UADER-Facultad de Ciencia y Tecnología
Laboratorios GUGLER

Tema: Virus informáticos

Integrante: Acosta, Agustina.

Curso: Reparación y Mantenimiento de PC con Herramientas Libres.

Índice:

Hoy en día es muy común hablar que nuestra computadora está infectada por uno o varios virus que pueden ser a través de internet desde un simple correo electrónico que tienen archivos adjuntos, publicidades, descargas de archivos en páginas poco confiables, o a través de un ataque cibernético a nivel mundial, que son perjudiciales para los usuarios y en su mayoría para los cuerpos gubernamentales.

Los hackers que usan un malware dependiendo de su tamaño son capaces de hasta entrar al sistema de una gran ciudad (que gran parte dependen de un sistema informático) y de ahí controlar los suministros eléctricos, agua, gas, etc. hasta llegar un corte de los mismos.

En el siguiente trabajo hablaremos sobre los virus y sus variedades, y luego una propuesta y prueba de un programa para combatir con la infección.

¿Qué son los virus informáticos?

Los virus informáticos es un programa malicioso también conocido como malware, que con lo cual se activan sin el permiso del usuario pasándose la barrera del firewall (que en español sería muro de anti-incendios), que nos protege de los agentes externos que quieran ingresar a nuestra computadora, que pueden alterar el funcionamiento del ordenador.

Su intención es entrar al computador, infectar y replicarse sin que el usuario se de cuenta, con lo cual ha sido programado que hiciera ciertas acciones. Puede infectar desde archivos diarios hasta entrar al sistema de arranque del computador.

En el caso de infectar un archivo, el mismo ingresa su propio código malicioso en las líneas del código del programa y se ejecutará cada vez que se inicia ese mismo programa.

Un malware puede: replicarse, controlar el equipo, robar información, alojarse en la memoria RAM y consumirla, dañar archivos, etcétera.

Tipos de virus:

Hoy en día, en promedio se crean como 50.000 virus diarios. Ante la variedad de virus podemos clasificar algunos de ellos de la siguiente manera:

- Virus de acción directa:
  Este tipo de virus se activan al momento de ejecutar el programa. Su ataque empieza cuando una determinada condición hace que se active. Su función es replicarse y llevar a cabo su tarea a la que ha sido programada.

- Virus residentes:
  Un virus residente se alojan en un sector de la memoria RAM del computador que puede ser permanente o residente. Tiene la particularidad de controlar las operaciones de entrada y salida de datos realizadas por nuestro sistema operativo.
  Su objetivo es infectar a cualquier programa y/o carpetas que sean ejecutado en esos momentos ya sea para modificar, abrir, copiar, etc.

- Virus de boot:
  Se alojan en el sector de arranque de nuestro computador, sector que por lo cual hace que inicie nuestro ordenador y sistema operativo. No infectan a ficheros si no a discos.

- Virus de macro:
  Esta clase de virus es codificado en lenguaje macro y se coloca en las líneas de código de un archivo o plantilla de texto que en ese momento el usuario no suele darse cuenta que está infectado. Se activan automáticamente cuando el mismo es ejecutado, siguiendo los pasos en que fue diseñado.

- Virus gusanos:
  Es un virus muy conocido y su intención es pasarse en computadora en computadora y a su vez autoreplicarse en el mismo computador en el que fue infectado. No necesita la intervención de un usuario. También busca información de otras direcciones de computadoras para poder infectar.
  Una manera de detectarlos es notando que el computador trabaja de manera tardia, con lo cual hay que revisar el consumo de la memoria RAM o también pueden consumir ancho de banda de red.

- Virus troyano:
  Este malware también es muy conocido y suelen ser programas que no aparentan nada malo pero cuando suelen ser ejecutados los hackers tienen acceso al computador y pueden robar información personal, controlar y descargar contenido malicioso al mismo.

- Virus polimorfos:
  Un virus polimorfos es capaz de replicarse a sí mismo pero a su vez modificándose a nivel de comportamiento y código para que no se lo logré identificar.

- Virus en ejecutables:
  Esta clase de virus infectan a los ejecutables con extensión: .exe, .com, .bat, .dll, entre otros.
  Cuando se ejecutan, primero infectan con su código y luego vuelve al curso normal al programa que está infectado. El mismo se resguarda en la memoria y comienza a infectar a otros archivos que son abiertos luego de la ejecución del ejecutable infectado.

- Virus por correo electrónico:
  El correo electrónico es una vía segura de infectar al usuario. Con lo cual varios virus informáticos mencionados anteriormente es enviado por esta vía como un archivo adjunto o direcciones de páginas web maliciosa.
  En este caso se puede evitar no abriendo el archivo o entrando al link y en lo posible comprobar el origen del mismo si es de una empresa o de un usuario confiable.
  Hoy en día los antivirus vienen con la protección de analizar los correos electrónicos.

Los virus en la actualidad

Día a día los hackers van cambiando de modalidad en su forma de atacar y sus intereses.

Actualmente sus objetivos es robar datos, sobre todo los datos bancarios e información personal, esta técnica es llamada Phishing. A través del robo de información de datos personales, se crea una identidad paralela a la persona con los mismos datos y puede traer diversas consecuencias de manera digital como también física. Como por ejemplo, al usuario le llega un link de una supuesta empresa conocida que a simple vista es igual al original pero por detrás están robando datos ya sea una página de red bancaria, una entidad pública, etc. Para poder evitarlo, es recomendable escribir uno mismo la dirección web ofrecida por la empresa o entidad pública ya que en un buscador es peligroso, controlar que la página sea segura y que cumpla ciertos requisitos.

También podemos encontrar los virus que te bloquean el acceso a tu computador o ciertos archivos a cambio de una suma de moneda virtual a un cierto tiempo como lo fue rasomware y el más actual WannaCry. Se pueden propagar como un gusano o también como un troyano. En este caso afectó a muchos países como también a grandes empresas teniendo muchas pérdidas monetarias.

Los Antivirus

Los antivirus es una de muchas herramientas de prevención ante una situación de infección. El mismo analiza en todo el computador en busca de amenazas y cuando las encuentra, el usuario elige si las guarda en cuarentena o da la orden de eliminarla directamente. Ante esta importancia es necesario poseer uno ya que mientras esta en uso la computadora ya sea navegando en internet o descargando un archivo no se sabe que amenazas pueden entrar y los daños que pueden ocasionar, es decir, es invisible a los ojos para el usuario, por ende esta herramienta nos da la seguridad de que nuestra computadora esta protegida mientras hacemos las cosas cotidianas en ella.

Hoy en día han ido evolucionado y poseen mas herramientas tales como: analizadores de correos electrónicos, de almacenamientos externos tales como USB, dispositivos móviles y discos extraibles, y también para páginas de web (también poseen su propio navegador seguro), una base de datos de virus (que día a día actualizan con nuevas amenazas y eso ayuda a prevenir a que ingresen a nuestra computadora).

➔ Top 5 de Antivirus

A continuación se hará un top 5 de antivirus bajo una mirada personal:

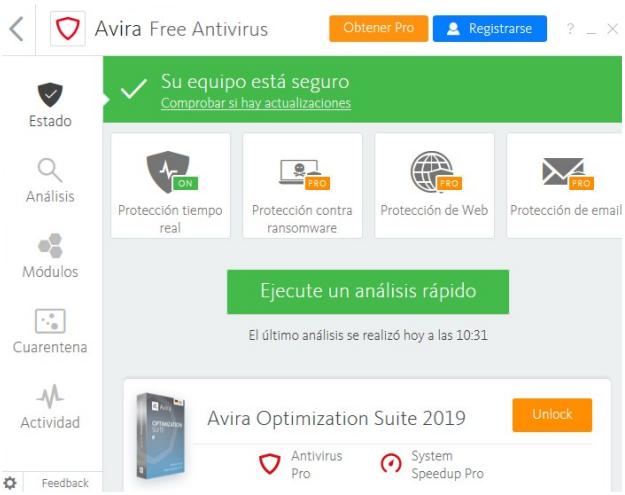
- **Bitdefender Antivirus:**

Posee un antivirus gratis y de pago. El antivirus gratis posee las protecciones básicas contra las infecciones, una protección completa de datos en tiempo real, bloquea las amenazas de tipo rasomware, prevención de ataques en vías de web, brinda una navegación segura ya que tiene protección contra anti-fraude y anti-phising. En la versión de pago posee las mismas características de un antivirus gratis y otras tales como: navegador seguro para realizar operaciones bancarias, protección para las contraseñas, prevención de amenazas de red, soporte en línea, entre otras. Posee versiones para dispositivos móviles y para Linux.

Fácil de usar y no ralentiza el computador.

- **Avira:**

Este programa llamado Avira free antivirus a pesar de que es gratis tiene muchos beneficios que nos ofrecen: Detección de virus, adware, spyware, archivos sospechosos, entre otros; no te ralentiza la computadora, cuenta con un laboratorio de virus donde podes buscar virus o algún archivo sospechoso y te da una breve explicación de lo que es, aparte del antivirus, trae varias herramientas tales como un optimizador, un navegador seguro, organizador de escritorio, liberador de memoria, entre muchas cosas más; y bloquea los malware que sean de tipo rasomware.

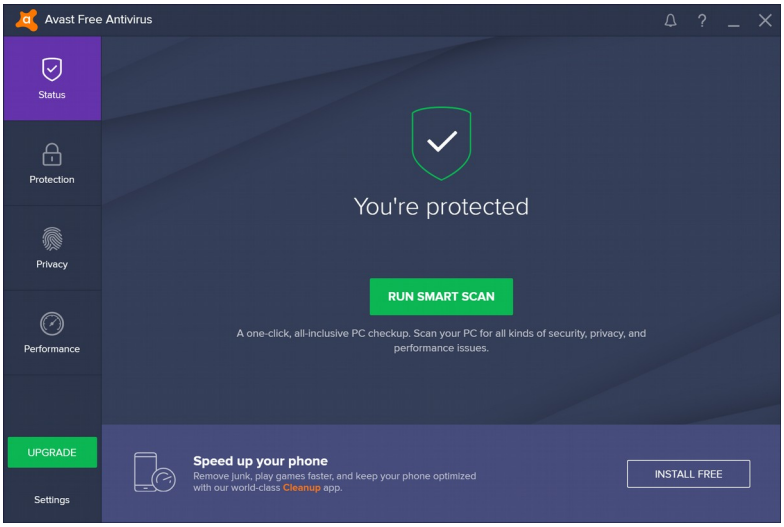


- **AVG:**

Este antivirus obtuvo buena puntuación en los laboratorios independientes. Posee una buena protección contra infecciones, en ataques por vía internet incluyendo a los correos electrónicos y páginas web maliciosas. Además, contiene herramientas variadas tales como: análisis de rendimiento de la pc y eliminación definitiva de archivos . También dispone de una versión para Linux y para servidores.

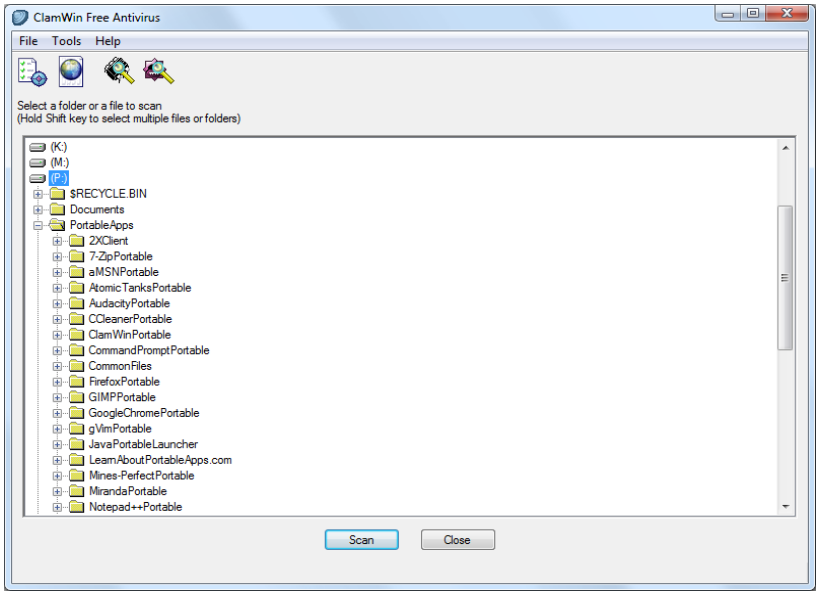
- **Avast:**

Es uno de los antivirus gratuitos mas usado por los usuarios y mas completos. Contiene una protección contra los malware con antispyware, mantiene las contraseñas seguras, antipshising, protección contra el rasomware, un navegador propio, una herramienta llamada cibercapture (Antes de ejecutarse una aplicación desconocida, es analizada por la nube avast y comprueba si es seguro o no), inspector de wi-fi y bloquea los elementos emergentes. Posee una versión para Linux.



- **ClamAV**

Es un antivirus con la particularidad que es de open source y existen versiones tanto para GNU-linux como para también Windows (ClamWin). Su función principal es prevenir ataques por vía correo electrónicos, también posee protección contra virus, gusanos y troyanos incluyendo macros. Tiene un escaneador de archivos y ficheros comprimidos. Se lo destaca por su rapidez de localización y actualización de virus en su base. Realiza actualizaciones automáticas en forma regular agregando los nuevos virus detectados.



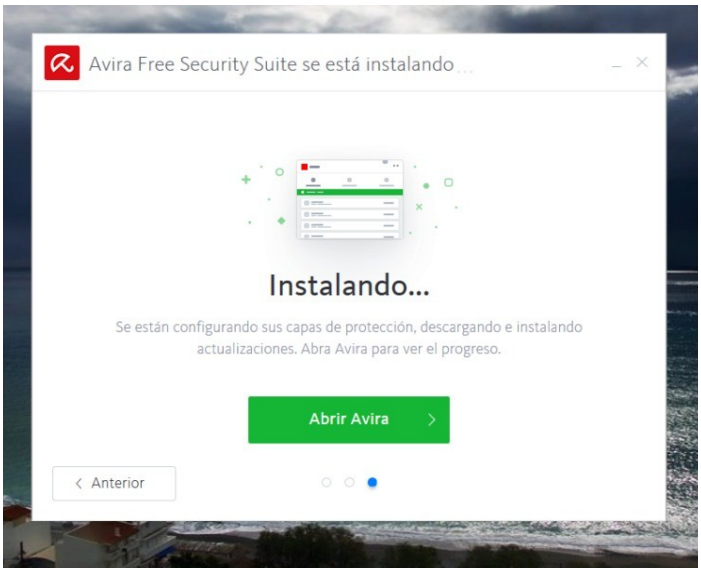
Avira free antivirus

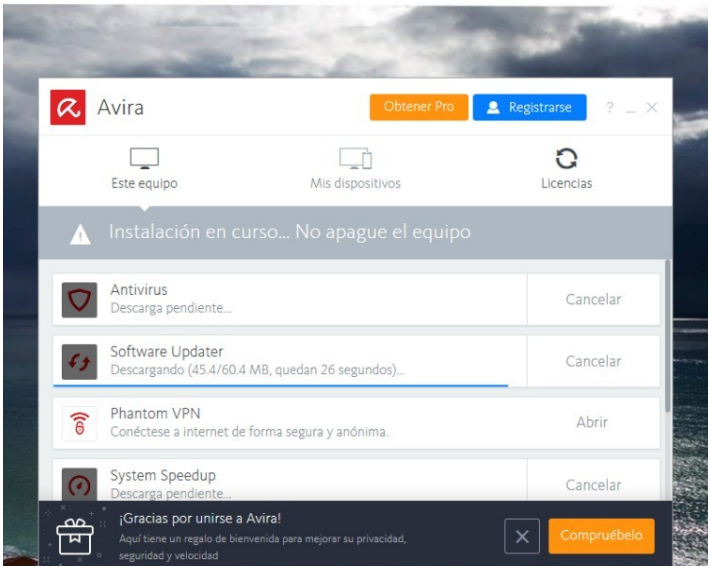
En la siguiente parte del Trabajo Práctico se realizará una prueba para el Avira free antivirus. El motivo de la elección de este antivirus es que: la computadora a analizar no posee muchos recursos por ende este antivirus no la ralentiza y no ocupa mucho espacio, dentro del paquete brinda muchas herramientas (nombradas anteriormente en el top) que son útiles que con lo cual no todos los antivirus te lo ofrecen (a las herramientas que no sean necesarias se pueden eliminar), es sencillo y fácil de usar.

Los requisitos mínimos que solicita Avira son:

- Sistema Operativo: Microsoft Windows 7 Service Pack 1 o superior con las últimas actualizaciones, parches y service packs instalados.
- Memoria RAM: 2 GB de memoria RAM o más.
- Espacio en disco: Al menos 2 GB de espacio libre en el disco duro (se necesita espacio adicional para los archivos temporales y en cuarentena).
- Tipo de CPU: procesador Intel Pentium 4 / AMD Athlon 64 o más potente (compatible con el conjunto de instrucciones SSE2).
- Navegador: Internet Explorer 8 o más reciente.
- Requisitos adicionales: Para que puedas instalarlo necesitarás tener derechos de administrador, conexión a Internet y navegador web.

En cuanto a la instalación solo se tiene que descargar desde la página oficial (https://www.avira.com/es/free-antivirus-windows) el programa a instalar y se abre el siguiente instalador:

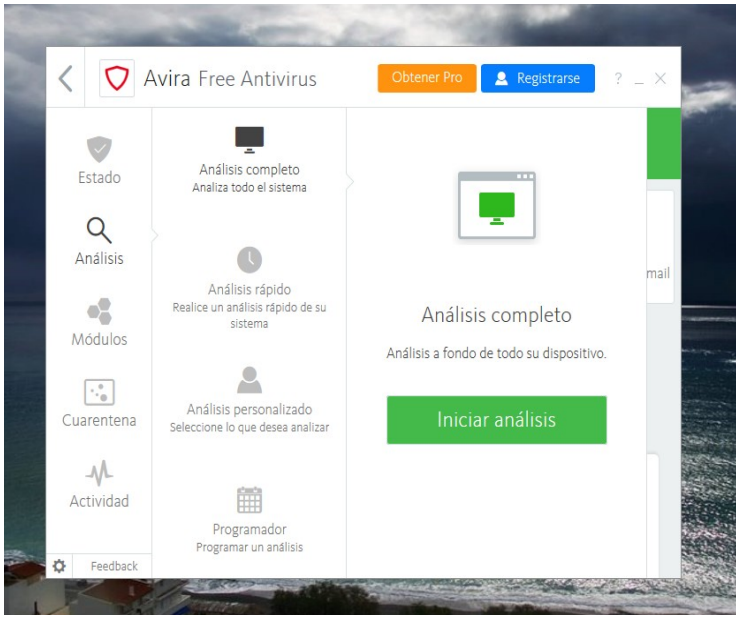


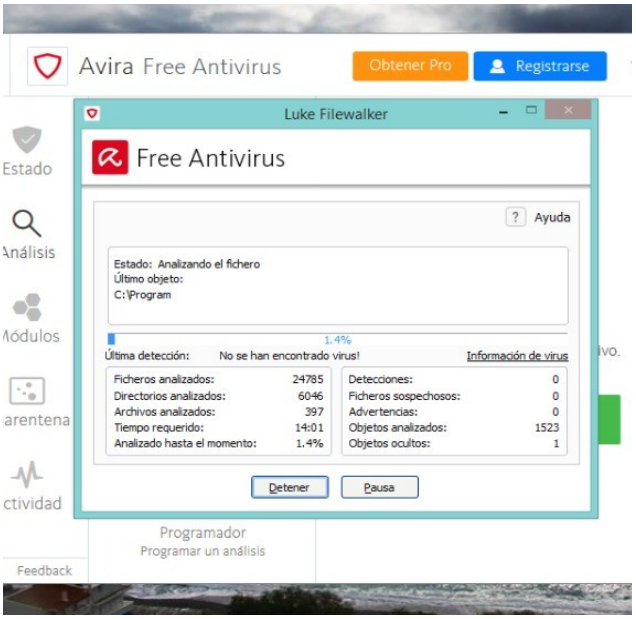


Luego de la instalación se decide qué herramientas desea permanecer en tu computador y cuáles no.

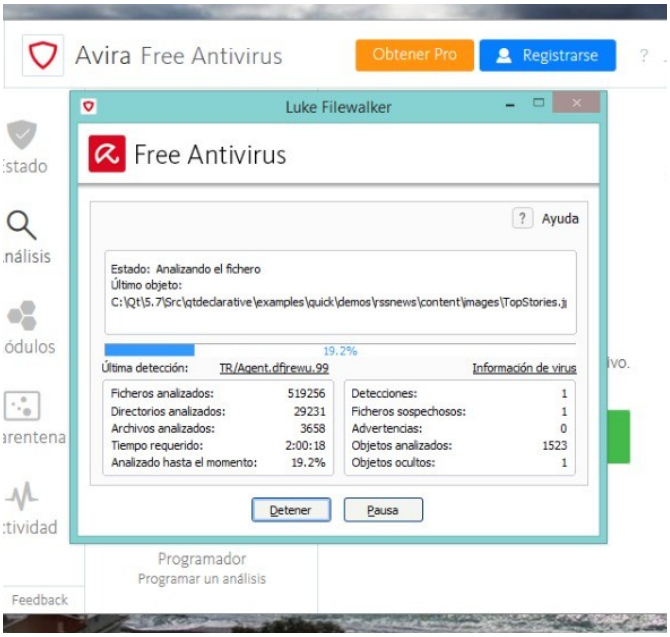
➔ Prueba de Avira free antivirus

Posterior a la instalación procederemos a realizar una prueba al programa.
En el siguiente caso analizaremos una notebook.
-Iniciamos el Programa y nos vamos al apartado de análisis y elegimos la opción de análisis completo. Cuando empecemos el análisis debemos contar con mucho tiempo ya que analiza todo el sistema, en nuestro caso nos llevó en promedio 6 horas cada análisis.

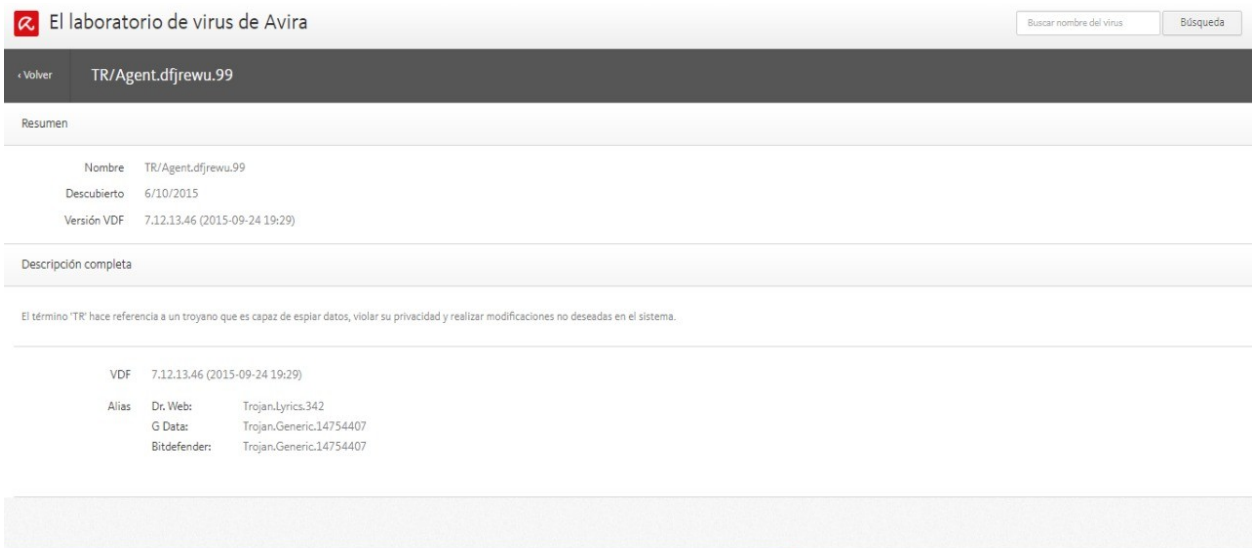




-Luego transcurrido un tiempo se logró detectar lo siguiente:

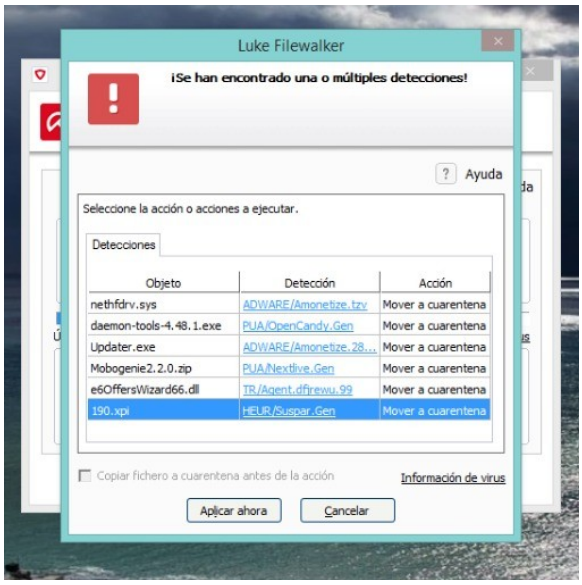


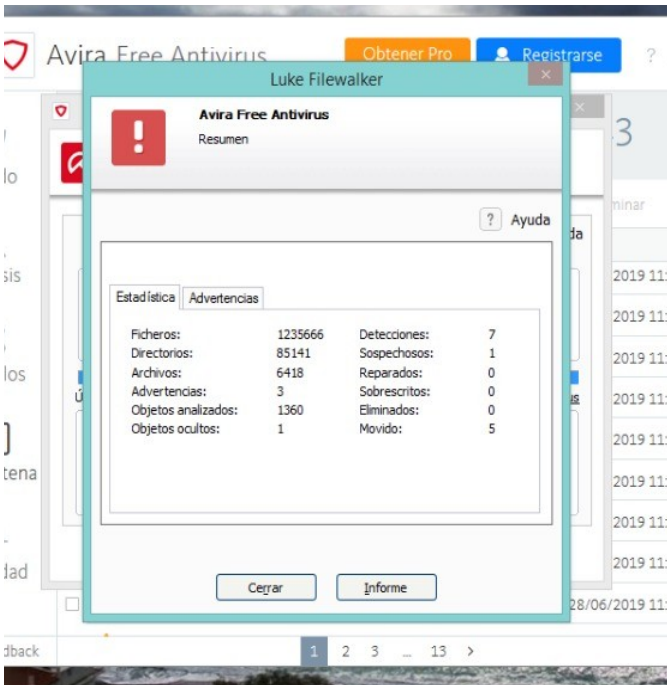
-Se detectó lo siguiente TR/Agent.dfjrewu.99 y haciendo click donde aparece dicho malware nos redirige a una pagina que es el laboratorio de virus de Avira y nos ofrece la siguiente información:



-Tal y como detalla la página encontramos un virus troyano.

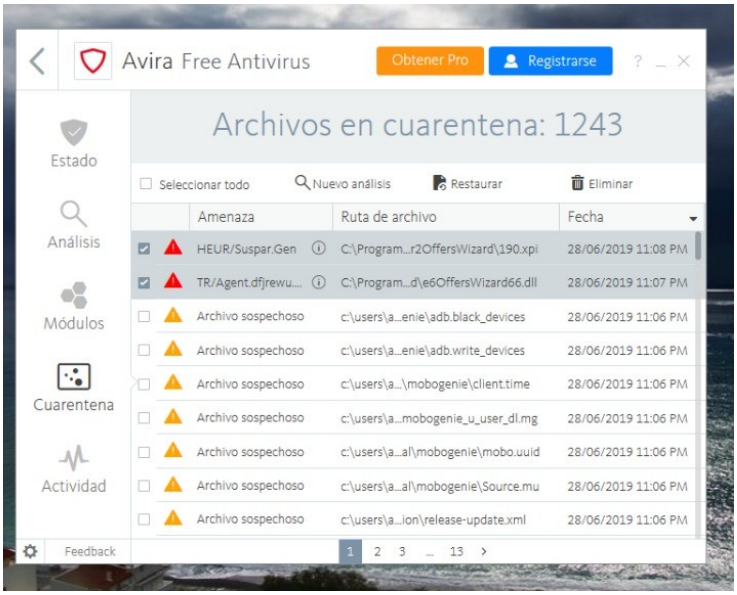
-Luego de finalizar con el análisis observamos que detectó 6 elementos sospechosos:

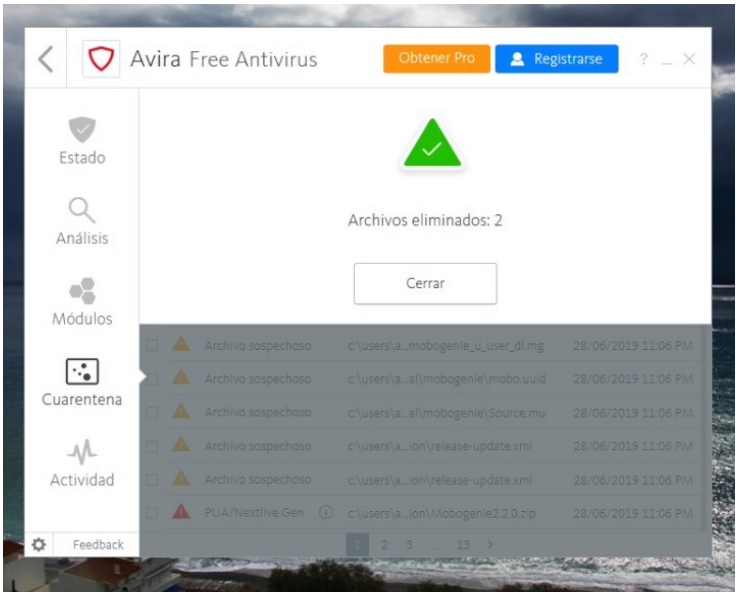




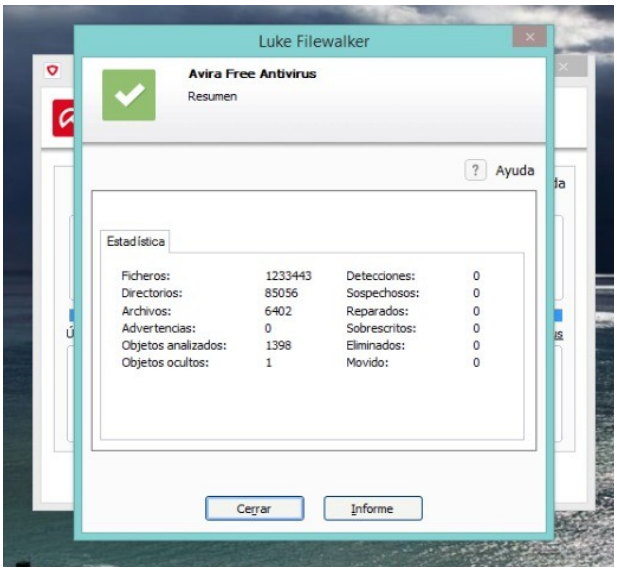
-A las amenazas encontradas las movimos a la cuarentena.

-Luego de reiniciar la computadora procederemos a eliminar dos de los archivos infectados:





-Para finalizar la prueba, se realizo un análisis más para comprobar si se eliminaron los elementos sospechosos y estos son los resultados:



Conclusión

A modo de conclusión de este trabajo puedo decir que día a día se crean nuevos malware por lo tanto es recomendable actualizar y diariamente nuestro antivirus, tomar precaución en la página en que uno ingresa datos personales como también en un correo electrónico, verificar si la fuente donde procede ese link es la correcta, comprobar si es segura la pagina como también observar la tipografía y colocar una herramienta en el navegador que bloquee las publicidades y mensajes emergentes.