TEMA 2

HERRAMIENTAS PALIATIVAS

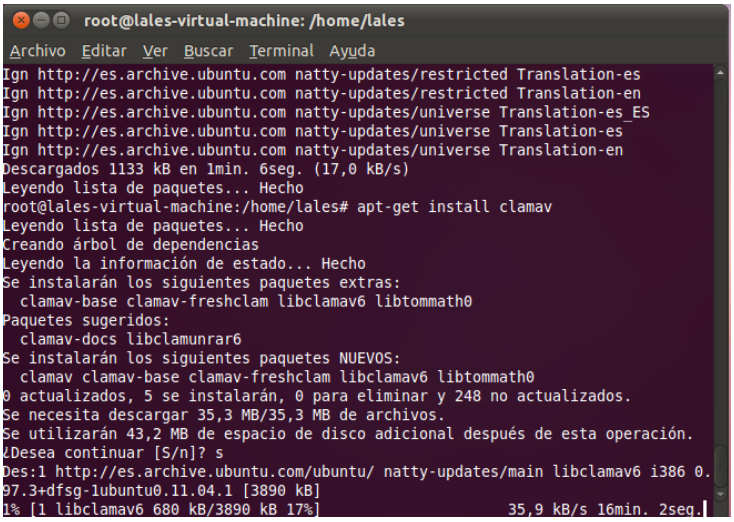
MARÍA ÁNGELES PEÑASCO SÁNCHEZ – 2º ASIR- SAD- TEMA 2

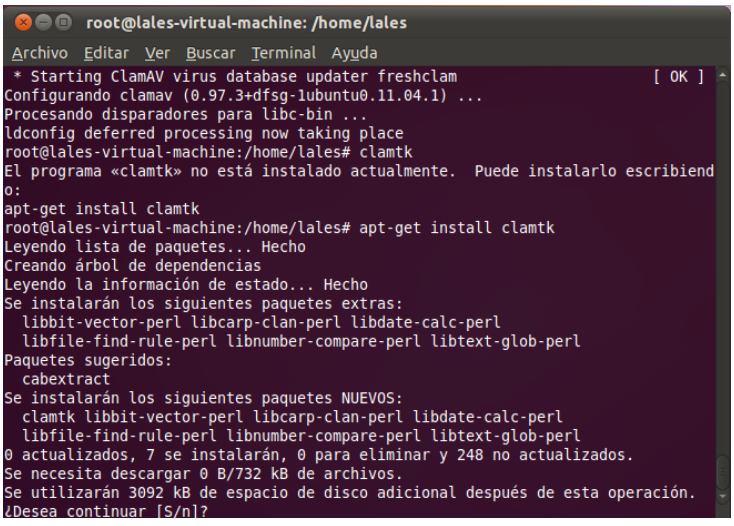
ATAQUES Y CONTRAMEDIDAS EN SISTEMAS PERSONALES:
HERRAMIENTAS PALIATIVAS

a) Instala en GNU/Linux el antivirus ClamAV, y su versión gráfica Clamtk.

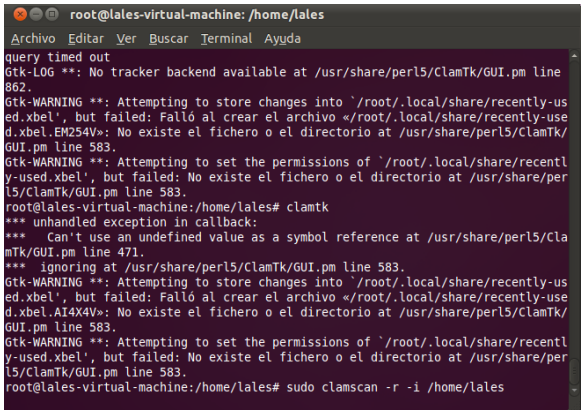
Sudo aptitude install ClamAV
Sudo aptitude install Clamtk
Escanear modo texto: sudo clamscan –r –i <directorio>
Escanear modo gráfico: sudo clamtk

En primer lugar vamos a instalar con apt-get install ClamAV

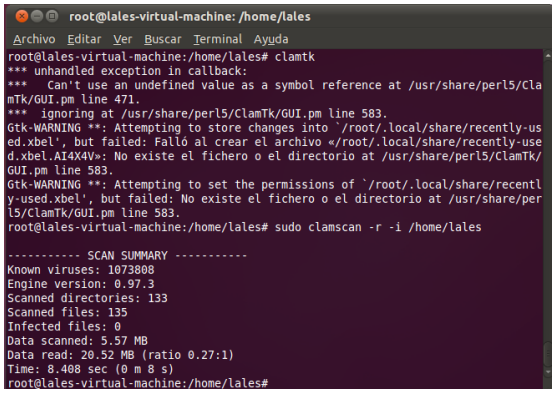




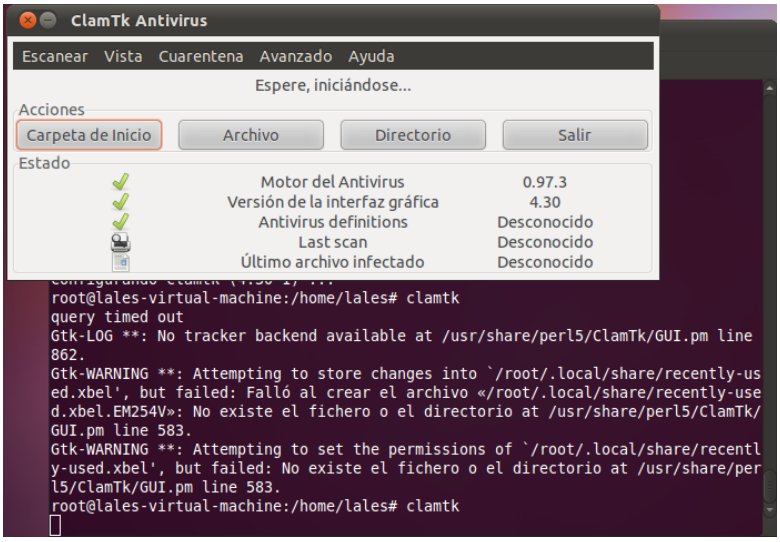
Una vez instalado vamos a probar que nos haga un escáner de /home/lales, para ello ponemos en modo comando sudo clamscan –r –i /home/lales



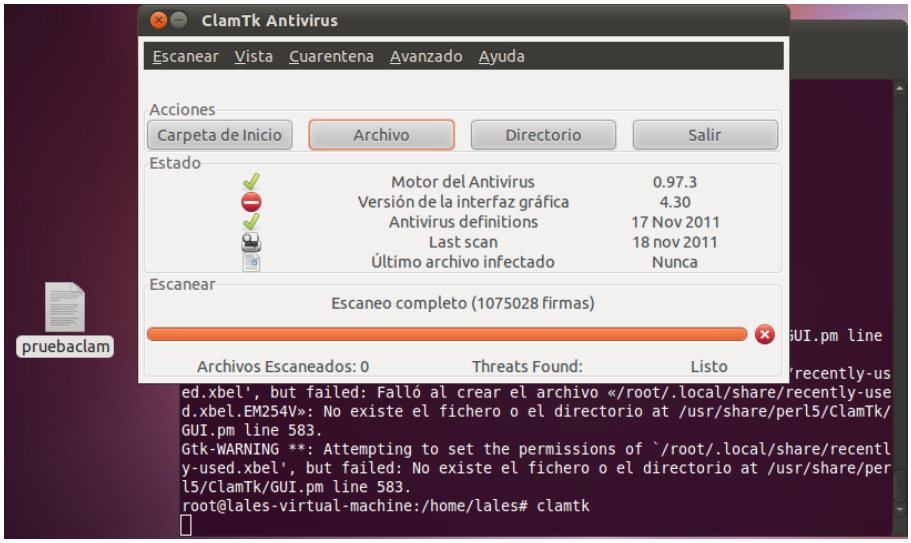
El resultado nos lo da con un resumen de lo que ha escaneado, tiempo y directorios y archivos que ha escaneado



Para modo gráfico lo hacemos de la siguiente forma, ponemos Clamtk en modo comando y nos aparece una ventana como la que mostramos a continuación

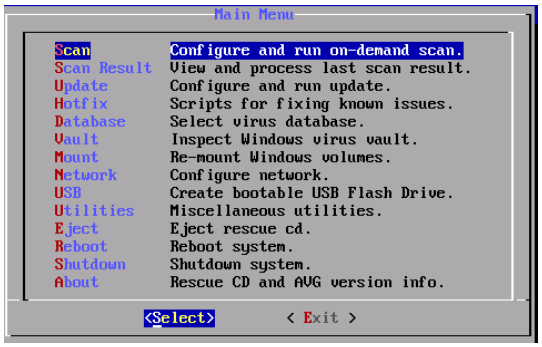


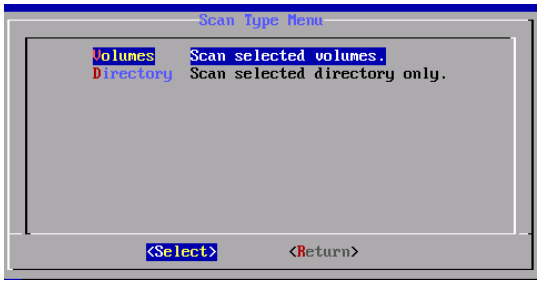
Elegimos un fichero que hemos creado en el directorio para que nos la escanee y nos da los resultados, si está infectado o no, en este caso no.



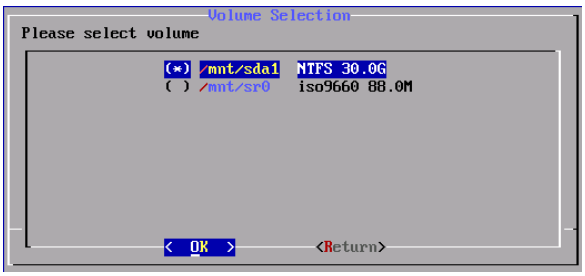
b) Instala y utiliza la herramienta de análisis antimalware Live AVG Rescue CD que se puede iniciar desde un CD o flash USB. Documenta dicho proceso.

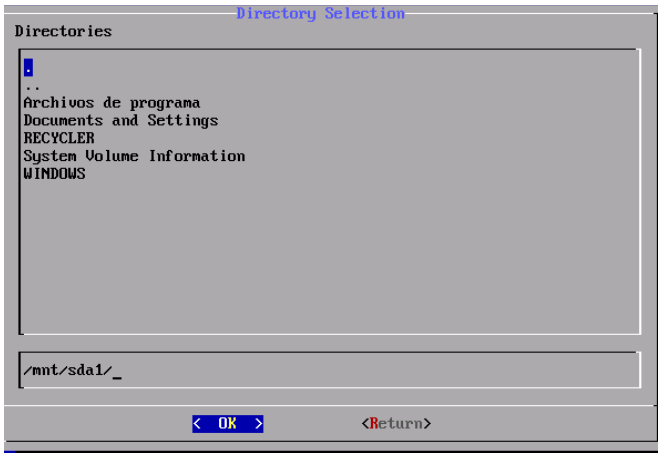
Vamos a arrancar nuestro ordenador, en este caso la máquina virtual, desde un flash usb o cd, y le damos a Scan en el menú que nos aparece, para escanear un fichero o carpeta

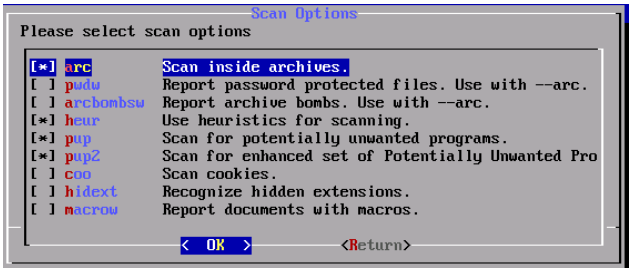


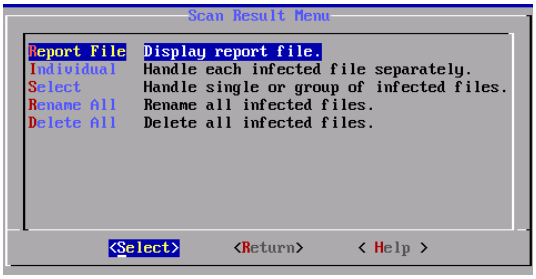


Una vez seleccionado el directorio que nos va a analizar, empieza el análisis

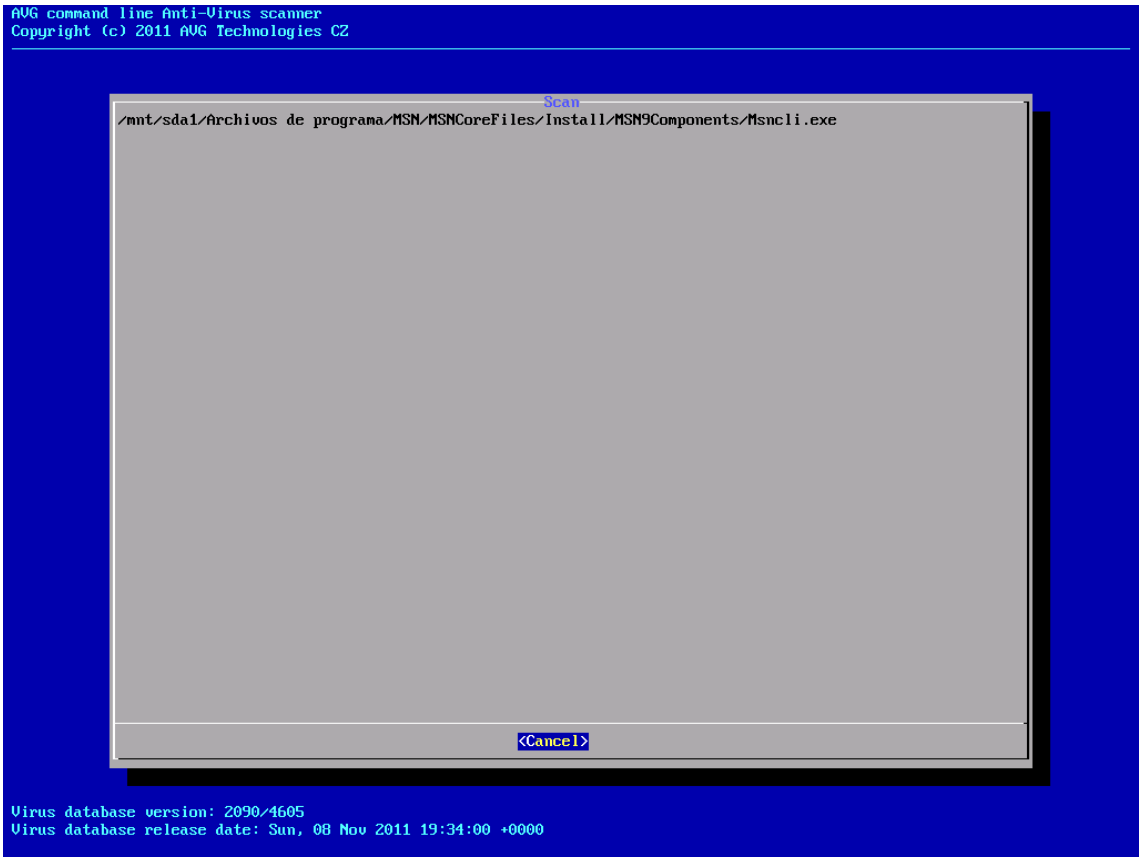




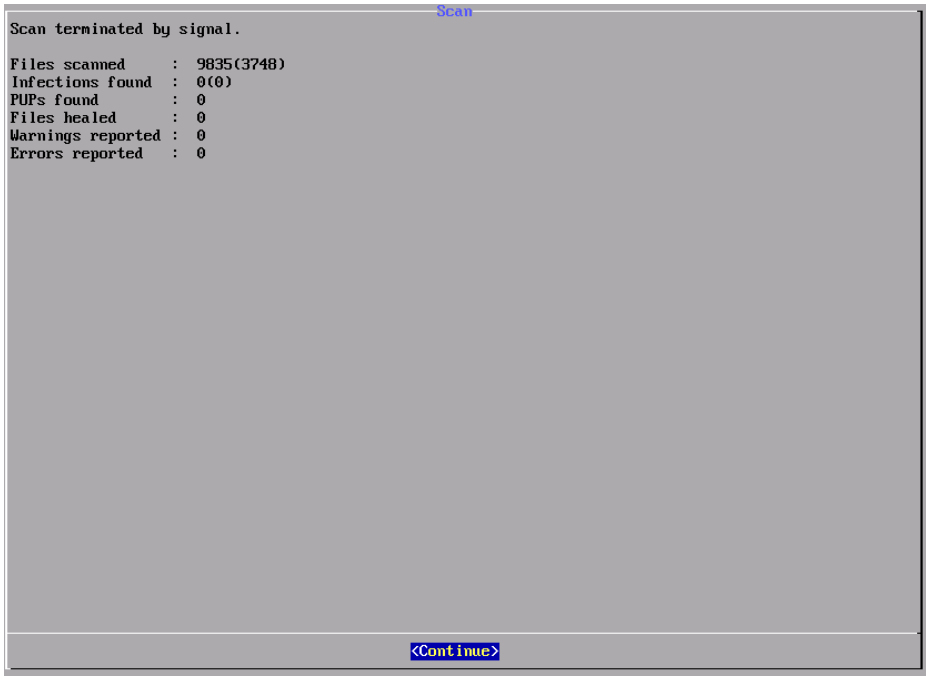




Una vez hecho el análisis nos da la información del archivo escaneado



Y vemos que no hemos tenido ningún problema al respecto

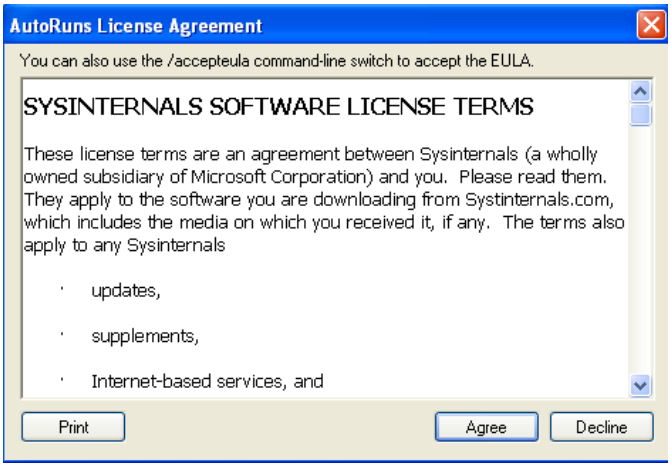


c) **En tu ordenador, realiza un análisis antimalware a fondo** (**msconfig**, procesos dudosos ejecutándose,…etc) mediante el **software de Microsoft:** suite **Sysinternals**. Indica en un documento todas las acciones que has realizado. Utiliza entre otros: **Autoruns** y **Process Explorer**

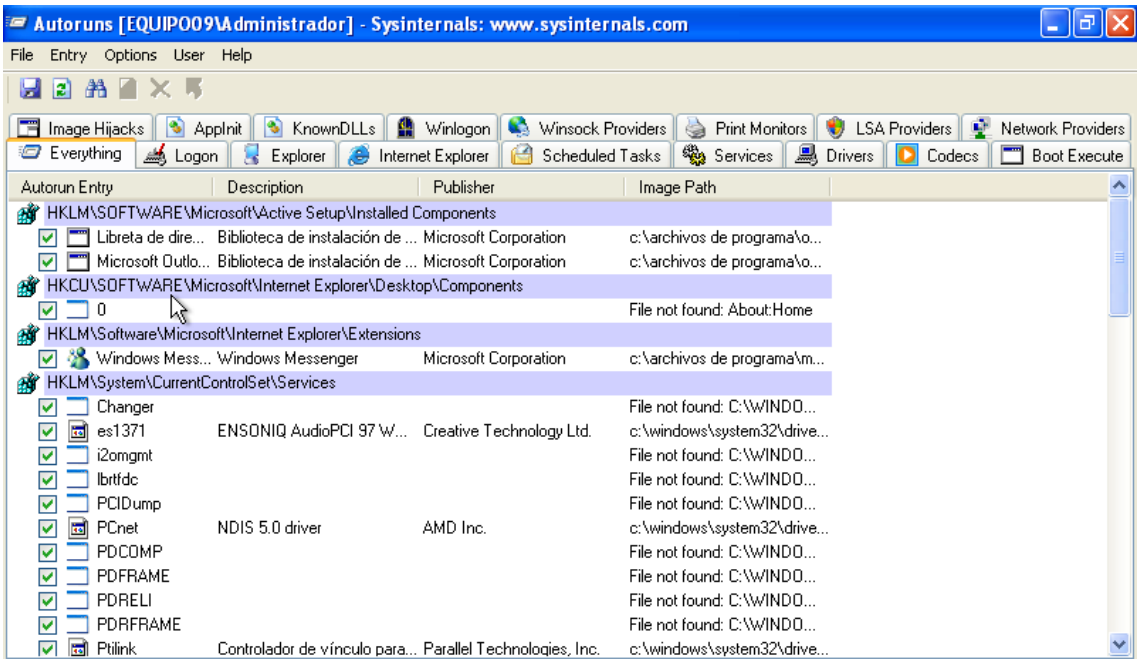
http://technet.microsoft.com/es-es/sysinternals/bb545021

Autoruns

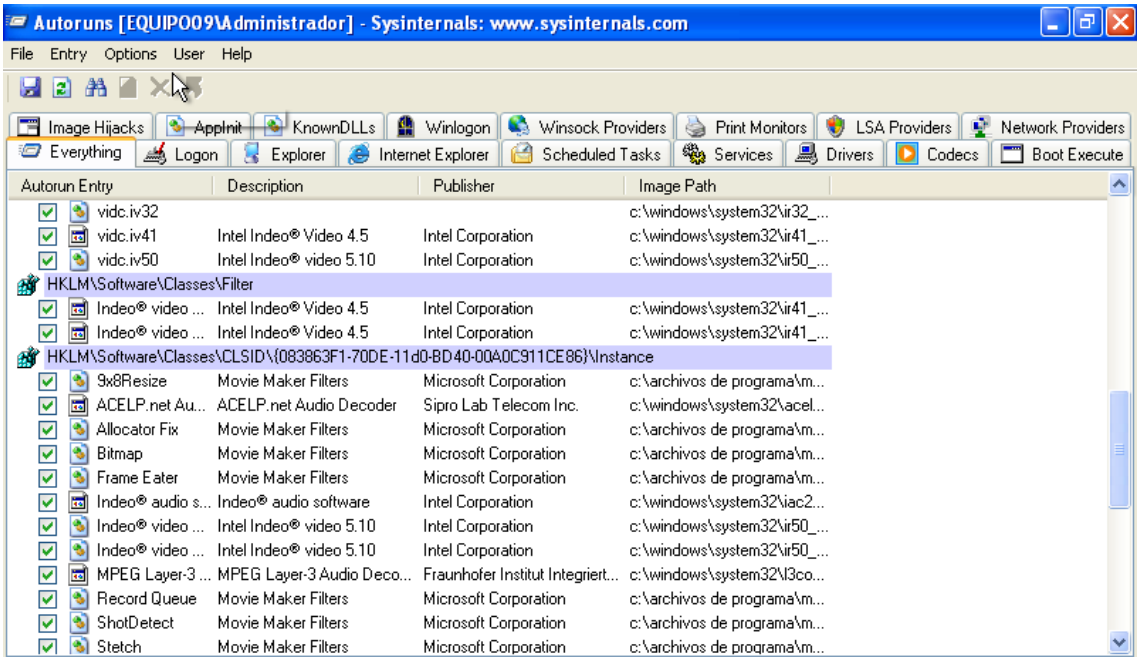
Nos descargamos Autoruns del enlace que tenemos arriba



Una vez ejecutado, nos va a hacer un análisis de todos los procesos que tenemos abiertos en el equipo



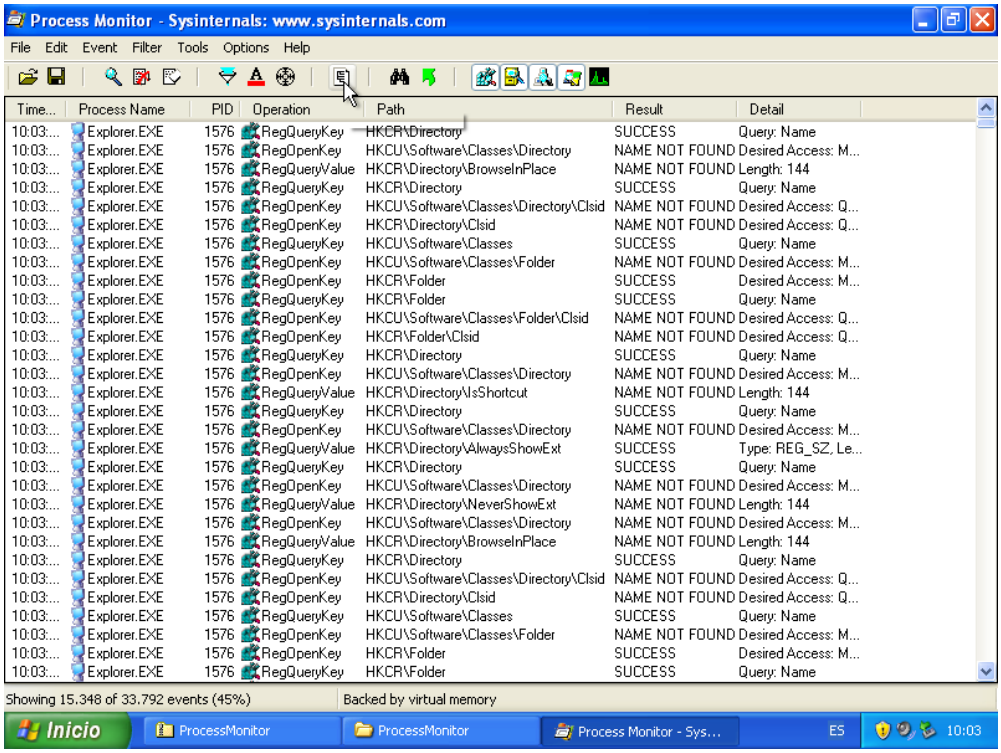
Y nos muestra si en las pestañas, proceso por proceso o en una general de todo el equipo

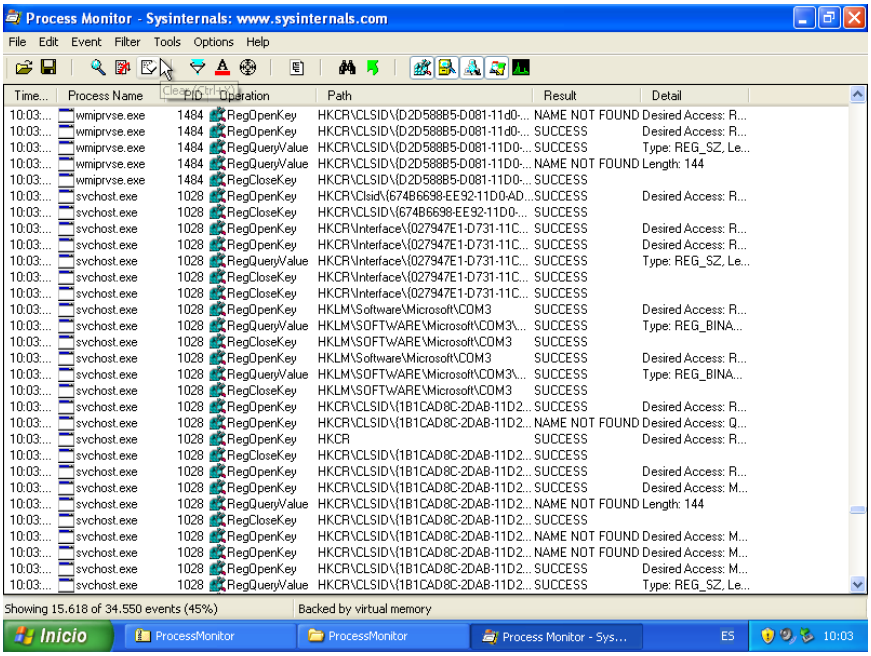


Process monitor

Hacemos lo mismo con Process monitor

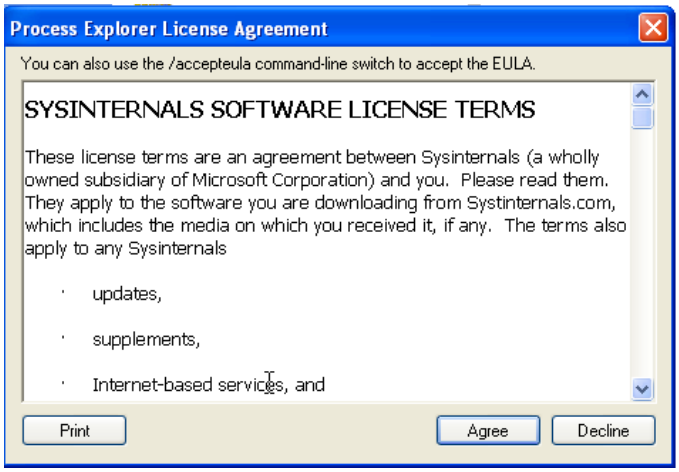
Aquí nos muestra el análisis que hace y la hora de todos los procesos que tenemos abiertos y nos da el resultado

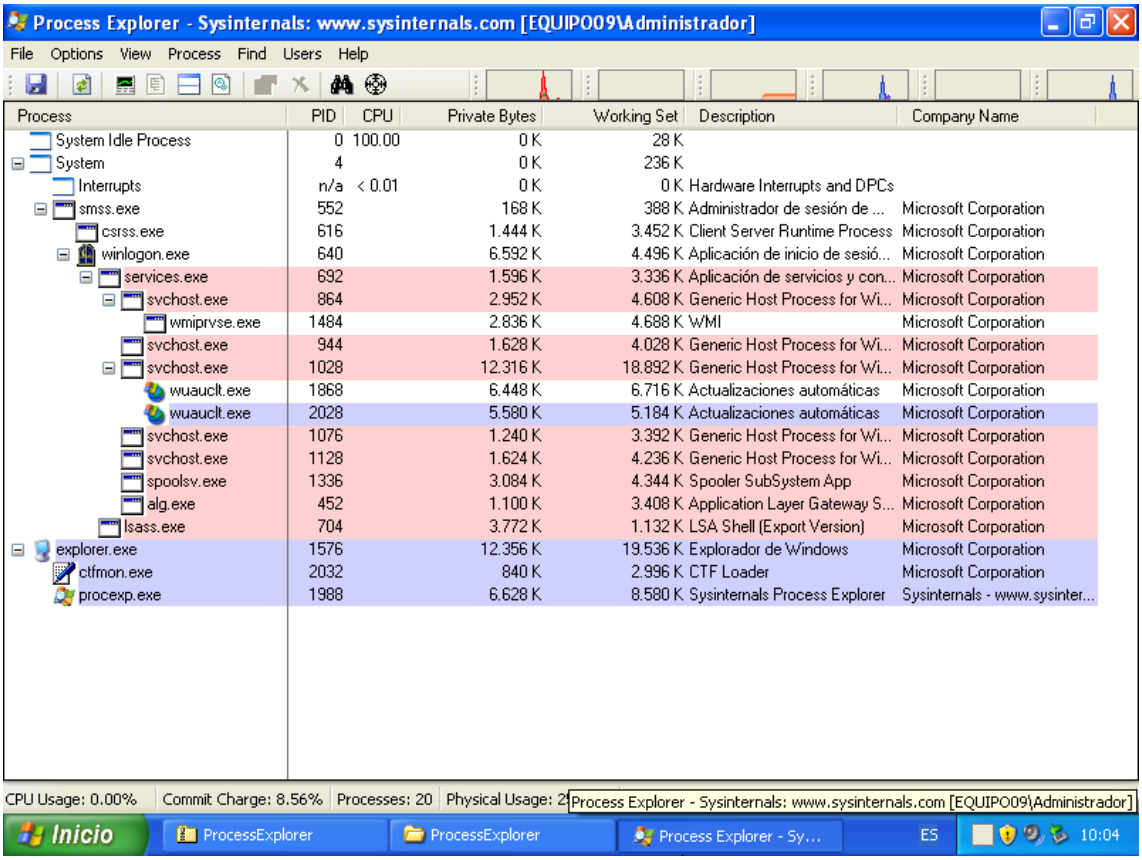


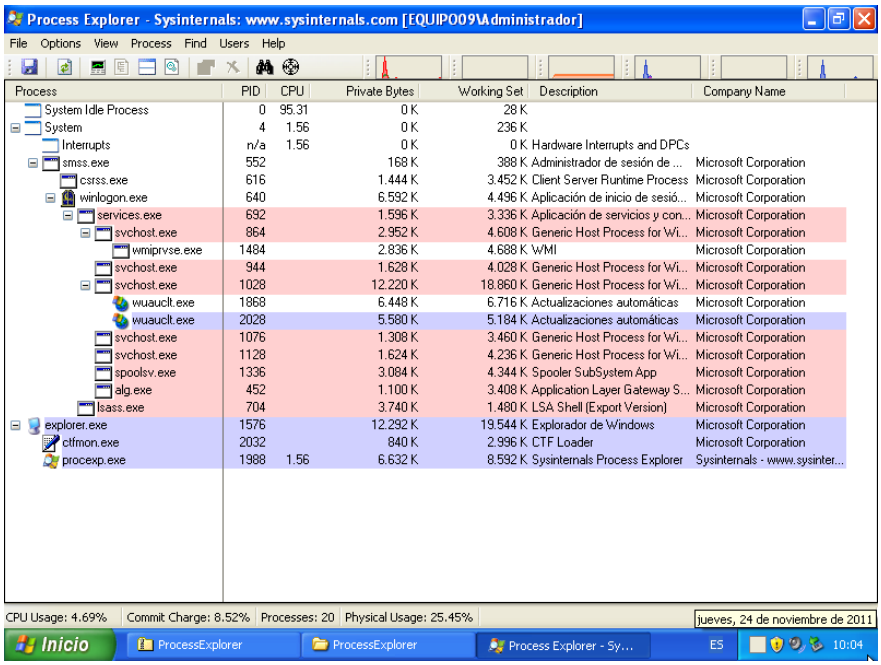


Process Explorer

Con Process Explorer, lo descargamos y vemos como nos analiza el equipo y nos muestra si tenemos algo sospechoso



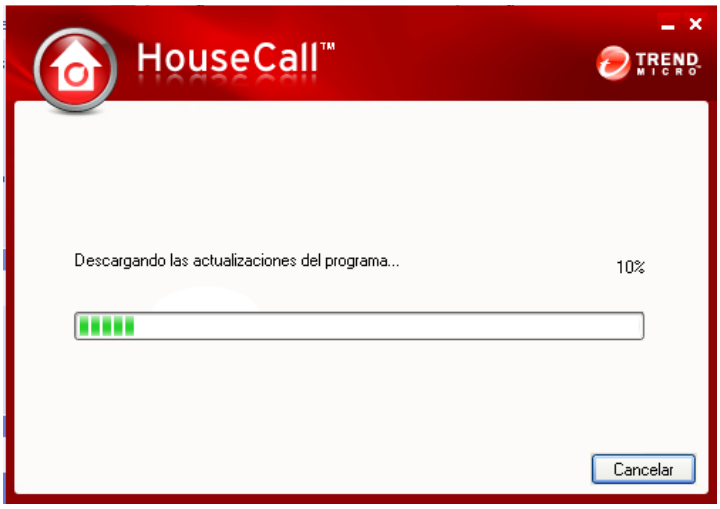




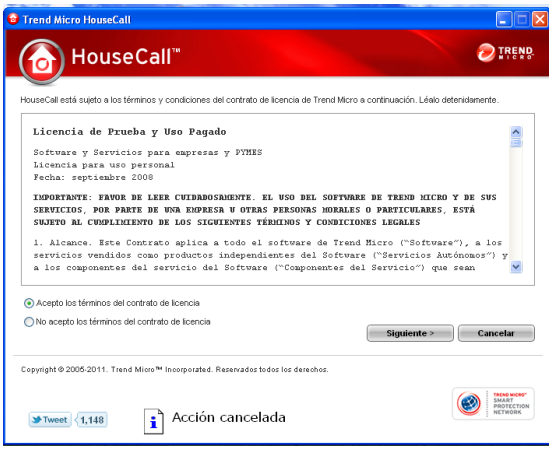
d) En tu ordenador, realiza un **análisis antimalware a fondo,** utilizando las herramientas gratuitas de **Trend Micro USA.** Documento dicho proceso. **Utiliza las herramientas: HouseCall, Browser Guard 2011, HiJackThis y RUBotted,** **http://es.trendmicro.com/es/products/personal/free-tools-and-services/**

HOUSE CALL

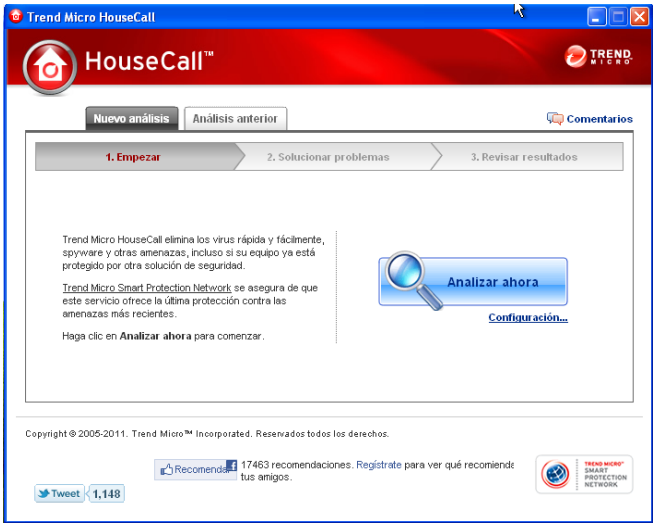
Vamos a instalar House Call, para ello nos lo descargamos de la página que nos muestra arriba



Aceptamos los términos del contrato de licencia



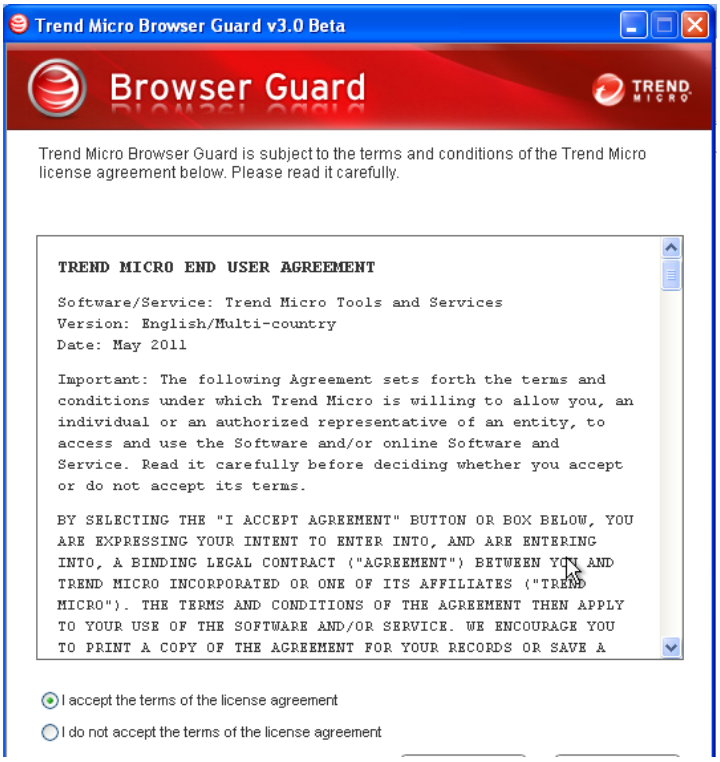
Y después de una instalación sencilla, empezamos el análisis del equipo, dándole a Analizar ahora



Después de un análisis rápido, vemos que no tenemos amenazas en el equipo

Browser Guard 2011

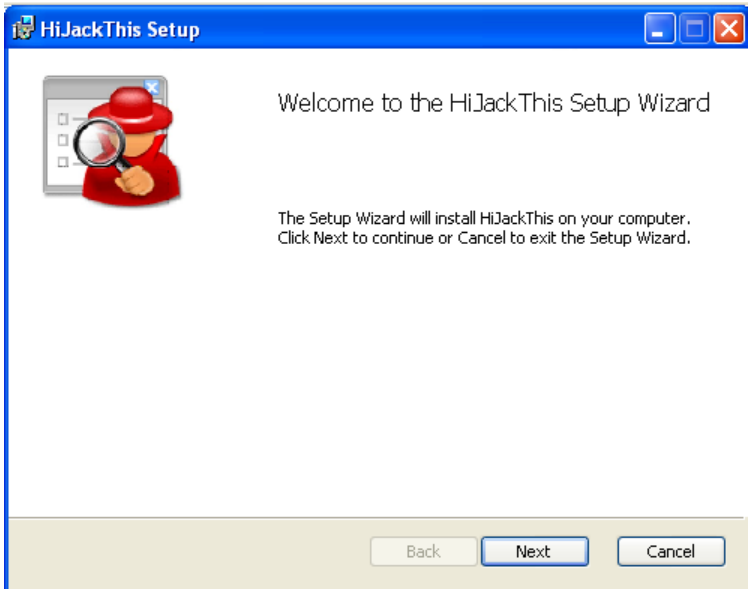
Hacemos lo mismo con Browser Guard 2011



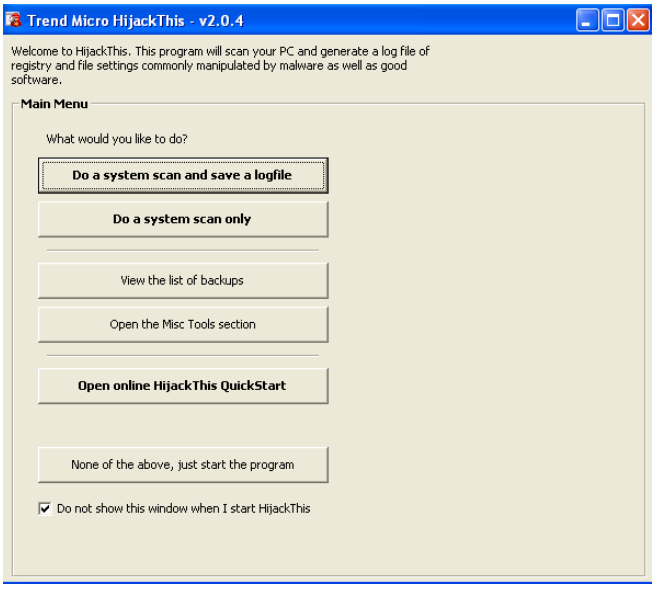
Este programa nos aparece instalado en la barra de herramientas del sistema operativo y únicamente nos avisa de alguna amenaza, y está siempre visible en la barra

HiJackThis

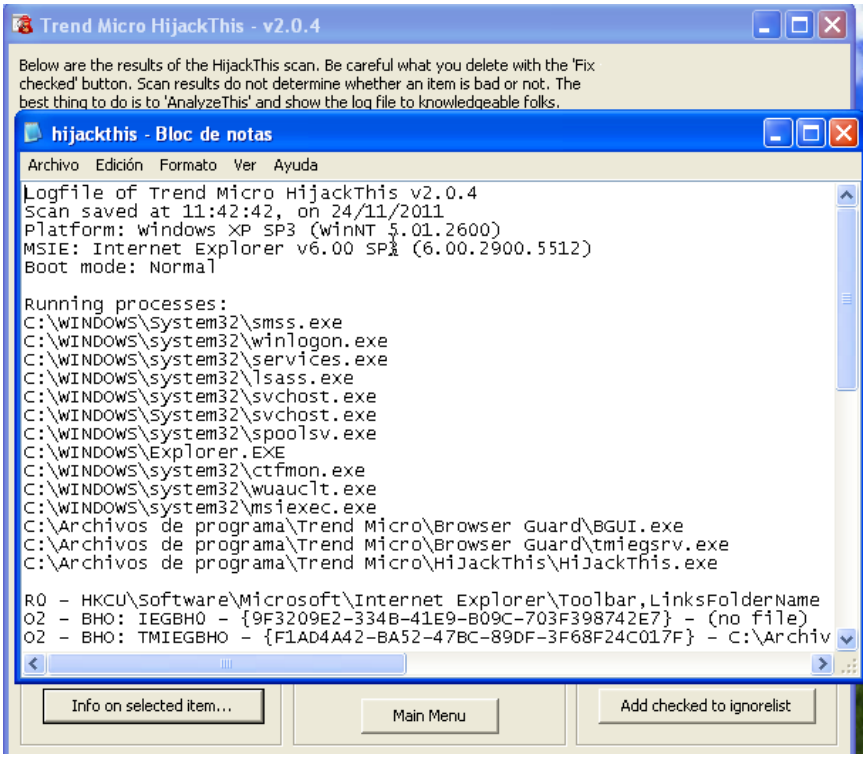
HiJackThis es otro antimalware para analizar el equipo, lo instalamos de manera sencilla



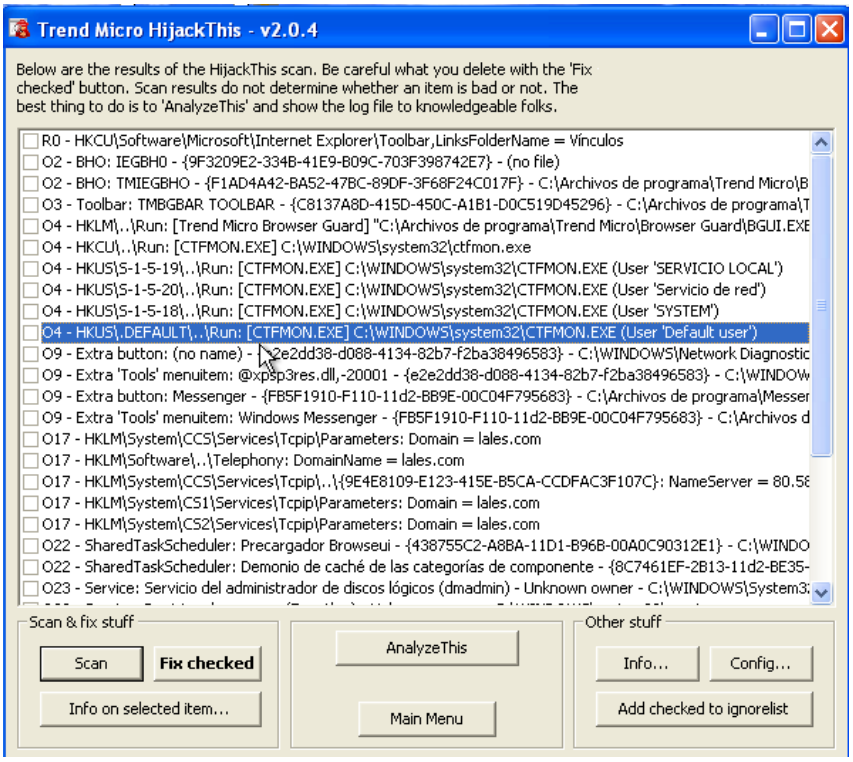
Después de la instalación, nos dice que queremos hacer, si escanear el sistema o también nos muestra el fichero donde se guarda ese escáner



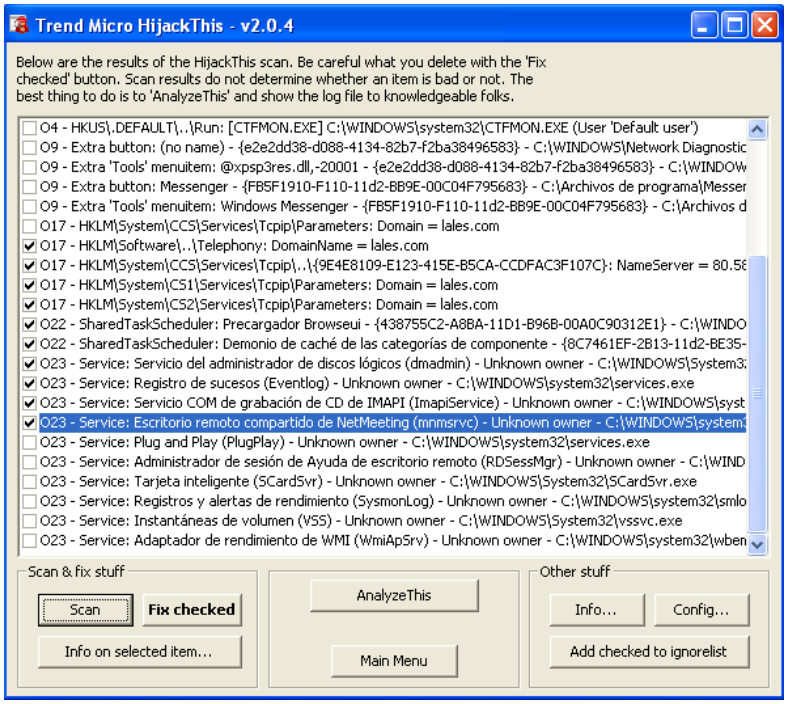
Aquí nos muestra el fichero en un bloc de notas y nos muestra todo el análisis



Nos muestra en el dominio en el que estamos, nos muestra lo que tenemos en ejecución y si encuentra algún fichero sospechoso

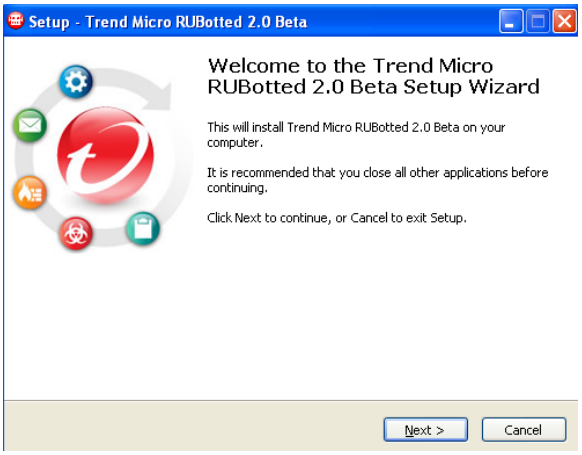


Elegimos lo que queremos escanear y le damos a Scan y empieza el análisis

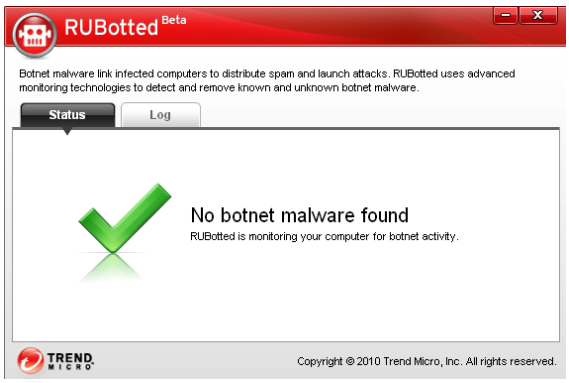


RUBotted

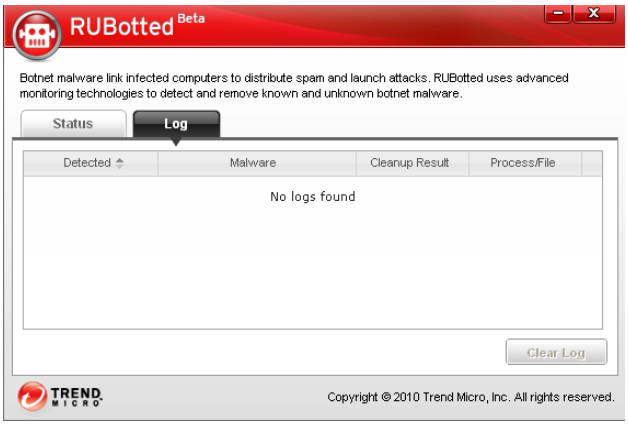
Instalamos Trend Micro RUBotted, otro antimalware para escanear el equipo



Aquí automáticamente en cuanto que lo instalamos nos hace el análisis, y en este caso nos da que todo es correcto



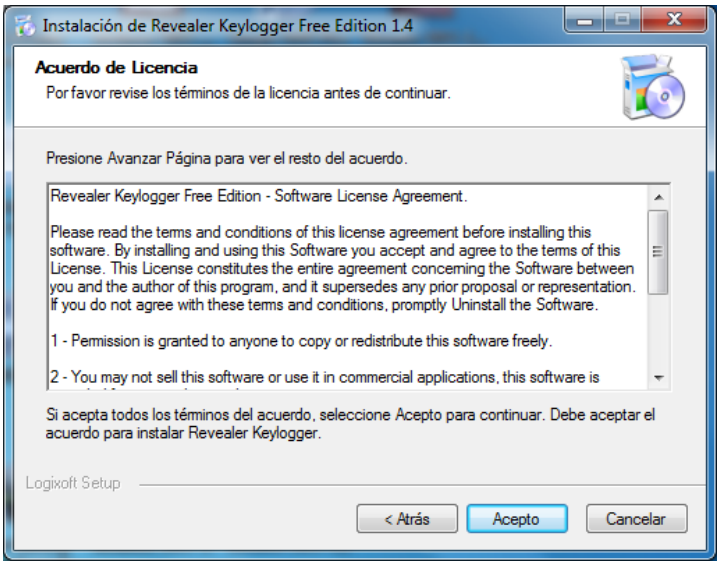
Y que no ha encontrado ningún archivo dañado o sospechoso



e) Instala y utiliza el **software de recuperación de pulsaciones de teclado denominado Revealer Keylogger.** Piensa como prevenir este software e informa en un documento. **Utiliza el software Malwarebyte para Windows. ¿Lo detecta?**

http://www.malwarebytes.org

Instalamos Revealer Keylogger

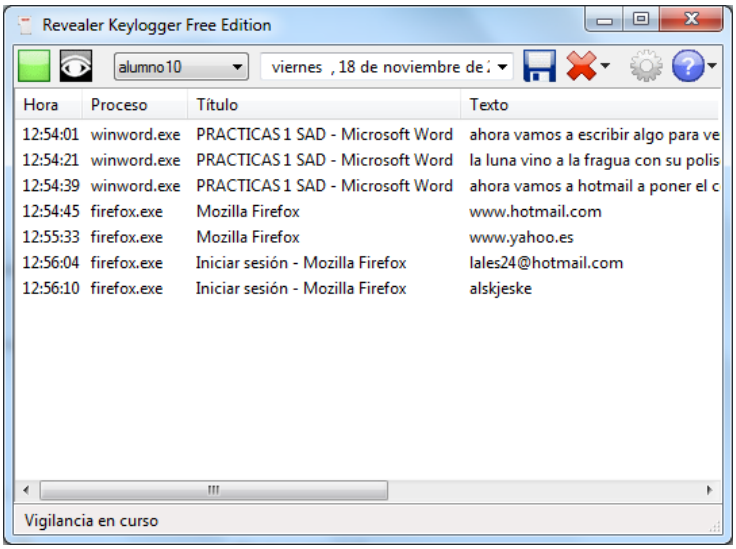


"Ahora vamos a escribir algo para ver como sale en el documento Keylogger

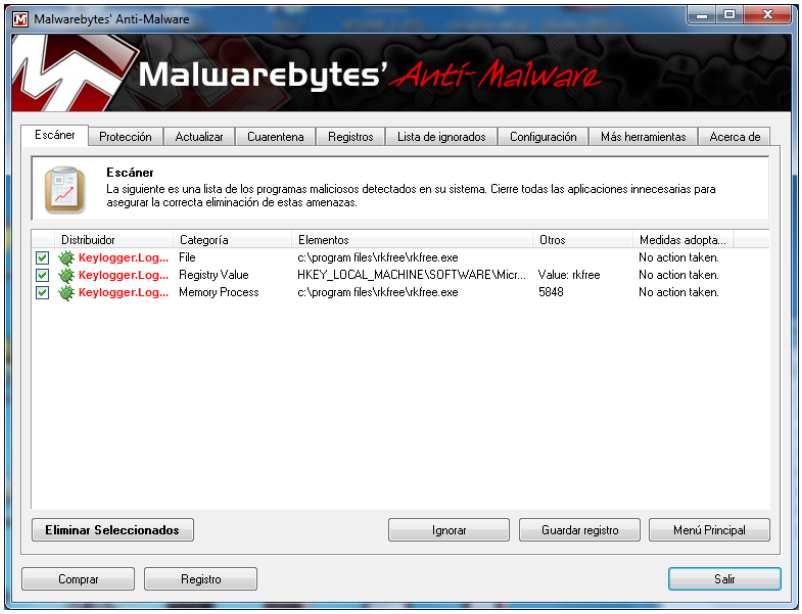
La luna vino a la fragua con su polisón de nardos, y ahora vamos a poner las contraseñas, mi contraseña es 123456123456

Ahora vamos a Hotmail a poner el correo"

Aquí vemos que todo lo que hemos ido escribiendo, nos ha salido en el programa



Ahora vamos a pasar el Antimalware para ver si nos detecta que tenemos instalado este programa para ver todo lo que se escribe por el teclado



Vemos que sí, que nos ha detectado el software, porque este tipo de programas, lo considera el antimalware como un software maligno o sospechoso

f) Investiga en Internet el término: **Hijacker**. Cómo puedes eliminar el **"Browser hijacker"**. ¿Qué efectos tiene sobre el sistema?

¿Qué es un hijacker?

El hijacker tiene como función el secuestrar nuestro navegador de internet. Esta acción es posible debido a que los programadores de este tipo de programas, aprovechan las vulnerabilidades de la máquina de Java dentro del Internet Explorer.

¿Cómo ocurre esto? Java, el lenguaje propiedad de Sun Microsystem tiene como particularidad el poder correr dentro de cualquier sistema operativo. Este hecho les permite a los programadores crear aplicaciones que puedan correr dentro de los sitios web, en donde ya no es necesario bajar plug-ing alguno.

Este hecho permite, por ejemplo, instalar pequeñas aplicaciones como puede ser un contador de visitas, un reloj, una calculadora e incluso una Tienda en línea.

Esta particularidad la han aprovechado distintos grupos de desarrolladores, no buen intencionados, quienes dentro del código de sus sitios, agregan instrucciones las cuales pueden modificar nuestra página de inicio, página de búsqueda entre otros elementos.

Aunque el secuestro del navegador sólo puede darse si se visitan las páginas de este tipo de personas, el riesgo comienza a crecer con el envío de correo electrónicos con temas engañosos, los cuales piden al usuario a cambio de instalar un programa de supuesta utilidad, entrar a estos sitios.

Algunos ejemplos de Hijacking

- IP hijacker: secuestro de una conexión TCP/IP por ejemplo durante una sesión Telnet permitiendo a un atacante inyectar comandos o realizar un DoS durante dicha sesión.
- Page hijacking: secuestro de página web. Hace referencia a las modificaciones que un atacante realiza sobre una página web, normalmente haciendo uso de algún bug de seguridad del servidor o de programación del sitio web, también es conocido como defacement o desfiguración.
- Reverse domain hijacking o Domain hijacking: secuestro de dominio
- Session hijacking: secuestro de sesión
- Browser hijacking: (Secuestro de navegadores en español). Se llama así al efecto de apropiación que realizan algunos spyware sobre el navegador web lanzando popups, modificando la página de inicio, modificando la página de búsqueda predeterminada etc. Es utilizado por un tipo de software malware el cual altera la configuración interna de los navegadores de internet de un ordenador. El término "secuestro" hace referencia a que estas modificaciones se hacen sin el permiso y el conocimiento del usuario. Algunos de éstos son fáciles de eliminar del sistema, mientras que otros son extremadamente complicados de eliminar y revertir sus cambios.

  La mayoría de los secuestradores de nuevo, no permitirá que un usuario cambie de nuevo a su página principal a través de Propiedades de Internet. La configuración de los secuestradores modernos "muy probablemente devuelvan en el arranque, sin embargo, el software antispyware actualizado bien es probable que retire el secuestrador. Algunos escáneres de spyware tiene una página del navegador restaurar la función de configurar su página de volver a la normalidad o que le avise cuando su página del navegador ha cambiado.

- Home Page Browser hijacking: secuestro de la página de inicio del navegador. Esto sucede cuando la página de inicio, en la que navegamos es cambiada por otra a interés del secuestrador. Generalmente son páginas en las que nos invita a usar los servicios de la página para que nuestro equipo esté seguro y funcione correctamente. No cabe decir que es a cambio de un pago y que el origen del error y mal funcionamiento del equipo es debido a nuestro secuestrador.
- Modem hijacking: secuestro del Modem. Esta expresión es en ocasiones utilizada para referirse a la estafa de los famosos dialers que tanta guerra dieron en su día (antes del auge del ADSL) y que configuran sin el consentimiento del usuario nuevas conexiones a números de cobro extraordinario.
- Thread hijacking: secuestro de un "tema" dentro de un foro de discusión de internet. Este término hace referencia a la situación que ocurre cuando dentro de un tema de discusión en un foro alguien intenta dirigir el hilo de la conversación hacia asuntos que no tienen nada que ver con el tema inicial. Esto puede realizarse de manera intencionada para irritar al autor del tema o bien producirse de manera natural y no intencionada generalmente por usuarios sin mucho conocimiento en el asunto a tratar o que desconocen la dinámica de comportamiento de los foros.

g) Busca información sobre el fichero **autorun.inf** que poseen los dispositivos de almacenamiento y cómo se camufla y opera malware a través de este archivo.
¿Cómo se propaga? ¿Qué efecto tiene?
¿A qué tipo de sistemas operativos afecta?
¿Qué medidas de seguridad puede tomar?
¿Qué es la desactivación de la ejecución automática?
¿Cómo se puede realizar?
¿Para qué sirve **USB Vaccine**?
¿Qué programa podemos utilizar para realizar la desinfección?

AUTORUN.INF

Junto con los ficheros Desktop.ini y thumbs.db para los usuarios de Windows, los Autorun.inf posiblemente sean de los ficheros que más se confunden con virus, no teniendo porqué ser así, ya que originalmente no son ningún virus (aunque en ellos se puedan camuflar), sino todo lo contrario, ficheros necesarios para el sistema operativo.

¿Qué es?

Normalmente, los ficheros AUTORUN.INF no son archivos maliciosos, y simplemente contienen información de los programas que pueden ejecutarse automáticamente cuando un dispositivo de almacenamiento extraíble (memorias USB, DVD, etc), son insertados en el ordenador.

Localización: son fácilmente identificables, ya que para funcionar de forma correcta deben de estar situados en el directorio raíz como un fichero de texto con el nombre Autorun.inf, en el que se incluye una serie de parámetros que indican al sistema operativo qué programa debe arrancar al insertar el CD/DVD/USB en la unidad, el icono que debe mostrar, etc.

Funcionamiento: para crear o ver el contenido de este tipo de ficheros simplemente necesitarás abrirlos con un editor de texto sencillo como puede ser el bloc de notas de Windows. Todo fichero tendrá un aspecto similar al siguiente:

Opciones de los parámetros

- Icon: permite establecer un icono al medio extraíble, el cual es visible en el Explorador de Windows y en Mi PC.
- Open: abre una aplicación o archivo ejecutable guardado en el medio extraíble. Se utiliza principalmente para iniciar la instalación de un programa de forma automática.
- Label: etiqueta que sustituirá al nombre del medio extraíble.
- Shellexecute: pensado para abrir ficheros que no son aplicaciones ejecutables y por lo tanto no se pueden ejecutar directamente (como por ejemplo: una página web o un documento PDF).

- Shell\verb: agrega opciones al menú contextual del medio extraíble, accesible desde el explorador de Windows (clic derecho).
- UseAutoPlay: especifica al sistema operativo si debe hacer caso (valor 1) o no (valor 0), de la información de auto ejecución (autorun.ini) contenida en el medio extraíble.

Virus en autorun.inf

Actualmente los virus en Autorun.inf se aprovechan de las características de ejecución automática del fichero autorun.inf en: CD, DVD o memorias USB incluyendo una gran cantidad de dispositivos como son los reproductores MP3. IKill es un antivirus específico que elimina los virus en ficheros Autorun.inf. Además iKill incluye: un gestor de procesos y servicios (similar al administrador de tareas de Windows) y un panel de herramientas con las cuales iKill activa o desactiva el acceso al: editor de registro, administrador de tareas, las opciones de carpeta, ocultación de ficheros, desactivación de los ficheros autorun.inf y reinicio del Explorer o reinicio completo del ordenador.

USB VACCINE

Panda USB Vaccine es una utilidad de seguridad gratuita desarrollada por Panda Security, que con sólo un par de clics nos permitirá bloquear el auto-arranque de las memorias USB (Pendrives, memorias flash, etc.) que se inserten en nuestro sistema, evitando así el contagio de los Malware del tipo Gusano que se aprovechan de esta funcionalidad.

La cantidad de virus que se aprovechan de la función de auto-arranque de Windows para infectar nuestros sistemas mediante unidades extraíbles como llaves de memoria, reproductores MP3, cámaras de fotos, etc, ha estado creciendo mucho últimamente como por ejemplo el famoso Conficker.

Además de la 'vacuna' para el sistema, Panda USB Vaccine nos permite también 'vacunar' memorias USB de forma individual, deshabilitando el auto-arranque y evitando que se creen nuevos ficheros de esta naturaleza.

Una característica bastante llamativa es la sencillez con la que la información es mostrada, ya que hace que cualquiera pueda manejar le herramienta sin conocimientos técnicos avanzados.