Windows Vista y Malware

Estos documentos han sido escritos y publicados por Juan Luis Rambla

Recopilación: Cristian Borghello, Director de www.segu-info.com.ar

V1.0 – 080415

Indice

Windows Vista y malware I

http://geeks.ms/blogs/vista-tecnica/archive/2007/05/23/windows-vista-y-malware-i.aspx

Comenzamos un nuevo ciclo de post y para ello vamos a analizar el comportamiento de Windows Vista con diferentes funciones de Malware, y para ello contaremos con la ayuda inestimable de un Windows Vista Ultimate y unos amiguitos de lo ajeno, más o menos reciente que nos permitirán estudiar el comportamiento del nuevo sistema operativo de Microsoft, con antiguos y nuevos amigos.

Para el estudio contaremos con todos los mecanismos de defensa con los que cuenta Windows Vista y que en función de las características se irán activando o desactivando comprobando todas las características y las circunstancias en cada uno de las pruebas que se realicen.

Cada post será un laboratorio donde se analizará algunos de estos elementos y se evaluarán las diferentes opciones de seguridad que aporta Windows Vista al laboratorio. Estableceremos el laboratorio desde la perspectiva de usuario avanzado y usuario básico, teniendo en cuenta los esquemas básicos de seguridad como son el uso del UAC, pero analizaremos también los comportamientos en caso de que estos hayan sido deshabilitados.

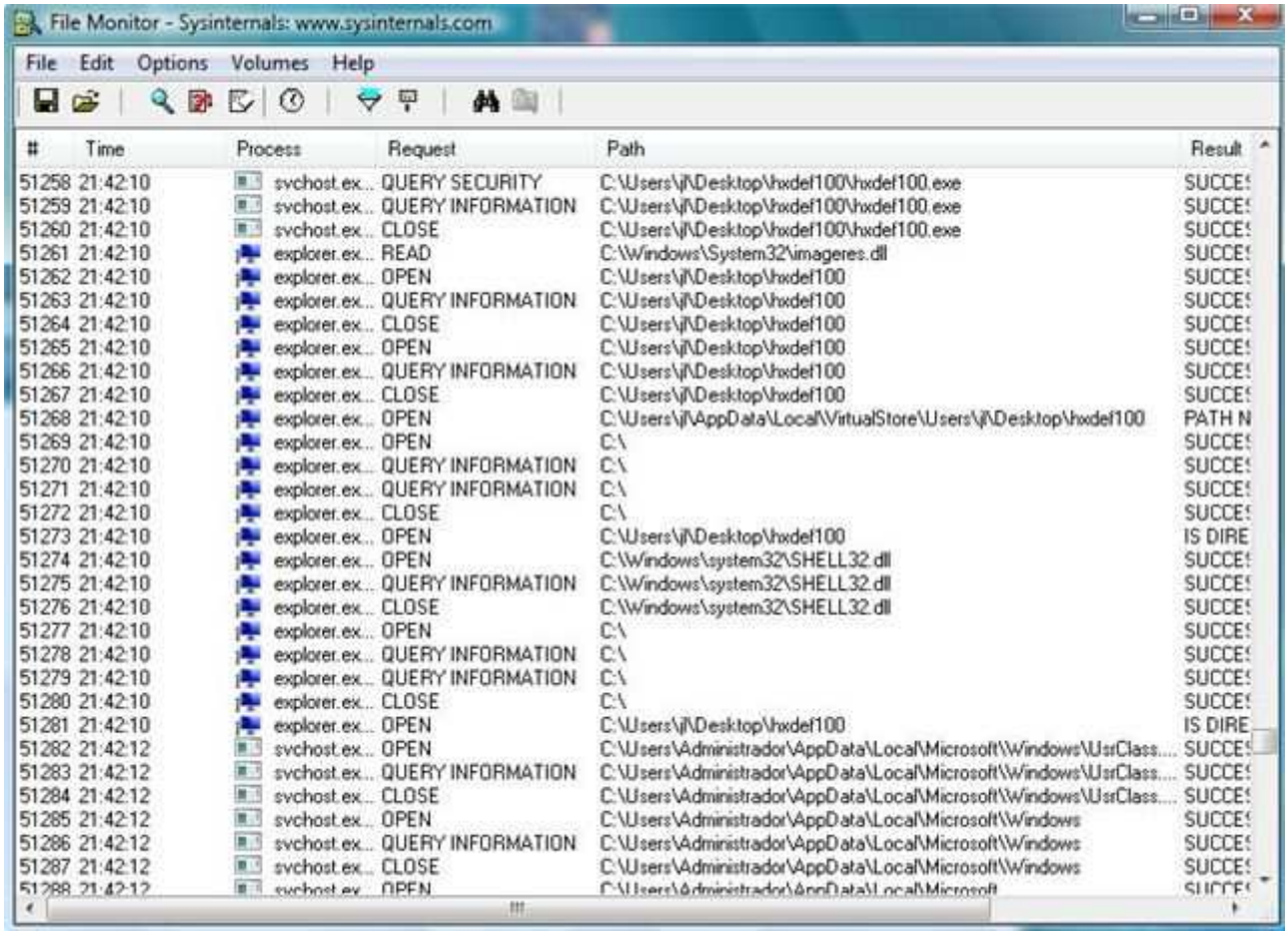
Para los laboratorios contaremos con la ayuda inestimable de Rootkits, troyanos, troyanos reversos, keyloggers, virus, gusanos, etc.

Para el primer laboratorio contaremos con un elemento Rootkits que conoceréis muchos de vosotros: Hackerdefender. Este Rootkit de tipo Kernell empezó a hacer sus pinitos allá por el 2004 y ha sido uno de los elementos más extendidos y del cual se han hecho algunas modificaciones.

Básicamente el objetivo es realizar la ocultación de ficheros y carpetas, elementos del registro y procesos y servicios. Engañaba con el espacio de disco existente en el sistema y oculta puertos localmente. Utiliza tecnología de redirector de puerto que junto con la funcionalidad de troyano, nos devuelve una Shell por cualquiera de los puertos que tengamos abiertos. En fin toda una pieza, compuesto por dos ficheros: el ejecutable y el fichero de configuración en un fichero ini.

Partimos de la base que el susodicho elemento necesita privilegios de administrador para poder ejecutarse, con lo que a priori puede encontrar el primer hándicap cuando se ejecute con el UAC activo y funcional.

Para la primera prueba vamos a contar con un usuario perteneciente al grupo de administradores (no el administrador) y que será el que lance el ejecutable. Por comparativa cuando se ejecutaba en Windows XP con un usuario con privilegios el Rootkit iniciaba todo el proceso malicioso para el que estaba configurado el fichero de configuración. En el caso de Windows Vista, la ejecución del mismo no comporta ninguna acción: el Rootkit no ha funcionado. ¡Vaya! la estructuración en capas de Windows Vista ha hecho su función y ha impedido que este usuario pueda llegar a ejecutar los drivers a nivel de Kernell, eso sí no ha intervenido el UAC. En este caso concreto el sistema tiene habilitado la función de UAC para que solicite credenciales y no se ha activado. En principio no hay ningún resultado significativo que evidencie el intento de acción que se ha empleado. El análisis a nivel de ficheros demuestra los intentos de acceso a las librerías shell32 son infructuosos y no puede cargar el driver: hxdefdrv, a nivel de sistema, lo que impide que su acción sea consecuente. La ejecución por lo tanto en un contexto no privilegiado no es satisfactorio.



En el siguiente post analizaremos el comportamiento de este mismo rootkit en un contexto privilegiado y en el contexto del administrador.

Referencias Externas

Rootkit

Hacker Defender

Filemon

Windows Vista y Malware II

http://geeks.ms/blogs/vista-tecnica/archive/2007/06/04/windows-vista-y-malware-ii.aspx

Tras haber analizado el intento de ejecución del Rootkit Hacker Defender con un usuario administrador y el UAC habilitado y haber sido infructuoso, vamos a proceder a realizar el ataque haciendo uso de los privilegios de Administrador.

Para realizar un rastreo al comportamiento del Rootkit evaluaremos 5 componentes básicos de este tipo de malware:

- Ocultación de ficheros y carpetas.
- Ocultación de procesos y servicios.
- Ocultación de Puertos.
- Ocultación de aplicaciones.
- Componente troyano con tecnología de redirector.

Partimos de la base de que tenemos tanto el fichero de ejecución del rootkit como su fichero de configuración se encuentran en el escritorio de usuario y lo ejecutamos con privilegios de administrador.

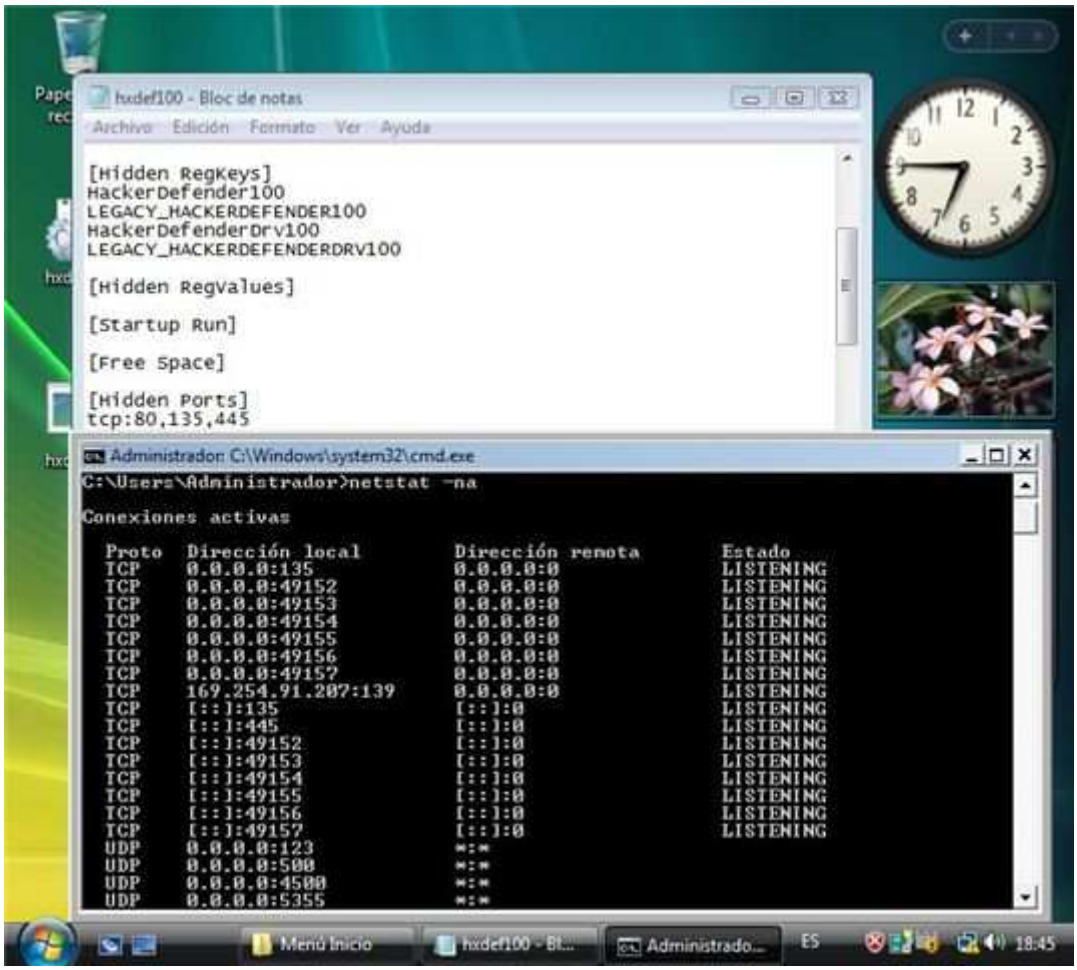


Imagen 1- Ejecutando HXDEF100 y comprobando puertos

Inicialmente no detectamos ningún comportamiento anómalo típico, como la desaparición automática de los ficheros hxdef100, ¿ha fallado o es un comportamiento anómalo? Pasamos a realizar las comprobaciones de rigor: no aparece el proceso, ni el servicio, los puertos no han desaparecido aunque desde el

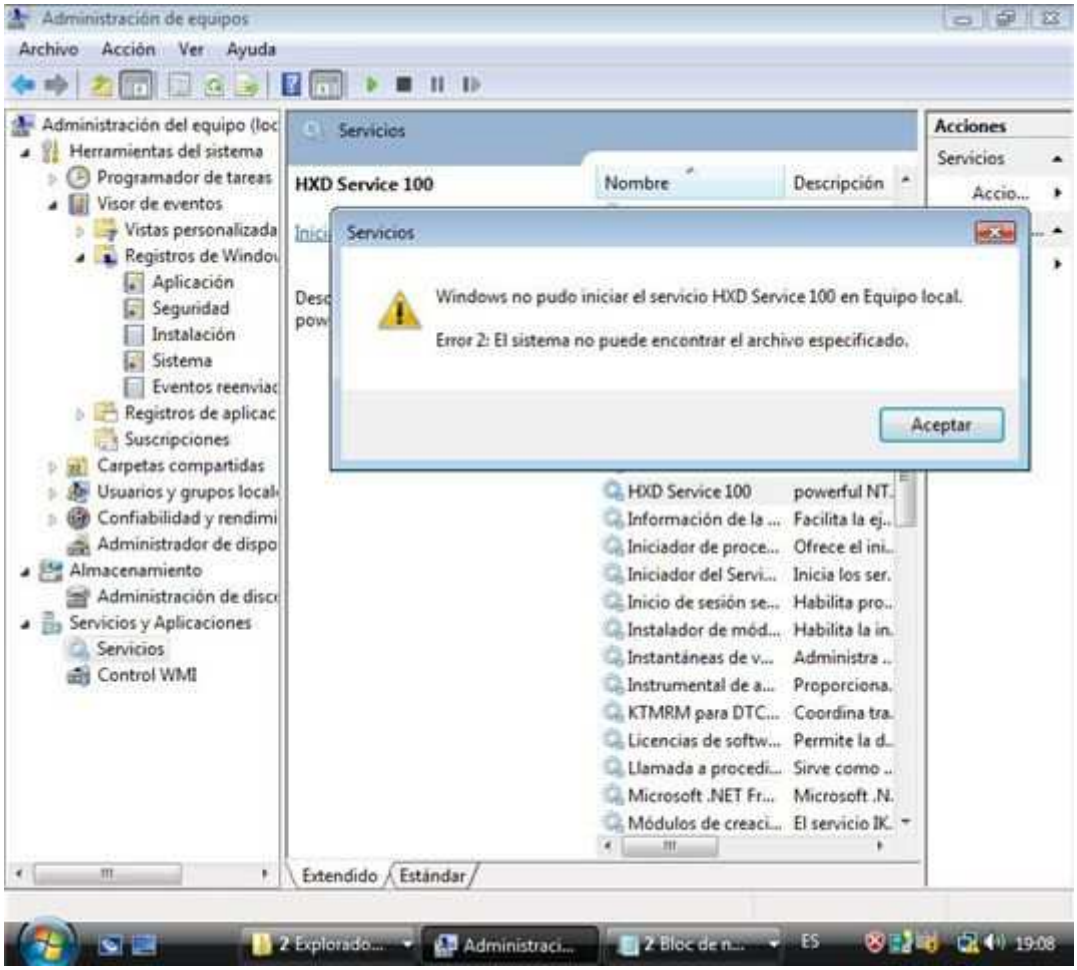
fichero de configuración se solicitaba la ocultación de los puertos TCP 135 y 445, el troyano con tecnología de redirector no es funcional, pero icuriosamente aunque nuestra aplicación de referencia: la calculadora, se ejecuta sin problema, el icono ha desaparecido!

Imagen 2 - Comprobando proceso ocultación de aplicaciones.

Bueno estos último nos deja una única funcionalidad: el rootkit se ha ejecutado con eficacia, aunque sus comportamientos para enlazar mediante Hooks las aplicaciones y procesos a engañar no han sido fructuosas, el tratamiento del modelo de UIPI y MIC ha funcionado correctamente.

Aún así como no me deja tranquilo las pruebas, vamos a poner a Windows Vista en más aprietos. Como uno de los comportamientos a esperar es la ocultación de las carpetas, vamos a crear una carpeta con el mismo nombre el ejecutable (hxdef100) y movemos los ficheros hxdef100.exe y hxdef100.ini a la carpeta. ¡Oh sorpresa! Los ficheros desaparecen, pero no la carpeta. Pues vamos a comprobar el proceso y este aparece en el administrador de proceso, aunque no queda oculto, tampoco cambia el comportamiento con respecto a los puertos ni a la calculadora.

¿Porque se ha producido este comportamiento? Se ha producido una posible manipulación en la devolución de datos en el proceso explorer.exe, que se está ejecutando en la capa del administrador, aunque no se ha podido incidir sobre otros procesos restringidos, ni en el Kernell del sistema. Tal y como esperaba, el hecho de reiniciar el Sistema, lleva consigo que el servicio que controla y ejecuta el proceso HXDEF100, no puede levantarse puesto que no encuentra el fichero para la ejecución del servicio.



El resultado final de las pruebas realizadas nos devuelven los siguientes resultados:

- El comportamiento del Rootkit no ofrece la misma funcionalidad que en un Windows XP o en un Windows 2003.
- Hemos tenido que forzar por predicción de comportamiento la ejecución y el proceso de acción del Rootkit.
- Se revela bajo el procedimiento convencional que existe un proceso anómalo en ejecución.
- Las funcionalidades para la ocultación de aplicaciones y puertos no ha resultado efectiva.
- El comportamiento del troyano en tecnología de redirector ha fallado, no devolviendo ninguna Shell de ejecución.

Pues como este laboratorio no me ha dejado satisfecho, para el siguiente, un Rootkit un poco más puñetero. Seguiremos probando a Windows Vista…

Referencias Externas

Rootkit

UIPI y MIC

Windows Vista y Malware III

http://geeks.ms/blogs/vista-tecnica/archive/2008/01/17/windows-vista-y-malware-iii.aspx

Tal y como comenté en el anterior post de Malware y Windows Vista, hoy procederemos a realizar un análisis sobre un rootkit de Kernell más agresivo con las librerías, que el Hacker Defender y comprobar el comportamiento de Windows Vista con el mismo. En Windows XP modificaba el comportamiento de las librerías dependientes de Rundll32 y colgándose del QueryInformation del sistema, impidiendo incluso posteriormente el acceso al administrador de tareas.

A diferencia con el anterior, el AFX-Rootkit no presenta un dichero de configuración sino que mediante una herramienta para la construcción del malware ya implementaremos los objetivos iniciales del ataque. Por un lado presenta la ventaja de que solo genera un ejecutable y no el fichero ini de configuración, pero por otra parte lo hace menos flexible al no permitir una configuración posterior de las operaciones del mismo.

En una primera instancia procederemos a crear un Rootkit que tenga como objetivo ocultar todos aquellos ficheros y carpetas que contengan la palabra "oculto". Posteriormente procederemos a intentar su instalación con un usuario con privilegios de administrador. Para este procedimiento dejaremos Windows Vista como viene de serie con la configuración del UAC activa y Windows Defender también activo.

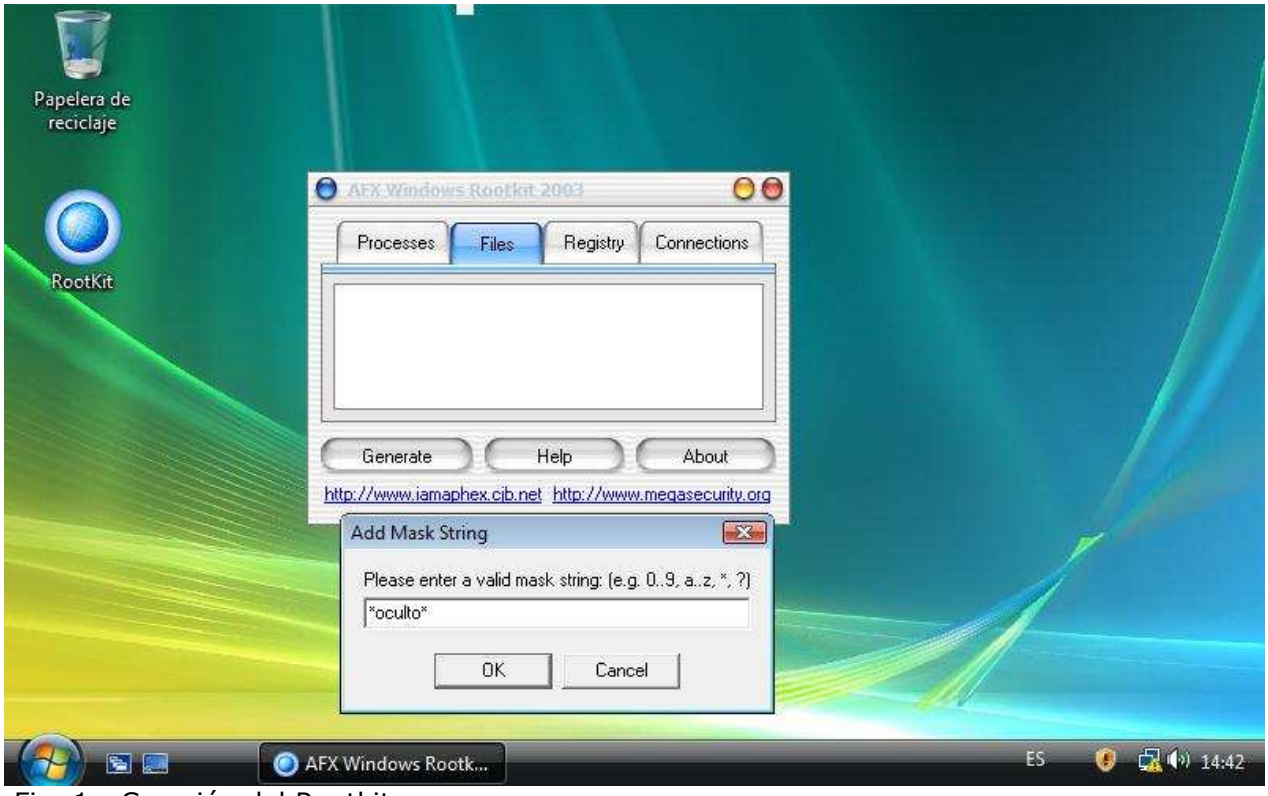


Fig. 1.- Creación del Rootkit

Una vez generado lo copiamos a una carpeta llamada oculta generada en el escritorio que contiene un fichero llamado "fichero oculto.txt"

Procedemos inicialmente a ejecutarlo sin elevar nuestros privilegios, pero no se observa ningún cambio, modificación de dll o ejecución de servicios y procesos. Ante esta ejecución infructuosa procederemos a elevar los privilegios.

Puesto que no proviene de un editor de confianza el UAC nos advierte de cambios que pudieran perjudicar a la máquina. Aún así procedemos a permitir la ejecución del programa.

El primer hecho descriptivo consiste en la desestabilización del escritorio que debe volver a ejecutarse, y que en 30 segundo vuelve a reiniciarse sin un aparente cambio significativo evidente, aunque lo comprobaremos.

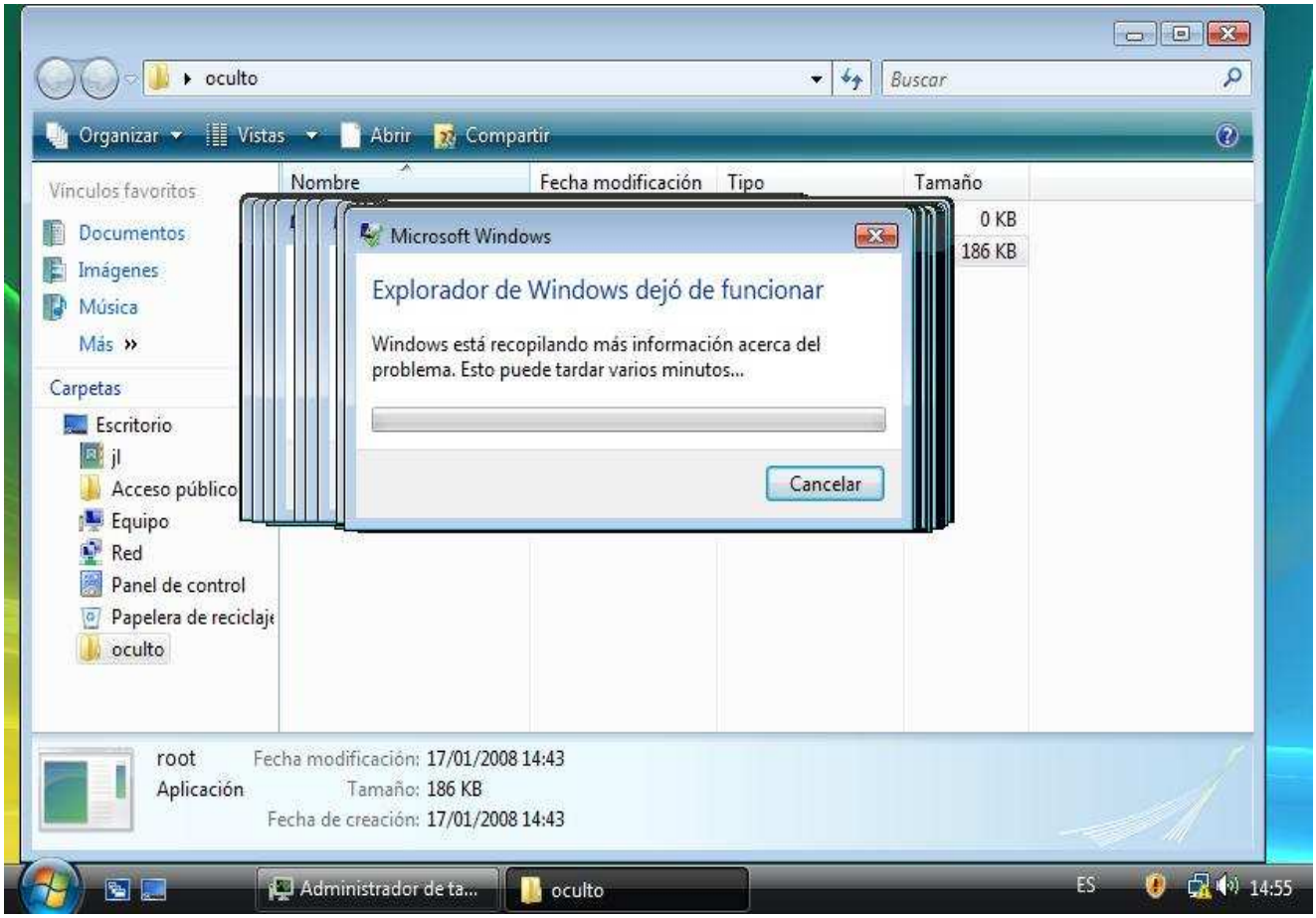


Fig. 2.- Ejecución del Rootkit en modo Administrador.

La primera comprobación consiste en determinar si se ha producido la ocultación, cosa que no se ha realizado, con lo cual seguramente no ha podido modificar las librerías del Kernell. La siguiente evidencia es que no ha podido bloquear ni el administrador de tareas, ni ha podido ejecutar el servicio correspondiente.

¿A que se debe la ineficacia de este Rootkit frente a su ejecución en Windows XP? Pues la respuesta es bastante clara, la nueva estructuración de capas y servicios de Windows Vista, con respecto a las capas presentes en Windows XP.

Fig. 3.- Estructura de capas de Windows Vista

Para las siguientes pruebas pasaremos a evaluar el comportamiento de Troyanos y Troyanos reversos y las respuestas ofrecidas por Windows Vista.

Referencias Externas

AFX Rootkit

Ejecución de Servicios en Windows Vista

Windows Vista y Malware IV

http://geeks.ms/blogs/vista-tecnica/archive/2008/02/12/windows-vista-y-malware-iv.aspx

Dentro del análisis de Malware que estamos recorriendo y antes de meternos en el análisis de los nuevos elementos maliciosos que están surgiendo, vamos a evaluar el comportamiento de los Troyanos de toda la vida. Aunque evidentemente los podemos considerar como una tecnología en desuso con respecto a otros, no por ello han desaparecido totalmente y por lo tanto veremos la respuesta de nuestro Windows Vista y la forma de detección de los mismos.

Para la prueba utilizaremos como juguetito el "DuckToy". Este elemento presenta el típico comportamiento de los Troyanos de toda la vida en el que el proceso de infección, pasa por copiarse a nuestro sistema, abrir un puerto de escucha para las peticiones del atacante y realizar cambios en el registro para que el proceso se active en la carga de la sesión del usuario. En esta circunstancia el proceso se cargará con el nombre "Explorer.exe". Para este tipo de comportamiento tendremos en cuenta una serie de los elementos incorporados por Windows Vista: UAC, Firewall y Windows Defender.

La ejecución del Troyano requiere del uso del privilegio del Administrador, por lo que lo ejecutamos con elevación de Privilegios. El primer resultado visible nos lo alerta el Firewall, indicándonos que una aplicación Server está intentado abrir una nueva conexión en la máquina, cosa que aún así permitimos para evaluar la siguiente barrera de defensa: Windows Defender.

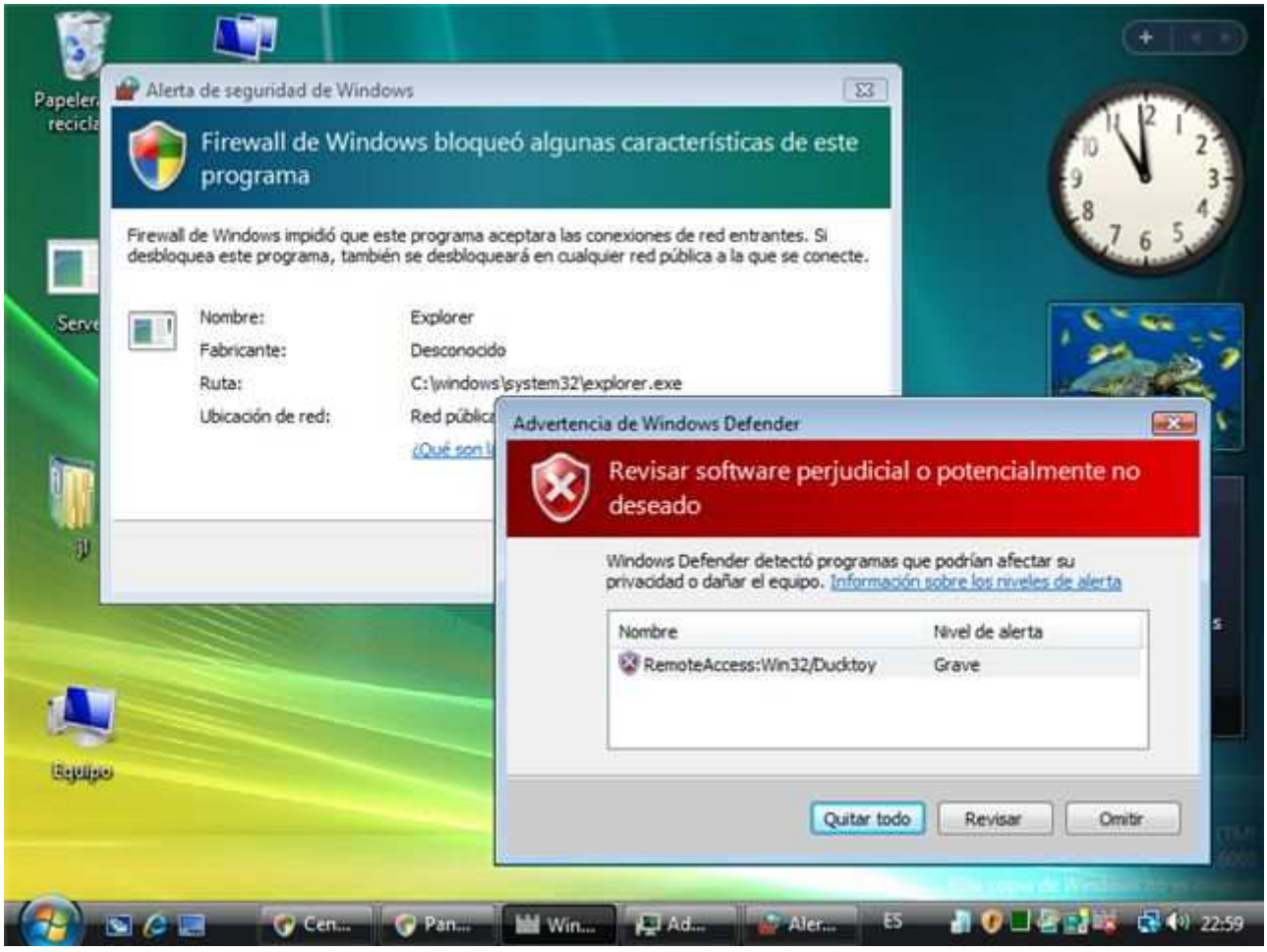


Fig. 1.- Detección amenaza

El sistema de Windows Defender aunque no constituye en sí misma una herramienta Antivirus en esencia si es capaz de detectar determinado software malicioso. En esta circunstancia detecta la firma del DuckToy como una aplicación de Acceso Remoto. El sistema detecta además un cambio en el comportamiento de ejecución de aplicaciones.

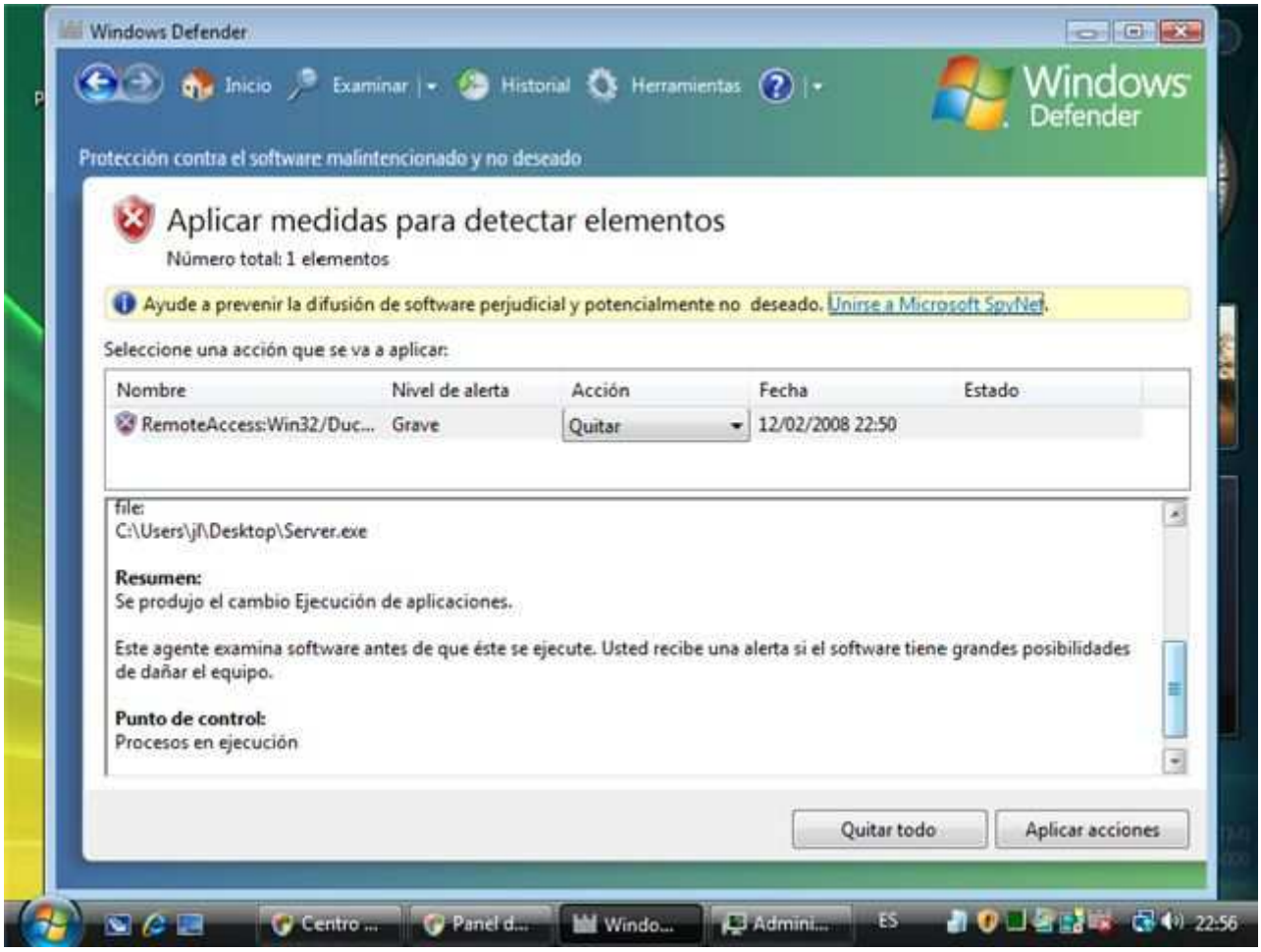


Fig. 2.- Análisis de la traza

El explorador de Software que incorpora Windows Vista nos ofrece la información necesaria para detectar la ruta de ejecución de la aplicación y la forma de arranque de la aplicación desde el registro del sistema.

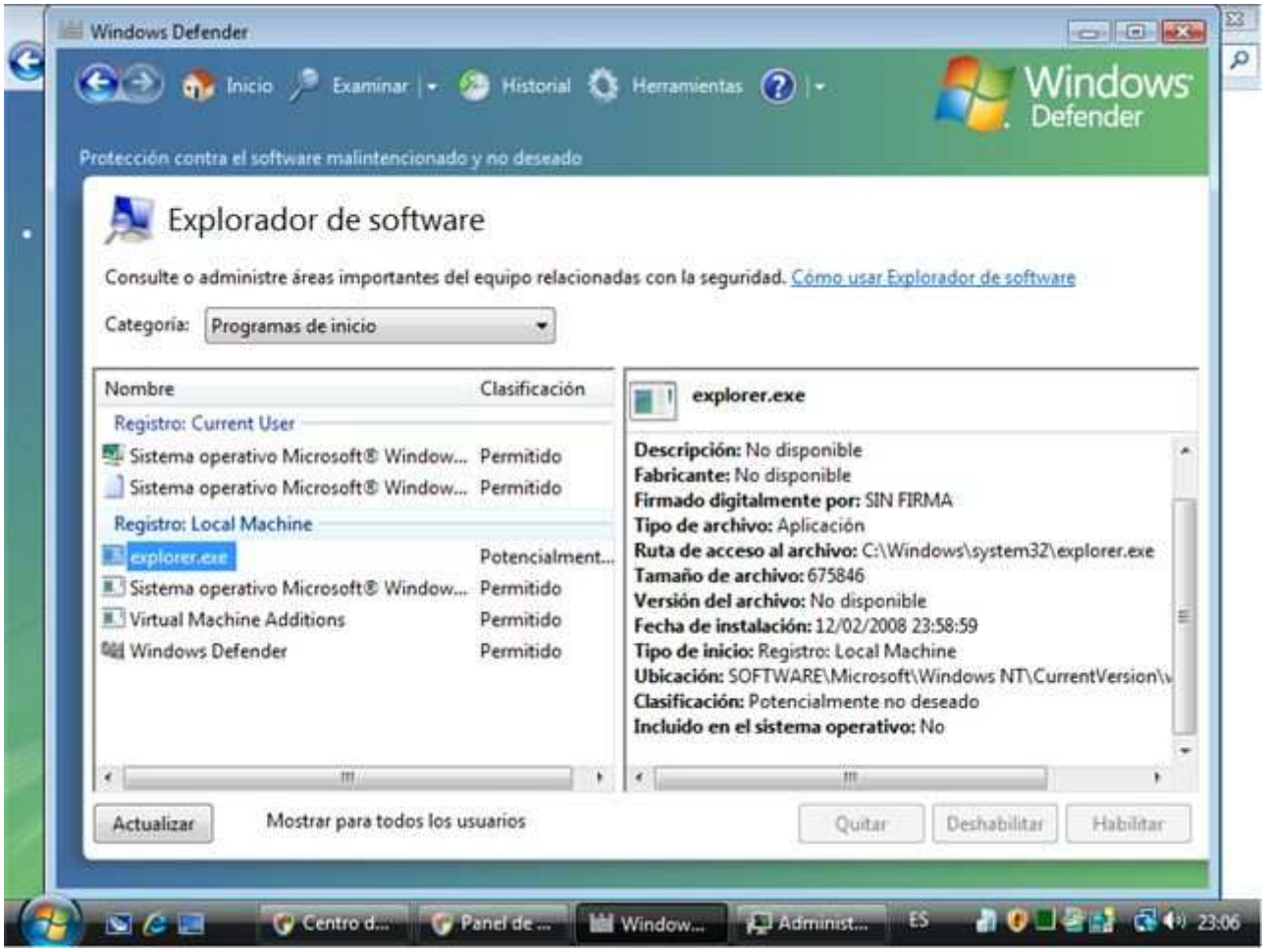


Fig. 3.- Explorador de Software

Si analizamos el historial de Windows Defender encontraremos las trazas del elemento malicioso detectado, así como las medidas que hemos aplicado para cada circunstancia. Para un análisis de amenazas y comprobar si es detectado por las herramientas antimalware de Microsoft os recomiendo la página de Security Intelligent Report, donde nos detallan el tipo de amenaza al que nos enfrentamos y desde cuando se detecta esta amenaza, entre otras posibilidades.

Windows Vista y Malware V

http://geeks.ms/blogs/vista-tecnica/archive/2008/04/14/windows-vista-y-malware-v.aspx

Continuamos con la serie de análisis del comportamiento de Windows Vista con diferentes tipos de Malware, y en esta circunstancia analizaremos las acciones con un troyano de tipo reverso. Este tipo de troyanos al contrario que los convencionales no abren un puerto en nuestros sistemas, sino que lo que intentan es establecer una conexión contra la máquina del atacante, manteniendo esta conexión, el atacante puede pasar las órdenes al proceso que estará en la máquina víctima. Este tipo de aplicaciones plantea muchas problemáticas para el afectado, puesto que el Router de tipo ADSL (o arquitectura similar), Proxy o Firewall de entrada no proporciona la capacidad por ellos mismos de constituir un tipo de barrera contra la acción perniciosa de este tipo de herramientas.

Para el análisis de este escenario contaremos con la ayuda de Turkojan Version 4 como troyano reverso y Windows Vista como víctima.

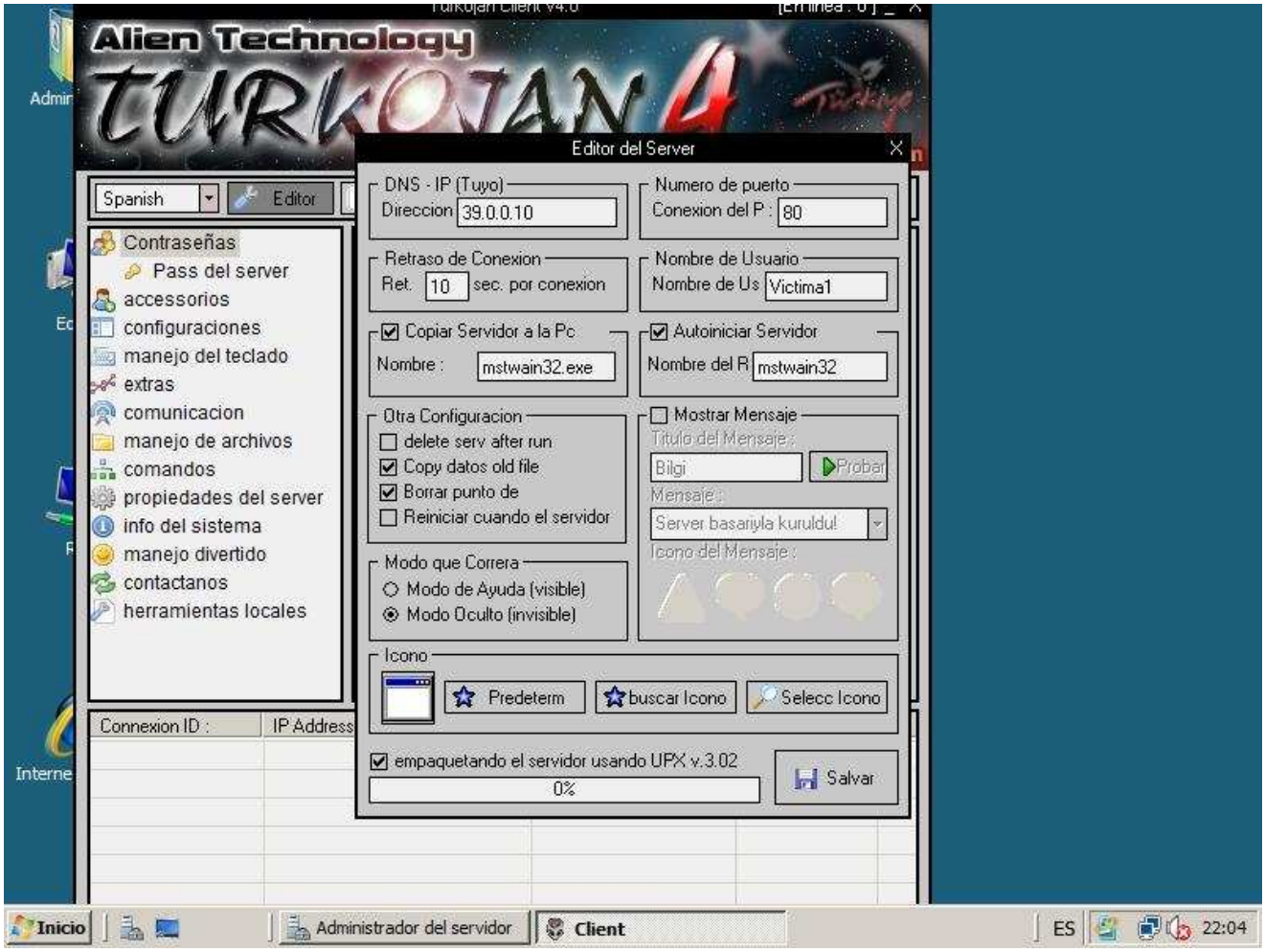


Fig.- Turkojan 4

El primer objetivo será evaluar el comportamiento que proporcionará la ejecución de la aplicación generada (cliente aunque lo definan servidor en todas las aplicaciones troyanos reversos), con el sistema de UAC activo. Ejecutamos la aplicación víctima y esta se ejecuta sin problemas, aunque notamos que no lanza el típico mensaje en pantalla indicando que la aplicación requiere la elevación de privilegios. Aún así comprobamos que la aplicación ha iniciado correctamente la conexión con el atacante, con lo cual ha realizado una de las características nativas de este tipo de Malware para la conexión reversa. Notamos además que el proceso

encargado de iniciar la conexión con el atacante está iniciado con nuestra cuenta y a través del administrador de tareas nos muestra la ruta de ejecución del proceso.

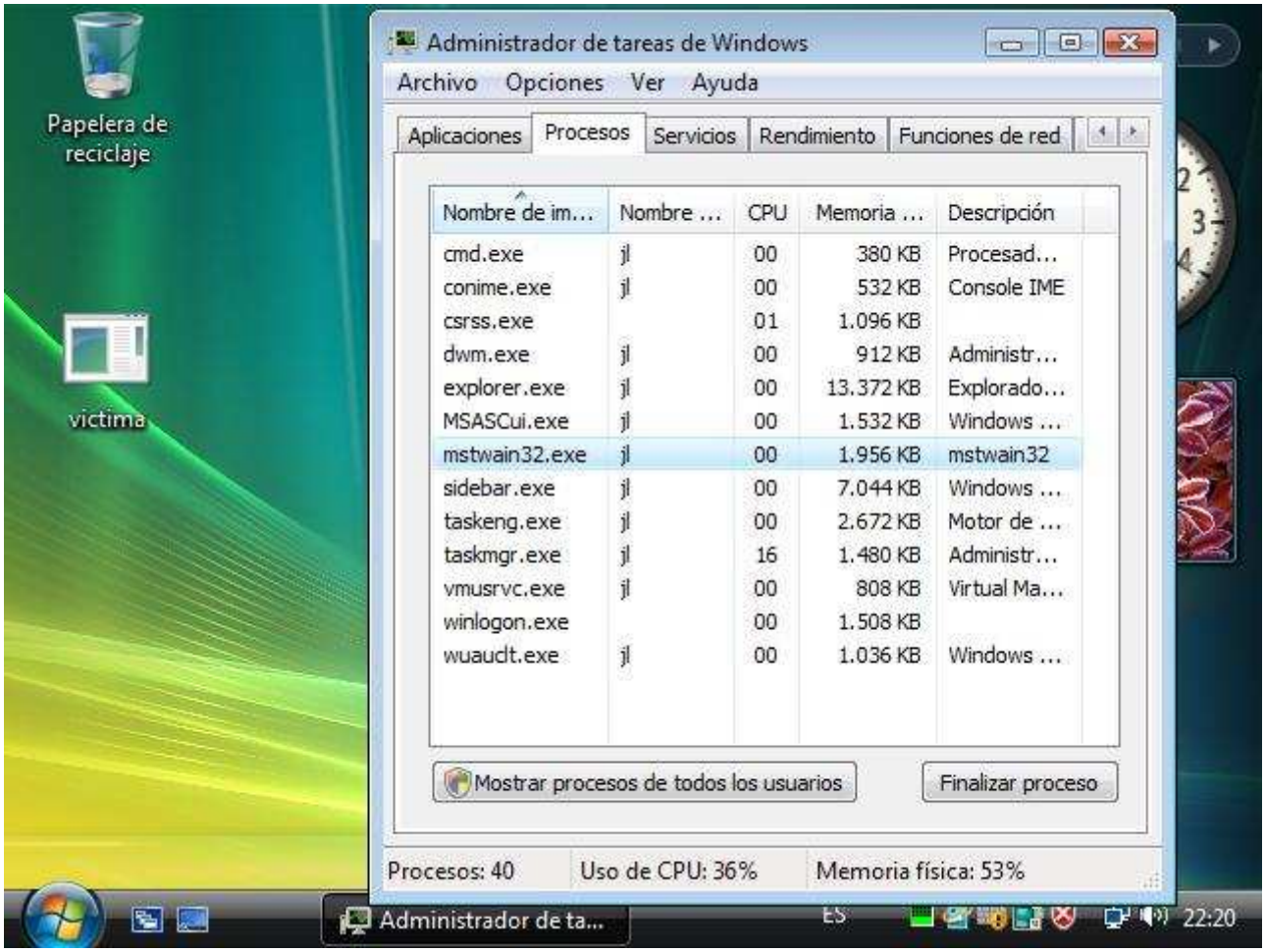


Fig.- Proceso y aplicación víctima sin icono de UAC.

Puesto que determinadas acciones requiere privilegios administrativos y supuestamente Windows Vista no ha solicitado la elevación de privilegios, es posible que muchas de las funciones del troyano reverso puedan no ser funcionales. La mayor parte de las funcionalidades requieren interaccionar con el sistema, modificar su comportamiento o acceder a determinados drivers para los cuales se requieren esos privilegios efectivos. Para ello vamos a probar alguna de las características fundamentales como la ejecución de la Shell Remota. Con la ejecución de la Shell, intentaremos la ejecución de alguna acción que requiere ser administrador para su ejecución, para ello intentaremos crer un usuario local que requiere obviamente unos privilegios administrativos, que en principio si tiene la cuenta pero que no debiera haber proporcionado el control del UAC.

Cuando intentamos ejecutar el comando advertimos que no tenemos el derecho necesario para la acción implementada.

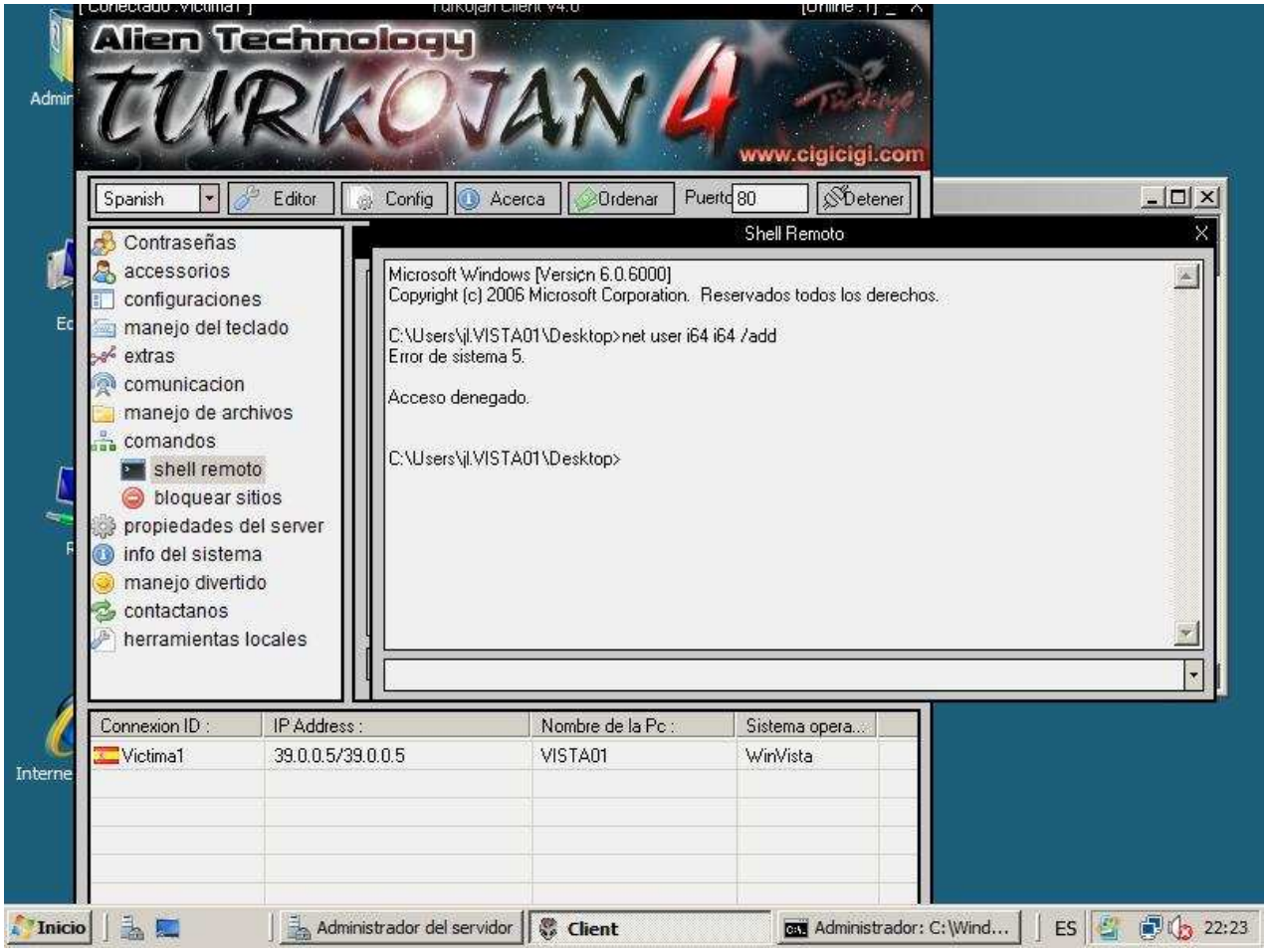


Fig.- Shell Turkojan

Bueno pues parece que el UAC está haciendo su papel, bien advertirnos o no permitir la ejecución de cualquier aplicación con privilegios independientemente de las cuenta con la que estemos trabajando. Eso sí cuidado con utilizar la cuenta predeterminada del Administrador que por defecto no implementa UAC.

Para el siguiente post evaluaremos que hubiera pasado si hubiéramos forzado la ejecución de la aplicación con privilegios administrativos.