(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 726 928**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/56 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.12.2015 PCT/US2015/066061**

(87) Fecha y número de publicación internacional: **23.06.2016 WO16100494**

(96) Fecha de presentación y número de la solicitud europea: **16.12.2015 E 15821216 (7)**

(97) Fecha y número de publicación de la concesión europea: **01.05.2019 EP 3234850**

(54) Título: **Métodos, sistemas y dispositivos para detectar y aislar un dispositivo que constituye una amenaza de seguridad**

(30) Prioridad:

19.12.2014 US 201414577405

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.10.2019

(73) Titular/es:

FEDEX CORPORATE SERVICES, INC. (100.0%)
30 FedEx Pkwy 1st Fl. Vertical
Collierville, TN , US

(72) Inventor/es:

PATTESON, CHRISTOPHER PERRY;
MAIER, EDWARD MICHAEL y
MINGS, MICHAEL JESSE

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Métodos, sistemas y dispositivos para detectar y aislar un dispositivo que constituye una amenaza de seguridad

Campo técnico

La presente divulgación se refiere al campo de la seguridad informática, y, más en particular, a métodos, sistemas y dispositivos para detectar y aislar dispositivos que constituyen una amenaza de seguridad.

Antecedentes

Dispositivos de almacenamiento no volátil, tal como Secure Digital (SD), Memory Stick™, memoria flash, unidad de estado sólido (SSD), disco duro portátil, etcétera, proporcionan un medio conveniente para los usuarios para almacenar y transferir archivos informáticos. Sin embargo, estos dispositivos, que actúan como un trasportador de archivos informáticos, también son muy propensos a ser infectados con virus informáticos y otros programas maliciosos, cuando son enchufados en un sistema informático para cargar o descargar un archivo informático. El riesgo de infección es alto cuando la gente utiliza un ordenador público para acceder a su dispositivo de almacenamiento no volátil privado, siempre y cuando un usuario, de entre muchos, enchufe un dispositivo infectado al ordenador público sin escanear primero el dispositivo en busca de virus informáticos o programas maliciosos, el ordenador público será muy posiblemente infectado, y el ordenador público infectado entonces propagará el virus o programa malicioso a los dispositivos de almacenamiento de otros usuarios. El riesgo es incluso más alto para ordenadores públicos ubicados en áreas públicas de alto tráfico como centros de impresión, cafeterías, hoteles, centros fotográficos, etcétera, en los que se espera que muchos usuarios utilicen los ordenadores públicos para acceder a sus dispositivos de almacenamiento con el fin de imprimir documentos o fotografías. Una solución a este problema es dedicar una persona para que maneje el ordenador público para estos usuarios, y para que escanee sus dispositivos de almacenamiento antes de acceder a su contenido. Sin embargo, esto no es económico desde el punto de vista empresarial, y va en contra del propósito de proporcionar estos ordenadores públicos para ofrecer a los usuarios una forma de autoservicio.

Además, incluso si un usuario ejecuta un escaneado de virus o de programa maligno en sus dispositivos de almacenamiento antes de acceder a los dispositivos con el ordenador público, pueden seguir existiendo brechas de seguridad. En primer lugar, ejecutar un escaneado en los dispositivos de almacenamiento, después de conectar los dispositivos de almacenamiento a un ordenador infectado, no protege los dispositivos informáticos de ser infectados por el ordenador. En su lugar, aunque es común para los antivirus o software de detección de programas maliciosos se enviarán a cuarentena los archivos sospechosos, el ordenador en el que funciona el software sin embargo tiene que leer el archivo dentro de la memoria del ordenador y, antes de sufrir la operación de cuarentena, el ordenador puede aún sí transmitir el programa malicioso a otros dispositivos conectados al ordenador a través de interfaces de entrada/salida (I/O). En tercer lugar, dado que el antivirus o el software de detección de programas maliciosos puede sólo detectar virus y programas maliciosos que son conocidos, el software no proporciona protección cuando el programa malicioso o virus se ha creado recientemente y no es conocido.

El documento US 2010/0011442 se refiere a un dispositivo de seguridad de datos para evitar la propagación de un programa malicioso. Después de que se suministra la energía desde un dispositivo informático al dispositivo de seguridad de datos, la unidad de control de programas anti-maliciosos del dispositivo de seguridad de datos es activada, tras lo cual el dispositivo informático ejecuta de forma automática instrucciones almacenadas en el dispositivo de seguridad de datos para lanzar un mecanismo de control de programas anti-maliciosos. Después de que el mecanismo de control de programas anti-maliciosos haya sido lanzado, se permita la trasmisión de datos a través de una ruta de datos en el dispositivo de seguridad de datos. Los datos transmitidos a través de la ruta de datos son escaneados en busca de programas maliciosos incluidos en los datos.

Resumen

De acuerdo con la invención, se proporciona: un aparato para detectar una amenaza de seguridad tal y como se indica por la reivindicación 1; un método implementado por ordenador de detección de una amenaza de seguridad tal y como se indica por la reivindicación 8; y un medio legible por ordenador no transitorio tal y como se indica por la reivindicación 13.

En vista de lo anterior, es deseable proporcionar un sistema de detección de amenazas que pueda actuar como una puerta de entrada entre el ordenador público mencionado anteriormente y el dispositivo de almacenamiento privado, en donde el sistema de detección de amenazas puede detectar de forma automática amenazas de seguridad tanto para el ordenador público como para el dispositivo de almacenamiento privado, y permitir al ordenador y al dispositivo a comunicarse entre sí sólo después de determinar que ni el ordenador ni el dispositivo de almacenamiento constituyen una amenaza de seguridad.

Modos de realización de la presente divulgación proporcionan un aparato y un método robustos para detectar una amenaza de seguridad. El aparato comprende una primera interfaz de entrada/salida (I/O) y una segunda interfaz de I/O, un dispositivo de memoria que almacena un conjunto de instrucciones, y un procesador capaz de ejecutar el conjunto de instrucciones. En algunos modos de realización, el procesador es capaz de ejecutar el conjunto de instrucciones para provocar que el aparato detecte que un primer dispositivo está conectado con la primera interfaz

I/O, y en respuesta a la detección de que el primer dispositivo está conectado con la primera interfaz de I/O, deshabilite de forma temporal la comunicación de datos entre la primera y la segunda interfaces de I/O. El procesador también es capaz de ejecutar un conjunto de instrucciones para provocar que el aparato adquiera un archivo del primer dispositivo detectado a través de la primera interfaz de I/O, para determinar si el archivo adquirido constituye una amenaza de seguridad, y en respuesta a la determinación de que el archivo adquirido no constituye una amenaza de seguridad, habilitar la comunicación de datos entre la primera y segunda interfaces de I/O. Deshabilitando la comunicación de datos entre la primera y segunda interfaces de I/O, se puede reducir la probabilidad de una transmisión inadvertida de software dañino que constituye la amenaza de seguridad, antes de que se descubra su naturaleza dañina.

En algunos modos de realización, después de adquirir un archivo desde la primera interfaz detectada a través de la primera interfaz de I/O y antes de que la comunicación de datos entre la primera y segunda interfaces sea habilitada, el aparato también puede detectar una petición para comunicar datos a la segunda interfaz de I/O, y en respuesta a adquirir dicha petición, determinar que el primer dispositivo detectado constituye una amenaza de seguridad. En algunos modos de realización, al aparato también puede detectar que un segundo dispositivo está conectado con la segunda interfaz de I/O, y determinar si el segundo dispositivo detectado envía datos al aparato a través de la segunda interfaz de I/O antes de que se habilite la comunicación de datos entre la primera y segunda interfaces de I/O. Si este es el caso, el aparato puede determinar que el segundo dispositivo también constituye una amenaza de seguridad. Detectando una petición para enviar datos a las interfaces de I/O antes de que se habilite la comunicación de datos entre la primera y segunda interfaces de I/O, la detección de una amenaza de seguridad puede llegar a ser más robusta.

Aspectos adicionales relacionados con los modos de realización se establecerán en parte en la descripción que sigue, y en parte serán obvios a partir de la descripción, o se pueden aprender llevando a la práctica la invención.

Se ha de entender que tanto la descripción general anterior como la descripción detallada siguiente son únicamente ejemplares y explicativas y no son restrictivas de la invención, tal y como se reivindica.

Breve descripción de los dibujos

La figura 1 es un diagrama de bloques de un sistema de ejemplo dentro del cual se pueden utilizar modos de realización descritos en el presente documento.

La figura 2 es un diagrama de bloques de un sistema de ejemplo para escaneado y aislamiento de un dispositivo de almacenamiento externo.

La figura 3 es un diagrama que representa un quiosco de ejemplo para escaneado y aislamiento de un dispositivo de almacenamiento externo.

La figura 4 es un diagrama de flujo que representa un método de ejemplo realizado con un dispositivo electrónico para escaneado y aislamiento de un dispositivo de almacenamiento externo.

Descripción detallada

Se hará a continuación referencia en detalle a los modos de realización de ejemplo, que son ilustrados en los dibujos que acompañan. Siempre que sea posible, se utilizarán las mismas referencias numéricas a través de todos los dibujos para referirse a partes iguales o similares.

La figura 1 es un diagrama de bloques de un sistema 100 de ejemplo dentro del cual se pueden utilizar modos de realización descritos en el presente documento. Tal y como se muestra en la figura 1, el sistema 100 incluye un sistema 110 anfitrión, un sistema 120 de detección de amenazas, y un dispositivo 130 de almacenamiento, donde el dispositivo 130 de almacenamiento puede comunicarse con el sistema 110 anfitrión a través del sistema 120 de detección de amenazas. El dispositivo 130 de almacenamiento puede ser cualquier dispositivo que pueda almacenar datos. En algunos modos de realización, el dispositivo 130 de almacenamiento puede ser un dispositivo de almacenamiento no volátil autónomo, que incluye pero no limitado a SD, Memory Stick™, un dispositivo de memoria flash, un SSD, un disco duro portátil, etcétera. El dispositivo 130 de almacenamiento pueda también ser parte de un sistema (por ejemplo, un disco duro de un ordenador). El sistema 110 anfitrión puede ser un sistema con un procesador, y un dispositivo de memoria para almacenar instrucciones que se van a ejecutar por el procesador, y puede acceder a una red 150. La red 150 puede ser una red de comunicación. Ejemplos de redes de comunicación incluyen una red de área local ("LAN"), y una red de área amplia ("WAN"), por ejemplo, Internet.

El sistema 110 anfitrión puede estar configurado para, por ejemplo, adquirir un archivo del dispositivo 130 de almacenamiento y proporcionar los datos del archivo a otras aplicaciones tal como para una impresión o una visualización. Si el dispositivo 130 de almacenamiento se permite que se conecte directamente al sistema 110 anfitrión, y si el dispositivo 130 de almacenamiento es infectado con un programa malicioso, el programa malicioso que reside en el dispositivo 130 de memoria puede copiarse a sí mismo en la memoria del sistema 110 anfitrión y puede provocar que el procesador de sistema 110 anfitrión propague, por ejemplo, el programa malicioso a otros ordenadores conectados a la red 150. De forma inversa, si el sistema 110 anfitrión es infectado con un programa malicioso, el programa malicioso puede también copiarse a sí mismo en el dispositivo 130 de almacenamiento.

El sistema 120 de detección de amenazas actúa como una puerta de entrada entre el sistema 110 anfitrión y el dispositivo 130 de almacenamiento, para evitar que virus informáticos, programas maliciosos o cualquier otro archivo informático que constituyen una amenaza de seguridad, sean transferidos entre el sistema 110 anfitrión y el dispositivo 130 de almacenamiento. En algunos modos de realización, el sistema 120 de detección de amenazas escanea el dispositivo 130 de almacenamiento para localizar virus y/o programas maliciosos, basándose en uno o más archivos de configuración pre-almacenados en el sistema 120 de detección de amenazas. Dichos archivos de configuración pueden incluir información de firmas de amenazas que incluyen atributos de archivo de virus informáticos y programas maliciosos conocidos. El sistema 120 de detección de amenazas también detecta actividades sospechosas originadas desde el dispositivo 130 de almacenamiento o desde el sistema 110 anfitrión. Dichas actividades sospechosas pueden incluir, por ejemplo, intentos por parte del dispositivo 130 de almacenamiento de acceder al sistema 110 anfitrión, o viceversa, cuando el dispositivo 130 de almacenamiento y el sistema 110 anfitrión no debieran iniciar la comunicación entre si mientras el sistema 120 de detección de amenazas está sufriendo el escaneado y la detección. Una vez que el sistema 120 de detección de amenazas completa el escaneado y la detección, y confirma que el sistema 110 anfitrión y el dispositivo 130 no constituyen una amenaza de seguridad, el sistema 120 de detección de amenazas permite al sistema 110 anfitrión y el dispositivo 130 a comunicarse entre sí. Tal y como se expondrá posteriormente, el sistema 120 de detección de amenazas incluye un procesador, y un dispositivo de memoria para almacenar un conjunto de instrucciones para provocar que el procesador lleve a cabo el escaneado de virus y de programas maliciosos, la detección de actividades sospechosas, y el aislamiento del dispositivo 130 de almacenamiento. Aunque en la figura 1 el sistema 120 de detección de amenazas está conectado a sólo un dispositivo 130 de almacenamiento, se entenderá que el sistema 120 de detección puede estar conectado a múltiples dispositivos.

En algunos modos de realización, el sistema 100 además incluye un primer sistema 160 remoto y un segundo sistema 170 remoto, los cuales ambos comunican con el sistema 110 anfitrión a través de la red 150. Ambos sistemas 160 y 170 pueden ser un ordenador similar al sistema 110 anfitrión. El sistema 160 puede ser utilizado para actualizar los archivos de configuración almacenados en el sistema 120 de detección de amenazas, que incluyen los archivos que incluyen la información de la firma de amenaza. El sistema 170 se puede utilizar para actualizar los componentes de software del sistema 120 de detección de amenazas. En algunos modos de realización, cualquiera de los sistemas 160 o 170 lleva a cabo la actualización de ambos archivos de configuración y los componentes de software del sistema 120 de detección de amenazas, por ejemplo, proporcionando los archivos relevantes al sistema 110 anfitrión, que puede entonces transferir los archivos al sistema 120 de detección de amenazas.

La figura 2 es un diagrama de bloques de un sistema 200 de ejemplo para el escaneado y el aislamiento de un dispositivo de almacenamiento externo. En algunos modos de realización, el sistema 120 de detección de amenazas de la figura 1 puede incluir características similares al sistema 200. Tal y como se muestra en la figura 2, el sistema 200 incluye interfaces 210 y 212 de salida/entrada (I/O), un procesador 220 y un dispositivo 230 de memoria. En algunos modos de realización, cada una de las interfaces 210 y 212 de I/O permite la transferencia de datos entre el sistema 200 y un dispositivo externo (por ejemplo, el dispositivo 130 de almacenamiento y el sistema 110 anfitrión de la figura 1) de acuerdo con un estándar de I/O especifico. Dicho estándar de I/O puede incluir pero no está limitado a: un Bus de Serie Universal (USB), un Secure Digital de entrada salida (SDIO), una Interfaz Multimedia de Alta Definición (HDMI) Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) 1934, etcétera. En algunos modos de realización, cada interfaz de I/O incluye un conector (no mostrado) utilizado para conectar físicamente con uno de, el dispositivo 130 de almacenamiento y el sistema 110 anfitrión, y además incluye circuitería y sistemas para soportar las funcionalidades de la interfaz de I/O. Aunque sólo se muestran dos interfaces de I/O en la figura 2, se entiende que el sistema 200 puede incluir más de dos interfaces de I/O. Como un ejemplo ilustrativo, las interfaces 210 y 212 de I/O pueden estar conectadas, respectivamente, al sistema 110 anfitrión y al dispositivo 130 de almacenamiento.

Cada una de las interfaces 210 y 212 de I/O puede ser controlada por el procesador 220 cuando ejecuta un programa 240 de software almacenado en el dispositivo 230 de memoria. El programa 240 de software incluye varios módulos que incluyen pero no están limitados a: un módulo 241 de escaneado de archivos, un módulo 242 de detección de actividad, un módulo 243 de acceso a interfaces de I/O, y un módulo 244 de indicación de estado. En algunos modos de realización, el programa 240 de software puede estar escrito utilizando un lenguaje de programación Java™. Los archivos de código fuente pueden ser compilados en códigos de bytes de Java™. El dispositivo 230 de memoria puede estar precargado con una máquina virtual de Java™ (no mostrada en la figura 2) para interpretar adicionalmente los códigos de bytes compilados para generar el lenguaje máquina, que después se pueden ejecutar mediante el procesador 220. Se ha de entender que el programa 240 software puede ser escrito utilizando otros lenguajes informáticos distintos del Java™ y puede que no requiera un dispositivo 230 de memoria para estar precargado con una máquina virtual.

El módulo 241 de escaneado de archivos adquiere la información de los archivos almacenados en el dispositivo 130 de almacenamiento a través de la interfaz 212 de I/O. En algunos modos de realización, el módulo 241 de escaneado adquiere la información sobre una estructura de directorios de los archivos almacenados en el dispositivo de almacenamiento. La información puede incluir una lista de los archivos, la ubicación de los archivos, la jerarquía de la estructura de directorios, etcétera. Basándose en la estructura de directorios, el módulo 241 de escaneado comprueba los atributos de cada uno de los archivos almacenados en el dispositivo 130 de almacenamiento para la amenaza de seguridad.

El módulo 242 de detección de actividad detecta tráfico en las interfaces de I/O, o una petición para enviar datos a las interfaces de I/O, y determina si dicho tráfico o petición son inesperados. En algunos casos, dicho tráfico o petición pueden indicar que un dispositivo almacenamiento está siendo conectado a la interfaz de I/O (por ejemplo, después de detectar una señal de establecimiento de comunicación). En algunos casos, dicho tráfico o petición pueden señalar la existencia de virus informáticos o programas maliciosos, cuando nos espera que suceda ningún tráfico o petición. Como un ejemplo ilustrativo, cuando el sistema 200 está leyendo los archivos del dispositivo 130 de almacenamiento a través de la interfaz 212 de I/O, puede no esperar detectar tráfico en la interfaz 210 de I/O, o solicitar enviar datos a la interfaz 210 de I/O. Esto puede ser debido, por ejemplo, a que sistema 200 no espera que el sistema 110 anfitrión inicie la trasmisión de datos al dispositivo 130 de almacenamiento, dado que el usuario está intentando utilizar el sistema 110 anfitrión para acceder al dispositivo 130 de almacenamiento, no a la inversa. Además el sistema 200 tampoco espera que el sistema 110 anfitrión solicite datos del dispositivo 130 de almacenamiento (y el dispositivo 130 de almacenamiento también debería no estar enviando datos al sistema 110 anfitrión sin recibir dicha petición), hasta que el sistema 110 anfitrión reciba una indicación del sistema 200 de que el dispositivo 130 de almacenamiento está libre de amenazas de seguridad, y el sistema 200 no ha enviado dicha indicación. Por lo tanto, la detección de tráfico de la interfaz 210 de I/O o una petición para enviar datos a la interfaz 210 de I/O, ambos de los cuales son contrarios a lo que espera el sistema 200, puede señalar que el dispositivo 130 de almacenamiento y/o el sistema 110 anfitrión están infectados. Por ejemplo, un archivo es adquirido desde el dispositivo 130 de almacenamiento por el sistema 200, que ahora reside en el dispositivo 230 de memoria, puede incluir un ejecutable malicioso que provoca que el procesador 220 intente enviar datos dañinos a la interfaz 210 de I/O. De forma alternativa, el sistema 110 anfitrión puede estar infectado, y los virus o el programa malicioso que residen en el sistema 110 anfitrión puede intentar enviar datos dañinos a la interfaz 210 de I/O, con la intención de que los datos sean reenviados al dispositivo 130 de almacenamiento. En ambos casos, el módulo 242 de detección de actividad puede determinar que el tráfico en la interfaz 210 de I/O, o una petición para enviar datos a esa interfaz, señalan la existencia de una amenaza de seguridad.

El módulo 243 de acceso a las interfaces de I/O controla y facilita el acceso de cada una de las interfaces 210 y 212 de I/O mediante el programa 240 de software. En algunos modos de realización, el programa 240 de software implementa una política de aislamiento de un dispositivo conectado a la interfaz 212 de I/O (por ejemplo, el dispositivo 130 de almacenamiento) de otro dispositivo conectado a la interfaz 210 de I/O (por ejemplo, el sistema 110 anfitrión), mientras el módulo 241 de escaneado de archivos está llevando a cabo el escaneado. Por ejemplo, mientras el módulo 241 de escaneado de archivos está escaneando el dispositivo 130 de almacenamiento a través de la interfaz 212 de I/O, el programa 240 de software instruye al módulo 243 de acceso a las interfaces de I/O a restringir los datos que pueden alcanzar la interfaz 210 de I/O o a ignorar una petición (o bien generada dentro del sistema 200 o recibida a través de la interfaz 212 de I/O) para transmitir datos a la interfaz 210 de I/O. El módulo 243 de acceso a las interfaces de I/O también adquiere datos de la interfaz 212 de I/O y proporciona los datos a, por ejemplo, el módulo 241 de escaneado de archivos, cuando escanea los archivos. El módulo 243 de acceso a las interfaces de I/O también proporciona los datos al módulo 242 de detección de actividad, para alertar al módulo sobre el tráfico en la interfaz, o para detectar que un dispositivo externo está conectado al sistema 200. Cuando ningún otro dispositivo excepto el sistema 110 anfitrión está conectado, el programa 240 de software también instruye al módulo 243 de acceso de las interfaces de I/O a permite al sistema 110 anfitrión a acceder al sistema 200 a través de cualquiera de las interfaces de I/O con el fin de, por ejemplo, actualizar los archivos de configuración y el propio programa 240 de software.

El módulo 244 de indicación de estado proporciona información del estado sobre el escaneado o la detección de una actividad sospechosa para mostrar. En algunos modos de realización, el módulo 244 de indicación de estado recibe un resultado del escaneado del módulo 241 de escaneado, o un resultado de detección de actividad del módulo 242 de detección de actividad, y proporciona el resultado al sistema 110 anfitrión a través del módulo 243 de acceso a las interfaces de I/O, y el estado puede ser mostrado en un dispositivo de visualización conectado al sistema 110 anfitrión. En algunos modos de realización, uno o más dispositivos de salida (por ejemplo, diodos emisores de luz (LED)] también se pueden conectar a las interfaces de I/O y pueden controlarse mediante el módulo 244 de indicación de estado, a través del módulo 243 de acceso a las interfaces de I/O, para indicar un estado del escaneado o la detección de actividad sospechosa.

El dispositivo 230 de memoria también puede almacenar datos 250 utilizados para el escaneado. Los datos 250 pueden incluir datos 251 de archivos recibidos de un dispositivo que está siendo escaneado, y datos 252 de configuración, que pueden incluir las firmas o atributos de una lista de virus informáticos y programas maliciosos conocidos. Tal y como se expuso anteriormente, los datos 252 de configuración, así como cualquier porción del programa 240 de software, pueden actualizarse por otro sistema a través de las interfaces de I/O. En algunos modos de realización, los archivos de configuración se pueden crear con Lenguaje de Marcado Extensible (XML), que se puede analizar fácilmente, por ejemplo, mediante el módulo 241 de escaneado.

La figura 3 es un diagrama que representa un kiosco 300 de ejemplo para el escaneado y el aislamiento de un dispositivo de almacenamiento externo. Varias funcionalidades del kiosco 300 pueden estar provistas mediante el sistema 200 ilustrado en la figura 2. Tal y como se muestra en la figura 3, el kiosco 300 incluye una interfaz 310 de visualización, que incluye indicadores 312, 314 y 316. Cada indicador puede ser un LED u otro dispositivo de iluminación, y está conectado a las interfaces de I/O el sistema 200. Cada indicador puede ser activado para indicar un estado del escaneado del dispositivo de almacenamiento externo. Por ejemplo, el indicador 312 puede ser activado para indicar que las firmas de amenaza de seguridad almacenadas en el sistema 200, utilizadas para detectar si un archivo almacenado en el dispositivo de almacenamiento interno porta una amenaza de seguridad, está actualizado.

El indicador 314 puede activarse para indicar que el escaneado del dispositivo externo se ha completado, y que no se detecta ninguna amenaza en el dispositivo externo, por lo tanto la transferencia de archivos desde el dispositivo externo se habilita. El indicador 316 también puede activarse para indicar que durante el escaneado del dispositivo externo, se ha detectado una amenaza de seguridad.

El kiosco 300 además incluye conectores 320 y 330. Los conectores 320 y 330 pueden conectarse respectivamente a, por ejemplo, las interfaces 210 y 212 de I/O del sistema 200, y se pueden gestionar mediante el módulo 243 de acceso a las interfaces de I/O del sistema 200. Los conectores 320 incluyen una colección de conectores hembra para diferentes estándares de I/O, tal como USB, SDIO, HDMI, IEEE 1394, etcétera. Los conectores 320 permiten a un usuario conectar un dispositivo de almacenamiento autónomo con un conector macho, tal como una unidad de enlace USB o una tarjeta SD, con el kiosco 300 (y el sistema 200). Los conectores 330 incluyen una conexión de conectores macho para los estándares de I/O mencionados anteriormente. Los conectores 330 permiten a un usuario conectar el kiosco, por ejemplo, a un ordenador con un disco duro, o cualquier otro dispositivo de almacenamiento autónomo con un conector hembra. A través de los conectores 320 y 330 el sistema 200 escanea amenazas de seguridad en el dispositivo de almacenamiento, y después envía un estado del escaneado a través de los indicadores de la interfaz 310 de visualización.

La figura 4 es un diagrama de flujo que representa un método 400 de ejemplo realizado mediante un dispositivo electrónico por ejemplo, el sistema de detección de amenazas de la figura 1, y el sistema 200 de la figura 2) para el escaneado y el aislamiento de un dispositivo de almacenamiento externo. Aunque el diagrama de flujo divulga las siguientes etapas en un orden particular, se apreciará que al menos alguna de las etapas se puede mover, modificar o eliminar donde sea apropiado, en consistencia con las enseñanzas de la presente divulgación. Y aunque las siguientes etapas son indicadas siendo realizadas por un dispositivo electrónico, se aprecia que las etapas se pueden realizar por más de un dispositivo electrónico. Por propósitos de ilustración únicamente, para la siguiente descripción se asume que el dispositivo electrónico del sistema 200 de la figura 2, y que el sistema 110 anfitrión de la figura 1 están conectados a la interfaz 210 de I/O de la figura 2.

En la etapa 402, el dispositivo electrónico confirma que sus datos de configuración almacenados (por ejemplo, los datos 252 de configuración de la figura 2) están actualizados. Los datos de configuración pueden incluir una lista de las firmas de amenaza de seguridad más actualizadas, y pueden estar asociados con una fecha. El dispositivo electrónico confirma que los datos de configuración están actualizados, por ejemplo, comunicando con otros sistemas abre paréntesis por ejemplo, sistemas 160 y/o 170 remotos en la figura 1) para confirmar que sus datos de configuración están actualizados, basándose en la fecha asociada con los datos de configuración, y si no, adquirir los datos de configuración actualizados de estos sistemas. En algunos modos de realización, la etapa 402 se puede omitir si, por ejemplo, los datos de configuración almacenados en el dispositivo electrónico son actualizados manualmente con los últimos datos.

En la etapa 404, el dispositivo electrónico detecta que el dispositivo 130 de almacenamiento en la figura 1, está conectado a una de sus interfaces de I/O disponibles (por ejemplo, la interfaz 212 de I/O en la figura 2). La detección se puede realizar mediante, por ejemplo, la detección de una señal de establecimiento de comunicación iniciada por el dispositivo de almacenamiento en la interfaz de I/O.

En la etapa 406, después de detectar que el dispositivo 130 de almacenamiento está conectado a una de sus interfaces de I/O, el dispositivo electrónico deshabilita la trasmisión de datos a todas las otras interfaces de I/O, excepto la interfaz 212 de I/O. Esto es para evitar que archivos dañinos almacenados en el dispositivo 130 de almacenamiento, si los hubiera, accedan a otros dispositivos conectados al dispositivo electrónico. La des habilitación se puede lograr, por ejemplo, ignorando de forma activa una petición (o bien generada dentro del dispositivo electrónico, o recibida a través de una interfaz de I/O) para trasmitir datos a todas las otras interfaces de I/O. En algunos modos de realización, la deshabilitación se puede llevar a cabo mediante el módulo 243 de acceso a las interfaces de I/O en la figura 2.

En la etapa 408, después de deshabilitar la trasmisión de datos a todas las otras interfaces de I/O en la etapa 406, el dispositivo electrónico detecta si hay un tráfico de I/O inesperado originado desde el sistema 110 anfitrión. Dicho tráfico de I/O puede ser o bien una petición del sistema 110 anfitrión para adquirir datos del dispositivo 130 de almacenamiento, o un intento del sistema 110 anfitrión para enviar datos al dispositivo 130 de almacenamiento. Para el primer caso, el dispositivo electrónico no espera tráfico de I/O desde el sistema 110 anfitrión debido a que, por ejemplo, el usuario está intentando utilizar el sistema 110 anfitrión para acceder al dispositivo 130 de almacenamiento, no a la inversa. Para el segundo caso, el dispositivo electrónico tampoco espera que el sistema 110 anfitrión adquiera datos del dispositivo 130 de almacenamiento hasta que recibe una indicación del dispositivo electrónico de que el dispositivo 130 de almacenamiento está libre de amenazas de seguridad y el dispositivo electrónico no ha enviado dicha indicación. La detección se puede realizar mediante, por ejemplo, el módulo 242 de detección de actividad de la figura 2. En respuesta a dicha detección del tráfico de I/O, el dispositivo electrónico determina que hay una amenaza de seguridad, potencialmente constituida por el sistema 110 anfitrión, y puede llevar a cabo la etapa 410 para enviar una amenaza de seguridad. Los datos de dicho informe se pueden generar mediante el módulo 244 de indicación de estado. Por otro lado, si el dispositivo electrónico no detecta ningún tráfico de I/O inesperado originado del sistema anfitrión, el dispositivo electrónico puede llevar a cabo la etapa 412.

En la etapa 412, el dispositivo electrónico adquiere un archivo del dispositivo 130 de almacenamiento. En algunos modos de realización, el dispositivo electrónico puede adquirir información sobre una estructura de directorios de los archivos almacenados en el dispositivo 130 de almacenamiento, y después adquirir los archivos de acuerdo con la información. Los datos de archivo adquiridos pueden ser almacenados de forma temporal en la memoria del dispositivo electrónico.

En la etapa 414, después de que los datos de archivo son adquiridos, el dispositivo electrónico analiza atributos del archivo para la amenaza de seguridad. En algunos modos de realización, el dispositivo electrónico compara la firma u otros atributos del archivo con respecto a atributos correspondientes de una lista de virus y programas maliciosos conocidos de los datos de configuración actualizados en la etapa 402.

En la etapa 416, el dispositivo electrónico determina si el archivo constituye una amenaza de seguridad basándose en un resultado del análisis en la etapa 414. Si el análisis indica que el archivo constituye una amenaza de seguridad, el dispositivo electrónico puede llevar a cabo la etapa 410 para informar de una amenaza de seguridad. Por otro lado, si el análisis no indica que el archivo constituye una amenaza de seguridad, el dispositivo electrónico puede llevar a cabo la etapa 418. En algunos modos de realización, las etapas 412 a 416 son llevadas a cabo por el módulo 241 de escaneado de archivos de la figura 2.

En la etapa 418, el dispositivo electrónico determina si hay una petición de I/O inesperada generada por el propio dispositivo electrónico. Por ejemplo, el dispositivo electrónico puede que no espere recibir una petición para enviar datos al sistema 110 anfitrión a través de la interfaz 210 de I/O (conectada al sistema 110 anfitrión) mientras que está procesando el archivo del dispositivo 130 de almacenamiento a través de la interfaz 212 de I/O. Esto puede ser debido a que, por ejemplo, el dispositivo 130 de almacenamiento no debería enviar datos al sistema 110 anfitrión sin primero recibir una petición de datos del sistema 110 anfitrión, y el dispositivo electrónico ha verificado que el sistema 110 anfitrión no ha enviado dicha petición en la etapa 408. Una petición para enviar datos a través de la interfaz 210 de I/O se puede detectar mediante, por ejemplo, el módulo 242 de detección de actividad de la figura 2. Si dicha petición es detectada, el dispositivo electrónico puede llevar a cabo la etapa 410 para informar de una amenaza de seguridad. Si dicha petición no es detectada, el dispositivo electrónico puede llevar a cabo la etapa 420 comprobando si todos los archivos han sido escaneados basándose en, por ejemplo, la información sobre la estructura de directorios de los archivos almacenada en el dispositivo 130 de almacenamiento. Si todos los archivos son escaneados, el dispositivo electrónico puede llevar a cabo la etapa 422, donde los dispositivos electrónicos permitan al dispositivo 130 de almacenamiento a comunicarse con el sistema 110 anfitrión. Si hay archivos restantes que no han sido escaneados, el dispositivo electrónico volverá a la etapa 412 para adquirir el siguiente archivo en la estructura de directorios, y repetir el análisis de acuerdo con las etapas 412 hasta 418, hasta que han sido escaneados todos los archivos.

En la memoria descriptiva anterior, se han descrito modos de realización con referencia a numerosos detalles específicos que pueden variar de una implementación a otra implementación. Se pueden realizar ciertas adaptaciones y modificaciones de los modos de realización descritos. Otros modos de realización pueden ser evidentes para los expertos en la técnica a partir de la consideración de la memoria descriptiva y la práctica de la invención divulgada en el presente documento. Se pretende que la memoria descriptiva y los ejemplos sean considerados únicamente como ejemplo, con un alcance verdadero de la invención que está indicado por las siguientes reivindicaciones. También se pretende que la secuencia de etapas mostradas en las figuras tanga sólo propósitos ilustrativos y no se pretende que esté limitada a cualquier secuencia de etapas particular. Como tal, los expertos en la técnica pueden apreciar que estas etapas se pueden realizar en un orden diferente siempre que implementen el mismo método.

REIVINDICACIONES

1. Un aparato (120) para detectar una amenaza de seguridad, el aparato que comprende:

una primera interfaz (212) de entrada/salida y una segunda interfaz (210) de entrada/salida;

un dispositivo (230) de memoria que almacena un conjunto de instrucciones; y

un procesador (220) configurado para ejecutar el conjunto de instrucciones para provocar que el aparato:

detecte (404) que un primer dispositivo (130) está conectado con la primera interfaz (212) de entrada/salida;

en respuesta a la detección de que el primer dispositivo (130) está conectado con la primera interfaz (212) de entrada/salida, deshabilite, de forma temporal, (406) la comunicación de datos entre la primera y segunda interfaces (212, 210) de entrada/salida;

adquiera (412) un archivo del primer dispositivo (130) detectado a través de la primera interfaz (212) de entrada/salida;

analice (414) atributos del archivo y determine (416) si el archivo adquirido constituye una amenaza de seguridad;

monitorice una petición para comunicar datos a la segunda interfaz (210) de entrada/salida;

en respuesta a detectar (418) una petición para comunicar datos a la segunda interfaz (210) de entrada/salida, determine que el primer dispositivo (130) constituye una amenaza de seguridad; y

en respuesta a una determinación de que el archivo adquirido y el primer dispositivo (130) no constituyan una amenaza de seguridad, habilite (422) la comunicación de datos

entre la primera y segunda interfaz (212, 210) de entrada/salida, en donde la monitorización tiene lugar después de la adquisición (412) del archivo y antes de la habilitación (422) de la comunicación de datos.

2. El aparato de la reivindicación 1, en donde el procesador (220) está configurado adicionalmente para ejecutar el conjunto de instrucciones para:

detectar que un segundo dispositivo (110) está conectado con la segunda interfaz (210) de entrada/salida;

determinar (408) si el segundo dispositivo (110) detectado envía datos al aparato (120) a través de la segunda interfaz (210) de entrada/salida antes de que se habilite la comunicación de datos entre la primera y segunda interfaces (212, 210) de entrada/salida; y

en respuesta a una determinación de que el segundo dispositivo detectado envía datos a la aparato (120) a través de la segunda interfaz (210) de entrada/salida antes de que se habilite la comunicación de datos entre la primera y segunda interfaces (212, 210) de entrada/salida, determinar que el segundo dispositivo (110) constituye una amenaza de seguridad.

3. El aparato de la reivindicación 1, en donde el procesador (220) está configurado adicionalmente para ejecutar el conjunto de instrucciones para:

almacenar primeros datos de configuración para determinar si el archivo adquirido constituye una amenaza de seguridad, los primeros datos de configuración que están asociados con una primera marca temporal;

basándose en la primera marca temporal, determinar si los primeros datos de configuración están actualizados; y

en respuesta a una determinación de que los primeros datos de configuración no están actualizados, adquirir segundos datos de configuración asociados con una segunda marca temporal, los segundos datos de configuración que son adquiridos para reemplazar a los primeros datos de configuración.

4. El aparato de la reivindicación 3, en donde al menos uno de los primeros y segundos datos de configuración incluyen atributos de uno o más virus informáticos y programas maliciosos.

5. El aparato de la reivindicación 1, en donde el procesador (220) está configurado adicionalmente para ejecutar el conjunto de instrucciones para:

adquirir información sobre una estructura de directorios de uno o más archivos almacenados en el primer dispositivo (130);

determinar (420) si todos los archivos almacenados en el primer dispositivo (130) han sido adquiridos, basándose en la información adquirida sobre la estructura de directorios; y

en respuesta a una determinación de que todos los archivos almacenados en el primer dispositivo (130) han sido adquiridos, y que ninguno de los archivos adquiridos constituye una amenaza de seguridad, habilitar (422) la comunicación de datos entre la primera y segunda interfaces (212, 210) de entrada/salida.

6. El aparato de la reivindicación 1, que además comprende un primer conector y un segundo conector, el primer conector y el segundo conector que están conectados con la primera interfaz (212) de entrada/salida y con la segunda interfaz (210) de entrada/salida, respectivamente.

7. El aparato de la reivindicación 1, que además comprende uno o más dispositivos (314, 316) de salida para indicar que el aparato (120) habilita la comunicación de datos entre la primera y segunda interfaces (212, 210) de entrada/salida, y/o para indicar que un dispositivo (110, 130) conectado a la primera o segunda interfaces (212, 210) de entrada/salida constituye una amenaza de seguridad.

8. Un método (400) implementado por ordenador para detectar una amenaza de seguridad, que comprende:

detectar (404) que un primer dispositivo (130) está conectado con una primera interfaz (212) de entrada/salida;

en respuesta a la detección de que el primer dispositivo (130) está conectado con la primera interfaz (212) de entrada/salida, deshabilitar, de forma temporal (406) la comunicación de datos entre la primera interfaz (212) de entrada/salida y una segunda interfaz (210) de entrada/salida;

adquirir (412) un archivo del primer dispositivo (130) detectado a través de la primera interfaz (212) de entrada/salida;

analizar (414) atributos del archivo adquirido y determinar (416) si el archivo adquirido constituye una amenaza de seguridad;

monitorizar una petición para comunicar datos a la segunda interfaz (210) de entrada/salida;

en respuesta a la detección (418) de una petición para comunicar datos a la segunda interfaz (210) de entrada/salida, determinar que el primer dispositivo (130) constituye una amenaza de seguridad; y

en respuesta a determinar que el archivo adquirido y el primer dispositivo (130) no constituyen una amenaza de seguridad, habilitar (422) la comunicación de datos entre la primera y segunda interfaces (212, 210) de entrada/salida, en donde la monitorización tiene lugar después de la adquisición (412) del archivo y antes de la habilitación (422) de la comunicación de datos.

9. El método de la reivindicación 8, que además comprende:

detectar que un segundo dispositivo (110) está conectado con la segunda interfaz (210) de entrada/salida;

determinar (408) si el segundo dispositivo (110) detectado envía datos a la segunda interfaz (210) de entrada/salida antes de que se habilite la comunicación de datos entre la primera y segunda interfaces (212, 210) de entrada/salida; y

en respuesta a la determinación (408) de que el segundo dispositivo (110) detectado envía datos a la segunda interfaz (210) de entrada/salida antes de que se habilite la comunicación de datos entre la primera y segunda interfaces (212, 210) de entrada/salida, determinar que el segundo dispositivo (110) constituye una amenaza de seguridad.

10. Método de la reivindicación 8, que además comprende:

almacenar primeros datos de comunicación para determinar que el archivo adquirido constituye una amenaza de seguridad, los primeros datos de configuración que están asociados con una primera marca temporal;

basándose en la primera marca temporal, determinar si los primeros datos de configuración están actualizados; y

en respuesta a la determinación de que los primeros datos de configuración no están actualizados, adquirir segundos datos de configuración asociados con una segunda marca temporal, los segundos datos de configuración que son adquiridos para reemplazar a los primeros datos de configuración.

11. El método de la reivindicación 10, en donde al menos uno de los primeros y segundos datos de configuración incluyen atributos de uno o más virus informáticos y programas maliciosos.

12. El método de la reivindicación 8, que además comprende:

adquirir información sobre una estructura de directorios de uno o más archivos almacenados en el primer dispositivo (130);

determinar (420) si todos los archivos almacenados en el primer dispositivo (130) han sido adquiridos, basándose en la información adquirida sobre la estructura de directorios; y

en respuesta a la determinación (420) de que todos los archivos almacenados en el primer dispositivo 130) han sido adquiridos, y de que ninguno de los archivos adquiridos constituye una amenaza de seguridad, habilitar (422) la comunicación de datos entre la primera y segunda interfaces (212, 210) de entrada/salida.

13. Un medio legible por ordenador no transitorio que almacena un conjunto de instrucciones que se pueden ejecutar por al menos un procesador de un dispositivo electrónico para provocar que el dispositivo electrónico realice el método de cualquiera de las reivindicaciones 8 a 12.

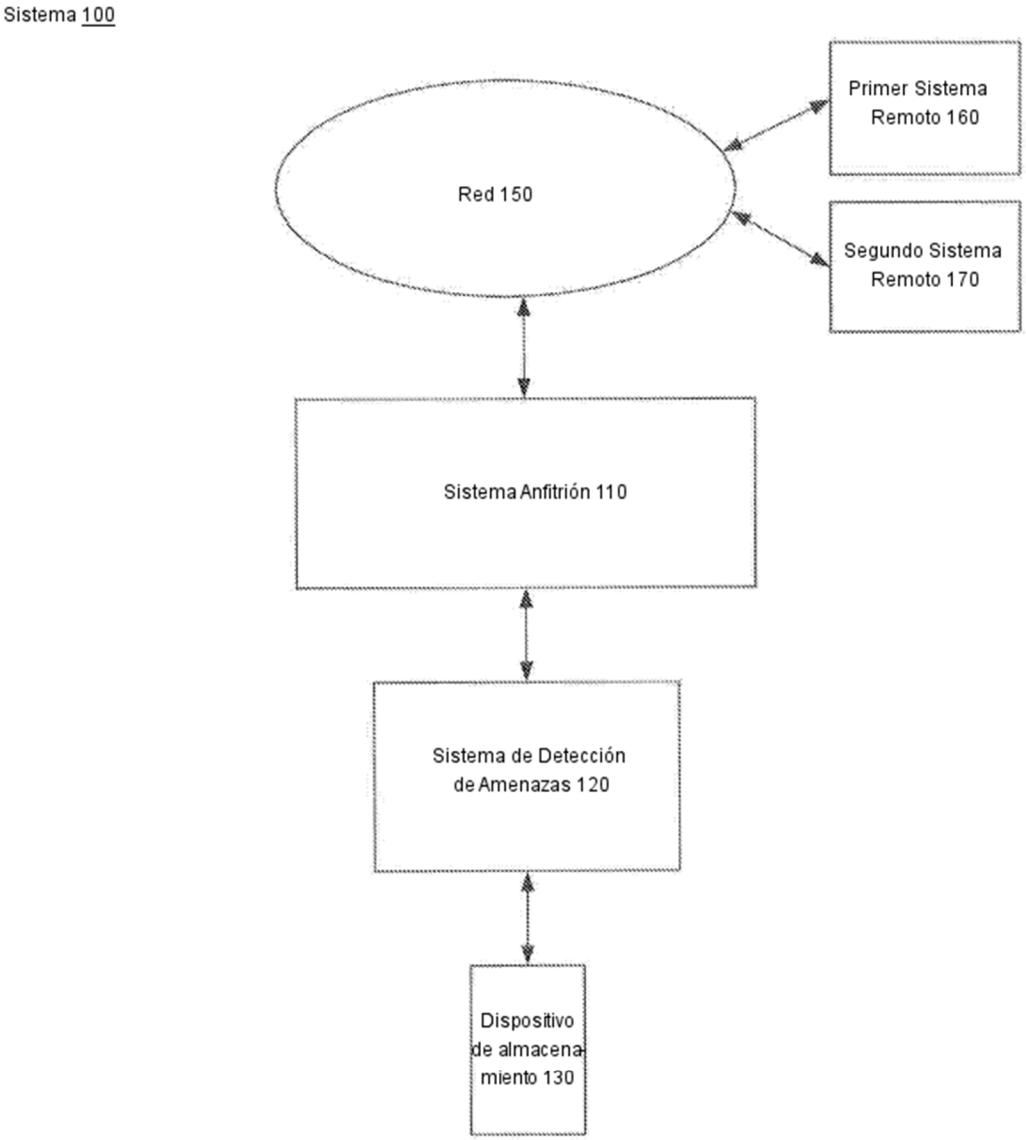
Sistema 100
Red 150
Primer Sistema Remoto 160
Segundo Sistema Remoto 170
Sistema Anfitrión 110
Sistema de Detección de Amenazas 120
Dispositivo de almacenamiento 130

FIG. 1

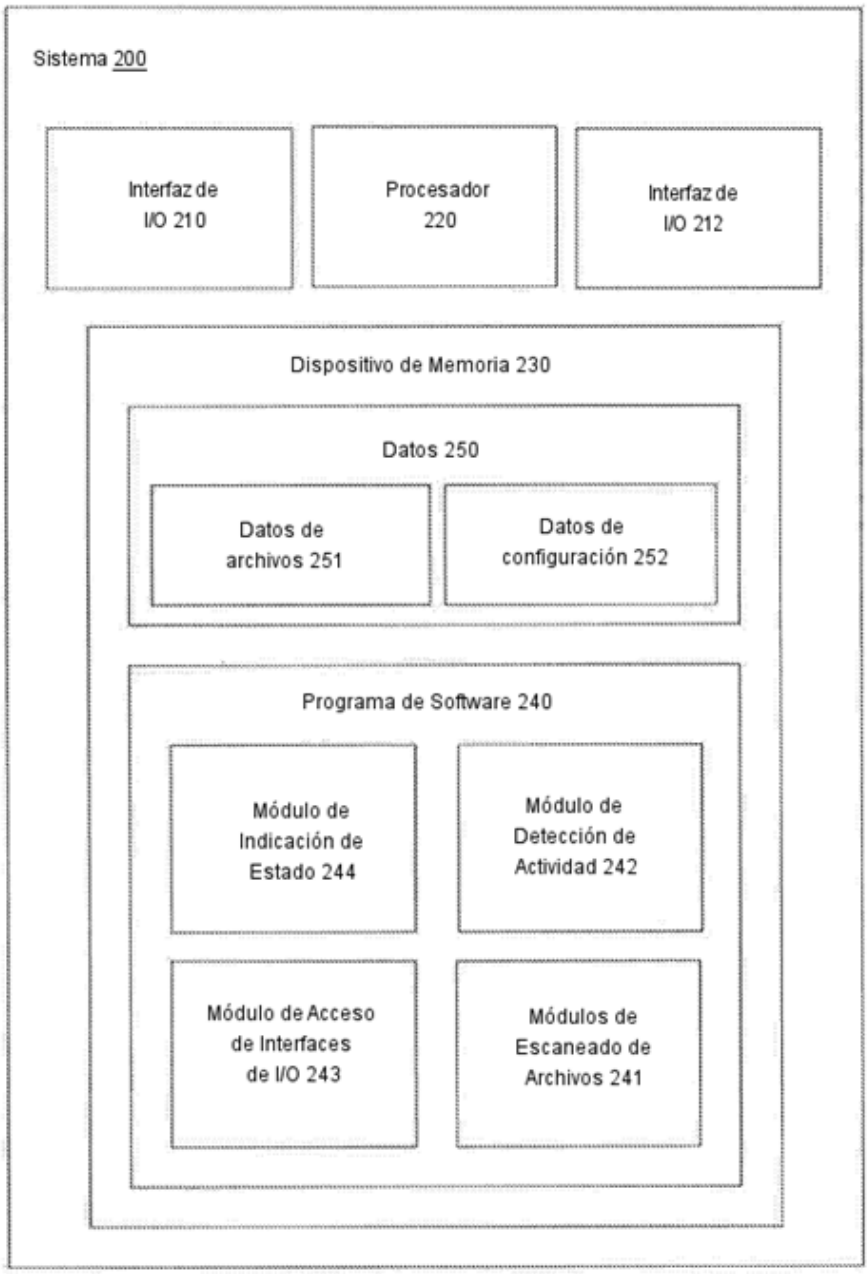
Sistema 200
Interfaz de I/O 210
Procesador 220
Interfaz de I/O 212
Dispositivo de Memoria 230
Datos 250
Datos de archivos 251
Datos de configuración 252
Programa de Software 240
Módulo de Indicación de Estado 244
Módulo de Detección de Actividad 242
Módulo de Acceso de Interfaces de I/O 243
Módulos de Escaneado de Archivos 241

FIG. 2

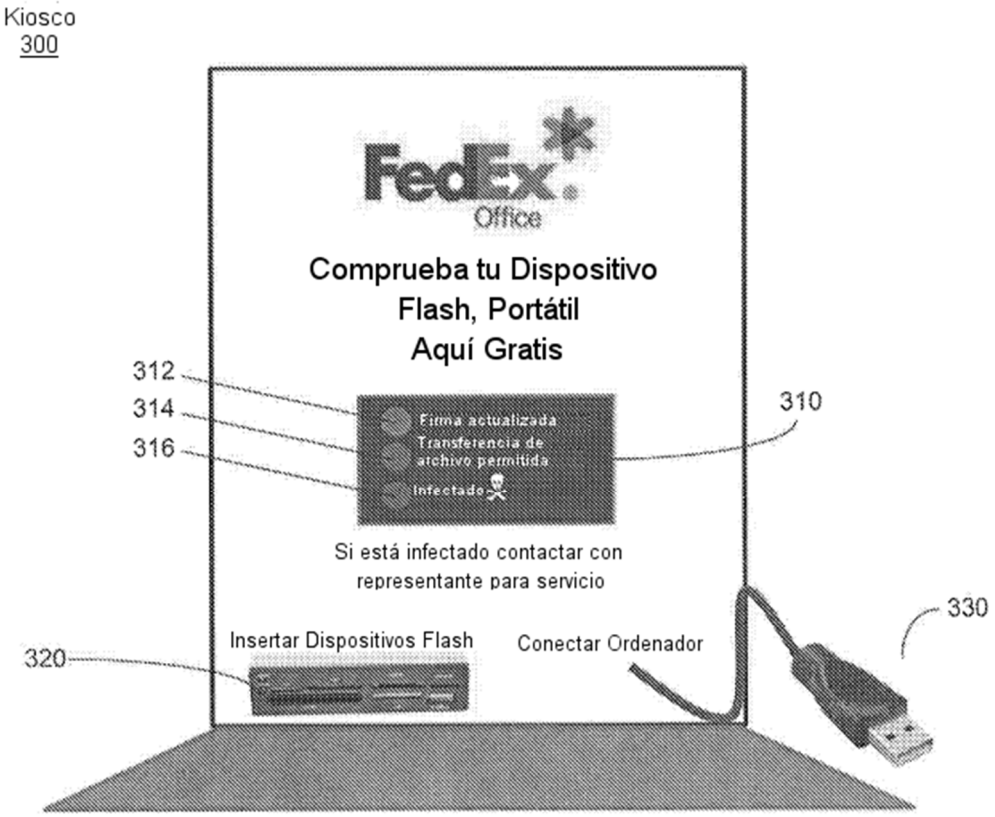
Kiosco
300
FedEx Office
Comprueba tu Dispositivo
Flash, Portátil
Aquí Gratis
312
314
316
310
Firma actualizada
Transferencia de archivo permitida
Infectado
Si está infectado contactar con representante para servicio
330
320
Insertar Dispositivos Flash
Conectar Ordenador

FIG. 3

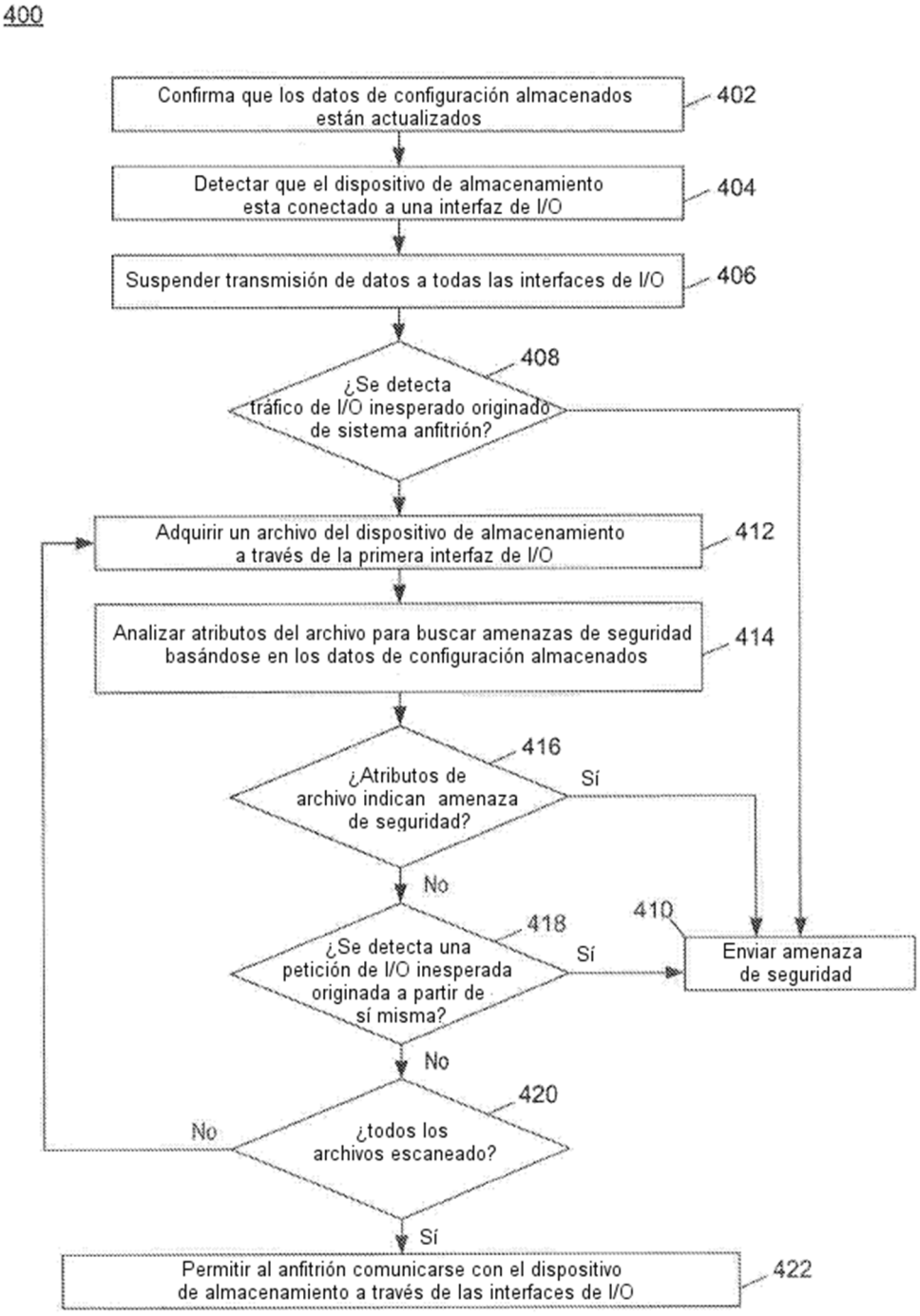
400
Confirma que los datos de configuración almacenados están actualizados
402
Detectar que el dispositivo de almacenamiento esta conectado a una interfaz de I/O
404
Suspender transmisión de datos a todas las interfaces de I/O
406
¿Se detecta tráfico de I/O inesperado originado de sistema anfitrión?
408
Adquirir un archivo del dispositivo de almacenamiento a través de la primera interfaz de I/O
412
Analizar atributos del archivo para buscar amenazas de seguridad basándose en los datos de configuración almacenados
414
¿Atributos de archivo indican amenaza de seguridad?
416
Sí
No
¿Se detecta una petición de I/O inesperada originada a partir de sí misma?
418
Sí
410
Enviar amenaza de seguridad
No
¿todos los archivos escaneado?
420
No
Sí
Permitir al anfitrión comunicarse con el dispositivo de almacenamiento a través de las interfaces de I/O
422

FIG. 4