

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 936 860**

51 Int. Cl.:

H04L 9/40 (2012.01)

G06F 21/56 (2013.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **08.08.2018 PCT/US2018/045814**

87 Fecha y número de publicación internacional: **14.02.2019 WO19032702**

96 Fecha de presentación y número de la solicitud europea: **08.08.2018 E 18844091 (1)**

97 Fecha y número de publicación de la concesión europea: **14.12.2022 EP 3665573**

54 Título: **Prevención en tiempo real de contenido malicioso a través de un análisis dinámico**

30 Prioridad:

08.08.2017 US 201715671445

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

22.03.2023

73 Titular/es:

**SONICWALL INC. (100.0%)
1033 McCarthy Blvd.
Milpitas, CA 95035, US**

72 Inventor/es:

**CHEETANCHERI, SENTHIL;
DUBROVSKY, ALEX y
HOLAGI, SACHIN**

74 Agente/Representante:

COBO DE LA TORRE, María Victoria

ES 2 936 860 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Prevención en tiempo real de contenido malicioso a través de un análisis dinámico

5 Antecedentes de la invención

Ámbito de la invención

(0001) La presente invención hace referencia, en general, a la identificación de si los datos transmitidos entre diferentes sistemas informáticos incluyen contenido malicioso. Más específicamente, la presente invención hace referencia a la identificación de si el software malicioso está incluido en uno o más paquetes de datos transmitidos desde un primer ordenador a un segundo ordenador.

Descripción de la técnica relacionada

(0002) Una de las mayores amenazas a la privacidad y para asegurar los datos informáticos hay varios tipos de software malicioso informático, tales como virus o software de intercepciones. Generalmente, el software malicioso puede ser cualquier tipo de programa de software que incluye un código que ejecuta sin el conocimiento o la autorización de un propietario o usuario de un dispositivo informático.

(0003) El software malicioso se distribuye normalmente por partes que tienen una intención nefasta. El software malicioso se usa comúnmente para robar o destruir datos informáticos o para curiosear o espiar las acciones de un usuario cuando el usuario está usando un ordenador. El software malicioso también se usa frecuentemente para dañar un ordenador o para dañar datos informáticos. Por ejemplo, el software malicioso puede usarse para robar información personal o financiera, para chantajear a los usuarios del ordenador denegando el acceso a sus propios datos a cambio de o hasta que se pague un importe, o para dañar los ordenadores infectados dañando los datos almacenados en dichos ordenadores infectados.

(0004) Además, el software malicioso desarrollado recientemente es cada vez más difícil de identificar. Frecuentemente, hasta que un tipo particular de software malicioso ha sido identificado y caracterizado, las técnicas convencionales que identifican si una comunicación incluye software malicioso puede fallar detectando la presencia de dicho software malicioso en la comunicación. Esto puede ocurrir cuando la información en uno o más paquetes de datos recibidos está oculta o cuando el software malicioso no se puede identificar mediante una firma asociada a la información en los paquetes de datos recibidos.

(0005) Habida cuenta que los datos informáticos son transmitidos frecuentemente desde un ordenador a otro ordenador a través de uno o más paquetes de datos, los paquetes de datos normalmente se escanean para detectar software malicioso con un cortafuego, un dispositivo de red o en un ordenador de un usuario, antes de que puedan ser recibidos o ejecutados en un dispositivo de usuario. Los métodos de escaneo, tales como la inspección profunda de paquetes (DPI) no son capaces de identificar las nuevas amenazas de software malicioso, habida cuenta que los mismos se basan en una concordancia de patrones que identifica los atributos o las firmas de los datos informáticos maliciosos que han sido previamente identificados y caracterizados. De este modo, los métodos convencionales para identificar si un conjunto de paquetes de datos recibido incluye software malicioso puede ser incapaz de identificar una nueva amenaza de software malicioso.

(0006) Lo que se necesita son nuevos métodos y sistemas que identifiquen las amenazas de software malicioso, que no se han encontrado antes, a través de la simulación del comportamiento dinámico de la amenaza en cuestión y, al mismo tiempo, que aseguren la prevención/ el bloqueo en tiempo real de semejantes amenazas, no quedando limitados sólo a la detección y a cortar las amenazas.

(0007) La Publicación de la Solicitud de Patente de E.E.U.U. nº US 2006/0224724 A1 manifiesta técnicas para proteger un ordenador de software malicioso. En particular, se proporciona un método implementado informáticamente para identificar el software malicioso en un punto de tránsito de red (por ejemplo, una puerta (en inglés: "gateway"). Cuando en una transmisión se recibe un paquete en el punto de tránsito de red, el paquete se traslada inmediatamente al ordenador de destino. Simultáneamente, el paquete y otros datos en la transmisión son escaneados para detectar software malicioso mediante un motor de antivirus. Si el software malicioso se identifica en la transmisión, al ordenador de destino se le notifica que la transmisión contiene software malicioso.

(0008) La Publicación de la Solicitud de Patente de E.E.U.U. nº US 2015/0227742 A1 hace referencia a sistemas y métodos para detectar programas maliciosos ofuscados dentro de los programas empaquetados. En particular, se ejecuta un programa empaquetado. El programa empaquetado incluye un código malicioso que ha sido ofuscado dentro del programa empaquetado y del código no empaquetado que des-ofusca y ejecuta el código malicioso cuando el programa empaquetado se ejecuta. Mientras que el programa empaquetado está siendo ejecutado, se monitorea cómo se comporta el programa empaquetado. Si se detectan comportamientos sospechosos del código malicioso, se desarrolla una operación de seguridad en el programa empaquetado.

(0009) Además, el artículo de Wikipedia para el "cifrado XOR" (en inglés: "XOR cipher") enseña un algoritmo de encriptación, usando la operación de disyunción (XOR) exclusiva.

Resumen de la invención reivindicada

(0010) La invención está definida en las reivindicaciones independientes. Las configuraciones particulares están expuestas en las reivindicaciones dependientes.

(0011) En particular, se manifiesta un método para impedir que el contenido malicioso alcance un ordenador de destino. El método incluye la recepción de una multitud de paquetes de datos enviados desde un ordenador de origen a un ordenador de destino, de manera que cada uno de estos paquetes de datos enviados desde el ordenador de origen al ordenador de destino se envían al ordenador de destino, excepto, al menos, un paquete. Después de que dichos paquetes de datos han sido recibidos, las instrucciones asociadas a la multitud de paquetes de datos pueden ser ejecutadas, mientras que se observan las acciones asociadas a dichas instrucciones. La observación de la ejecución de las instrucciones, que puede identificar una acción desarrollada por las instrucciones ejecutadas, es una acción no autorizada, y se puede hacer una identificación de que la multitud de paquetes de datos incluye software malicioso, cuando una acción desarrollada es la acción no autorizada. Este método puede incluir también el no enviar, al menos, un paquete de datos al ordenador de destino, cuando el software malicioso ha sido identificado como que incluye en la multitud de paquetes de datos, de este modo impidiendo que el ordenador de destino reciba el software malicioso en un estado funcional.

(0012) Cuando el método se desarrolla por un medio de almacenamiento legible por ordenador no transitorio, un procesador que ejecuta las instrucciones desde una memoria puede recibir también una multitud de paquetes de datos enviados desde un ordenador de origen a un ordenador de destino, en el cual cada uno de estos paquetes de datos enviados desde el ordenador de origen al ordenador de destino son entonces enviados al ordenador de destino, excepto, al menos, un paquete. Después de que dichos paquetes de datos han sido recibidos, las instrucciones asociadas a la multitud de paquetes de datos pueden ser ejecutadas, mientras que se observan las acciones asociadas a dichas instrucciones. La observación de la ejecución de las instrucciones, que puede identificar una acción desarrollada por las instrucciones ejecutadas, es una acción no autorizada y se puede hacer una identificación de que la multitud de paquetes de datos incluye software malicioso, cuando una acción desarrollada es la acción no autorizada. Este método puede incluir también el no enviar, al menos, un paquete de datos al ordenador de destino, cuando el software malicioso ha sido identificado como que está incluido en la multitud de paquetes de datos, de este modo impidiendo que el ordenador de destino reciba el software malicioso en un estado funcional.

(0013) También se describe un aparato para impedir que el contenido malicioso alcance un ordenador de destino. El aparato incluye un ordenador de análisis que recibe una multitud de paquetes de datos enviados desde un ordenador de origen a un ordenador de destino, incluyendo el ordenador del análisis una memoria, un procesador que ejecuta instrucciones desde la memoria, y una interfaz de red que recibe una multitud de paquetes de datos enviados desde un ordenador de origen a un ordenador de destino, de manera que cada uno de estos paquetes de datos enviados desde el ordenador de origen al ordenador de destino son entonces enviados al ordenador de destino, excepto, al menos, un paquete. Después de que dichos paquetes de datos han sido recibidos, las instrucciones asociadas a la multitud de paquetes de datos pueden ser ejecutadas, mientras que se observan las acciones asociadas a dichas instrucciones. La observación de la ejecución de las instrucciones, que puede identificar una acción desarrollada por las instrucciones ejecutadas, es una acción no autorizada y se puede hacer una identificación de que la multitud de paquetes de datos incluye software malicioso, cuando una acción desarrollada es la acción no autorizada. Este método puede incluir también el no enviar, al menos, un paquete de datos al ordenador de destino, cuando el software malicioso ha sido identificado como que está incluido en la multitud de paquetes de datos, de este modo impidiendo que el ordenador de destino reciba el software malicioso en un estado funcional.

Breve descripción de los dibujos

(0014)

La FIG. 1 ilustra un diagrama de flujo acorde con la exposición presente, en la cual los datos incluidos en los paquetes de datos descargados se reciben y se analizan para detectar la presencia del software malicioso.

La FIG. 2 ilustra un conjunto de pasos, a modo de ejemplo, que pueden desarrollarse cuando un conjunto de paquetes de datos se recibe por un dispositivo informático.

La FIG. 3 ilustra un conjunto de pasos que se puede desarrollar, cuando se reciben los paquetes de datos asociados a un conjunto de paquetes de datos.

La FIG. 4 ilustra un conjunto de pasos de programa, a modo de ejemplo, que puede desarrollarse, cuando los paquetes de datos asociados con un conjunto de paquetes de datos son analizados por un dispositivo informático.

La FIG. 5 ilustra un cortafuego que se comunica con un ordenador de análisis cuando los paquetes de datos enviados desde un ordenador de origen son recibidos por y enviados desde el cortafuego.

La FIG. 6 ilustra un sistema informático que puede ser usado para implementar una configuración de la presente

invención.

Descripción detallada

(0015) Esta manifestación está relacionada con métodos y aparatos usados para impedir que un contenido malicioso alcance un destino, a través de un motor de análisis dinámico, que puede operar en tiempo real, cuando se han recibido datos empaquetados. Los datos empaquetados enviados desde un ordenador de origen a un ordenador de destino pueden ser recibidos inicialmente por un cortafuego y pueden ser transferidos a un ordenador de análisis. El ordenador de análisis puede entonces monitorear las acciones desarrolladas por el código del programa ejecutable incluido dentro del conjunto de paquetes de datos cuando se hacen determinaciones referentes a si el conjunto de paquetes de datos debería ser clasificado como software malicioso. En ciertos casos, todos, excepto un último paquete de datos del conjunto de paquetes de datos, puede ser enviado también al ordenador de destino, mientras que el ordenador de análisis ejecuta y monitorea el código del programa incluido en el conjunto de paquetes de datos. Mediante la recepción de operaciones de desarrollo en dichos paquetes de datos, tales como la transmisión de dichos paquetes de datos al ordenador de análisis o el no envío del último paquete de datos al ordenador de destino, el cortafuego desarrolla la función de "interceptar" los paquetes de datos, cuando recibe dichos paquetes de datos. El análisis dinámico puede desarrollarse en tiempo real o cercano al tiempo real, de este modo, optimizando la eficiencia de la detección de la amenaza del software malicioso, mientras que se optimiza la anchura de banda de red. Cuando el análisis se desarrolla mediante un motor de análisis específico, se posibilita también el desarrollo de un cortafuego para ser mejorado.

(0016) Cuando el ordenador de análisis identifica que el conjunto de paquetes de datos no incluye software malicioso, el software malicioso puede ser bloqueado para que no alcance el ordenador de destino, mediante el no envío del último paquete de datos al ordenador de destino. Los métodos y aparatos descritos aquí pueden preparar también los datos incluidos en un conjunto o flujo de paquetes de datos, para las evaluaciones que pueden identificar si el software malicioso está incluido en el conjunto de paquetes de datos.

(0017) Cuando el dispositivo del ordenador recibe los paquetes de datos del cortafuego, el dispositivo del ordenador puede preparar datos incluidos en los paquetes de datos para la evaluación, después de la cual el dispositivo informático puede analizar los datos incluidos en el conjunto de paquetes de datos para ver si dichos datos incluyen software malicioso. La preparación de los datos en los paquetes de datos para la evaluación puede incluir la des-ofuscación de los datos incluidos en los paquetes de datos, de forma que la des-ofuscación puede incluir la des-criptación o la re-ordenación/re-secuenciación de los datos incluidos en los paquetes de datos. Cuando los paquetes de datos están encriptados, los datos incluidos en dichos paquetes de datos pueden ser des-encriptados usando un algoritmo de des-cifrado asociado a una sesión de transferencia segura. En ciertos casos, una parte de los datos incluidos en el conjunto de paquetes de datos puede ser des-encriptada. La des-encriptación puede incluir el cifrado XOR de, al menos, una parte de los datos incluidos en el conjunto de paquetes de datos con otros datos o con otros datos incluidos en el conjunto de paquetes de datos. En ciertos casos, la des-encriptación según métodos seguros estándar para entregar paquetes puede ser considerada como una función autorizada, de forma que las des-encriptaciones inesperadas pueden ser asociadas con una función no autorizada. Como tal, el cifrado XOR de datos en un conjunto de paquetes puede causar que un conjunto de paquetes de datos sea clasificado como software malicioso.

(0018) Un ejemplo de la re-ordenación/re-secuenciación de los datos recibidos incluye la re-organización de los datos recibidos, según un proceso de intercalado que re-estructura. Semejante proceso es similar a estructurar una baraja de cartas, de forma que cada carta es equivalente a uno o más bits/bytes de datos. En dichos casos, los datos de las diferentes partes de un paquete o de diferentes paquetes puede ser re-organizado formando un conjunto de datos ejecutables que pueden incluir software malicioso. Para cumplir con esto, el código incluido en uno o más paquetes puede incluir instrucciones para re-ordenar los datos incluidos en el conjunto de datos después de que se reciben. La ejecución de dichas instrucciones puede generar un código malicioso de datos que ha sido intencionadamente ofuscado, para impedir que un motor de inspección profunda de paquetes detecte el software malicioso escondido dentro del conjunto de paquetes de datos.

(0019) El análisis de los datos en los paquetes de datos puede incluir la ejecución de un código de programa incluido en los paquetes de datos y el monitoreo de la ejecución de aquel código de programa, cuando se vigilan las acciones no autorizadas o sospechosas, desarrolladas por el código del programa. Las acciones no autorizadas incluyen, sin embargo, no quedan limitadas, la escritura de un bloque de arranque, la actualización de un registro de sistema, la realización de cambios en el sistema del archivo, la eliminación de datos informáticos, la copia de datos, la transmisión de datos a otro ordenador o la interceptación de llamadas a un conjunto de instrucciones básicas de entrada/salida (BIOS) de un ordenador que ejecuta dicho código de programa. La interceptación de las llamadas BIOS por el código del programa puede identificarse mediante la observación del código del programa, que sustituye un comando relacionado con el BIOS original por otro comando, o mediante la observación aquellos parámetros, que modifican el código del programa que estaba incluido en el comando relacionado con el BIOS original, antes de que el comando BIOS original pueda ser ejecutado. Como tal, la función del análisis puede ejecutar un código de programa para el ordenador de destino, usando una técnica "Sandboxing", es decir, el permitir que el código del programa sea evaluado con respecto al software malicioso en un entorno seguro. En ciertos casos, los métodos y aparatos conformes a la presente manifestación pueden combinar "Sandboxing" con la inspección profunda de paquetes (DPI). Una vez que el software malicioso ha sido identificado, las firmas pueden ser generadas desde los

datos del paquete para un uso futuro por procesadores que desarrollan una función DPI. "Sandboxing y DPI" pueden desarrollarse en paralelo, de este modo, la detección del software malicioso que no ha sido identificado previamente puede ser identificada por una técnica del "Sandboxing" o la detección del software malicioso que ha sido identificado previamente puede ser identificada mediante la combinación de técnicas DPI.

(0020) El análisis de datos incluido en el conjunto de paquetes de datos puede observar también la ejecución de un código de programa e identificar que el código de programa ejecutado desarrolle una función relativa a organizar otras instrucciones para la ejecución desde datos incluidos en la multitud de paquetes de datos. Una vez observado, este análisis puede clasificar entonces esta reorganización de datos como una acción no autorizada, después de lo cual el conjunto de paquetes de datos puede ser bloqueado. Como tal, el contenido incluido en un conjunto de datos puede ser clasificado como software malicioso basándose en cómo o qué código de programa de funciones se desarrolla dentro de dicho conjunto de datos.

(0021) Las determinaciones en relación con la identificación del software malicioso también puede estar basado en un conjunto de reglas que identifican qué comportamientos del programa están autorizados o cuáles son no autorizados. Por ejemplo, una regla puede usarse para clasificar los datos dentro de dicho conjunto de paquetes de datos como software malicioso, siempre que los datos dentro de dicho conjunto de datos sean re-organizados/re-estructurados o cuando los datos dentro de dicho conjunto de datos sean manipulados o des-ofuscados por una función XOR. Alternativamente, otra regla puede indicar que la des-criptación de los datos de los paquetes es aceptable siempre que sea desarrollada de un modo compatible con un tipo de des-criptación estándar o previsto (tales como la des-criptación asociada a una comunicación TCP). Esta otra regla puede indicar también que es necesario otro análisis de los datos del programa, después de que la des-criptación ha sido desarrollada.

(0022) Incluso en casos en los que se observa la reorganización de los datos, los métodos compatibles con la presente manifestación pueden incluir la continuación con el análisis del código del programa incluido en un conjunto de paquetes de datos con la intención de identificar si dicho código de programa desarrolla acciones maliciosas y qué actos maliciosos no desarrolla. Además, las firmas pueden ser generadas desde los datos re-organizados para un uso posterior por un motor de inspección profunda de paquetes (DPI), por ejemplo.

(0023) La FIG. 1 ilustra un diagrama de flujo según la manifestación presente, en el que se reciben los datos incluidos en los paquetes de datos descargados y son analizados para detectar la presencia de software malicioso. El paso 105 de la FIG. 1 recibe un paquete asociado a un conjunto de paquetes. Después de que el paquete del conjunto de paquetes ha sido recibido en el paso 105, el paso 110 de la FIG. 1 identifica si el paquete recibido es un último paquete del conjunto de datos, y si no es así, el flujo del programa fluye al paso 115, en el cual el paquete recibido se envía a un destino y al dispositivo informático. En el momento en el tiempo en que el paquete recibido se envía al destino y al dispositivo informático, no se ha hecho ninguna determinación sobre si el conjunto de paquetes incluye software malicioso. En ciertos casos, el dispositivo informático puede ser un ordenador en la nube que es accesible a través de internet y el dispositivo informático puede desarrollar un servicio de identificación de si los conjuntos de paquetes de datos recibidos incluyen software malicioso. Estos servicios pueden proveerse para usuarios suscritos. Alternativamente, el dispositivo informático puede residir en una red corporativa o ser parte de una red informática asociada a un ordenador de usuario que es un destino asociado a un conjunto de paquetes de datos. En ciertos casos, un ordenador que inicialmente recibe paquetes de datos puede ser también el dispositivo informático que desarrolla operaciones relativas a la identificación de si los paquetes de datos recibidos incluyen software malicioso. En otros casos, más de un ordenador puede desarrollar estas funciones, por ejemplo, un cortafuego puede recibir paquetes de datos y enviarlos a otro ordenador para el análisis.

(0024) Después del paso 115, el flujo del programa se mueve al paso 120, en que las operaciones son desarrolladas con el paquete recibido en el dispositivo informático. Las operaciones desarrolladas en el dispositivo informático pueden incluir la des-ofuscación de información en el paquete de datos, puede incluir la re-secuenciación del orden de los datos recibidos, o puede incluir cualquier operación que preste o transforme información recibida asociada al conjunto de paquetes recibidos en una forma ejecutable por un procesador. Como tales, las operaciones desarrolladas en el paso 120 pueden estar relacionadas con la des-criptación de datos incluida en los paquetes recibidos, los conjuntos de instrucciones ejecutables que re-clasifican el orden de las instrucciones incluidas en los paquetes recibidos y/o las instrucciones ejecutables incluidas en los paquetes de datos recibidos.

(0025) Después del paso 120, el paso de determinación 125 de la FIG. 1 identifica si el software malicioso ha sido detectado / identificado en el conjunto del paquete. Cuando el paso 125 identifica que el conjunto de paquetes de datos incluye software malicioso, el flujo del programa se mueve al paso 130 en que una acción correctiva puede ser desarrollada. Esta acción correctiva puede incluir la supresión de una conexión asociada a los paquetes recibidos, la detención de la recepción de paquetes de datos o la detención de la retransmisión de paquetes asociados con el conjunto de paquetes. Las acciones correctivas pueden incluir también el almacenamiento de información que ayuda a caracterizar o identificar que un origen de los paquetes no es un origen fiable de paquetes de datos. Otra acción correctiva puede tener relación con el almacenamiento de firmas u otros atributos de identificación asociados a los paquetes de datos recibidos, de manera que estas firmas o atributos de identificación pueden usarse para identificar más rápidamente el software malicioso cuando se recibe posteriormente. Como tales, los métodos y aparatos compatibles con la presente manifestación pueden combinar el "Sandboxing", en el cual las instrucciones incluidas en un conjunto de paquetes de datos son ejecutadas en el dispositivo informático, con la inspección profunda de paquetes (DPI) que identifica modelos y firmas que han sido previamente identificadas como que son maliciosos.

(0026) Cuando los paquetes de datos recibidos incluyen un código ejecutable, todos los paquetes de datos asociados al conjunto de paquetes que están siendo recibidos pueden tener que ser recibidos por el dispositivo informático antes de que el código ejecutable sea ejecutado en el dispositivo informático. Como tal, el flujo del programa puede, alterativamente, no incluir el paso 125 que se desarrolla después del paso 120. En ciertos casos, el flujo del programa puede fluir desde el paso 120 de vuelta al paso 105, sin desarrollar el paso 125. Cuando el software malicioso no es detectado, el flujo del programa se mueve desde el paso 125 al paso 105, en el cual los paquetes de datos adicionales pueden ser recibidos.

(0027) Cuando el paso de determinación 110 identifica que el paquete de datos recibido es el último paquete de datos, el último paquete de datos puede ser enviado al dispositivo informático en el paso 135 de la FIG. 1. A continuación, en el paso 140 de la FIG. 1, las operaciones pueden desarrollarse con datos incluidos en las últimas operaciones y en los últimos paquetes asociados, después de que el conjunto de paquetes de datos se haya recibido en su totalidad. Como tales, las operaciones incluidas en el paso 140 pueden incluir algunas o todas las operaciones expuestas con respecto al paso 120 de la FIG. 1. En los casos en los que los paquetes de datos son recibidos con defectos, el último paquete recibido puede no ser un paquete que sea verdaderamente el último paquete del conjunto de paquetes, sino que puede ser un último paquete recibido del conjunto de paquetes.

(0028) Después del paso 140, el paso de determinación 145 identifica si el software malicioso ha sido detectado en el conjunto de paquetes. Cuando el software malicioso es detectado, el flujo del programa se mueve al paso 130, en el cual una o más acciones correctivas pueden ser desarrolladas. De nuevo, aquí, las acciones pueden incluir la supresión de una conexión asociada a los paquetes recibidos, la detención de la recepción de paquetes de datos, la detención de la retransmisión de paquetes asociados al conjunto de paquetes, el almacenamiento de información que ayuda a caracterizar o identificar que un origen de los paquetes no es un origen fiable de los paquetes de datos y/o el almacenamiento de firmas u otros atributos de identificación asociados a los paquetes de datos recibidos. Además, estas firmas o atributos de identificación pueden usarse para identificar con más rapidez el software malicioso cuando se encuentra posteriormente.

(0029) Cuando el software malicioso no se detecta en el conjunto de paquetes, el flujo del programa puede moverse desde el paso 145 al paso 150 de la FIG. 1, en el cual el último paquete se envía al destino.

(0030) La FIG. 2 ilustra un conjunto, a modo de ejemplo, de pasos que pueden ser desarrollados cuando un conjunto de paquetes de datos es recibido por un dispositivo informático. De nuevo, aquí, todos hasta un último paquete de datos del conjunto de paquetes de datos pueden ser enviados al ordenador de destino, mientras que otro ordenador evalúa los datos incluidos en el conjunto de paquetes de datos para detectar software malicioso. La no transmisión del último paquete de datos al ordenador de destino en el paso 210 de la FIG. 2 puede causar que el ordenador que envió el conjunto de los paquetes de datos identifique que el último paquete de datos fue "eliminado" o "perdido" en la transmisión.

(0031) Después del paso 210, el paso 220 de la FIG. 2 identifica si una determinación se ha hecho en relación con si el conjunto de paquetes de datos incluye software malicioso. Cuando una determinación no ha sido hecha aún en el paso de determinación 220, el flujo del programa puede moverse desde el paso 220 al paso 270 y el último paquete de datos puede ser eliminado, entonces el flujo del programa se mueve al paso 280, en el cual se recibe una retransmisión del último paquete de datos. La retransmisión del último paquete de datos puede haber sido desarrollada por el ordenador que originalmente envió el conjunto de los paquetes de datos, basándose en que el ordenador de envío no había recibido un acuse indicando que el último paquete de datos fue recibido en el ordenador de destino. Semejantes retransmisiones son una parte de la operación estándar de la transferencia de datos empaquetados de unos datos de ordenador, por ejemplo, las comunicaciones enviadas a través del protocolo de control de transmisión (TCP) serán retransmitidas desde un ordenador de envío cuando el ordenador de envío no recibe un acuse indicando que un paquete de datos particular fue recibido por un ordenador de destino.

(0032) Después del paso 270, el flujo del programa se mueve de vuelta al paso 210, en el cual el último paquete de datos se elimina de nuevo. El flujo del programa puede moverse del paso 210 al paso 220, después al paso 270, y de vuelta al paso 210 de forma repetitiva hasta que se ha hecho una determinación en el paso 220.

(0033) Después de que se ha hecho una determinación en el paso 220, el paso 240 puede identificar si se ha detectado software malicioso en el conjunto de paquetes de datos. Cuando un software malicioso ha sido detectado en el conjunto de paquetes de datos, el flujo del programa puede moverse desde el paso 240 al paso 250 de la FIG. 2, cuando se desarrolla una acción correctiva. Aquí, de nuevo, la acción correctiva desarrollada puede corresponderse con una o más acciones correctivas expuestas en relación con la FIG. 1 arriba.

(0034) Cuando el paso 240 indica que el software malicioso no ha sido detectado en el conjunto de paquetes de datos, el flujo del programa se mueve desde el paso 240 al paso 260, en el cual el último paquete de datos se envía al destino.

(0035) La FIG. 3 ilustra un conjunto de pasos que pueden ser desarrollados cuando los paquetes de datos asociados a un conjunto de paquetes de datos son recibidos. El paso 310 es un paso en el cual los datos incluidos en uno o más paquetes de datos del conjunto de paquetes de datos son des-ofuscados. Esta operación de des-ofuscación puede incluir uno o más pasos, incluyendo, pero no quedando limitado, la des-criptación de datos en

los paquetes de datos recibidos o en los datos re-secuenciados en los paquetes de datos.

(0036) Después del paso 310, el paso 320 puede ejecutar una o más instrucciones incluidas en o asociadas al conjunto de paquetes de datos recibidos. El paso 330 de la FIG. 3 es un paso en el que se observan las acciones desarrolladas cuando las instrucciones son ejecutadas. Después del paso 330, el paso 340 identifica si se desarrolla cualquier acción no autorizada por el código ejecutable cuando se ejecuta. Las acciones no autorizadas son acciones en las que el código del programa incluido en un conjunto de paquetes de datos accede o envía información que es considerada inapropiada. La acción no autorizada puede incluir también el escribir a una o más ubicaciones de almacenamiento de datos que son considerados confidenciales. Ejemplos de acciones no autorizadas incluyen, sin embargo, no están limitadas, el acceso o transmisión de datos: tales como datos de registro, contraseñas, información de cuenta de usuario, información histórica de búsqueda WEB, datos del sistema del expediente y/o información financiera. Ejemplos adicionales de acciones no autorizadas incluyen el escribir a un registro informático, el escribir a un bloque de arranque de un dispositivo de almacenamiento de datos, tal como escribir a la "Dirección lógica de bloques" (en inglés: "Logical Block Address zero" (LBA 0)) de una unidad de disco, el escribir a una ubicación de almacenamiento de datos, en el que se almacenan los datos del programa y/o la operación del "código ef", que impide el arranque o la operación normal de un sistema de ordenador. Semejantes acciones no autorizadas pueden afectar significativamente al desarrollo de un ordenador de destino o puede convertir el sistema informático en inutilizable por un usuario. Por ejemplo, la sobreescritura del LBA 0 de una unidad de disco puede impedir el arranque de un sistema informático, porque el LBA 0 es normalmente usado para almacenar datos que son necesarios para dicho ordenador para arrancar (arranque e inicializar).

(0037) Cuando una acción no autorizada se identifica en el paso 340, el flujo del programa puede moverse desde el paso 340 al paso 350 de la FIG. 3. Aquí, de nuevo, las acciones correctivas desarrolladas pueden incluir cualquiera de las acciones correctivas expuestas en relación con la FIG. 1.

(0038) Cuando una acción no autorizada no está identificada en el paso 340, el flujo del programa puede moverse al paso 360 que determina si la ejecución de las instrucciones incluidas en el conjunto de paquetes de datos ha sido completada, cuando ningún flujo del programa se mueve desde el paso 360 de vuelta al paso 320, en el cual se continúa la ejecución de las instrucciones incluidas en el conjunto de paquetes de datos.

(0039) Cuando el paso 360 identifica que las instrucciones incluidas en el conjunto de paquetes de datos han sido completadas, el flujo del programa se mueve al paso 370, en el cual el último paquete asociado al conjunto de paquetes de datos se envía al destino.

(0040) La FIG. 4 ilustra un conjunto de pasos de programa, a modo de ejemplo, que puede ser desarrollado cuando los paquetes de datos asociados a un conjunto de paquetes de datos son analizados por un dispositivo informático. Estos paquetes de datos pueden ser analizados tras un requerimiento del usuario para acceder a un Localizador Universal de Recursos (URL) de página web o para descargar un archivo que ha sido recibido desde un ordenador de destino. El paso 410 de la FIG. 4 es un paso en el que se hace la identificación de que el ordenador de destino ha intentado descargar un conjunto de paquetes de datos. Esta identificación puede hacerse inmediatamente, cuando el ordenador de destino intenta descargar el conjunto de paquetes de datos. Después del paso 410, el paso 420 de la FIG. 4 es donde el conjunto de paquetes de datos es analizado para detectar la presencia de software malicioso.

(0041) A continuación, se puede realizar, en el paso 430 de la Fig. 4, una determinación de si el análisis de software malicioso del conjunto de paquetes de datos ha sido completado. Cuando el análisis del software malicioso no ha sido completado aún, el flujo del programa se mueve al paso 440, en el cual se continúa con el análisis del conjunto de paquetes de datos, después del cual el flujo del programa se mueve de vuelta al paso 430 de la FIG. 4. Cuando este análisis continúa, un mensaje (no ilustrado) puede ser enviado al ordenador de destino para la presentación a un usuario. El mensaje puede indicar que un proceso de fondo asociado con el análisis del conjunto de paquetes de datos está siendo desarrollado para determinar si aquéllos paquetes de datos incluyen software malicioso o si son benignos (aparentemente están libres de software malicioso). Este mensaje puede también informar al usuario de que los datos relativos al intento de descarga se suministran al ordenador de destino, si el análisis indica que la descarga no incluye software malicioso.

(0042) Cuando el paso 440 identifica que el análisis de software malicioso ha sido completado, el flujo del programa se mueve al paso 450 que identifica si el software malicioso ha sido detectado en el conjunto de paquetes. Cuando el software malicioso ha sido detectado en el conjunto de paquetes, el flujo del programa se mueve al paso 460 en el cual se desarrolla una acción correctiva. Esta acción correctiva puede incluir el bloqueo de la descarga (no enviar un último o restante paquete al dispositivo de destino) y puede incluir también el envío de un mensaje al ordenador de destino para informar al usuario de que el software malicioso ha sido detectado en los datos de descarga.

(0043) Cuando el software malicioso ha sido identificado como que no está presente en los datos de descarga en el paso 440, se puede permitir que uno o más paquetes de datos sean enviados al ordenador de destino, de forma que el ordenador de destino recibe los datos descargables requeridos. Los pasos de la FIG. 4 pueden ser desarrollados por uno o más dispositivos informáticos, que analizan el contenido de los paquetes de datos como una tarea de fondo que el usuario no tiene que gestionar activamente. Incluso cuando el análisis de los paquetes de datos recibidos conlleve una gran cantidad de tiempo, el usuario del ordenador de destino será libre para desarrollar otras tareas, mientras que el análisis del software malicioso está siendo desarrollado.

(0044) El método de la FIG. 4 puede impedir que un usuario intente descargar un archivo específico, un conjunto de datos o una página web, repetidamente. En los casos en que un usuario no intenta repetidamente descargar el mismo archivo, mientras que se está desarrollando un análisis, puede proporcionarse un mensaje que indique que un "veredicto" relativo a si la descarga incluye software malicioso está aún "pendiente". Los requerimientos repetitivos pueden ser interceptados por un ordenador, como con un cortafuego, y pueden no ser enviadas al ordenador de destino desde el cual la descarga ha sido requerida, de este modo evitando que el ordenador de origen reciba requerimientos repetitivos y guardando la anchura de banda de red en una red doméstica que, de otro modo, se consumiría desarrollando transferencias de datos repetitivos innecesarios relativas a los requerimientos repetitivos. Uno o más ordenadores que implementan la funcionalidad de la FIG. 4 pueden desarrollar funciones asociadas a la recepción de conjuntos de datos, al análisis de conjuntos de datos, a la gestión de la entrega de los conjuntos de datos al ordenador de destino o pueden desarrollar una descarga repetitiva de aquel conjunto de datos sólo como es requerido, sin que el usuario del ordenador de destino intente repetitivamente descargar el conjunto de datos.

(0045) Mientras que se pueden desarrollar la recepción y la transmisión de paquetes de datos de la presente manifestación por un cortafuego y mientras que se pueden desarrollar el análisis de los datos contenidos dentro de dichos paquetes de datos y el "Sandboxing" por un ordenador de análisis, estas acciones pueden ser desarrolladas alternativamente por un único ordenador.

(0046) La FIG. 6 ilustra un cortafuego que se comunica con un ordenador de análisis cuando los conjuntos de paquetes de datos son recibidos por un ordenador de origen y enviados por el cortafuego. La FIG. 5 incluye un ordenador de origen 510, un cortafuego 530, un ordenador de análisis 550 y un ordenador de destino 570. La FIG. 5 incluye también comunicaciones 520 enviadas desde/hacia el ordenador de destino 570 a través de un cortafuego 530, comunicaciones 560 enviadas hacia/desde el ordenador de destino 570, y comunicaciones 550 enviadas entre el cortafuego 530 y el ordenador de análisis 550. Hay que tener en cuenta que las comunicaciones 520 pueden ser transmitidas a través de una red informática tal como el internet, que las comunicaciones 560 pueden enviarse a través de una interfaz de red informática al cortafuego 530 y al ordenador de destino 560, y que las comunicaciones 540 pueden ser enviadas entre el cortafuego y el ordenador de análisis a través de interfaces de red informática al cortafuego 530 y al ordenador de análisis 550. Hay que tener en cuenta que cualquiera de las redes informáticas, a través de las cuales se envían las comunicaciones 520, 540 y 560, pueden incluir interfaces de red alámbricas o inalámbricas. El ordenador de análisis 550 puede ser también remoto respecto al cortafuego 530 y el ordenador de análisis 550 puede encontrarse en la nube. Las interfaces de red asociadas a la manifestación presente pueden incluir cualquier forma de interfaz de red alámbrica o inalámbrica conocida por la técnica.

(0047) Los varios componentes de la FIG. 5 pueden implementar funciones asociadas a la recepción y al análisis de los datos del ordenador que pueden haber sido requeridos por el ordenador de destino 570 y que han sido suministrados por un ordenador de origen 510. En semejantes casos, el cortafuego 530 y el ordenador de análisis 550 pueden desarrollar funciones relativas a la recepción de paquetes, el suministro de mensajes o el análisis de datos informáticos enviados desde un ordenador de origen 510, cuando se identifica si los datos descargados requeridos incluyen contenido malicioso. Como tal, el cortafuego 530 y el ordenador de análisis 550 pueden desarrollar funciones según la manifestación presente, incluyendo aquellas funciones descritas con respecto a las FIGS. 1-4.

(0048) La FIG. 6 ilustra un sistema informático que puede ser usado para implementar una configuración de la presente invención. El sistema informático 600 de la FIG. 6 incluye uno o más procesadores 610 y una memoria principal 620. La memoria principal 620 almacena, en parte, instrucciones y datos para la ejecución por un procesador 610. La memoria principal 620 puede almacenar el código ejecutable cuando está en la operación. El sistema 600 de la FIG. 6 incluye además un dispositivo de almacenamiento masivo 630, una/s unidad/es de medio de almacenamiento portable/s 640, dispositivos de salida 650, dispositivos de entrada de usuario 660, un indicador de gráficos 670, dispositivos periféricos 680 y una interfaz de red 695.

(0049) Los componentes mostrados en la FIG. 6 están representados como que están siendo conectados a través de un único bus 690. Sin embargo, los componentes pueden ser conectados a través de uno o más medios de transporte de datos. Por ejemplo, la unidad del procesador 610 y la memoria principal 620 pueden ser conectadas a través de un bus de microprocesador local y el dispositivo de almacenamiento masivo 630, el/los dispositivo/s periférico/s 680, el dispositivo de almacenamiento portable 640, y el sistema indicador 670 pueden ser conectados a través de uno o más buses de entrada/salida (I/O).

(0050) El dispositivo de almacenamiento masivo 630, que puede ser implementado con una unidad de disco magnética o una unidad de disco óptica, es un dispositivo de almacenamiento no volátil, para almacenar datos e instrucciones para el uso por una unidad de procesador 610. El dispositivo de almacenamiento masivo 630 puede almacenar el software del sistema para implementar configuraciones de la presente invención con finalidades de cargar aquel software dentro de la memoria principal 620.

(0051) El dispositivo de almacenamiento portable 640 opera en conjunción con un medio de almacenamiento no volátil, tal como una memoria FLASH, un disco compacto o un disco de video digital, para introducir y extraer datos y codificar dentro del y desde el sistema de ordenador 600 de la FIG. 6. El software del sistema para implementar las configuraciones de la presente invención puede ser almacenado en semejante medio portable y puede ser

introducido en el sistema informático 600, a través del dispositivo de almacenamiento portable 640.

(0052) Los dispositivos de entrada 660 proporcionan una parte de una interfaz de usuario, los dispositivos de entrada 660 pueden incluir un teclado alfanumérico, tal como un teclado, para introducir información alfanumérica u otra información, o un dispositivo de señalización, tal como un ratón, una rueda de desplazamiento, un lápiz óptico o unas teclas de dirección de cursor. Adicionalmente, el sistema 600, como se muestra en la FIG. 6, incluye dispositivos de salida 650. Ejemplos de dispositivos de salida adecuados incluyen altavoces, impresoras, interfaces de red y monitores.

(0053) El sistema de pantalla 670 puede incluir una pantalla de cristal líquido (LCD), una pantalla de plasma, una pantalla de diodos emisores de luz orgánica (OLED), una pantalla de tinta electrónica, una pantalla basada en un proyector, una pantalla holográfica u otro dispositivo de pantalla adecuado. El sistema de pantalla 670 recibe información textual y gráfica y procesa la información para la salida a través del dispositivo de pantalla. El sistema de pantalla 670 puede incluir capacidades de entrada de pantalla táctil de múltiples puntos de contacto, tales como la detección táctil capacitiva, la detección de tacto resistiva, la detección táctil de onda acústica de superficie o la detección táctil por infrarrojos. Semejantes capacidades de entrada de pantalla táctil pueden permitir o pueden no permitir la presión variable o la detección forzada.

(0054) Los periféricos 680 pueden incluir cualquier tipo de dispositivo de soporte informático para añadir la funcionalidad adicional al sistema informático. Por ejemplo, el/los dispositivo/s periférico/s 680 pueden incluir un modem o un router.

(0055) La interfaz de red 595 puede incluir cualquier forma de interfaz informática de un ordenador, tanto si es una red alámbrica o una interfaz inalámbrica. Como tal, la interfaz de red 595 puede ser una interfaz de red de ethernet, una interfaz inalámbrica de Bluetooth™, una interfaz 802.11 ó una interfaz de teléfono celular.

(0056) Los componentes contenidos en el sistema informático 600 de la FIG. 6 son aquéllos que se encuentran normalmente en sistemas informáticos que pueden ser adecuados para el uso con configuraciones de la presente invención y pretenden representar una categoría amplia de semejantes componentes informáticos que son bien conocidos por la técnica. De este modo, el sistema informático 600 de la FIG. 6 puede ser un ordenador personal, a un dispositivo informático portátil, un teléfono ("inteligente" o de otro tipo), un dispositivo informático móvil, una estación de trabajo, un servidor (en un "rack" de servidor u otro tipo), un miniordenador, un ordenador central, un dispositivo informático de Tablet, un dispositivo portable (tal como un reloj, un anillo, unas gafas u otro tipo de joya/ropa/accesorio), una consola de juegos de video (portable o de otro tipo), un lector de libro electrónico, un dispositivo reproductor de medios (portable o de otro tipo), un ordenador basado en un vehículo, alguna combinación de los anteriores o cualquier otro dispositivo informático. El ordenador puede incluir también diferentes configuraciones de bus, plataformas en red, plataformas multi-procesadoras, etc. El sistema informático 600 puede ser, en algunos casos, un sistema informático virtual ejecutado por otro sistema informático. Varios sistemas operativos pueden usarse, incluyendo Unix, Linux, Windows, Macintosh OS, Palm OS, Android, iOS y otros sistemas operativos adecuados.

(0057) La presente invención puede ser implementada en una aplicación que puede ser operativa usando una variedad de dispositivos. Los medios de almacenamiento legibles informáticamente no transitorios hacen referencia a cualquier medio o medios que participan en proveer instrucciones a una unidad de procesamiento central (CPU) para la ejecución. Semejantes medios pueden tener muchas formas, incluyendo (pero no quedando limitados) medios no volátiles y volátiles, tales como discos ópticos o magnéticos y memorias dinámicas, respectivamente. Las formas comunes de medios legibles informáticamente no transitorios incluyen, por ejemplo, un disquete, un disco flexible, un disco duro, una cinta magnética u otro tipo de medio magnético, un disco CD-ROM, un disco de video digital (DVD), cualquier otro medio óptico, RAM, PROM, EPROM, un FLASHEPROM y cualquier otro chip o cartucho de memoria.

(0058) Mientras que varios diagramas de flujo provistos y descritos arriba pueden mostrar un orden particular de operaciones desarrolladas por ciertas configuraciones de la invención, se debe entender que semejante orden es a modo de ejemplo (por ejemplo, las configuraciones alternativas pueden desarrollar las operaciones en un orden diferente, combinar ciertas operaciones, superponer ciertas operaciones, etc.).

(0059) La descripción detallada anteriormente de la tecnología presente ha sido presentada para finalidades de ilustración y descripción. No se pretende ser exhaustivo o limitar la tecnología a la forma precisa expuesta. Son posibles muchas modificaciones y variaciones a la luz de la enseñanza de arriba. Las configuraciones descritas fueron elegidas para explicar mejor los principios de la tecnología y su aplicación práctica para así posibilitar a otros expertos en la técnica la mejor utilización de la tecnología en varias configuraciones y con varias modificaciones, como es adecuado para el uso particular contemplado. Se pretende que el ámbito de la tecnología sea definido por la reivindicación.

REIVINDICACIONES

1. Un método para impedir que el contenido malicioso alcance un ordenador de destino (570), comprendiendo el método:

- la recepción de una multitud de paquetes de datos en un ordenador de análisis (550) que fueron enviados (115, 135) por un cortafuego (530), en el cual se envía (115) la multitud de paquetes de datos excepto, al menos, un paquete de datos de la multitud de paquetes de datos al ordenador de destino (570);

- la ejecución (320) de instrucciones incluidas en la multitud de paquetes de datos recibidos en el ordenador de análisis (550);

- la observación (330) de una o más acciones que se desarrollan cuando son ejecutadas las instrucciones incluidas en la multitud de paquetes de datos recibidos en el ordenador de análisis (550);

- la identificación de que una o más acciones observadas incluyen las instrucciones de des-ofuscación en la multitud de paquetes de datos recibidos en el ordenador de análisis (550) que, cuando se ejecutan, accederían a información inapropiada o escribirían a una ubicación de almacenamiento de datos confidenciales; y

- la identificación de que la multitud de paquetes de datos recibidos en el ordenador de análisis (550) incluyen software malicioso basado en la identificación de las instrucciones que accederían a la información inapropiada o que escribirían a la ubicación de almacenamiento de datos confidenciales, de manera que una conexión asociada a, al menos, un paquete de datos no enviado al ordenador de destino (570) es eliminado entonces (130, 250, 350, 460) por el cortafuego (530) como resultado del software malicioso que es identificado como que está presente en la multitud de paquetes de datos recibidos en el ordenador de análisis (550).

2. El método de la reivindicación 1, en el que las instrucciones de des-ofuscación incluyen la des-encryptación de, al menos, una parte de los datos incluidos en la multitud de paquetes de datos.

3. El método de la reivindicación 1 ó 2, en el que las instrucciones de des-ofuscación incluyen el reordenamiento de, al menos, una parte de los datos incluidos en la multitud de los paquetes de datos.

4. El método de cualquiera de las reivindicaciones anteriores, en el que:

- cada uno de la multitud de paquetes de datos están interceptados por el cortafuego (530),
 - la multitud de los paquetes de datos son enviados desde el cortafuego (530) al ordenador de análisis (550), y
 - el cortafuego (530) envía la multitud de los paquetes de datos excepto, al menos, un paquete al ordenador de destino (570).

5. El método de cualquiera de las reivindicaciones anteriores, en el que un mensaje se envía al ordenador de destino (570), indicando dicho mensaje que la multitud de los paquetes de datos están siendo analizados para detectar el contenido malicioso.

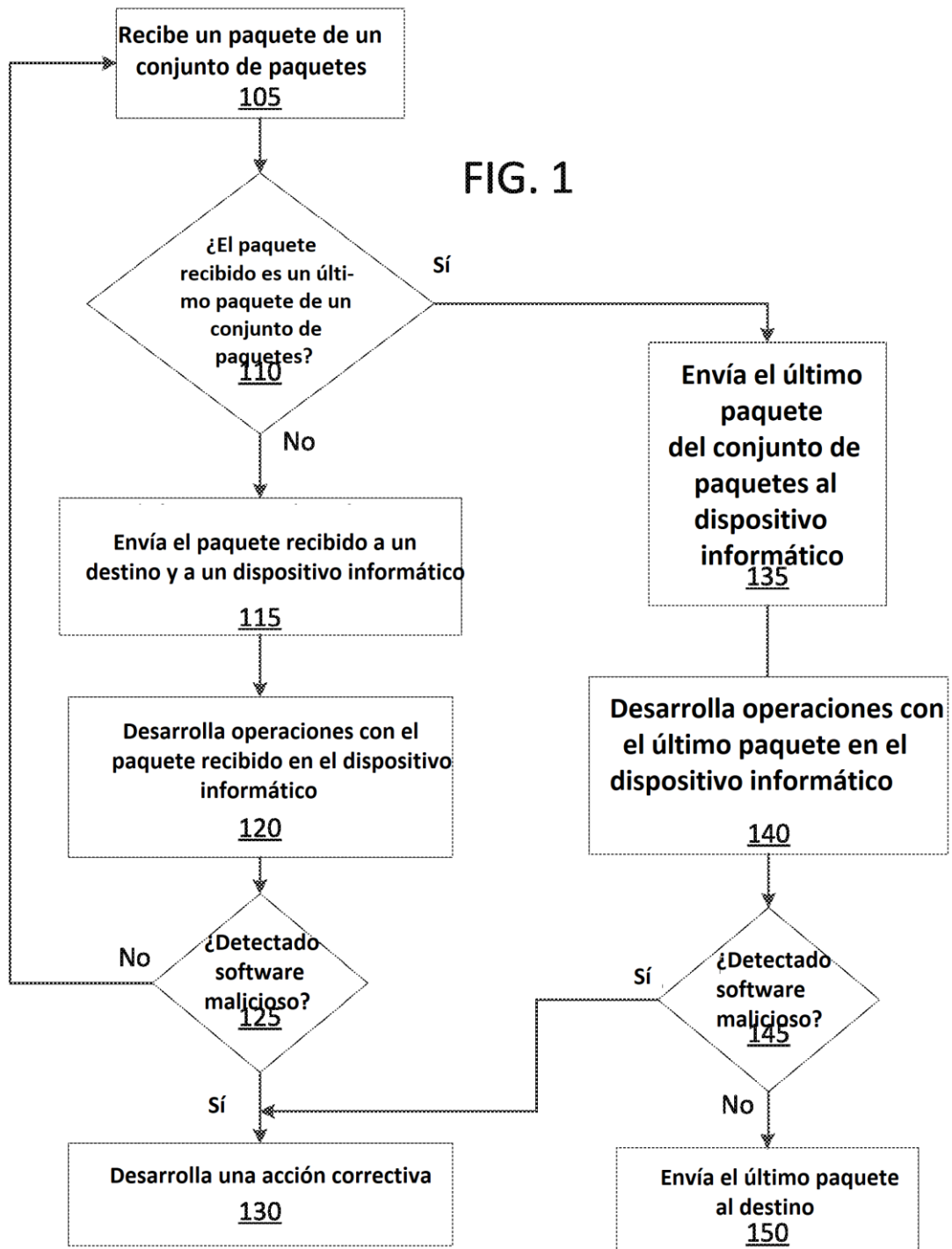
6. El método de cualquiera de las reivindicaciones anteriores, en el que la multitud de los paquetes de datos son recibidos basándose en un requerimiento enviado por el ordenador de destino (570) a los datos de descarga desde un ordenador de envío (510) y un requerimiento posterior de descargar los datos desde el ordenador de envío (510) es interceptado y no se envía al ordenador de envío (510).

7. El método de cualquiera de las reivindicaciones anteriores, en el que el acceso a la información inapropiada o el escribir a la ubicación de almacenamiento de datos confidenciales es una acción no autorizada asociada a, al menos, una de las acciones siguientes: escribir a un bloque de arranque, cambiar una configuración de registro, transmitir datos desde un ordenador receptor, eliminar datos en el ordenador receptor y cambiar o interceptar una entrada/salida básica, un BIOS, una instrucción asociada al ordenador receptor.

8. Un medio de almacenamiento legible informáticamente no transitorio que tiene configurado en el mismo un programa ejecutable por un procesador (610) para implementar un método para impedir que el contenido malicioso alcance un ordenador de destino (570) según cualquiera de las reivindicaciones 1-7.

9. Un aparato para impedir que el contenido malicioso alcance un ordenador de destino (570), comprendiendo el aparato un ordenador de análisis (550), incluyendo el ordenador de análisis (550) una memoria (620), un procesador (610) que ejecuta las instrucciones a partir de la memoria (320) y una interfaz de red (695), de modo que el procesador (610) en el ordenador de análisis (550) está configurado para desarrollar un método según cualquiera de las reivindicaciones 1-7.

FIG. 1



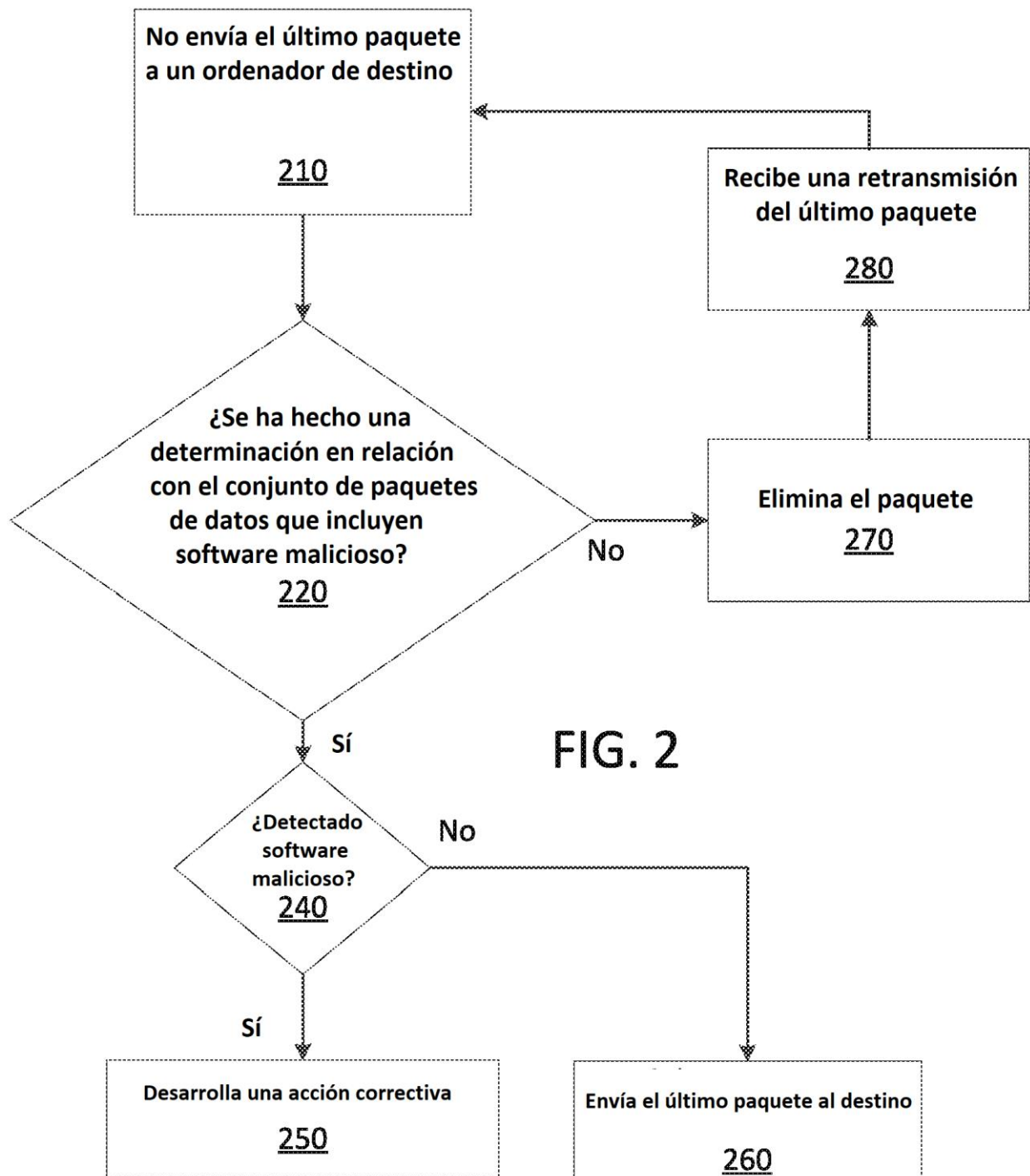


FIG. 3

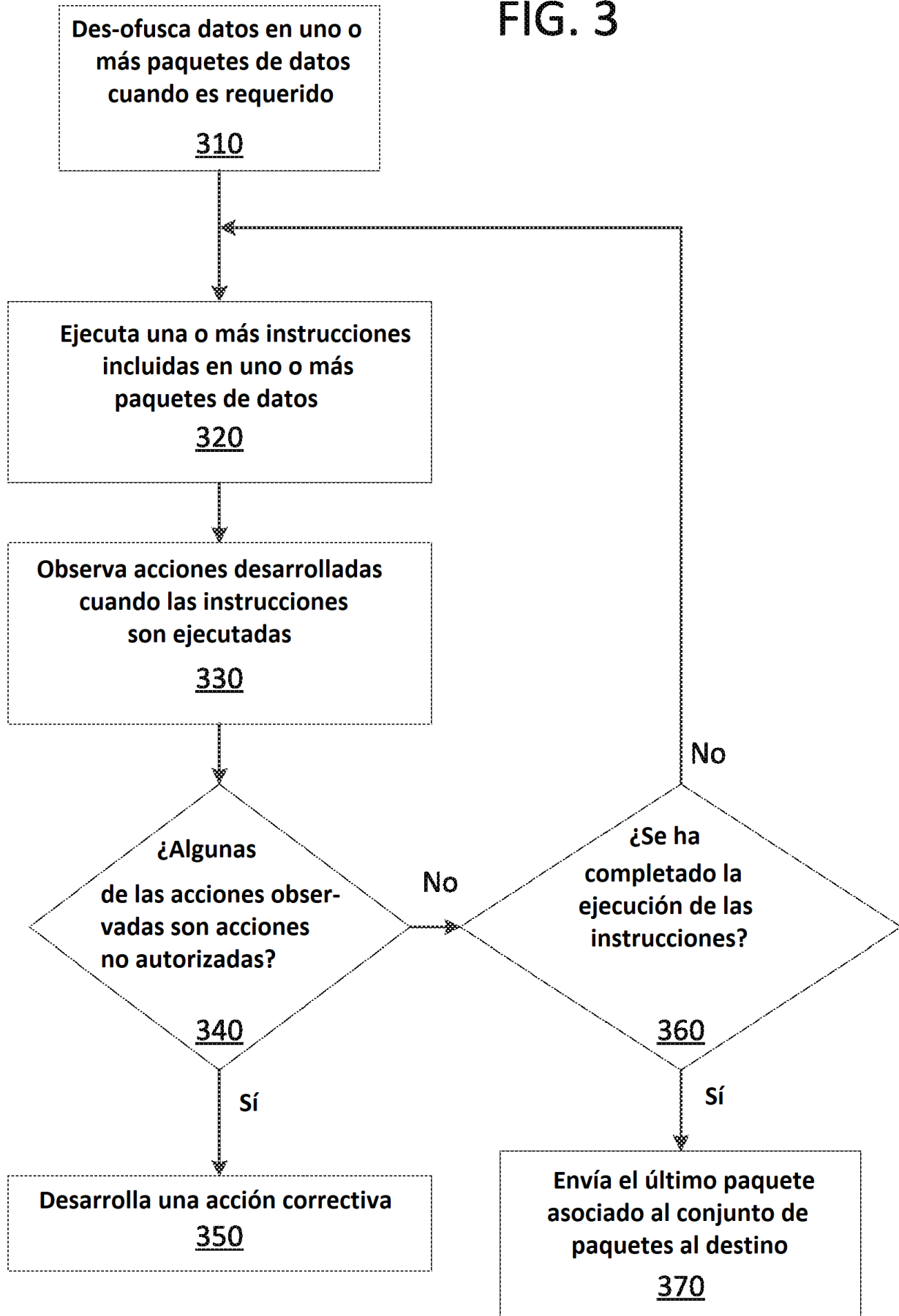
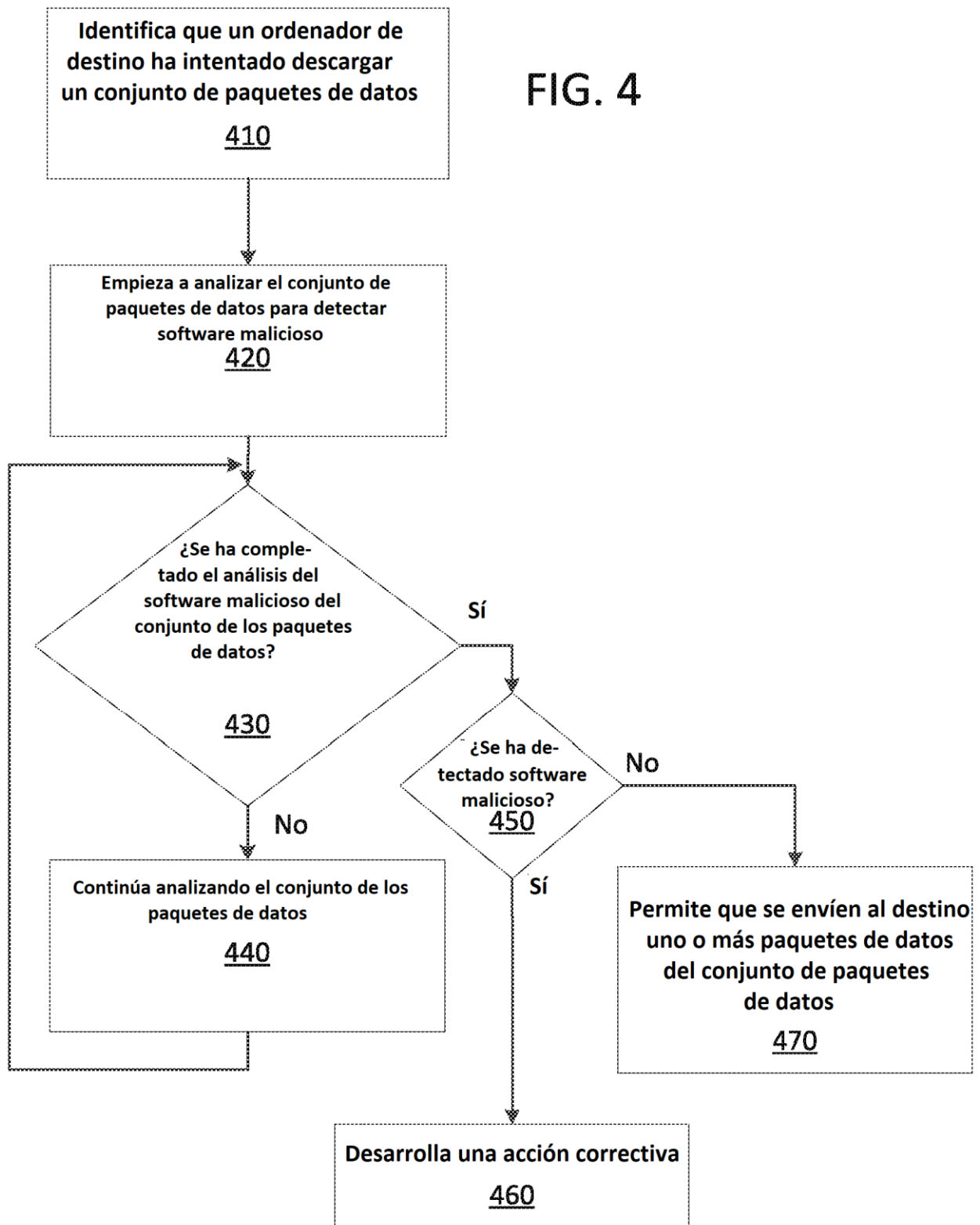


FIG. 4



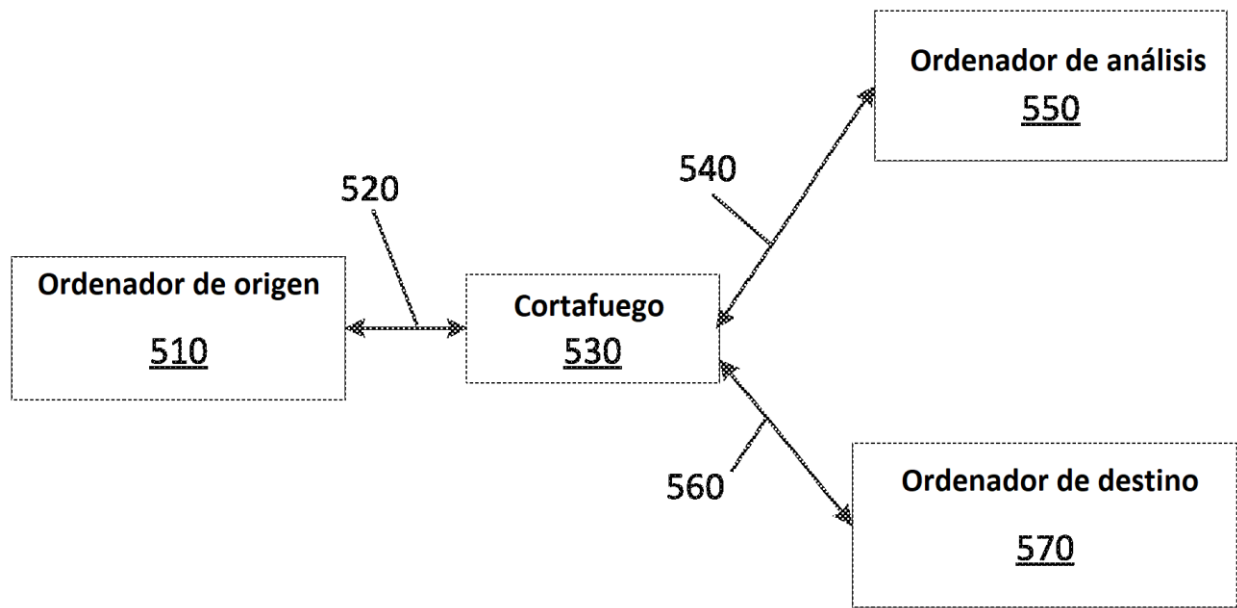


FIG. 5

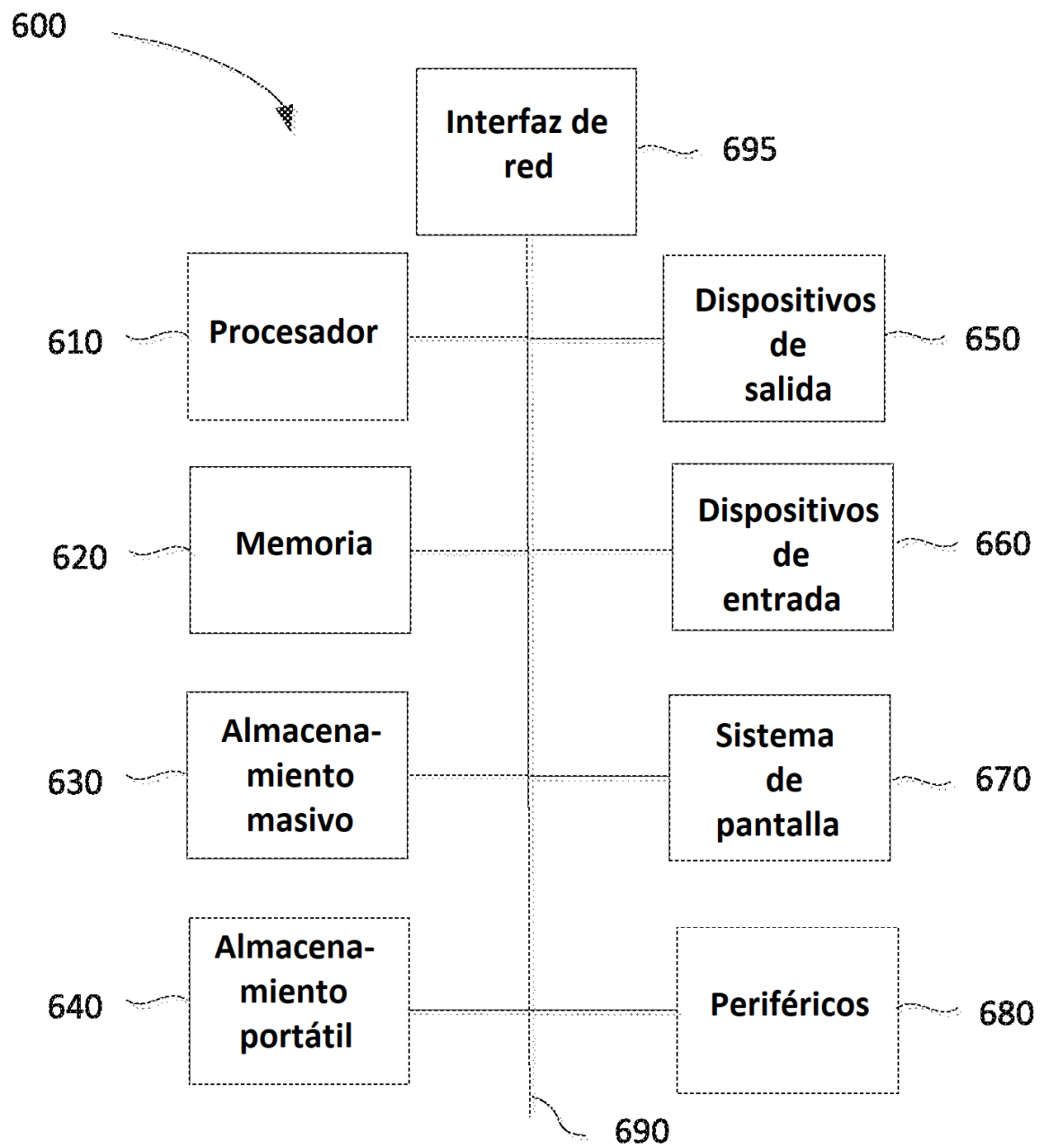


FIG. 6