INTECO
Instituto Nacional de Tecnologías de la Comunicación

CUENTA DE ADMINISTRADOR VS. CUENTA LIMITADA

A través de nuestros estudios trimestrales, puede constatarse que los ordenadores de muchos hogares tienen más de una cuenta o perfil de usuario, una para cada miembro de la familia que utiliza el equipo. Sin embargo, las razones que están detrás de la utilización de las cuentas diferentes para cada usuario se deben más a la intención de separar documentos de trabajo, fondos de pantalla personalizados, etc., que no al interés de fortificar la seguridad del sistema.

Por otro lado, en el caso de la utilización habitual del ordenador con permisos reducidos, existe un evidente desfase entre realidad y percepción. La diferencia es realmente notable: menos de la mitad de los usuarios que creen utilizar su equipo con permisos reducidos realmente lo hacen. Detrás de esta discrepancia podría figurar un error de concepto en cuanto a qué es y/o cómo se configura un usuario no administrador. Para paliar esta limitación formativa, el presente artículo analiza monográficamente las implicaciones de la utilización de usuario administrador y no administrador (con permisos limitados).

I Introducción

Debido al uso más extendido de los sistemas informáticos basados en el sistema Windows de Microsoft, éstos constituyen un objetivo de ataque más prioritario para los ciberdelincuentes a la hora de extender malware.

En la Tabla 1 se puede ver el nivel de uso de los diferentes sistemas operativos así como el nivel de infección de cada uno de ellos. Dentro de los basados en el sistema Windows, el análisis muestra un 70,5% de penetración y un 66,4% de equipos infectados por parte de Windows XP, convirtiéndolo en el SO más extendido a la vez que el mas compatible con el malware actual.

Tabla 1: Tasa de utilización de cada sistema operativo e infecciones por sistema operativo en septiembre de 2009 (%)

Sistema Operativo	Uso (sep'09)	Equipos infectados (sep'09)
Microsoft Windows XP	70,5	66,4
Microsoft Windows Vista	25,7	31,6
Otros Microsoft Windows	1,8	70,7
Mac	1,3	0,0
Linux	0,7	0,0

Fuente: INTECO

Ahora bien, ¿cuál es la diferencia entre Windows Vista y Windows XP que motiva el desnivel tan notable en el porcentaje de equipos que alojan malware?

El motivo principal es que Windows Vista fuerza un control más estricto de los privilegios del usuario mediante su gestor de usuarios UAC *(User Access Control)*. Con UAC se evita que se usen los privilegios elevados si no son absolutamente necesarios.

Por esta razón, y dado que el impacto sobre la seguridad del sistema es evidente en términos de infección, a continuación se orienta al usuario a configurar Windows XP para adquirir un nivel de restricción similar al de Windows Vista. Esta restricción constituye una de las capas más efectivas contra el código malicioso y otro tipo de atacantes. Se trata de una recomendación general de seguridad que es conveniente seguir: *Realizar los cambios necesarios en el sistema para conseguir una configuración más robusta, eliminando las cuentas y los servicios innecesarios y cambiando los permisos y privilegios por defecto*[1].

II Diferencias entre el tipo de cuentas y principio de mínimo privilegio

Cuenta Administrador/Cuenta Limitada

Microsoft Windows XP es un sistema multiperfil (aunque no siempre es usado como tal). Cada perfil se corresponde con un usuario, que tiene ciertas capacidades sobre el sistema operativo.

Cuantos más privilegios tiene un usuario sobre el sistema, más riesgo existe en la realización de tareas bajo ese perfil, ya que cualquier acción que realice pone en peligro las partes más delicadas de la configuración de Windows. Si el perfil tiene un poder restringido sobre el sistema operativo, no se pueden realizar tareas de administración, y el uso diario del equipo no resulta tan peligroso. Por defecto, todo usuario nuevo que se crea en Windows XP es añadido al sistema con privilegios de administración.

La Tabla 2 presenta un resumen de las tareas que permite cada tipo de cuenta. La idea global es la siguiente: una cuenta de usuario limitada permite hacer uso de la mayoría de las herramientas cotidianas del sistema, pero sólo las cuentas con privilegios de administrador pueden realizar cambios que afectan a otros usuarios.

[1] Gómez Vieites, A. Enciclopedia de la Seguridad Informática. Capítulo 17, Seguridad en redes Windows. Pág. 415.

Tabla 2: Tareas permitidas con cada tipo de cuenta de usuario

Cuenta Administrador	Cuenta Limitada
Instalación del sistema y del hardware y software inicial.	Crear, modificar o eliminar archivos de la propia cuenta.
Parametrización de preferencias (fecha y hora, fondo de escritorio, etc.) y reparación de problemas (modificación del registro, etc.)	Programas cotidianos de tratamiento de datos: procesadores de texto, hojas de cálculo, bases de datos, navegador, programas de descarga, lectores de correo electrónico, reproductores de video y audio, edición de fotografías, etc.
Adición de nuevo software (ej. programas de descarga) y hardware (ej. impresora).	Ver archivos de la carpeta Documentos compartidos.
Todas las tareas que permite una cuenta limitada: uso de procesadores de texto, navegador web, etc.	Guardar documentos, leer documentos del propio usuario.
Crear, modificar y eliminar cuentas.	Cambiar o quitar sus propias contraseñas
Tener acceso a todos los archivos del sistema.	Cambiar su imagen, tema y otras configuraciones de su escritorio.

Fuente: INTECO

Principio de mínimo privilegio

En el ámbito de la seguridad existe un principio básico que se ha de aplicar a todo proceso: el principio de mínimo privilegio. Se trata de una de las piedras angulares de la seguridad: realizar las tareas necesarias con los mínimos privilegios; así cualquier fallo, accidente o vulnerabilidad tiene también un impacto mínimo[2].

En base a este principio, es recomendable que el usuario mantenga, al menos, dos cuentas: una con privilegios de administrador (para la gestión del sistema e instalación de software) y otra cuenta con permisos reducidos (para su uso cotidiano). Todo usuario adicional que se agregue (personas que comparten el uso del mismo equipo) debe añadirse como cuenta limitada.

III Beneficios de la cuenta limitada

Gracias al uso de una cuenta limitada, las acciones que pueden ser llevadas a cabo por otro usuario o por algún tipo de código malicioso están acotadas.

Acceso a la carpeta "Mis Documentos"

Si un usuario (no administrador) intenta acceder a los documentos de otro usuario recibe un error de "Acceso denegado". De la misma manera, si el equipo es atacado por

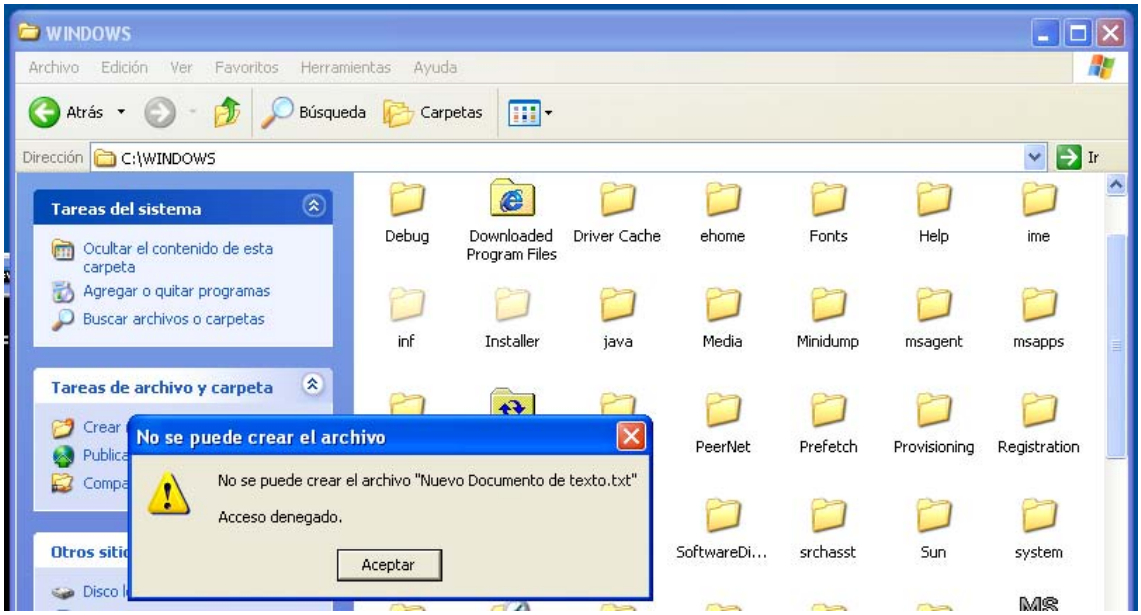
[2]Nótese que se habla de impacto mínimo y no nulo. En algunos casos puede ser nulo, pero seguir este principio no garantiza la ausencia de incidencias, sino la mitigación de éstas.

malware al utilizar una cuenta con permisos limitados, el código malicioso no puede acceder a las carpetas personales de otros usuarios, imposibilitando así el acceso de éste a otros documentos importantes.

Escritura en la carpeta del sistema

Si se trata de escribir o borrar contenido de una carpeta crítica para el correcto funcionamiento del sistema (por error o intencionadamente), la acción se impide con un error de "Acceso denegado", como se muestra en la Ilustración 1.

Ilustración 1: Intento de escritura en carpeta del sistema con una cuenta limitada



Fuente: INTECO

Instalación de un driver

Si se intenta instalar un driver[3] (malicioso o legítimo) con una cuenta limitada, se recibe un error de "Acceso denegado". Esto implica que el código malicioso basado en drivers no puede infectar el sistema.

[3] Un driver es un programa informático que permite al sistema operativo interactuar con un periférico, haciendo una abstracción del hardware y proporcionando una interfaz (posiblemente estandarizada) para usarlo. Viene a ser un manual de instrucciones que le indica cómo debe controlar y comunicarse con un dispositivo en particular. La peculiaridad de un driver es que se trata de código que se ejecuta en el corazón del sistema operativo. Este hecho está siendo aprovechado por los creadores de malware, que desarrollan código malicioso en forma de drivers para comprometer el sistema operativo en el nivel más bajo, de forma muy silenciosa y peligrosa. Cualquier error de programación en este nivel de abstracción puede impedir la carga del sistema operativo.

Modificación del registro de Windows

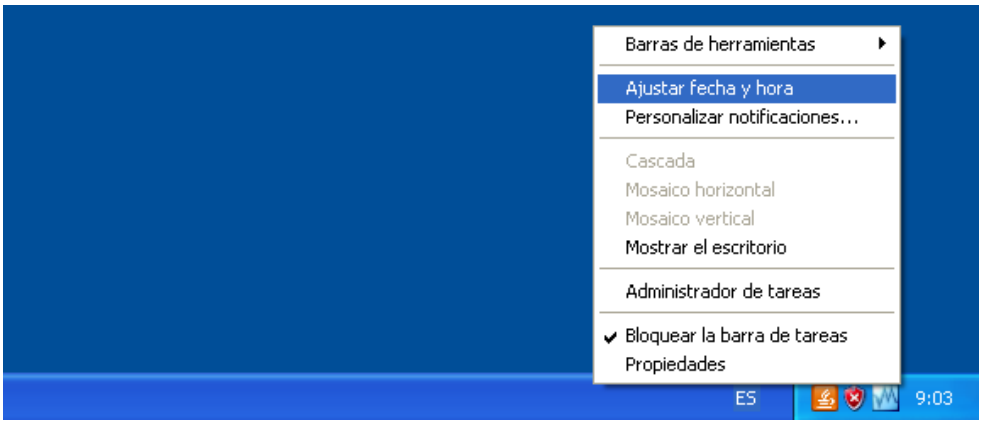
El registro de Windows alberga la configuración del sistema operativo y de algunos de los programas instalados. Para persistir en el sistema y comprometer programas, el malware ha de realizar ciertas modificaciones en el registro. Con la utilización de un usuario limitado, muchas de estas acciones están denegadas, reduciendo drásticamente el impacto del malware.

IV ¿Cómo averiguar qué tipo de cuenta se está utilizando?

La forma más sencilla de saber si se utiliza una cuenta limitada o administradora consiste en forzar una situación a la que sólo tenga derecho un usuario administrador y ver si la acción está permitida.

La acción más simple es tratar de cambiar la hora del sistema. Para ello se ha de mover el puntero del ratón sobre el reloj situado en la parte inferior derecha de la pantalla, y con el botón secundario del ratón seleccionar la opción “Ajustar fecha y hora” (Ilustración 2).

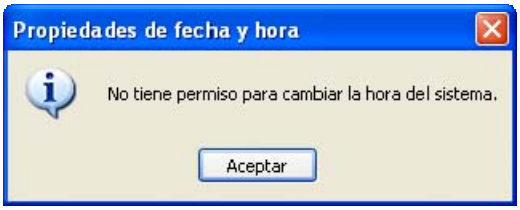
Ilustración 2: Ajuste de fecha y hora



Fuente: INTECO

Si se está utilizando una cuenta de usuario limitada, se muestra un cuadro de diálogo con el texto "No tiene permiso para cambiar la hora del sistema" (Ilustración 3).

Ilustración 3: Intento de cambiar la fecha y hora del sistema con una cuenta limitada



Fuente: INTECO

En cambio, si se utiliza una cuenta de administrador, se abre una ventana con controles que permiten cambiar la fecha y la hora del equipo (Ilustración 4).

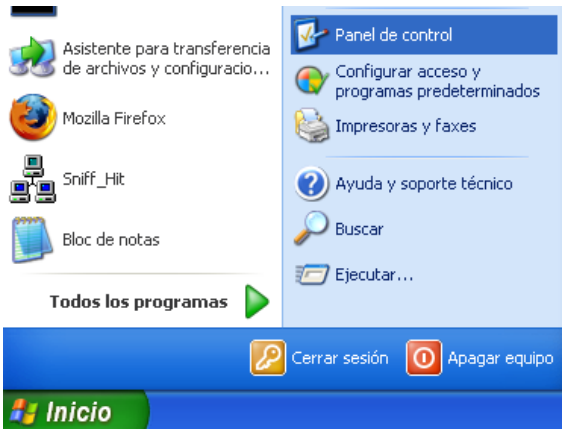
Ilustración 4: Intento de cambiar la fecha y hora del sistema con una cuenta con privilegios de administrador

Fuente: INTECO

V ¿Cómo configurar la cuenta personal como limitada?

Para configurar una cuenta de usuario limitada hay que asegurarse de que se ha iniciado sesión con un usuario con privilegios de administrador. En las siguientes ilustraciones se muestra como llevar a cabo el proceso para convertir una cuenta de administrador a una con permisos reducidos[4].

Ilustración 5: Acceso al panel de control desde el menú de inicio



Fuente: INTECO

El primer paso consiste en acceder al panel de control (Ilustración 5) y una vez allí, a la pantalla de cuentas de usuario.

[4] Para llevar a cabo este proceso se ha tomado un equipo (en el que el usuario se llama: John Doe) en el que no se hicieron modificaciones tras la instalación de su sistema operativo y cualquier usuario opera normalmente como administrador.

Ilustración 6: Opciones del panel de control

Fuente: INTECO

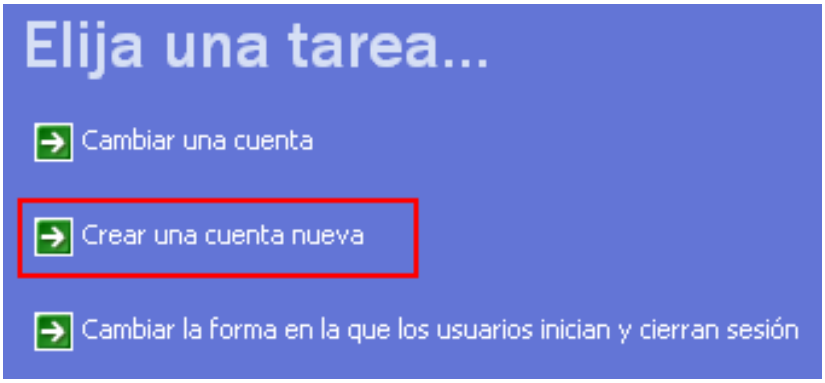
Seleccionando esta opción, el usuario se encuentra una pantalla como la que se muestra en la Ilustración 7, en la cual se pueden visualizar los usuarios que existen en el equipo y el tipo de perfil asociado a cada uno.

Ilustración 7: Pantalla de cuentas de usuario del panel de control

Fuente: INTECO

Siempre debe existir al menos un usuario “Administrador de equipo”. En consecuencia lo que se debe hacer es añadir un usuario “Administrador de equipo” nuevo y modificar la cuenta del usuario “John Doe” a una limitada. Para ello hay que seleccionar la opción “Crear una cuenta nueva” situada en la parte superior de la ventana anterior (Ilustración 8).

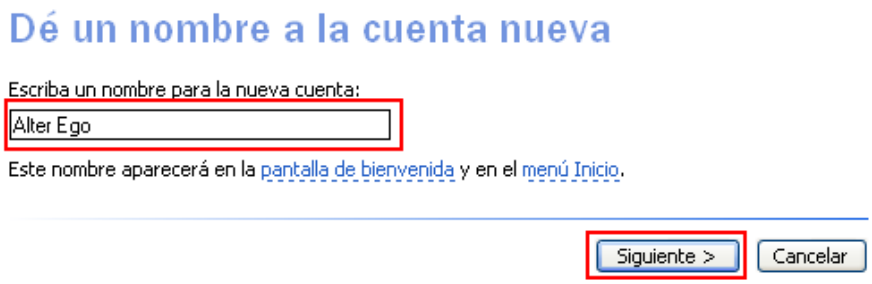
Ilustración 8: Creación de cuenta de administrador de equipo (paso 1)



Fuente: INTECO

Esto conduce a una nueva pantalla en la que se ha de indicar el nombre de la nueva cuenta (Ilustración 9). Para que no sea trivial para un atacante adivinar el nombre de una cuenta con privilegios de administrador, se recomienda que no se emplee el nombre "Administrador" o similares.

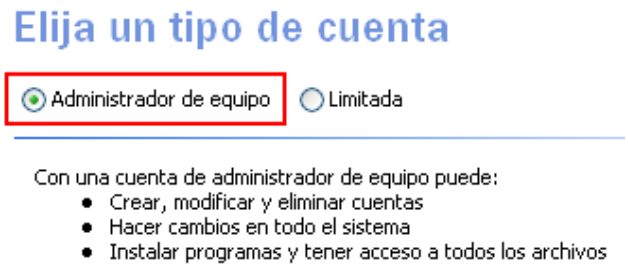
Ilustración 9: Creación de cuenta de administrador de equipo (paso 2)



Fuente: INTECO

El siguiente paso consiste en configurar la cuenta efectivamente como "Administrador de equipo" y finalizar el proceso de creación (Ilustración 10).

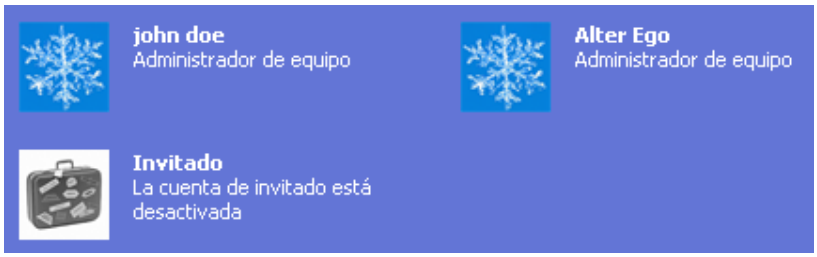
Ilustración 10: Creación de cuenta de administrador de equipo (paso 3)



Fuente: INTECO

A partir de este momento, aparece una cuenta más en la pantalla de configuración de usuarios del panel de control.

Ilustración 11: Pantalla de cuentas de usuario del panel de control



Fuente: INTECO

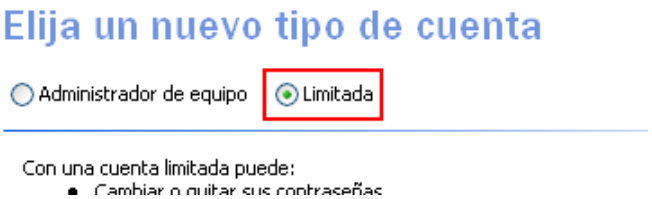
El siguiente paso consiste en modificar los privilegios de la cuenta, "John Doe". Para ello se ha de seleccionar dicho usuario (Ilustración 11) y acceder a la opción "Cambiar mi tipo de cuenta" en la nueva pantalla que aparece.

Ilustración 12: Configuración de una cuenta de usuario

Fuente: INTECO

Ahora es el momento de modificar el tipo de cuenta seleccionando la opción "Limitada" (Ilustración 13).

Ilustración 13: Configuración de una cuenta de usuario como cuenta limitada



Fuente: INTECO

Ahora, cada vez que se acceda al equipo, en la pantalla de inicio de sesión se debe seleccionar el usuario limitado, tal y como muestra la Ilustración 14.

Ilustración 14: Inicio de sesión cuando hay varias cuentas de usuario

Fuente: INTECO

Además de configurar la cuenta como limitada es recomendable añadir una contraseña a todos los usuarios. De esta forma se evita que las personas no autorizadas inicien sesión en el sistema operativo. La contraseña se puede añadir fácilmente desde el menú de configuración de cada cuenta (Ilustración 12, "Crear una contraseña"). Si no se crean contraseñas cualquiera puede iniciar sesión como usuario del sistema, incluyendo al "Administrador de equipo".

¿Cuál es el problema principal que se va a encontrar el usuario al operar con una cuenta limitada? El usuario no va a poder instalar programas que realicen cambios sobre el sistema y/o que afecten a otros usuarios (la mayoría del software de hoy día).

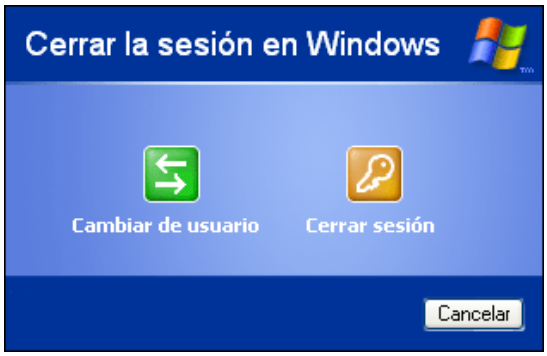
VI Adquisición puntual de privilegios de administrador

Existen opciones para adquirir puntualmente privilegios de administrador de cara a instalar un determinado programa o realizar una determinada tarea. Se detallan a continuación.

Cambio rápido de usuario

Para no tener que reiniciar el sistema ni perder el contexto en el que se está trabajando con la cuenta de usuario limitado, lo más sencillo es realizar un cambio de usuario. Para ello es suficiente con seleccionar la opción "cerrar sesión de (nombre de usuario)" del menú desplegable "Inicio". Así en "Cambiar de usuario" (Ilustración 15) se accede a la opción de cambio a la cuenta de administrador. Para volver a la cuenta limitada se sigue el mismo proceso.

Ilustración 15: Cambio rápido de usuario



Fuente: INTECO

Si el programa que se está instalando pregunta si se desea instalar de tal forma que esté disponible para todos los usuarios se ha de decir que sí. De lo contrario, no será visible desde la cuenta limitada.

Opción "Ejecutar como"

Para instalar un programa desde una cuenta limitada se puede seleccionar el ejecutable, y pulsar el botón secundario del ratón. Entre las opciones disponibles, se visualiza una nueva denominada "Ejecutar como", que permite ejecutar un programa como un usuario distinto al de la cuenta que se está utilizando.

Se selecciona ejecutar como "El siguiente usuario", se introducen los datos de la cuenta de administrador, y el programa es instalado como si lo estuviera haciendo el administrador.

Ilustración 16: Ejecutar como

Fuente: INTECO

Ejecución desde la consola del sistema

La última opción (quizá la más compleja) consiste en ejecutar la aplicación deseada desde la consola con los privilegios del usuario administrador. Para ello se utiliza la herramienta del sistema operativo RunAs.exe (como el comando *su* en Linux).

Se ha de abrir el símbolo del sistema (Inicio > Programas > Accesorios > Símbolo del Sistema) y allí se teclea lo siguiente:

runas /user:*nombre_de_usuario_administrador* "*ruta_completa_a_fichero*"

RunAs.exe solicita la contraseña del usuario administrador para poder llevar a cabo la aplicación deseada.

VII Comprobación de los beneficios de la cuenta limitada

Para mostrar al lector de manera práctica las implicaciones positivas del uso del equipo con permisos limitados, se ha procedido a infectar una máquina real con un ejemplar de código malicioso. La infección se lleva a cabo en una cuenta con permisos de administrador y en una cuenta limitada con el fin de demostrar los efectos en ambos casos. A continuación se describen las consecuencias.

Identificación del ejemplar malicioso empleado en la prueba de concepto

El fichero de código malicioso elegido es detectado por los distintos antivirus que se emplean en la herramienta iScan[5] de la siguiente manera:

Ilustración 17: Detecciones antivirus del código malicioso usado en de la demostración

Resultado: 25/41 (60.98%)

Compactar | Imprimir resultados

Motor antivirus	Versión	Última actualización	Resultado
	4.5.0.43	2009.11.25	Trojan.Win32.VB.xyn!A2
	5.0.0.2	2009.11.24	Win-Trojan/Xema.variant
	7.9.1.70	2009.11.24	TR/Hosts.yu.2
	2.0.3.7	2009.11.25	Trojan/Win32.VB.gen
	5.2.0.5	2009.11.24	-
	4.8.1351.0	2009.11.25	Win32:Malware-gen
	8.5.0.425	2009.11.24	Generic15.AOKX
	7.2	2009.11.25	Trojan.Generic.2644759
	10.00	2009.11.25	Trojan.Agent.ATV
	0.94.1	2009.11.25	Trojan.VB-8016
	3029	2009.11.25	Heur.Suspicious
	5.0.0.12182	2009.11.25	-
	7.0.17.0	2009.11.24	-
	35.1.7141	2009.11.25	-
	4.5.1.85	2009.11.24	-
	9.0.15370.0	2009.11.24	-
	4.0.14.0	2009.11.25	W32/VB.XYN!tr

Fuente: INTECO

[5]Potente herramienta desarrollada por INTECO que analiza los sistemas y ofrece información empírica sobre las herramientas instaladas, el nivel de actualización de los sistemas, y el grado de infección de los equipos.

Se trata de un troyano bancario que busca modificar el archivo *hosts* del sistema para dirigir las visitas a las páginas de ciertos bancos a un servidor malicioso, realizando una réplica falsa del espacio de banca electrónica de cada entidad. Captura las credenciales de banca electrónica de la víctima para luego iniciar sesión en la página legítima del banco y hacer transferencias a cuentas relacionadas con el atacante.

El archivo *hosts* de un ordenador es, en su origen, un vestigio de los tiempos en que sólo había unos pocos dominios y se enviaba la lista con todos ellos y sus respectivas IPs en un archivo llamado *hosts*. En la actualidad, todas las peticiones se realizan a servidores DNS (un sistema distribuido de servidores de nombres). No obstante, los sistemas operativos actuales mantienen este archivo, de modo que es posible modificar a mano a qué dirección IP deben resolver determinados dominios.

Cuando tecleamos un dominio en el navegador, lo primero que hace el ordenador es comprobar si ya tenemos información del mismo en el archivo *hosts*. En caso negativo, comprueba si se pidió hace poco y lo tiene en la caché. De no haberlo hecho, lo solicita a su servidor DNS para que le comunique la IP de ese dominio. Luego la guarda en la caché para futuras consultas. Esta caché se vacía al poco tiempo (al reiniciar el equipo, etc.) En cambio, los datos del archivo *hosts* son permanentes, por lo que se puede modificar apuntando a las direcciones más utilizadas para ganar tiempo (milisegundos) en webs de acceso frecuente. Esto ha sido aprovechado por los ciberdelincuentes, que encuentran trivial la creación de un troyano que modifique el archivo *hosts* local del sistema infectado para forzar la redirección a una página fraudulenta cuando se visita la página web de un banco.

El archivo *hosts* de Windows XP se encuentra en la ruta:

C:\WINDOWS\system32\drivers\etc\hosts

El contenido de este fichero en un sistema virgen es el siguiente:

Ilustración 18: Fichero *hosts* de un sistema virgen

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# Éste es un ejemplo de archivo HOSTS usado por Microsoft TCP/IP para Windows.
#
# Este archivo contiene las asignaciones de las direcciones IP a los nombres de
# host. Cada entrada debe permanecer en una línea individual. La dirección IP
# debe ponerse en la primera columna, seguida del nombre de host correspondiente.
# La dirección IP y el nombre de host deben separarse con al menos un espacio.
#
#
# También pueden insertarse comentarios (como éste) en líneas individuales
# o a continuación del nombre de equipo indicándolos con el símbolo "#"
#
# Por ejemplo:
#
#      102.54.94.97     rhino.acme.com          # servidor origen
#       38.25.63.10     x.acme.com              # host cliente x

127.0.0.1       localhost
```

Fuente: INTECO

El lector puede apreciar que tan sólo se indica un nombre, *localhost*, que apunta a la dirección IP 127.0.01, el bucle local que identifica la propia máquina.

Este troyano lo que hace es modificar el fichero *hosts* para añadir las siguientes entradas[6]:

- XXX.237.245.58 banco1.com
- XXX.237.245.58 banco2.com.pe
- XXX.237.245.58 banco3.com.pe

Las entradas se añaden periódicamente. De esta forma, si un usuario las detecta y las borra, se vuelven a escribir. El efecto de este cambio es que al tratar de visitar la página de, por ejemplo, "banco1.com", la víctima es dirigida al servidor que responde a la dirección IP "XXX.237.245.58". Dicho servidor es malicioso y responde con una imitación de la página del banco al ser contactado, así, todos los datos introducidos en esa página son capturados.

Además de este cambio, el troyano también se copia con el nombre *svhostss.exe* en la ruta:

C:\WINDOWS\system\

Tras copiarse, el troyano agrega el valor *malware* = *svhostss.exe* a la siguiente clave del Registro de Windows:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

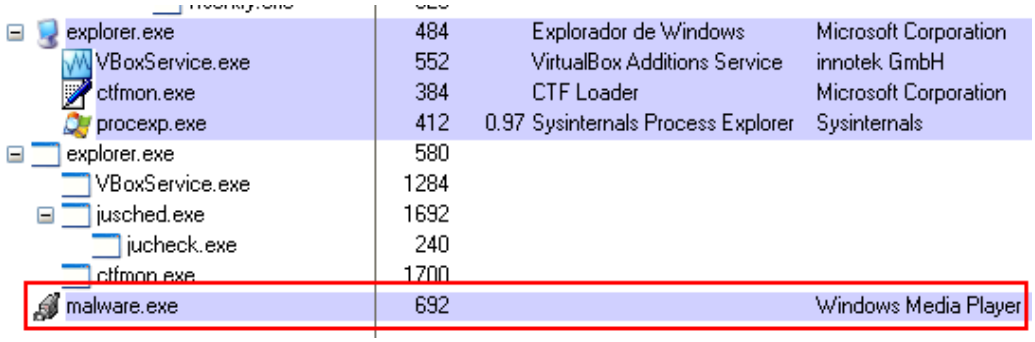
Esta modificación fuerza la ejecución automática del espécimen en cada reinicio del sistema, de tal forma que el equipo permanece troyanizado aunque se reinicie o apague.

Ejecución del troyano en una cuenta limitada

Cuando se lanza el troyano (nombrado *malware.exe* para la prueba) en una cuenta con permisos limitados, éste se ejecuta y permanece corriendo en memoria, tal y como muestra el listado de procesos de la Ilustración 19. Nótese en dicho listado que el ejemplar malicioso ha fijado su descripción a "Windows Media Player" y está empleando el icono de una cámara para que el usuario no sospeche que se trata de código malicioso.

[6]Se ha omitido el primer byte – primeras tres cifras – de la dirección IP y se han transformado los nombres de dominio para conservar la privacidad de los bancos implicados

Ilustración 19: Procesos en ejecución en el sistema tras lanzar el troyano



Fuente: INTECO

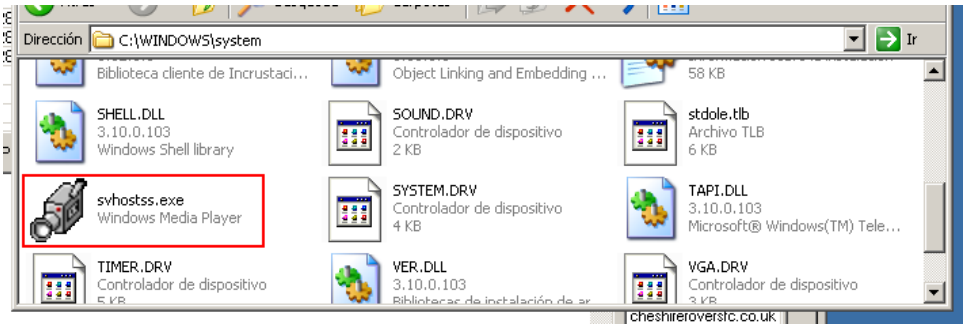
¿Cuál es la ventaja de que el troyano se haya ejecutado en una cuenta con permisos limitados? El troyano se ha ejecutado, pero no ha podido realizar todas las acciones maliciosas para las que estaba programado. El espécimen no ha podido copiarse en la ruta *C:\WINDOWS\system\ svhostss.exe* y tampoco ha podido modificar el registro para troyanizar el sistema tras cada reinicio. En el momento en que se reinicie el equipo el ejemplar deja de estar ejecutándose en memoria y el peligro es nulo. Adicionalmente, el troyano tampoco ha podido cambiar el fichero *hosts* del sistema, con lo cual no puede cometer fraude bancario.

Hay que señalar que habrá ciertos troyanos cuyas acciones sí puedan ser realizadas en una cuenta limitada. Es el caso de los ejemplares que se limitan a borrar los documentos del propio espacio del usuario (de “Mis Documentos” por ejemplo)

Ejecución del troyano en una cuenta con privilegios de administrador

La ejecución del troyano en una cuenta con privilegios de administrador tiene consecuencias más graves. Después de ser lanzado, el troyano permanece en ejecución en memoria como en el caso anterior. En esta ocasión sí logra copiarse a la ruta desde la que es ejecutado en cada inicio del sistema:

Ilustración 20: Copia del troyano para ser ejecutado tras cada reinicio



Fuente: INTECO

De igual forma, el troyano consigue modificar el registro de Windows para que se ejecute en cada reinicio. Por último, el fichero *hosts* también es modificado para dirigir a los usuarios de ciertos bancos a plataformas maliciosas:

Ilustración 21: Archivo *hosts* modificado por el troyano en una cuenta con privilegios de administrador

```
#        38.25.63.10      x.acme.com                # host cliente x

[redacted].234.219.149 [redacted].com
[redacted].234.219.149 [redacted].com.pe
[redacted].234.219.149 [redacted].com.pe
```

Fuente: INTECO

Toda víctima que visite “www.banco1.com” es dirigido a una página falsa y al tratar de iniciar sesión en esa página falsa sus credenciales son capturadas y empleadas para realizar transferencias desde su cuenta sin su consentimiento.

VIII Conclusiones

El proceso expuesto en este artículo no es un sistema infalible de protección para el usuario sino una manera de acotar el impacto que pueda ocasionar una incidencia de seguridad. No obstante, si no se es cauto y se ignoran estas pequeñas directrices de seguridad, el código malicioso puede residir en el espacio de usuario, modificar sus claves del registro y acceder a sus datos.

Entender las implicaciones de las cuentas limitadas y utilizarlas de forma habitual puede suponer un importante beneficio en términos de seguridad.

Aun así, no se debe caer en el error de la falsa sensación de seguridad y adoptar hábitos poco prudentes por el simple hecho de estar operando con una cuenta limitada. La cuenta limitada debe ser únicamente un ladrillo más en el esquema multicapa de seguridad. Así, esta medida ha de complementar, y no sustituir, el uso de otras herramientas como antivirus, cortafuegos, etc.

Existen parametrizaciones más avanzadas que se pueden realizar sobre una determinada cuenta para restringir aun más los permisos y los tipos de acciones con el fin de mitigar el impacto del malware. En futuros artículos, dependiendo de la penetración de Windows Vista y del nuevo sistema operativo de Microsoft, Windows 7, quizá sea interesante seguir incidiendo en la seguridad de Windows XP y explorar estas opciones de configuración avanzadas.