**Guía de instalación para keylogger**

Keylooger, es una aplicación desarrollada por Andessy compañía que presta servicios de tecnología a otras empresas basando sus productos en el uso de Amazon web services (AWS), inicialmente la función de la aplicación es capturar todos los movimientos que el usuario haga durante el día, así mismo como los clics que realice en este periodo de tiempo, para luego ser montados en una base de datos, con el fin de determinar factores importantes para la compañía Aircraft Digital, como la productividad y eficiencia de cada uno de los usuarios, durante el día. Sin embargo la aplicación también puede cumplir con muchos más propósitos en un futuro, luego de realizar un poco más de desarrollo tecnológico sobre esta herramienta, como lo son aportar datos importantes y de gran relevancia para la obtención de los indicadores de rendimiento claves de cada usuario (KPIs), para la identificación de patrones consecutivos que se den durante la operación diaria y de esta forma poder desarrollar una automatización de estos procesos, por medio del uso de inteligencia artificial y machine learning, además de tener la capacidad para adaptarse y poder realizar un reconocimiento óptico de caracteres con el fin de poder llevar a cabo tareas repetitivas de forma mas eficiente sin que el usuario tenga que intervenir con el proceso y tener una mayor capacidad del personal calificado para tareas que demanden de mayor complejidad.

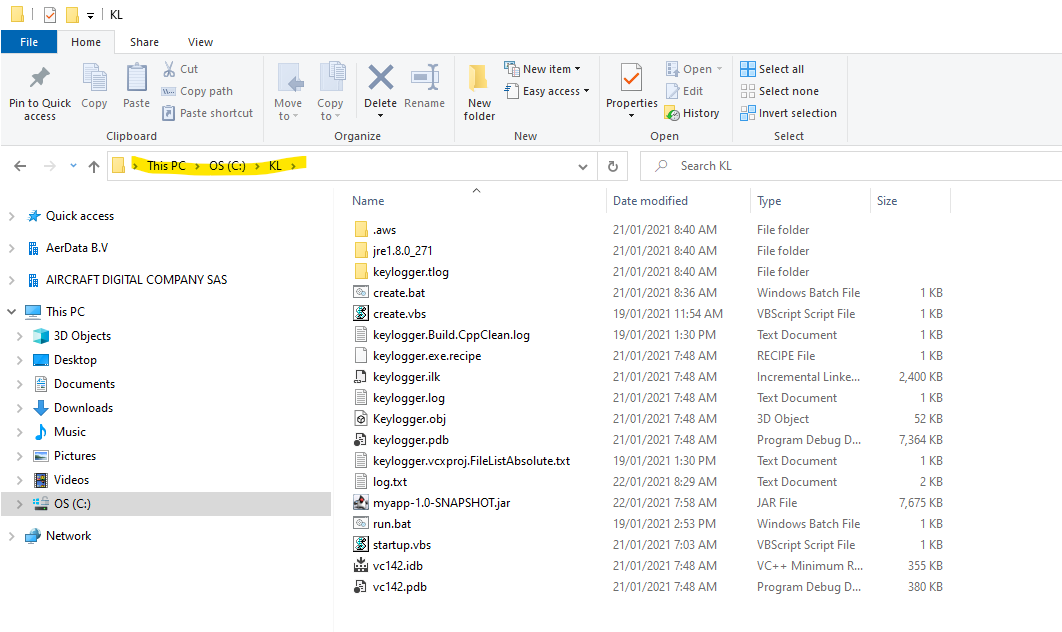
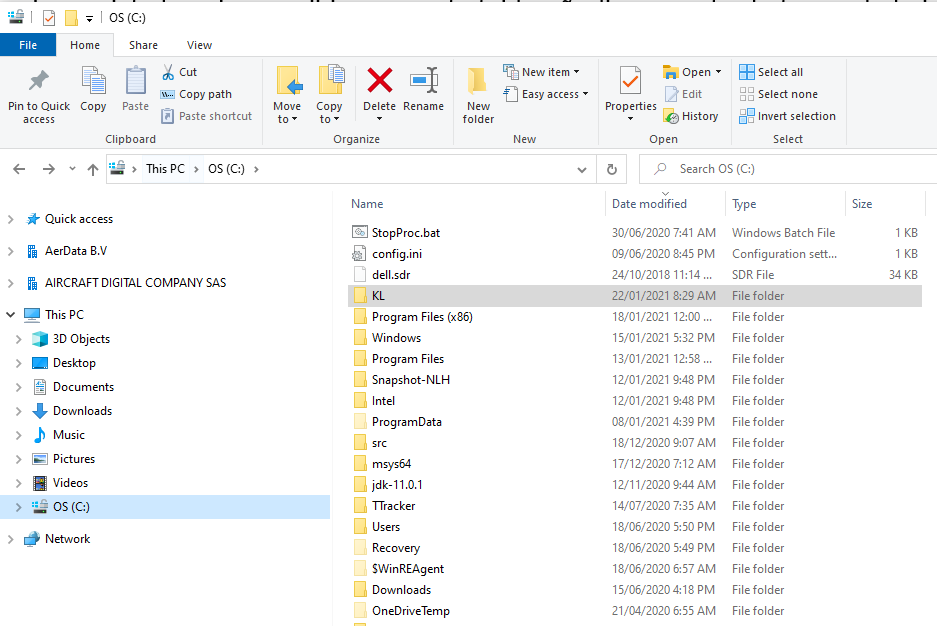
Así pues, el keylogger fue desarrollado en C++ ya que este es el lenguaje mas cercano al lenguaje de la computadora, ya que de esta forma va ser más fácil extraer las pulsaciones hechas por el usuario y que quedan registradas en el computador. La base de datos destinada para este proceso es DynamoDB, una base de datos no relacional (NoSQL) con el fin de almacenar grandes cantidades de datos y con distinto tipo de información lo que permitirá una mayor flexibilidad en la adición de datos importantes, además que es parte del paquete de Amazon web services, compañía con la cual Andessy presta sus servicios. El código de la aplicación se divide en dos, uno encargado de capturar los eventos del teclado y ratón, desarrollado en C++, el segundo se encarga de tomar los datos y montarlos en la base de datos, desarrollado en java.

Para el funcionamiento del código que captura los eventos se creó un archivo llamado “keylogger.cpp” el cual crear un archivo llamado “log.txt” en la carpeta de la aplicación en el cual se escriben todos los eventos capturados, dentro de lo que se escribe por cada evento se encuentra la tecla, en código ASCII el cual nos devuelve un numero al cual pertenece ese carácter bajo esa norma, el nombre del usuario registrado para la computadora, es decir el nombre local del usuario, el timestamp el cual es un numero que nos proporciona la fecha y hora en la cual se hizo la entrada, y una constante “uuid” con la cual obtendremos mas adelante el identificador único de la entrada. Una vez en el archivo “log.txt” llega a las 5000 líneas, o en el código se alcanza el loop número 5000, el código en c++ llama al archivo run.bat, el cual es un archivo montado como parte de un proceso en el fondo, de forma tal que el usuario no pueda ver lo que esta sucediendo y no sea una molestia en el momento de estar trabajando. El archivo “run.bat” ejecuta en una ventana de comando el archivo ejecutable obtenido en java. Una vez terminado este proceso se reinicia el ciclo y se borran los datos del archivo de testo “log.txt”.

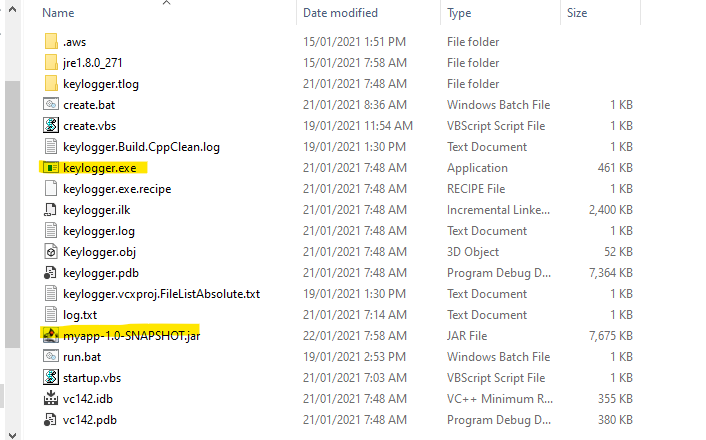
Por otra parte, se encuentra el código encargado de subir los archivos a la base de datos, este fue creado usando el IDE Intellij en el lenguaje java, el IDE es importante hacer uso de este ya que fue el único con el que se pudo ejecutar el código sin errores. Para realizar este código primero se den descargar las librerías de aws para poder conectar con la base de datos para realizar ese proceso se uso un SDK obtenido desde la pagina oficial de aws o en el siguiente link <https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-started.html> donde muestran el paso a paso de como configurar las librerías de Amazon para java, para este proceso es necesario configurar las credenciales de aws, para esto es necesario pedir los accesos al arquitecto de Andessy quien tiene acceso a todas estas funciones. Una vez montado el SDK de java el código consiste en crear una tabla llamada “keylogger” en caso de no existir, si ya existe la sobrescribirá, y a esta tabla añadir una entrada tomando la información del archivo “log.txt” el cual se encuentra en la misma carpeta de la aplicación, de este archivo toma cada una de las líneas y separa las palabras en cada línea lo que nos permitirá ubicar cada una de esas palabras en una variable diferente que necesitemos, y generar un ciclo para que complete esta misma acción para cada una de las líneas, y así poder montar cada línea como un registro independiente. Una vez completa el ciclo y sube cada una de las líneas del archivo el programa termina y se completa la actualización de la base de datos.

Para la instalación de la aplicación se necesita la carpeta “KL” la cual se puede encontrar dentro de los archivos del proyecto Andessy en su respectivo GitHub, para la solución ADC.

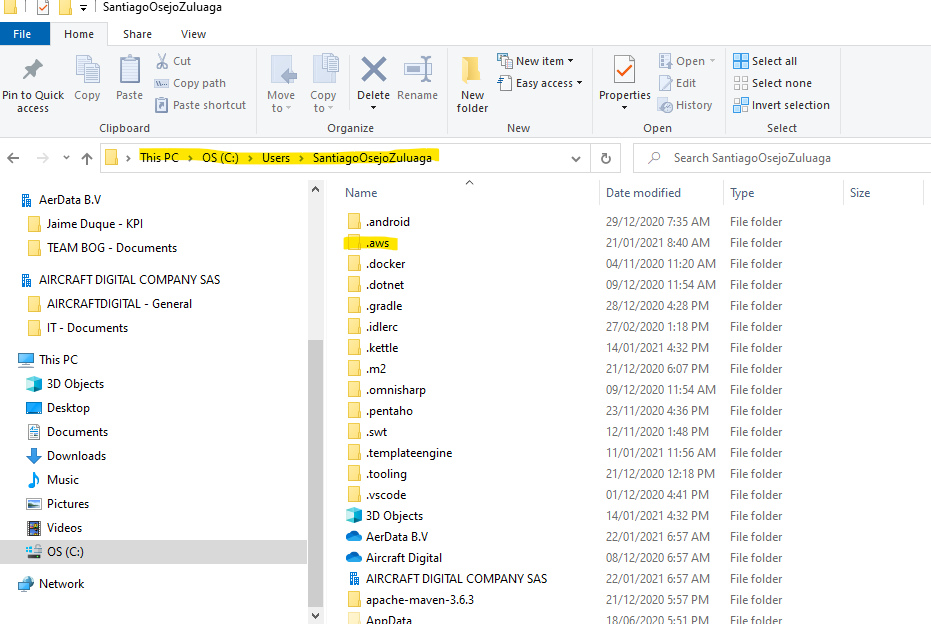
El primer paso para instalar el programa es descargar la carpeta en el computador que se desea instalar y copiar todos los archivos y carpetas que se encuentran allí y pegarlos en una carpeta, la cual se debe crear en el disco local C: con el nombre “KL”.



allí se encuentran los dos archivos ejecutables tanto el .exe del keylogger del programa escrito en c++ como el ejecutable .jar del programa escrito en java como se muestra a continuación



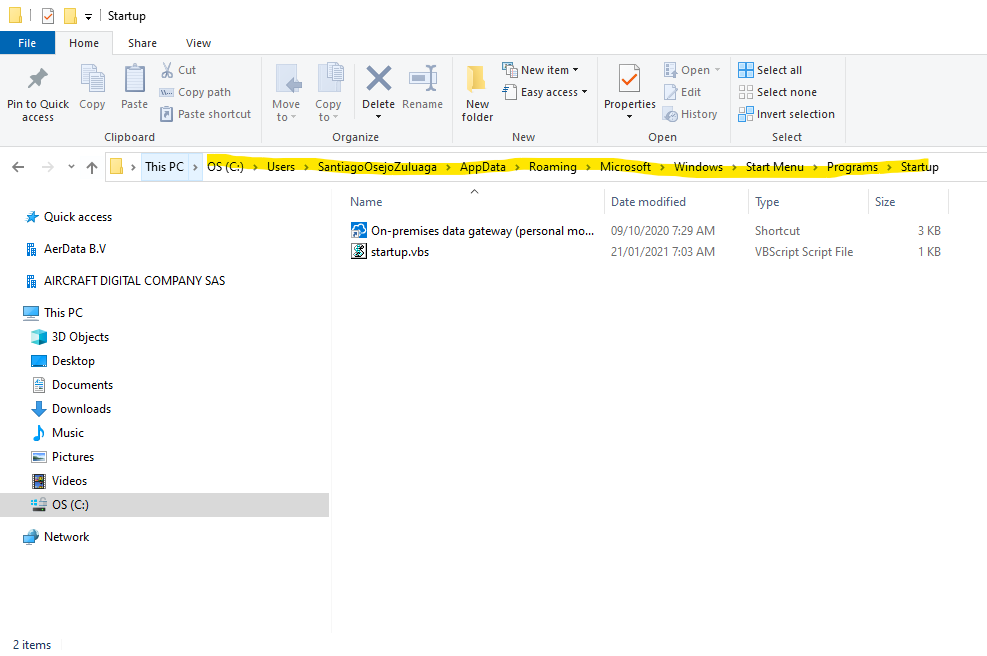
Además, se encuentra dos carpetas una es .aws, la cual debe ser instalada en la carpeta local del usuario del computador que se encuentra en el disco C, tal como se muestra a continuación.



Esto con el fin de que cada usuario tenga acceso a la cuenta de aws donde se van a montar los datos y donde esta la base de datos.

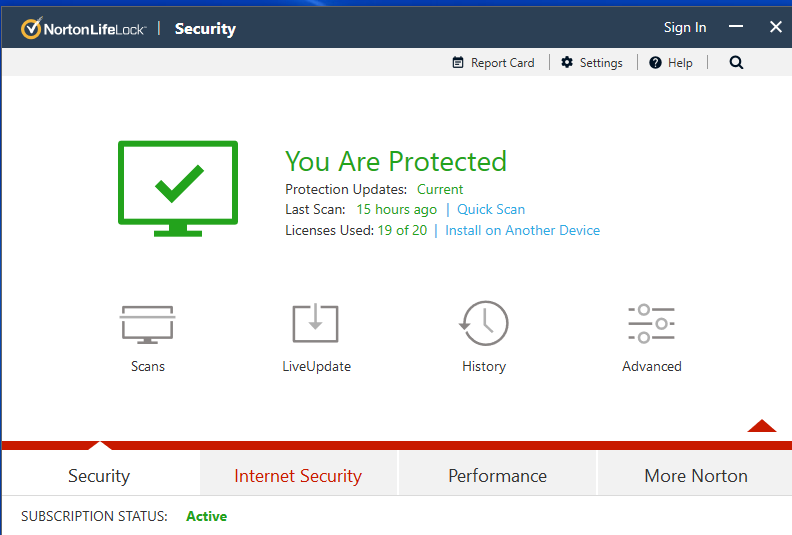
La otra carpeta se llama “jre1.8.0\_271” la cual contiene el ejecutable de java con el cual va a correr el .jar y la cual va a ser usada para que este código pueda funcionar, esta carpeta se debe dejar ahí.

Luego se debe copiar el archivo “startup.vbs” en la carpeta local de usuario startup, para llegar a dicha carpeta, dentro de las opciones del explorador de archivo bajo view, seleccionar la opción hidden ítems una vez hecho esto seguir la siguiente ruta, C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup, donde %USERNAME% hace referencia a el usuario local al que se le esta instalando el programa, una vez el archivo este en esta carpeta la aplicación iniciará automáticamente cuando se enciende el computador.

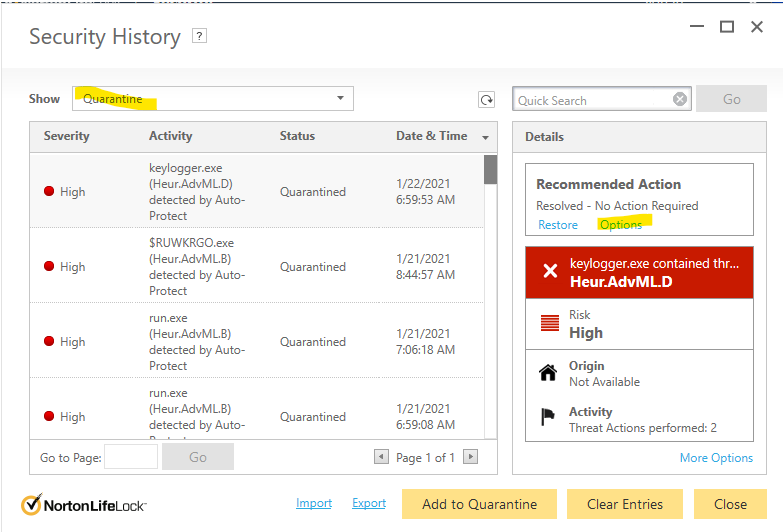


El ejecutable de keylogger inicia el archivo run.bat que se encuentra en la misma carpeta después de 5000 iteraciones o apenas la aplicación abre por lo que todo lo que se dejo de subir el día anterior se subirá a primera hora en la mañana. El .exe de la carpeta KL puede ser eliminada por el antivirus ya que es una aplicación que correo con el sistema operativo y de una fuente de desarrollo desconocida, para evitar que se elimine el ejecutable se debe realizar los siguientes pasos. Si el archivo ya fue eliminado por el antivirus se debe seguir los siguientes pasos, de lo contrario seguir a “Permisos del antivirus para .exe”

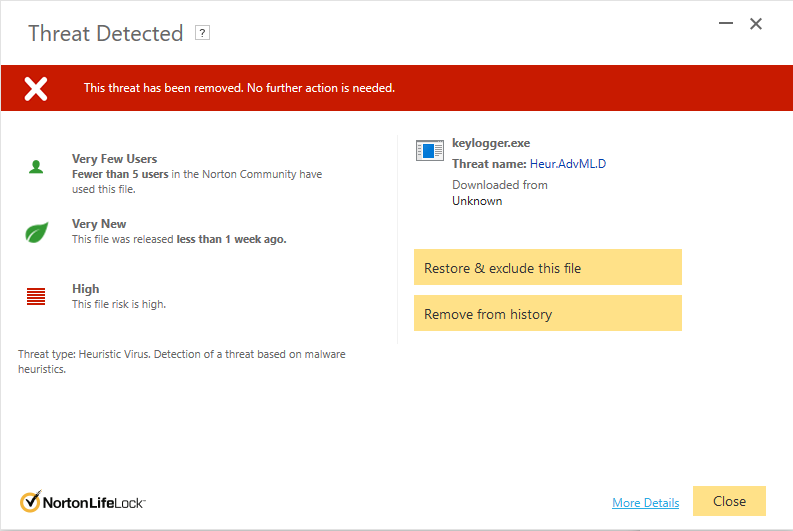
Se debe ingresar como admistrador, una vez en la sesión de administrador se va a la opción de “Security” y “History”.



Dentro del historial del antivirus se encuentra un menú desplegable en la parte superior del cual debemos elegir la opción de “Quarantine”, la cual nos mostrara los archivos borrados dentro de los cuales se debe encontrar el archivo de keylogger.exe lo seleccionamos y en el recuardo de la izquierda seleccionar “Options”.



Se desplegara una ventana emergente en la cual se debe seleccionar la opción de “Restore & exclude this file”, se aceptan los cambios y el archivo debe quedar restaurado en la carpeta KL.

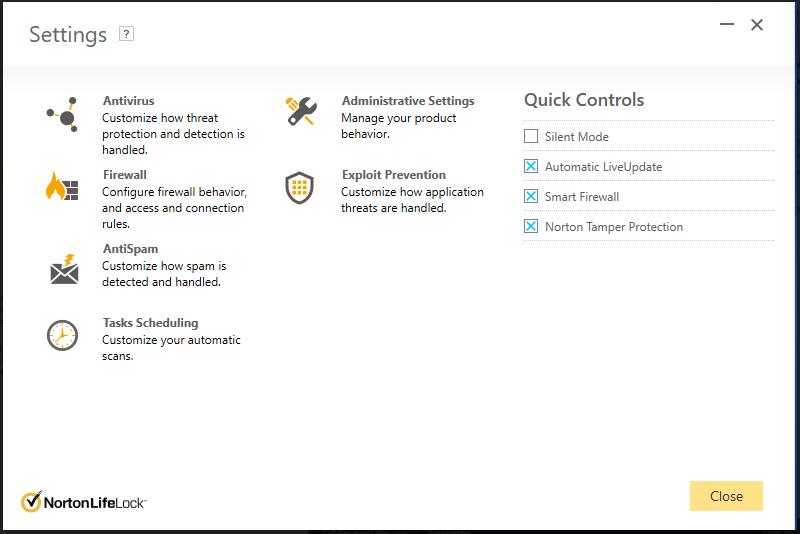


**Permisos del antivirus para .exe**

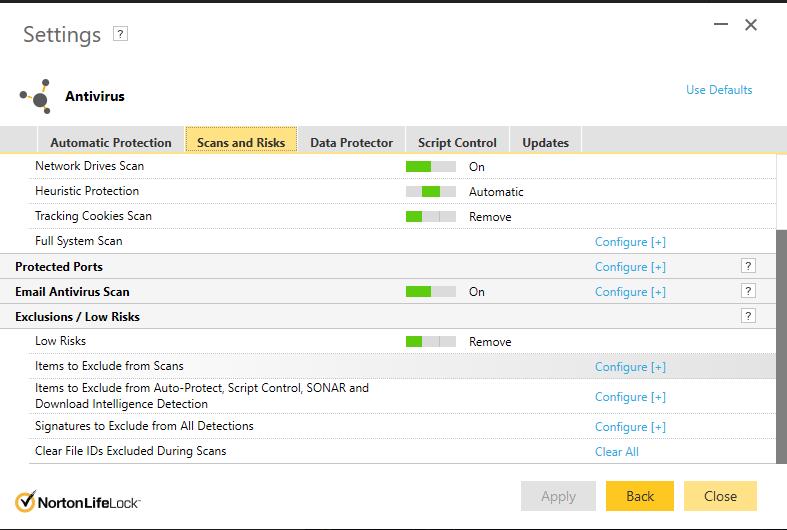
Una vez realizados los pasos anteriores para recuperar el archivo ejecutable que nos borró el antivirus se debe ingresar a la cuenta de administrador, donde se debe abrir la aplicación del antivirus, donde se debe seleccionar la opción de “settings” o “ajustes”.



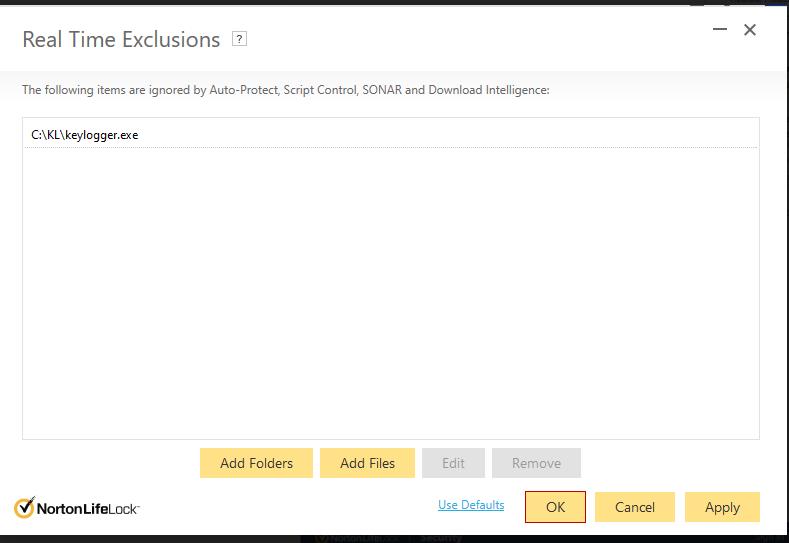
Se desplegará una ventana en la cual se debe elegir la opción “Antivirus”.



Al seleccionar la opción saldara una ventana emergente de la cual se debe elegir la ventana de “Scans and Risks”, luego buscar dentro de las opciones el subtítulo de “Exclusions/Low Risks” dentro de este menú se debe buscar la opción de “Items to Exclude from Auto-Protect, Script Control, SONAR and Download Intelligence Detection” y seleccionar “Configure [+]”.



De allí aparecerá una ventana en la cual se debe elegir “Add files” y escoger desde el navegador de archivo el archivo de keylogger.exe, es importante elegir el archivo ejecutable con extensión .exe ya que este es el que nos sirve para correr la aplicación, una vez hecho se esto se aceptan y aplican todos los cambios hechos en el antivirus.

****

Con esto concluye la instalación del programa, el cual se ejecutara automáticamente sin ningún problema.