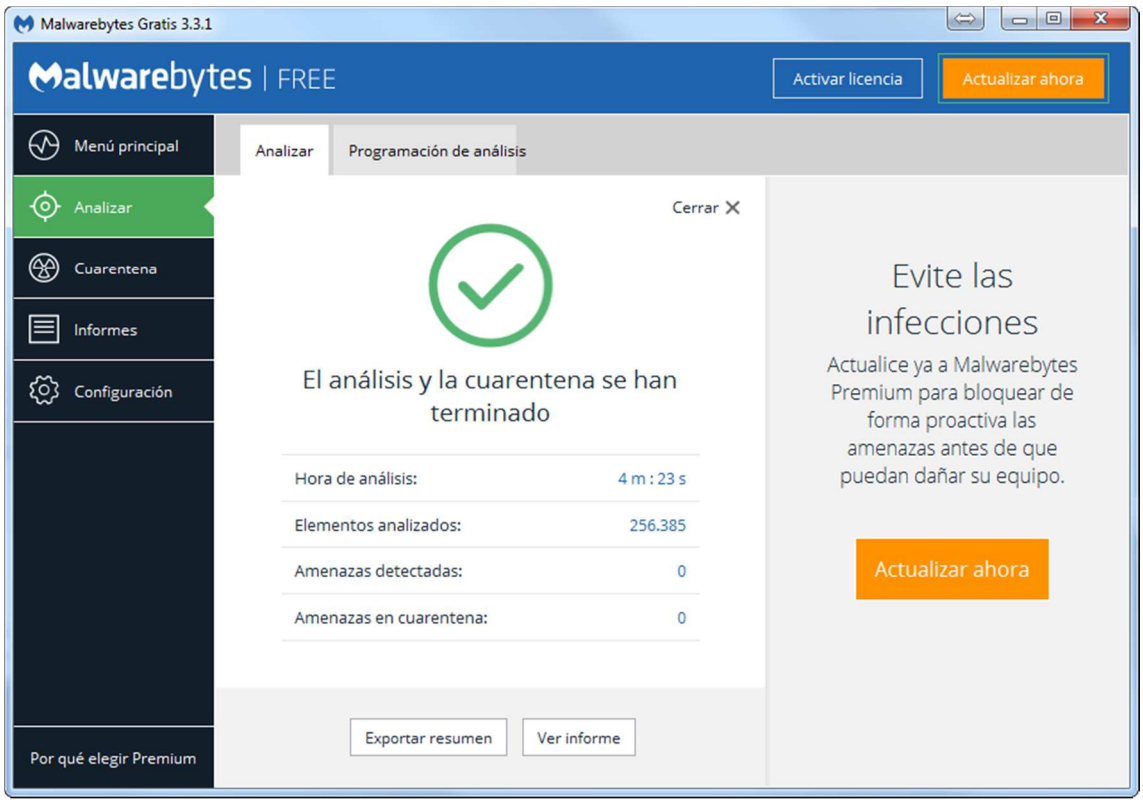


Tenemos la opción de hacer distintos tipos de análisis (general o personalizado). Pulsando el botón **Iniciar Análisis** comenzará el análisis:

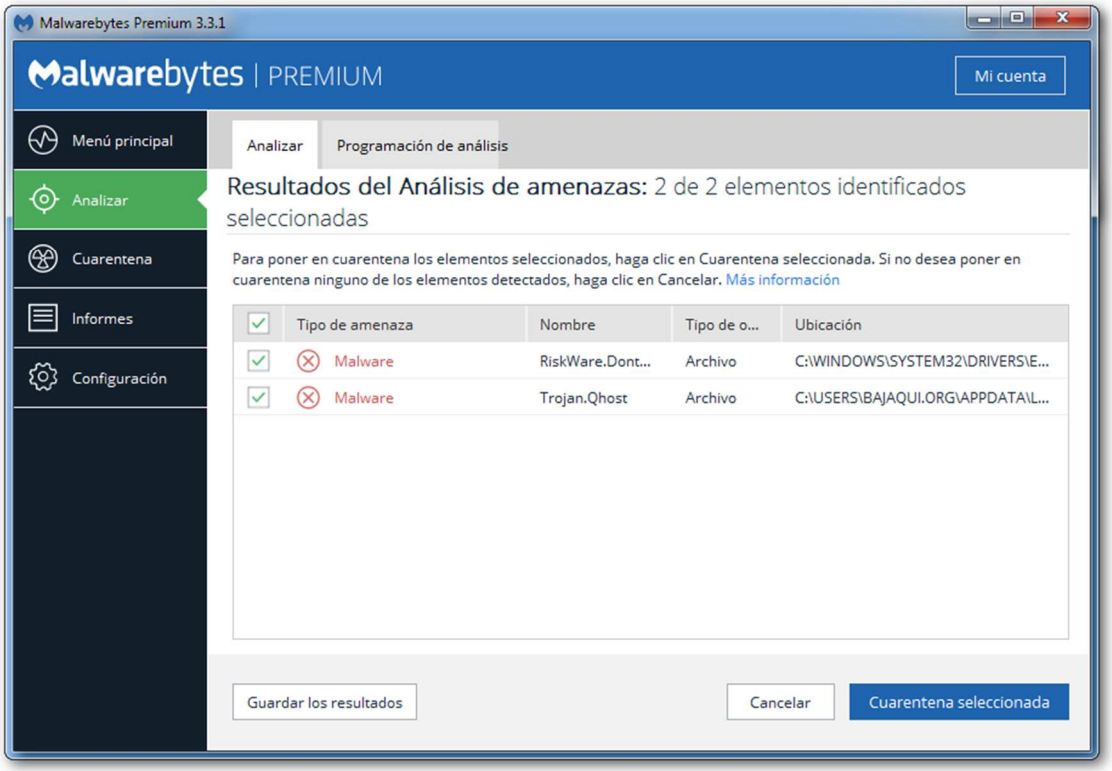




Una vez finalizado, nos muestra los resultados de análisis:



En caso de que se hayan encontrado elementos maliciosos, se indicará el número de elementos maliciosos detectados. Podemos ver el detalle, haciendo clic sobre cada uno de los resultados:



En esta ventana de detalle, podemos marcar individualmente cada uno de los elementos maliciosos detectados. Una vez marcados, pulsando el botón **"Cuarentena seleccionada"** el programa procederá a la limpieza y moverá a cuarentena los elementos maliciosos seleccionados.

En algunas ocasiones, dependiendo del tipo de malware y lo rebelde que este sea, la herramienta nos indicará que para la efectiva y correcta desinfección del equipo debemos reiniciar el sistema para que se puedan eliminar los archivos que faltan por desinfectar.

NOTA: Los distintos informes de Malwarebytes Antimalware también lo podremos encontrar de forma detallada seleccionando la opción **Informes**.

Notas a tener en cuenta

Como se ha indicado, el programa ofrece una versión gratuita que no ofrece todas las funcionalidades de la versión comercial, pero aun así, las funciones básicas de análisis y desinfección sí que están disponibles. Algunas de las funciones no disponibles en la versión gratuita son:

- Módulo residente de protección en tiempo real (sólo permite una prueba de 14 días).
- Protección anti-exploits (sólo permite una prueba de 14 días).
- Protección anti-ransomware (sólo permite una prueba de 14 días).
- Protección frente a sitios web maliciosos (sólo permite una prueba de 14 días).

Para que sea efectivo, Malwarebytes Antimalware necesita ser actualizado. Las actualizaciones se producen con mucha frecuencia y el propio programa nos recuerda cuándo tenemos que hacer una actualización. No obstante, al realizar un análisis el primer paso que realiza es el programa es la actualización de las bases de datos, por lo que no debemos preocuparnos.

5. Referencias en Internet

- Instituto Nacional de Ciberseguridad (INCIBE)
  http://www.incibe.es
- Oficina de Seguridad del Internauta (OSI)
  http://www.osi.es/
- CCN-CERT
  https://www.ccn-cert.cni.es/
- Guardia Civil - Grupo de Delitos Telemáticos:
  https://www.gdt.guardiacivil.es
- Policía Nacional – Brigada de Investigación Tecnológica
  http://www.policia.es/org_central/judicial/udef/bit_alertas.html
- Vídeos Intypedia: Lección 6 – Malware (con ejercicios)
  http://www.criptored.upm.es/intypedia/video.php?id=malware&lang=es
- InfoSpyware:
  http://www.infospyware.com/articulos/que-son-los-malwares/
- Eset Security:
  http://www.eset-la.com/centro-amenazas/tipos-amenazas