(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 794 624**

(51) Int. CI.:

G06F 21/55 (2013.01)
G06F 21/56 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **04.07.2016 PCT/EP2016/065737**

(87) Fecha y número de publicación internacional: **02.02.2017 WO17016814**

(96) Fecha de presentación y número de la solicitud europea: **04.07.2016 E 16741887 (0)**

(97) Fecha y número de publicación de la concesión europea: **25.03.2020 EP 3326100**

(54) Título: **Sistemas y métodos para rastrear comportamiento malicioso a través de múltiples entidades de software**

(30) Prioridad:

24.07.2015 US 201514808173

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.11.2020

(73) Titular/es:

BITDEFENDER IPR MANAGEMENT LTD. (100.0%)
Kreontos 12
1076 Nicosia, CY

(72) Inventor/es:

HAJMASAN, GHEORGHE-FLORIN y
PORTASE, RADU-MARIAN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistemas y métodos para rastrear comportamiento malicioso a través de múltiples entidades de software

Antecedentes

La invención se relaciona con los sistemas y métodos para proteger los sistemas informáticos del software malicioso.

El software malicioso, también conocido como malware, afecta a un gran número de sistemas informáticos alrededor del mundo. En sus muchas formas tales como virus, gusanos, rootkits, adware no solicitados, ransonware, y spyware informático, el malware presente un serio riesgo para millones de usuarios informáticos, que los hacen vulnerables a la pérdida de datos e información sensible, robo de identidad, y pérdida de productividad, entre otras cosas. El malware puede presentar además material que es considerado por algunos usuarios como obsceno, excesivamente violento, acosador, u objetable de alguna otra manera.

El software de seguridad se puede usar para detectar malware que infecta un sistema informático del usuario, y de manera adicional para eliminar o evitar la ejecución de dicho malware. Diversas técnicas de detección de malware son conocidas en la técnica. Algunas se basan en hacer corresponder un fragmento de código del agente de malware con una biblioteca de firmas indicativas de malware. Otros métodos convencionales detectan un comportamiento indicativo de malware, tal como un conjunto de acciones realizadas por el agente de malware. El documento US 2010/293615 describe una detección de malware que usa la monitorización de procesos y el agrupamiento de procesos sospechosos en conjuntos.

El software malicioso se basa en diversas estrategias para evadir la detección. Una de dichas estrategias involucra técnicas de ofuscación, por ejemplo, que cifran el código malicioso, o usar versiones de código ligeramente diferentes en cada ordenador infectado (una característica comúnmente conocida como polimorfismo). Otro método de evasión de detección ejemplar divide las actividades maliciosas entre una pluralidad de agentes, en donde cada agente realiza un conjunto separado de acciones, que no se pueden considerar indicativas de malware cuando se toman de manera aislada de las acciones realizadas por otros agentes.

Existe un fuerte interés en desarrollar sistemas y métodos de detección de dicho malware avanzado.

Compendio

Según un aspecto, un sistema de servidor comprende al menos un procesador de hardware y una unidad de memoria, el al menos un procesador de hardware configurado para ejecutar un gestor de entidades y un motor heurísticos, configurado el al menos un procesador de hardware para ejecutar un gestor de entidades y un motor de heurísticos. El gestor de entidades se configura para organizar una colección de entidades ejecutables monitorizadas en una pluralidad de grupos de entidades, en donde organizar la colección comprende, en respuesta a la detección de que una primera entidad de la colección ha generado una entidad hija, que determina si la primera entidad pertenece a una categoría de entidades creadores de grupos. Organizar la colección comprende, además, en respuesta a determinar si la primera entidad pertenece a la categoría de creadores de grupos, cuando la primera entidad pertenece a la categoría de creadores de grupo, añadir un nuevo grupo de entidades a la pluralidad de grupos de entidades, y asignar la entidad hija al nuevo grupo de entidades. Organizar la colección comprende, además, en respuesta a determinar si la primera entidad pertenece a la categoría de creadores de grupo, cuando la primera entidad no pertenece a la categoría de creadores de grupo, seleccionar un primer grupo de entidades de la pluralidad de grupos de entidades de manera que la primera entidad es un miembro del primer grupo de entidades, y asignar la entidad hija al primer grupo de entidades. El motor de heurísticos se configura, en respuesta a la primera acción realizada por la entidad hija, seleccionar un segundo grupo de entidades de la pluralidad de grupos de entidades de manera que la entidad hija es un miembro del segundo grupo de entidades, y en respuesta seleccionar el segundo grupo de entidades, para determinar si la primera acción es indicativa de un ataque de malware según una segunda acción realizada por otro miembro del segundo grupo de entidades.

Según otro aspecto, un método comprende el empleo de al menos un procesador de malware de un sistema de servidor para organizar una colección de entidades ejecutables monitorizadas en una pluralidad de grupos de entidades. Organizar la colección comprende, en respuesta a la detección de que una primera entidad de la colección ha generado una entidad hija, determinar si la primera entidad pertenece a una categoría de entidades creadoras de grupos. Organizar la colección comprende, además, en respuesta a la determinación de si la primera entidad pertenece a la categoría de creadores de grupo, cuando la primera entidad pertenece a la categoría de creadores de grupo, añadir un nuevo grupo de entidades a la pluralidad de grupos de entidades, y asignar la entidad hija al nuevo grupo de entidades. Organizar la colección comprende, además, en respuesta a la determinación de si la primera entidad pertenece a la categoría de creadores de grupo, cuando la primera entidad no pertenece a la categoría de creadores de grupo, seleccionar un primer grupo de entidades de la pluralidad de grupos de entidades de manera que la primera entidad sea un miembro del primer grupo de entidades, y asignar la entidad hija al primer grupo de entidades. El método además comprende, en respuesta a una primera acción realizada por la entidad hija, emplear al menos un procesador de hardware del sistema de servidor para seleccionar un segundo grupo de entidades de la pluralidad de grupos de entidades de manera que la entidad hija sea un miembro del segundo grupo

de entidades. El método comprende, además, en respuesta a seleccionar el segundo grupo de entidades, emplear al menos un procesador de hardware del sistema de servidor para determinar si la primera acción es indicativa de un ataque de malware según una segunda acción realizada por otro miembro del segundo grupo de entidades.

Según otro aspecto, un medio legible por ordenador no transitorio almacena instrucciones que, al ser ejecutadas por al menos un procesador de hardware de un sistema de servidor, provoca que el sistema de servidor cree un gestor de entidades y un motor de heurísticos. El gestor de entidades se configura para organizar una colección de entidades ejecutables monitorizadas en una pluralidad de grupos de entidades, en donde organizar la colección comprende, en respuesta a detectar que una primera entidad de la colección ha generado una entidad hija, determinar si la primera entidad pertenece a una categoría de entidades creadores de grupo. Organizar la colección comprende, además, en respuesta a determinar si la primera entidad pertenece a la categoría de creadores de grupo, cuando la primera entidad pertenece a la categoría de creadores de grupo, añadir un nuevo grupo de entidades a la pluralidad de grupos de entidades, y asignar la entidad hija al nuevo grupo de entidades. Organizar la colección comprende, además, en respuesta a la determinación de si la primera entidad pertenece a la categoría de creadores de grupo, cuando la primera entidad no pertenece a la categoría de creadores de grupo, seleccionar un primer grupo de entidades de la pluralidad de grupos de entidades de manera que la primera entidad sea un miembro del primer grupo de entidades, y asignar la entidad hija al primer grupo de entidades. El motor de heurísticos se configura, en respuesta a una primera acción realizada por la entidad hija, para seleccionar un segundo grupo de entidades de la pluralidad de grupos de entidades de manera que la entidad hija sea un miembro del segundo grupo de entidades, y en respuesta a seleccionar el segundo grupo de entidades, determinar si la primera acción es indicativa de un ataque de malware según una segunda acción realizada por otro miembro del segundo grupo de entidades.

Según otro aspecto, un sistema de servidor comprende al menos un procesador de hardware y una unidad de memoria, el al menos un procesador de hardware se configura para ejecutar un gestor de entidades y un motor de heurísticos. El gestor de entidades se configura para organizar una colección de entidades ejecutables monitorizadas en una pluralidad de grupos de entidades según un conjunto de relaciones entre entidades, de manera que al menos una entidad de la colección pertenece de manera simultánea a múltiples grupos de entidades, en donde el conjunto de relaciones entre entidades se selecciona de un grupo de relaciones que consisten en una relación de filiación y una relación de inyección de código. El motor de heurísticos se configura, en respuesta a una primera acción realizada por la al menos una entidad, para seleccionar un grupo de entidades de la pluralidad de grupos de entidades de manera que la al menos una entidad sea un miembro del grupo de entidades; y en respuesta a la selección del grupo de entidades, determinar si la primera acción es indicativa de un ataque de malware según una segunda acción realizada por otro miembro del grupo de entidades.

Breve descripción de los dibujos

Los aspectos y ventajas anteriores de la presente invención se entenderán mejor tras la lectura de la siguiente descripción detallada y tras la referencia a los dibujos donde:

La Fig. 1 muestra un conjunto ejemplar de objetos de software que incluyen una aplicación de seguridad que se ejecuta en un sistema de cliente según algunas realizaciones de la presente invención.

La Fig. 2 ilustra una configuración de hardware ejemplar de un sistema informático de cliente según algunas realizaciones de la presente invención.

La Fig. 3 muestra una estructura ejemplar de una aplicación de seguridad según algunas realizaciones de la presente invención.

La Fig. 4 ilustra un flujo de ejecución ejemplar de un conjunto de procesos en un entorno de Windows ©. Las flechas sólidas indican el flujo típico en ausencia de la aplicación de seguridad. Las flechas discontinuas indican las modificaciones al flujo de ejecución, las modificaciones introducidas por una pluralidad de eventos interceptores que operan según algunas realizaciones de la presente invención.

La Fig. 5-A ilustra un conjunto de grupos de entidades que comprende entidades ejecutables monitorizadas para un comportamiento malicioso según algunas realizaciones de la presente invención. Las flechas sólidas representan la creación de entidades; las flechas discontinuas representan la inyección de código.

La Fig. 5-B ilustra otro conjunto de grupos de entidades según algunas realizaciones de la presente invención.

La Fig. 6 muestra una secuencia ejemplar de pasos realizados por el gestor de entidades (Fig. 3) según algunas realizaciones de la presente invención.

La Fig. 7 muestra una secuencia de tiempo ejemplar de acciones realizadas por malware evasivo, y una firma de comportamiento según algunas realizaciones de la presente invención.

La Fig. 8-A ilustra otra firma de comportamiento ejemplar según algunas realizaciones de la presente invención.

La Fig. 8-B ilustra aún otra firma de comportamiento ejemplar según algunas realizaciones de la presente invención.

La Fig. 9 ilustra una secuencia ejemplar de pasos realizados por el motor de heurísticos (Fig. 3) según algunas realizaciones de la presente invención.

La Fig. 10-A muestra una pluralidad de objetos de puntuación de entidades (ESO), cada ESO determinado por una entidad ejecutable respectiva según algunas realizaciones de la presente invención.

La Fig. 10-B muestra una pluralidad de objetos de puntuación de grupos (GSO), cada GSO determinado por un grupo respectivo de entidades ejecutables, según algunas realizaciones de la presente invención.

La Fig. 11-A ilustra un conjunto ejemplar de valores de puntuación de entidades y de aumentos de puntuación de entidades asociados según algunas realizaciones de la presente invención.

La Fig. 11-B ilustra un conjunto ejemplar de valores de puntuación de grupos y de aumentos de puntuación de grupos asociados según algunas realizaciones de la presente invención.

La Fig. 12-A muestra una secuencia ejemplar de pasos realizada por el motor de puntuación (Fig. 3) según algunas realizaciones de la presente invención.

La Fig. 12-B muestra una secuencia alternativa de pasos realizada por el motor de puntuación según algunas realizaciones de la presente invención.

La Fig. 12-C muestra aún una secuencia alternativa de pasos realizada por el motor de puntuación según algunas realizaciones de la presente invención.

La Fig. 13 ilustra una secuencia ejemplar de pasos realizada por el módulo de limpieza (Fig. 3) según algunas realizaciones de la presente invención.

Descripción detallada de las realizaciones preferidas

En la siguiente descripción, se entiende que todas las conexiones entre estructuras indicadas pueden ser conexiones operativas directas o conexiones operativas indirectas a través de estructuras intermedias. Un conjunto de elementos incluye uno o más elementos. Cualquier indicación de un elemento se entiende como una referencia a al menos un elemento. Una pluralidad de elementos incluye al menos dos elementos. A menos que se requiera otra cosa, cualesquiera pasos de método descritos necesitan ser realizados necesariamente en un orden ilustrado concreto. Un primer elemento (por ejemplo, los datos) derivado de un segundo elemento abarca un primer elemento igual al segundo elemento, así como un primer elemento generado procesando el segundo elemento y opcionalmente otros datos. Tomar una determinación o una decisión según un parámetro abarca tomar la determinación o la decisión según el parámetro y de manera opcional según los otros datos. A menos que se especifique otra cosa, un indicador de alguna cantidad/datos puede ser la cantidad/datos en sí, o un indicador diferente de la cantidad/datos en sí. La seguridad informática abarca proteger a los usuarios y a los equipos contra accesos a los datos y/o al hardware no deseados o no autorizados, contra modificación de datos y/o de hardware no deseados o no autorizados, y contra la destrucción de datos y/o de hardware. Un programa informático es una secuencia de instrucciones de procesador que llevan a cabo una tarea. Los programas informáticos descritos en algunas realizaciones de la presente invención pueden ser entidades o sub entidades de software independientes (por ejemplo, sub rutinas, bibliotecas) de otros programas informáticos. A menos que se especifique de otra manera, un proceso es una instancia de un programa informático, tal como una aplicación o una parte de un sistema operativo, y se caracteriza por tener al menos un hilo de ejecución y un espacio de memoria virtual asignado a éste, en donde un contenido del espacio de memoria virtual respectivo incluye el código ejecutable. A menos que se especifique de otra manera, un heurístico es un procedimiento ejecutado para determinar si la ocurrencia de un conjunto de eventos es indicativa de una amenaza de seguridad informática. Los medios legibles por ordenador abarcan medios no transitorios tales como medios de almacenamiento magnéticos, ópticos, y semiconductores (por ejemplo, discos duros, discos ópticos, memoria flash, DRAM), así como enlaces de comunicación tales como cables conductivos y enlaces ópticos de fibra. Según algunas realizaciones, la presente invención proporciona, entre otras cosas, sistemas informáticos que comprenden hardware (por ejemplo, uno o más microprocesadores) programado para realizar los métodos descritos en la presente memoria, así como instrucciones de codificación de medios legibles por ordenador para realizar los métodos descritos en la presente memoria.

La siguiente descripción ilustra las realizaciones de la invención a modo de ejemplo y no necesariamente a modo de limitación.

La Fig. 1 muestra un conjunto ejemplar de objetos de software que se ejecutan en un sistema 10 de cliente protegido de las amenazas de seguridad informática según algunas realizaciones de la presente invención. El sistema 10 de cliente puede representar un sistema informático (por ejemplo, un ordenador de usuario final, un servidor corporativo, etc.). Otros sistemas 10 de cliente ejemplares incluyen los dispositivos informáticos móviles (por ejemplo, portátiles, PC tabletas), dispositivos de telecomunicación (por ejemplo, teléfonos inteligentes), aparatos de entretenimiento digitales (TV, videoconsolas, etc.), dispositivos informáticos portátiles (por ejemplo, relojes

inteligentes), o cualquier otro dispositivo electrónico que tenga un procesador y una memoria, y que requiera protección de seguridad informática.

En algunas realizaciones, un sistema operativo 30 (OS) comprende un software que proporciona una interfaz al hardware del sistema 10 de cliente, y actúa como un servidor para un conjunto de aplicaciones 32a-c y 36 de software. El OS 30 puede comprender cualquier sistema operativo ampliamente disponible tal como Windows®, MacOS®, Linux®, iOS®, o Android®, entre otros. Las aplicaciones 32a-c representan de manera genérica software de usuario, que puede incluir, por ejemplo, el procesamiento de texto, el procesamiento de imagen, las bases de datos, el navegador, y aplicaciones de comunicación electrónica, entre otros. En algunas realizaciones, una aplicación 36 de seguridad se ejecuta de manera concurrente con las aplicaciones 32a-c y se configura para determinar si cualquier software que se ejecuta en un sistema 10 cliente (incluyendo las aplicaciones 32a-c y el OS 30) plantea una amenaza a la seguridad informática. Por ejemplo, la aplicación 36 puede detectar malware y/o spyware. La aplicación 36 se puede configurar además para eliminar o de otra manera incapacitar dicho software malicioso, y para alertar a un usuario del sistema 10 de cliente o un administrador de sistema. La aplicación 36 de seguridad puede ser un programa independiente, o puede formar parte de un paquete de software que comprende, entre otras cosas, componentes anti malware, anti spam, y anti fraude. El funcionamiento de la aplicación 36 de seguridad se describe en detalle más adelante.

La Fig. 2 ilustra una configuración de hardware ejemplar del sistema 10 de cliente, en donde el sistema 10 de cliente es un sistema informático. Una persona experta apreciará que la configuración de hardware de otros dispositivos tales como las tabletas PC, los teléfonos inteligentes, los relojes inteligentes, etc., puede diferir de la configuración ilustrada, pero que la presente descripción se puede adaptar a dichos dispositivos. El sistema 10 de cliente comprende un conjunto de dispositivos físicos, que incluyen un procesador 12 de hardware, una unidad 14 de memoria, un conjunto de dispositivos 16 de entrada, un conjunto de dispositivos 18 de salida, un conjunto de dispositivos 20 de almacenamiento, y un conjunto de adaptadores 22 de red, todos interconectados por un centro 24 controlador.

En algunas realizaciones, un procesador 12 comprende un dispositivo físico (por ejemplo, un microprocesador, un circuito integrado multi núcleo formado en un sustrato semiconductor) configurado para ejecutar operaciones computacionales y/o lógicas con un conjunto de señales y/o datos. En algunas realizaciones, dichas operaciones lógicas se transmiten al procesador 12 desde una unidad 14 de memoria, en forma de una secuencia de instrucciones de procesador (por ejemplo, código máquina u otro tipo de software). La unidad 14 de memoria puede comprender medios legibles por ordenador volátiles (por ejemplo, una RAM) que almacenan datos/señales accedidas o generadas por el procesador 12 en el curso de la ejecución de las instrucciones. Los dispositivos 16 de entrada pueden incluir interfaces de hardware y/o adaptadores que permiten a un usuario introducir datos y/o instrucciones en el sistema 10 de cliente. Los dispositivos 18 de salida pueden incluir dispositivos de presentación tales como monitores y altavoces, entre otros, así como interfaces/adaptadores de hardware tales como tarjetas gráficas, que permitan el sistema 10 de cliente comunicar los datos a un usuario. En algunas realizaciones, los dispositivos 16 de entrada y los dispositivos 18 de salida pueden compartir una pieza común de hardware, como en el caso de los dispositivos de pantallas táctiles. Los dispositivos 20 de almacenamiento incluyen medios legibles por ordenador que permiten el almacenamiento no volátil, la lectura, y la escritura de instrucciones de procesador y/o datos. Los dispositivos 20 de almacenamiento ejemplares incluyen discos magnéticos y ópticos y dispositivos de memoria flash, así como medios extraíbles tales como discos y unidades CD y/o DVD. El conjunto de adaptadores 22 de red permite a un sistema 10 de cliente conectarse a una red (por ejemplo, a una red de área local, a una red inalámbrica, etc.) y/o a otros dispositivos/sistemas informáticos. El centro 24 controlador representa generalmente la pluralidad de buses de sistema, periféricos, y/o del conjunto de chips, y/o toda la otra circuitería que permite la comunicación entre el procesador 12 y los dispositivos 14, 16, 18, 20 y 22. Por ejemplo, el centro 24 controlador puede comprender un procesador 12 de conexión de puente norte a la memoria 14, y/o un procesador 12 de conexión de puente sur a los dispositivos 16, 18, 20 y 22.

La Fig. 3 muestra componentes ejemplares de una aplicación 36 de seguridad según algunas realizaciones de la presente invención. La aplicación 36 de seguridad comprende un motor 48 de puntuación y un módulo 56 de limpieza, ambos conectados a un gestor 42 de comportamiento, El gestor 42 de comportamiento comprende además un gestor 44 de entidades acoplado a un motor 46 de heurísticos.

En algunas realizaciones, el gestor 42 de comportamiento recibe un conjunto de notificaciones 40 de eventos desde un conjunto de interceptores 28a-c de eventos instalados dentro de diversos objetos de software que se ejecutan en un sistema 10 de cliente. Las notificaciones 40 de eventos puede informar por tanto al gestor 42 de comportamiento sobre la ocurrencia de diversos eventos durante la ejecución de software. Los eventos notificados ejemplares pueden incluir, entre otras cosas, la creación de un proceso o hilo, la inyección de código, una llamada de sistema, un intento de crear un nuevo archivo de disco, un intento de escribir a un archivo de disco existente, un intento de editar una clave de registro de sistema, y un intento de escribir en una sección de memoria concreta. Algunos de los eventos notificados pueden ser indicativos de malware. Otros eventos pueden no ser en sí indicativos de una amenaza de seguridad, pero puede indicar una amenaza potencial al ocurrir junto con otros eventos. En respuesta a la recepción de la notificación o notificaciones 40, algunas realizaciones del gestor 42 de comportamiento pueden acceder a la base de datos 26 de heurísticos y seleccionar las rutinas de detección según los detalles de la notificación o notificaciones 40, implementando las rutinas seleccionadas el heurístico o heurísticos concretos. El

gestor 42 de comportamiento puede enviar además las rutinas de detección respectivas al motor 46 de heurísticos para su ejecución. La ejecución de las respectivas rutinas puede proporcionar una alerta 50 de puntuación al motor 48 de puntuación. El motor 48 de puntuación puede mantener una pluralidad de dichos indicadores de evaluación (por ejemplo, las puntuaciones) y puede alcanzar una alerta cuando al menos uno de dichos indicadores indica una amenaza de seguridad informática. El funcionamiento de los componentes 44, 46, 48 y 56 se describe en detalle más adelante.

Para ilustrar el funcionamiento de los interceptores 28a-c de eventos. La Fig. 4 muestra un flujo de ejecución ejemplar de un conjunto de entidades 60a-b de software según algunas realizaciones de la presente invención. Por simplicidad, las entidades 60a-b elegidas son procesos que se ejecutan en una instancia de un OS Windows®, se pueden procesar diagramas similares para otros sistemas operativos tales como Linux, por ejemplo, Las flechas sólidas representan el flujo de ejecución en ausencia de los interceptores de eventos. Las flechas discontinuas representan las modificaciones al flujo debidas a la presencia de los interceptores 28a-c de eventos que se ejecutan según algunas realizaciones de la presente invención.

El proceso 60a ejemplar carga una pluralidad de bibliotecas 62a-c de enlace dinámico (DLL); en el ejemplo de la Fig. 4, la DLL 62c se inyecta en el proceso 60a mediante el proceso 60b (posiblemente malicioso). Cuando el proceso 60a (o uno de sus DLL descargadas) ejecuta una instrucción que llama a alguna funcionalidad de sistema, por ejemplo, escribir algo a un archivo de disco, o para editar una clave de registro, la respectiva instrucción llama a una interfaz de programación de aplicaciones (API) tal como KERNEL32.DLL o NTDLL.DLL. En el ejemplo de la Fig. 4, la respectiva llamada API de modo usuario es interceptada por un interceptor 28a de eventos de nivel de usuario. Dichas intercepciones se pueden conseguir mediante un método tal como la inyección o enganche de DLL, entre otros. El enganche es un término genérico usado en la técnica para un método de llamadas, mensajes, o eventos de función de intercepción, pasados entre los componentes de software. Un método de enganche ejemplar comprende alterar el punto de entrada de una función objetivo, insertando una instrucción (en este caso, el interceptor 28a de eventos) que redirige la ejecución a una segunda función. Después de dicho enganche, la segunda función puede ser ejecutada en su lugar, o antes, de la función destino. En el ejemplo de la Fig. 4, la aplicación 36 de seguridad puede enganchar en ciertas funciones de las bibliotecas KERNEL32.DLL y/o NTDLL.DLL, para dar instrucciones a las respectivas funciones para redirigir la ejecución a un componente de la aplicación 36. Por tanto, la aplicación 36 puede ser notificada cuando el proceso 60a está intentando realizar una acción concreta, identificada según la función de enganche.

En un flujo típico de ejecución, la función API del modo usuario llamada por la entidad 60a puede solicitar servicio desde el sistema operativo del núcleo. En algunas realizaciones, dichas operaciones son llevadas a cabo emitiendo una llamada al sistema, tal como SYSCALL y SYSENTER en las plataformas x86. En el ejemplo de la Fig. 4, dichas llamadas al sistema son interceptadas por el interceptor 28b de eventos. En algunas realizaciones, dicha intercepción comprende, por ejemplo, modificar una rutina manejadora de llamadas de sistema cambiando un valor almacenado en un registro específico de modelo (MSR) del procesador 12, que efectivamente redirige la ejecución de la rutina del manejador al interceptor 28b o directamente a un componente de la aplicación 36. Dichas técnicas son conocidas en la técnica como enganche MSR, y pueden permitir a la aplicación 36 ser notificada cuando una entidad de software está intentando realizar ciertas llamadas al sistema.

Siguiendo la llamada de sistema, el control del procesador es normalmente entregado al núcleo del OS 30. En algunas realizaciones, se configura un interceptor 28c de eventos para interceptar ciertas acciones del núcleo del OS, y por lo tanto determinar que el proceso evaluado está intentando realizar ciertas operaciones, que pueden ser indicativas de malware. Para interceptar dichas acciones, algunas realizaciones pueden emplear un conjunto de mecanismos de filtrado construidos en y expuestos por el OS 30. Por ejemplo, en un OS de Windows®, se puede usar el FiltroRegistroFlt para interceptar operaciones como la creación, apertura, escritura y, eliminación de un archivo. En otro ejemplo, el interceptor 28c de eventos puede usar LlamadaRegistroOb para interceptar la creación de nuevos procesos. En aún otro ejemplo, las operaciones de registro de Windows tales como la creación y configuración de las claves/valores de registro pueden ser interceptadas usando ExLlamadaRegistroCm. Mecanismos de filtrado de eventos similares son conocidos en la técnica para otros sistemas operativos tales como Linux®. En respuesta a la detección de la ocurrencia de un evento/acción concreto, el interceptor 28 de eventos puede transmitir la notificación o notificaciones 40 a la aplicación 36 de seguridad.

En algunas realizaciones, la aplicación 36 de seguridad monitoriza una pluralidad de entidades de software en busca de un comportamiento malicioso. Las entidades de software monitorizadas pueden variar en complejidad desde los hilos de ejecución individuales, a los procesos, las aplicaciones completas, los entornos de trabajo y las máquinas virtuales. Por simplicidad, la siguiente representación supondrá que las entidades monitorizadas son procesos, pero esta suposición no debería limitar el alcance de la presente invención. Una persona experta apreciará que los sistemas y métodos descritos se pueden extender a otros tipos de entidades ejecutables además de los procesos individuales.

Algunas realizaciones de la presente invención dividen las entidades ejecutables (por ejemplo, los procesos) en varias distintas categorías desde la perspectiva de la monitorización de un comportamiento malicioso. Dichas categorías pueden incluir, entre otras cosas, creadores de grupos, herederos de grupos, y entidades no monitorizadas. En algunas realizaciones, los creadores de grupos incluyen ciertos procesos, componentes, y

servicios del sistema operativo, tales como el Winlogon y el Service Host (svchost.exe) en Windows®. Otras entidades creadores de grupo pueden incluir, entre otros, los procesos de gestores de archivos y/o los componentes (por ejemplo, Windows Explorer®, File Explorer®, Total Commander®, etc.), y o procesos o componentes de navegador (por ejemplo, Internet Explorar®, Firefox®, Chrome®, etc.). la categoría de herederos de grupo puede incluir la mayoría de los procesos de usuario, así como las entidades desconocidas o las entidades que no pueden ser identificadas como creadores de grupo. Una categoría adicional puede representar las entidades que están exentas de monitorización. Dichas entidades no monitorizadas pueden incluir, por ejemplo, ciertos procesos protegidos por el sistema operativo (por ejemplo, csrss.exe y el smss.exe en las plataformas Windows®), y las entidades que forman parte de la aplicación 36 de seguridad. En algunas realizaciones, una categoría de entidad puede cambiar durante su tiempo de vida. Por ejemplo, una entidad creadora de grupo puede resultar un heredero de grupo, tal como se muestra a continuación.

Algunas realizaciones de la aplicación 36 de seguridad pueden determinar que categoría de cada entidad pertenece a según ciertas características de la entidad respectiva, tal como una ruta, un nombre de archivo, un conjunto de recursos (por ejemplo, bibliotecas cargadas en el lanzamiento), una entrada de registro de OS, una firma digital, y una ubicación de memoria de la entidad respectiva. Otros indicativos de datos de si una entidad pertenece a una categoría concreta comprende un indicador de si la entidad respectiva usa ciertos dispositivos de hardware (por ejemplo, los adaptadores 22 de red). En una realización ejemplar, la aplicación de seguridad puede realizar una auditoría del sistema 10 de cliente y/o del OS 30 para ubicar un conjunto de recursos asociados a entidades creadores de grupos tales como los servicios de OS, los navegadores, y los gestores de archivos, y más tarde utilizar esa información para determinar si una entidad existente pertenece a una categoría u otra. La aplicación 36 de seguridad puede identificar además una entidad y establecer su categoría comparando un conjunto de hashes de la entidad respectiva a una base de datos de hashes de entidades conocidas.

En algunas realizaciones, el gestor 44 de entidades mantiene una estructura de datos (por ejemplo, una lista) de entidades que se ejecutan en el sistema 10 de cliente, y actualiza de manera dinámica la estructura de datos respectiva para reflejar la adición de nuevas entidades (por ejemplo, en respuesta a la creación de procesos) y la eliminación de otras entidades (en respuesta a la terminación de procesos). Por simplicidad, las entidades actualmente en la lista de entidades de ejecución se consideran de aquí en adelante entidades actuales. En algunas realizaciones, cada entidad en la lista de entidades actuales representa una instancia distinta de un objeto ejecutable. La lista de entidades actuales puede comprender por lo tanto múltiples instancias del mismo objeto ejecutable. En uno de dichos ejemplos en donde una aplicación de navegador web ejecuta cada pestaña del navegador como un proceso separado, cada uno de dichos procesos puede ser una entidad monitorizada separada.

El gestor 44 de entidades divide además las entidades actuales en una pluralidad de grupos, cada grupo comprendiendo sólo entidades mutuamente relacionadas, y mantiene un conjunto de asociaciones que indican, por ejemplo, que entidad es parte de cada grupo. Las entidades pueden estar relacionadas a través de filiación y/o inyección de código, entre otras maneras. Por filiación en el presente documento se refiere a una entidad del grupo que es hija o padre de otra entidad. Los procesos hijos se pueden crear, por ejemplo, a través de generación (en Windows®) o bifurcación (en OS derivados de Unix). En algunas realizaciones, la misma entidad puede pertenecer de manera simultánea a una pluralidad de distintos grupos. En uno de dichos ejemplos, una entidad es parte de un primer grupo porque es bien la hija o el padre de otro miembro del primer grupo, y a la vez es parte de un segundo grupo porque otro miembro del segundo grupo ha inyectado código en ésta.

Las Fig. 5-A-B ilustran diversos grupos de entidades ejemplares mantenidas por el gestor 44 de entidades según algunas realizaciones de la presente invención. Las ilustracionrd usan triángulos para denotar las entidades creadoras de grupo, círculos para denotar entidades herederas de grupos, y cuadrados para denotar entidades no monitorizadas. Las flechas sólidas indican filiación, mientras que las flechas discontinuas indican inyección de código. La dirección de cada flecha puede indicar una dirección de la relación entre las respectivas entidades conectadas. Por ejemplo, en a Fig. 5-A, la entidad E_6 es hija de una entidad E_5, mientras que la entidad E_7 ha inyectado código en la entidad E_{14}.

Los creadores de grupo pueden pertenecer o no a un grupo. Algunas realizaciones asignan un grupo distinto a cada entidad creadora de grupo (por ejemplo, grupos como G_1 y G_6 en la Fig. 5-A). Dichos grupos puede tener sólo un miembro, esto es, la respectiva entidad creadora de grupo. En algunas realizaciones, los creadoras de grupo crean nuevos grupos cuando generan nuevas entidades. En el ejemplo de la Fig. 5-A, la entidad E_1 creadora de grupo crea un grupo G_5 cuando genera la entidad E_5 hija. En algunas realizaciones, cuando un a entidad heredera de grupo genera otra entidad o inyecta código en otra entidad, la otra entidad se incluye en el mismo grupo como la entidad heredera de grupos. En el ejemplo de la Fig. 5-A, la entidad E_6 se incluye en el mismo grupo que su entidad E_5 padre De manera similar, la entidad E_{14} se incluye en el mismo grupo como entidad E7 en respuesta a recibir el código inyectado desde E_7.

En algunas realizaciones, una categoría de la entidad puede cambiar en respuesta a ciertos eventos y/o en respuesta a resultar parte de un grupo. En el ejemplo de la Fig. 5-A, la entidad E_{14} fue inicialmente una entidad creadora de grupo (véase el grupo G_{11}). Después, en respuesta a la recepción del código inyectado desde un miembro del grupo G_5, la entidad E_{14} resulta parte del grupo G_5y se volvió a marcar como una heredera de grupo. El mismo tratamiento se puede aplicar a la entidad E_1 en la Fig. 5-B.

Una entidad puede pertenecer de manera simultánea a múltiples grupos. En el ejemplo de la Fig. 5-B, la entidad E_5 (una heredera de grupo) es simultáneamente un miembro de los grupos G_3, G_5 y G_6. E_5 es parte de G_3 como que es una destinataria de código inyectado desde la entidad E_3. De manera similar, E_5 es parte de G_6 ya que E_5 recibe código inyectado desde E_6. La entidad E_5 es además parte del grupo G_5 ya que este fue generado por el creador E_2 de grupo. Cuando la entidad E_5 genera la entidad E_9 hija, E_9 resulta un miembro de ambos grupos G_3 y G_5. De manera similar, en la Fig. 5-A, cuando la entidad E_{14} (ahora una heredera de grupo, vea la discusión anterior) genera una nueva entidad E_{15}, la entidad $E1_5$ puede ser incluida en ambos grupos G_5 y G_{11}.

La Fig. 6 muestra una secuencia ejemplar de pasos realizada por el gestor 44 de entidades (Fig. 3) para gestionar la lista de entidades actuales según algunas realizaciones de la presente invención. En una secuencia de pasos 150-152, el gestor 44 de entidades intercepta un evento de ciclo de vida de la entidad, y cuando dicho evento ha ocurrido, la secuencia de pasos 154-155 identifica el tipo de evento y las entidades afectadas. En algunas realizaciones. Los eventos de ciclo de vida comprenden la creación de procesos, la inyección de código, y la terminación de procesos, entre otras cosas. Detectar dichos eventos puede comprender recibir una notificación o notificaciones 40 de eventos desde un interceptor de eventos apropiado, por ejemplo, el interceptor 28c en la Fig. 4. El gestor 44 de entidades puede identificar las entidades afectadas por el evento de ciclo de vida actual (por ejemplo, el proceso padre e hijo, en el caso de generación) analizando una estructura de datos usada por el OS 30 para gestionar los procesos actualmente en ejecución. En el OS Windows®, cada proceso está representado como un bloque de procesos ejecutivos (EPROCESS), que comprende, entre otras cosas, referencias a cada uno de los hilos del proceso respectivo, y un único ID de proceso que permite al OS 30 identificar al proceso respectivo de una pluralidad de procesos en ejecución. Representaciones similares de procesos/hilos están disponibles para otros OS, tales como Linux.

Un paso 156 determina si el evento comprende una creación de una nueva entidad (por ejemplo, un nuevo proceso), y cuando no, el gestor 44 de entidades avanza hasta un paso 170 descrito más adelante. Cuando el evento comprende la creación de entidades, en un paso 158, el gestor 44 determina si la entidad padre es un heredero de grupo, y cuando no, el gestor 44 avanza al paso 164. Cuando si, en una secuencia de pasos 160-162, el gestor 44 puede añadir la entidad hija al grupo o grupos de la entidad padre y marcar la entidad hija como una heredera de grupo. En el paso 164, el gestor 44 determina si la entidad padre es una creadora de grupo. Cuando si, en una secuencia de pasos 166-168, el gestor 44 puede crear un nuevo grupo y añadir la entidad hija al grupo recientemente creado.

En algunas realizaciones, el paso 170 determina si el evento de ciclo de vida detectado comprende una inyección de código, y cuando no, el gestor 44 puede avanzar a un paso 174. Como regla general, la aplicación 36 de seguridad puede interpretar cada evento de inyección de código como sospechoso, lo que posiblemente indica actividades maliciosas. Sin embargo, algunas entidades del OS inyectan de manera legítima código dentro de otras entidades, en situaciones muy específicas. Dichas situaciones son comúnmente conocidas en la comunidad de seguridad como excepciones, y normalmente están exentas de procesamiento anti malware para no generar de manera accidental una detección de falso positivo. En algunas realizaciones, un paso 171 comprueba si se puede confiar en que la inyección sea legítima, por ejemplo, intentando hacer coincidir los detalles del evento de inyección respecto a una lista de excepciones. Cuando la inyección de código respectiva no es reconocida como un tipo conocido de inyección legítima, en un paso 172 un gestor 44 puede añadir la entidad que recibe el código inyectado al grupo o grupos de la entidad que realiza la inyección de código. En algunas realizaciones, un paso 173 adicional marca la entidad receptora como un heredero de grupo.

En el paso 174, el gestor 44 determina si el evento comprende la terminación de una entidad, y cuando no, el gestor 44 vuelve al paso 150. Por ejemplo, se termina un proceso cuando todos los hilos del proceso respectivo han finalizado su ejecución. Algunas realizaciones pueden mantener una entidad terminada como parte de un grupo, por ejemplo, hasta que sus entidades hijas estén terminadas, o hasta que todos los miembros del grupo respectivo estén terminados. En dichas realizaciones, la entidad terminada puede estar marcada como muerta (paso 176). Esta estrategia puede permitir limpiar al sistema 10 de cliente de los efectos del malware evasivo, por ejemplo, de los efectos de una entidad que genera hijos maliciosos y después sale. En otras realizaciones, cuando el evento de ciclo de vida detectado comprende la terminación de la entidad, el gestor 44 elimina la entidad terminada de todos los grupos.

En algunas realizaciones, el motor 46 de heurísticos (Fig. 3) realiza un conjunto de pruebas o procedimientos, llamados genéricamente en la presente memoria heurísticos, para determinar si la ocurrencia de un conjunto de eventos dentro del sistema 10 de cliente es indicativo de una amenaza de seguridad, por ejemplo, es indicativa de malware. Cuando el heurístico o heurísticos concluyen que el conjunto de eventos es indicativo de malware, el motor 46 puede transmitir una alerta 50 de puntuación al motor 48 de puntuación, que puede determinar si el sistema 10 de cliente comprende malware. El motor 46 de heurísticos es notificado de la ocurrencia de un evento mediante los interceptores 28a-c de eventos.

Algunos heurísticos pueden estar relacionados a la entidad, en el sentido de que determinan si la ocurrencia de un evento es indicativa de que una entidad individual es maliciosa. Dichos heurísticos serán referidos de aquí en adelante como heurísticos de entidad. Otros heurísticos pueden estar relacionados a un grupo (y llamados en la

presente memoria heurísticos de grupo), en el sentido de que determinan si la ocurrencia de un evento es indicativa de que un grupo completo de entidades es malicioso.

Cada heurístico puede realizar un método de detección de malware distinto. En algunas realizaciones, cada heurístico se puede configurar para detectar la presencia de una categoría, familia, tipo, o variante de agente malicioso concreto. Los diversos heurísticos distintos pueden colaborar en la detección de una única categoría, familia, tipo, o variante de agente malicioso. En algunas realizaciones, un heurístico único puede participar en la detección de diversas categorías, tipos, familias, o variantes de malware. Un ejemplo concreto de heurístico comprueba la ocurrencia de una secuencia concreta de eventos (una firma de comportamiento) en el sistema 10 de cliente. No todos los eventos de la secuencia necesitan ser provocados por la misma entidad. Sin embargo, la ocurrencia de dicha secuencia de eventos puede ser indicativa de malware. En uno de dichos ejemplos, ilustrado en la Fig. 7, las actividades maliciosas se dividen entre un grupo de entidades E_1-E_4, llevando a cabo cada miembro del grupo una pequeña parte de las actividades maliciosas. La secuencia concreta de acciones A_1-A_6 se suma a una firma 68 de comportamiento que identifica un ataque de malware concreto.

La Fig. 7 ilustra una firma de comportamiento ejemplar asociada con un ataque de ransomware. El ransomware es un tipo concreto de malware, que cifra un conjunto de archivos en el ordenador de un usuario, y después pide al usuario pagar par recuperar los respectivos archivos. La creación de entidades se ilustra en una flecha zigzagueante. Cada línea vertical sólida muestra el historial de vida de cada entidad. Por ejemplo, la entidad E_1 muere después de generar la entidad E_2. La entidad E_3 se convirtió en parte del grupo ilustrado en respuesta a la recepción del código inyectado de E_2. Algunas acciones de las respectivas entidades no son parte de la firma 68. Por ejemplo, la generación en la entidad E_3 de la entidad E_4 no está incluida en la firma 68.

Las Fig. 8A-B ilustran dichas firmas de comportamiento ejemplares. La firma 68a requiere que las acciones A_1-A_6 sean llevadas a cabo en el orden indicado exacto. Al contrario, la firma 68b ejemplar permite que algunas acciones (A_3, A_4 y A_5) sean realizadas en cualquier orden, siempre que se produzcan entre A_2 y A_6. La flexibilidad ofrecida por firmas tales como la 68b puede permitir detectar diversas versiones, variantes, o una familia completa de agentes maliciosos. En algunas realizaciones, un heurístico que usa una firma de comportamiento concreta se configura para detectar la ocurrencia de la secuencia concreta de eventos (o acciones) indicada por la respectiva firma de comportamiento. El respectivo heurístico puede verificar además las relaciones entre las entidades que realizan las acciones (por ejemplo, pueden verificar que todas las entidades participantes son parte del mismo grupo). En algunas realizaciones son implícitas. Por ejemplo, un grupo de heurísticos configurados para implementar una firma de comportamiento concreta pueden ser inicializados una vez para un grupo de entidades seleccionadas. El respectivo heurístico de grupo puede ser desencadenado después sólo cuando un miembro del grupo respectivo realice una acción. Discusión y ejemplos adicionales de los heurísticos de grupo se proporcionan más adelante.

En algunas realizaciones, el motor 46 de heurísticos interactúa con una base de datos 26 de heurísticos, que puede residir en los dispositivos 20 de almacenamiento del sistema 10 de cliente, o en un medio legible por ordenador acoplado de manera comunicativa con el sistema 10 de cliente. La base de datos 26 puede comprender una colección de heurísticos disponibles y un indicador de una asociación entre los heurísticos y los tipos de eventos que desencadenan el uso de los heurísticos respectivos. Dichas asociaciones permiten al motor 46 de heurísticos recuperar de manera selectiva un heurístico en respuesta a ser notificado de la ocurrencia de un evento de un tipo concreto. Una realización ejemplar de la base de datos 26 es una biblioteca de software, por ejemplo, una DLL.

En algunas realizaciones, los heurísticos se codifican en código de byte (un conjunto de instrucciones multi plataforma). Los ejemplos de códigos de byte incluyen los lenguajes de programación Java® y Lua®. Cada heurístico puede ser codificado y entregado como una rutina de código de byte separada. En dichas realizaciones, el motor 46 de heurísticos puede incluir una máquina virtual de traducción de códigos de byte (por ejemplo, un interpretador o un compilador a tiempo) que traduce el código de byte en una secuencia de instrucciones nativas de procesador y ejecuta la secuencia respectiva. Dichas realizaciones pueden facilitar el desarrollo y acortan el tiempo hasta estar en mercado de la aplicación 36 de seguridad.

La Fig. 9 ilustra una secuencia ejemplar de pasos realizados por el motor 46 de heurísticos, según algunas realizaciones de la presente invención. Una secuencia de pasos 200-202 escucha en busca de notificaciones de eventos desde los interceptores 28a-c. En respuesta a la recepción de la notificación 40 de evento, un paso 204 determina un tipo y un conjunto de parámetros de evento del respectivo evento notificado. Los tipos de eventos ejemplares incluyen, entre otros casos, la inyección de código, una llamada de sistema concreta, la creación de un archivo de disco, y una solicitud HTTP. Los parámetros de eventos pueden ser específicos de cada tipo de evento notificado. Algunos parámetros de eventos ejemplares incluyen, entre otras cosas, un identificador de un proceso o hilo (por ejemplo, un ID de proceso) que realiza la acción notificada, un nombre de archivo, una ruta, una dirección de memoria, y un operando de una instrucción de procesador. Los parámetros de eventos pueden ser determinados por los interceptores 28a-c e incluidos en la notificación o notificaciones 40 de eventos o puede ser determinado por el motor 46 heurístico en respuesta a la recepción de notificaciones 40. En un ejemplo en donde el evento notificado es un intento de crear un nuevo archivo de disco, los parámetros de evento pueden incluir el nombre del archivo que se crea. El nombre de archivo respectivo puede ser determinado por el interceptor de eventos y transmitido al motor 46 de heurísticos como parte de la notificación 40. En algunas realizaciones, los parámetros de eventos incluyen una marca de tiempo que indica el momento en el tiempo en que el respectivo evento ocurrió o fue detectado. Las

marcas de tiempo pueden ser usadas además por el motor 46 de heurísticos para determinar si ciertos eventos se producen en secuencia (véase, por ejemplo, la descripción anterior en relación con las firmas de comportamiento).

En una secuencia de pasos 206-208, el motor 46 puede acceder a la base de datos 26 de heurísticos y recuperar de manera selectiva un conjunto de heurísticos según el tipo y los parámetros del evento notificado. Un paso 209 adicional aplica el heurístico o heurísticos seleccionados para determinar si el evento notificado es indicativo de malware. Cuando el respectivo heurístico o heurísticos indican una sospecha de malicia, en un paso 212, el motor 46 envía una alerta 50 de puntuación al motor 48 de puntuación. La alerta 50 de puntuación puede incluir un identificador del respectivo heurístico o heurísticos, y puede incluir además un identificador de una entidad y/o grupo sospechoso.

Algunas realizaciones del motor 46 de heurísticos operan con diversos tipos distintos de variables tales como LOCALES, ESTÁTICAS, ENTIDADES, GRUPOS, y GLOBALES, entre otras. Las variables de tipo LOCAL pueden ser únicas para cada instancia de un heurístico. Las variables de tipo ESTÁTICO pueden ser específicas para cada heurístico, en el sentido de que su valor puede ser compartido a través de múltiples instancias de este heurístico. Las variables de tipo GLOBAL pueden ser compartidas a través de todos los heurísticos e instancias de este. Las variables de tipo ENTIDAD pueden estar unidas de manera única a una dupla <heurístico, entidad>, compartida a través de las múltiples instancias de este heurístico, pero que difieren de una entidad a otra. Las variables de tipo ENTIDAD pueden ser inicializadas una vez para cada entidad mencionada, y eliminadas tras la terminación de la respectiva entidad. Las variables de tipo GRUPO pueden estar unidas de manera única a una dupla <heurístico, grupo>, compartida a través de las múltiples instancias de este heurístico, pero que difieren de un grupo de entidades a otro. Las variables de tipo GRUPO pueden ser inicializadas una vez para cada grupo de entidades. Dichas realizaciones permiten a ciertos heurísticos comprobar, por ejemplo, en busca de firmas de comportamiento complejas en donde las actividades maliciosas se distribuyen a través de las múltiples entidades.

En algunas realizaciones, el motor 48 de puntuaciones mantiene y actualiza una pluralidad de puntuaciones de malicia determinadas para una pluralidad de entidades monitorizadas y/o grupos de entidades que se ejecutan en el sistema 10 de cliente. El motor 48 de puntuaciones puede determinar además si el sistema 10 de cliente comprende software malicioso según las respectivas puntuaciones. En algunas realizaciones, el motor 48 de puntuaciones recibe la alerta 50 de puntuación del motor 46 de heurísticos cuando el motor 46 determina que la ocurrencia de un evento concreto es indicativa de malicia. En respuesta a la detección de malware, el motor 48 de puntuación puede enviar además un indicador 58 de malicia al módulo 56 de limpieza.

La Fig. 10-A muestra una pluralidad de objetos 74a-c de puntuación de entidades ejemplares (ESO), estando cada ESO determinado por el motor 48 de puntuación para una entidad 70a-c de software respectiva, según algunas realizaciones de la presente invención. Cada ESO puede comprender una pluralidad de campos de datos, algunos de los cuales se ilustran en la Fig. 10-A. Dichos campos incluyen un identificador 76a de entidad único, una pluralidad de puntuaciones 76b de evaluación de entidad actual, y una puntuación 76d de agregación de entidad actual. En algunas realizaciones, las puntuaciones 76b de evaluación de entidad son determinadas por el motor 48 según las alertas 50 de puntuación recibidas desde el motor 46 de heurísticos. Cada puntuación 76b puede estar determinada según un criterio diferente. Por ejemplo, las puntuaciones 76b pueden tener una correspondencia uno a uno con un conjunto de heurísticos 76c, de manera que cada puntuación de evaluación de entidad es atribuida según el heurístico respectivo. En uno de dichos ejemplos, un heurístico H_k concreto comprende la determinación de si una entidad monitorizada descarga un archivo desde una red informática tal como Internet. La puntuación S_k respectiva puede entonces ser premiada o aumentada sólo cuando la respectiva entidad evaluada intenta una descarga. En algunas realizaciones, la puntuación 76d de agregación de entidad se calcula como una suma de las puntuaciones 76b de evaluación de entidades actuales (véanse detalles adicionales más adelante).

En algunas realizaciones, cada ESO puede incluir además un indicador de una asociación entre la entidad respectiva y los grupos a los que pertenece. Por ejemplo, en el ejemplo de la figura 10-A, el elemento 76f ilustra dicha lista de grupos de entidades. En una realización alternativa, el motor 48 de puntuaciones puede recuperar de manera dinámica una lista de grupos que tienen una cierta entidad como un miembro del gestor 44 de entidades.

Algunas realizaciones del motor 48 de puntuación mantienen además un conjunto de puntuaciones asociadas con cada grupo de entidades. La Fig. 10-B muestra una pluralidad de objetos 75a-c de puntuación de grupos ejemplares (GSO), estando cada GSO determinado por un grupo distinto de entidades de software. Cada GSO ilustrado comprende un identificador 77a de grupo único GID, una pluralidad de puntuaciones 77b de evaluación de grupo actuales, y una puntuación 77d de agregación de grupo actual (el superíndice G indica que los elementos respectivos están asociados con un grupo de entidades a diferencia de una entidad única). En algunas realizaciones, cada puntuación de evaluación de grupo se premia y/o se aumenta según un criterio distinto (por ejemplo, un heurístico distinto). Un heurístico ejemplar que establece y/o aumenta las puntuaciones de evaluación de grupos implementa una firma de comportamiento tal como se ilustra en la Fig. 7. Usando ese ejemplo, una puntuación de evaluación de grupo correspondiente al grupo que comprende las entidades E_1, E_2 y E_3 se puede aumentar cuando las entidades E_1, E_2 y E_3 realizan las acciones A_1-A_6 en el orden ilustrado. Los heurísticos de grupo correspondientes a cada puntuación de evaluación de grupo se ilustran como los elementos 77c en la Fig. 10-B-

En algunas realizaciones, cada GSO puede además comprender un indicador de una asociación entre el grupo respectivo y sus entidades miembro. En el ejemplo de la Fig. 10-B, las entidades $E_1^{(G1)}$, $E_2^{(G1)}$, etc., son miembros del grupo G_1. De manera alternativa, los motores 48 de puntuación pueden solicitar datos sobre la pertenencia a un grupo del gestor 44 de entidades en cualquier momento. En algunas realizaciones, la puntuación 77d de agregación de grupos se calcula sumando las puntuaciones 77b de evaluación de grupos, tal como se detalla en mayor medida más adelante.

Algunas realizaciones del motor 48 de puntuación aumentan cada puntuación de evaluación de entidad y/o grupo en una cantidad específica al heurístico correspondiente a la puntuación específica. Las Figs. 11-A-B muestran dichos aumentos de puntuación, correspondiente a las puntuaciones de entidades y las puntuaciones de grupos, respectivamente. Cuando el motor 48 de puntuación recibe una alerta 50 de puntuación generada en respuesta a la ejecución de un heurístico concreto, la puntuación de evaluación de entidad y/o grupo correspondiente al respectivo heurístico puede ser aumentada por el valor de incremento respectivo. Algunos heurísticos de entidad pueden ser también heurísticos de grupo, por ejemplo, el heurístico H_1 puede coincidir con el heurístico $H_1^{(G)}$. En algunas realizaciones, una alerta de puntuación generada por dicho heurístico puede resultar en la actualización de una puntuación de evaluación de entidad de la entidad respectiva y/o una puntuación de evaluación de grupo de un grupo que tiene la entidad respectiva como un miembro.

La Fig. 12-A muestra una secuencia ejemplar de pasos realizada por el motor 48 de puntuación (Fig. 3) según algunas realizaciones de la presente invención. Una secuencia de pasos 300-302 escucha en busca de alertas de puntuación del motor 46 de heurísticos. En algunas realizaciones, la alerta 50 de puntuación incluye un indicador de un heurístico que generó la alerta respectiva, y un indicador de una entidad y/o un grupo de entidades para el que la alerta respectiva fue generada. En respuesta a la recepción de la alerta 50 de puntuación, un paso 304 determina si la alerta 50 fue generada por un heurístico de entidad (esto es, un heurístico configurado para determinar si un evento es indicativo de una entidad individual que es maliciosa). Cuando no, el motor 48 de puntuación avanza a un paso 310. En caso afirmativo, en un paso 306, el motor 48 de puntuación identifica la entidad respectiva de acuerdo con la alerta 50 y actualiza la puntuación o puntuaciones de evaluación de la entidad respectiva según el heurístico o heurísticos que generaron la alerta. Por ejemplo, cuando la alerta 50 fue generada por el heurístico H_k, el motor 48 de puntuación puede aumentar la puntuación S_k correspondiente al heurístico H en un incremento apropiado (véase por ejemplo la Fig. 11-A). Un paso 308 adicional calcula la puntuación de agregación de la respectiva entidad, por ejemplo, sumando todas las puntuaciones de evaluación de entidad de la respectiva entidad.

El paso 310 determina si la alerta 50 de puntuación fue generada por un heurístico de grupo (esto es, un heurístico configurado para determinar si un evento es indicativo de un grupo de entidades que son maliciosas). Cuando no, el motor 48 de puntuación avanza a un paso 316. Cuando si, en un paso 312, el motor 48 de puntuación identifica un conjunto de grupos según la alerta 50 y actualiza una puntuación de evaluación de grupo del respectivo grupo o grupos según el heurístico o heurísticos que generaron la alerta. En el paso 314, el motor 48 calcula una puntuación de agregación del respectivo grupo o grupos, por ejemplo, como una suma de puntuaciones de evaluación de grupo.

En el paso 316, el motor 48 de puntuación determina si la puntuación de agregación de la respectiva entidad y/o grupo excede un umbral predeterminado. Cuando no, el motor 48 vuelve al paso 300. Cuando si, el motor 48 envía un indicador 58 de malicia al módulo 56 de limpieza.

La Fig. 12-B muestra una secuencia alternativa de pasos realizados por el motor 48 de puntuación. En respuesta a la recepción de la alerta 50, un paso 326 identifica una entidad y un heurístico que genera la respectiva alerta. Después, se determinan la puntuación o puntuaciones de evaluación y agregación para la respectiva entidad según la alerta 50. En un paso 332, el motor 48 de puntuación identifica al menos un grupo que tiene la respectiva entidad como un miembro. Un paso 336 aumenta después la puntuación de agregación del grupo respectivo. Cuando la puntuación de agregación de bien la entidad o el grupo (o ambos) excede un predeterminado umbral, un paso 340 envía el indicador 58 de malicia al módulo 56 de limpieza. La realización ejemplar ilustrada en la Fig. 12-B puede aumentar una puntuación de grupo cada vez que un miembro del respectivo grupo realiza una acción indicativa de malware. Por lo tanto, incluso cuando las actividades maliciosas se dividen entre diversos miembros del grupo, y cuando las puntuaciones de agregación correspondientes a cada miembro individual no son suficientes para indica malicia, la puntuación de todo el grupo puede exceder el umbral de detección de malware.

La Fig. 12-C muestra aún otra secuencia alternativa ejemplar de pasos realizados por el motor 48 de puntuación según algunas realizaciones de la presente invención. Al contrario de las Fig. 12-A-B, la Fig. 12-C puede describir la operación de una realización que no calcula puntuaciones de grupo, basándose en su lugar exclusivamente en las puntuaciones de entidad. Sin embargo, dicha realización puede aún detectar malware evasivo usando heurísticos de grupo. Usando el ejemplo de firma 68 de comportamiento en la Fig. 7, un heurístico que detecta la ocurrencia de la secuencia de eventos A_1-A_6 puede generar la alerta 50 de puntuación en respuesta a la detección de que la entidad E_4 ha realizado la acción A_6, y por tanto completa la secuencia de acciones indicativas de malware mediante la firma 68 de comportamiento. En respuesta a la recepción de dicha alerta, el paso 348 puede aumentar la puntuación de evaluación de entidad de la entidad E_4, la puntuación correspondiente al heurístico correspondiente. Si se elige que el aumento asociado al respectivo heurístico sea suficientemente grande, el aumento de la puntuación de evaluación de entidad respectiva puede ser suficientemente grande de manera que la puntuación de agregación calculada para la entidad E_4 excede el umbral de detección de malware.

La Fig. 13 ilustra una secuencia ejemplar de pasos realizada por el módulo 56 de limpieza (Fig. 3), según algunas realizaciones de la presente invención. En un paso 402, el módulo 56 recibe un indicador 58 de malicia desde el motor 48 de puntuación. En algunas realizaciones, el indicador 58 de malicia incluye un indicador de una entidad sospechosa y/o un indicador de un grupo de entidades sospechosas, por ejemplo, las entidades y/o los grupos cuyas puntuaciones de agregación exceden los umbrales de detección de malware (véase más arriba). En un paso 404, el módulo 56 identifica la entidad sospechosa que desencadena el motor 48 de puntuación para el envío del indicador 58 de malicia.

En algunas realizaciones, un paso 406 comprueba si la entidad sospechosa respectiva es un miembro de un grupo único. Cuando no, el módulo 56 avanza hasta el paso 410. Cuando si, en el paso 408, el módulo 56 de limpieza limpia todo el grupo de la entidad sospechosa. En algunas realizaciones, la limpieza de un grupo de entidades comprende limpiar cada entidad miembro del respectivo grupo. La limpieza puede implicar cualquier método conocido en la técnica de seguridad Informática. En algunas realizaciones, limpiar una entidad comprende suspender o terminar la ejecución de la entidad respectiva. Limpiar la entidad puede comprender además eliminar un archivo de disco que comprende el código de la entidad respectiva. Limpiar la entidad puede comprender además deshacer o hacer retroceder un conjunto de cambios realizados por la respectiva entidad durante su tiempo de vida (dichos cambios pueden incluir cambios a un registro del OS, a un sistema de archivos, etc.). Limpiar la entidad puede comprender analizar la respectiva entidad usando un escáner de malware separado. En algunas realizaciones, la limpieza incluye además alertar a un usuario del sistema 10 de cliente y/o a un administrador del sistema.

En un ejemplo de limpieza, cuando las actividades maliciosas se han rastreado hasta un evento de inyección de código, el módulo 56 de limpieza termina la entidad receptora y deshace todos los cambios a la memoria y/o el sistema de archivos que ocurrieron después del respectivo evento de inyección. Cuando es posible, el módulo 56 de limpieza puede deshacer sólo los cambios producidos como resultado del respectivo evento de inyección. En otro ejemplo de limpieza, cuando una entidad maliciosa usa una entidad limpia (tal como cmd.exe, regedit.exe, un procesador de navegador legítimo, etc.) para llevar a cabo parte de un ataque malicioso, el módulo 56 de limpieza puede terminar la respectiva entidad limpia, pero no elimina sus archivos ejecutables.

En algunas realizaciones, cuando la entidad sospechosa pertenece a múltiples grupos de entidades el paso 410 intenta identificar cual de los grupos respectivos puede ser malicioso. El paso 410 puede incluir determinar cómo la entidad sospechosa resulta un miembro de cada grupo respectivo (por ejemplo, en respuesta a la creación de entidad vs Inyección de código). El paso 410 puede determinar además qué heurístico desencadenó la alerta de puntuación que determinó el motor de puntuación para concluir que el sistema 10 de cliente estaba bajo ataque. Identificar el heurístico que desencadena la detección de malware puede permitir determinar qué acción estaba realizando la entidad sospechosa, que desencadenó la respectiva alerta de puntuación. Para llevar a cabo el paso 410, el módulo 58 de limpieza puede determinar además qué componente de la entidad sospechosa estaba ejecutándose cuando se desencadenó la respectiva alerta de puntuación.

En un escenario ejemplar, la entidad sospechosa resulta un miembro de un primer grupo a través de la creación de entidad y un miembro de un segundo grupo a través de inyección de código. El paso 410 ha determinado que la alerta de puntuación que provoca la detección de malware fue desencadenada mientras que el código del módulo ejecutable principal de la entidad sospechosa se estaba ejecutando. Entonces, el módulo 58 de limpieza puede concluir que el primer grupo es malicioso. Al contrario, si la entidad sospechosa hubiera estado ejecutando el código inyectado en el momento que la alerta de puntuación fue desencadenada, el módulo 58 de limpieza puede haber concluido que el segundo grupo era malicioso.

En un paso 412, el módulo 56 determina si la identificación del grupo malicioso fue exitosa. Cuando si, en el paso 414, el módulo 56 limpia el grupo malicioso identificado. Cuando el paso 410 no puede identificar un grupo malicioso de entidades, en un paso 416, el módulo 56 limpia sólo la entidad sospechosa. El paso 416 puede así evitar la identificación de falsos positivos de malware, esto es, la identificación errónea de una entidad benigna como una entidad maliciosa, lo que puede llevar a la pérdida de datos para el usuario.

Los sistemas y métodos ejemplares descritos anteriormente permiten proteger un sistema informático de software malicioso, tal como los virus, los Troyanos y el spyware. En algunas realizaciones de la presente invención, una aplicación de seguridad monitoriza el comportamiento de un conjunto de entidades (por ejemplo, procesos) que se ejecutan actualmente en el sistema de cliente. La aplicación de seguridad es notificada mediante un conjunto de interceptores de eventos de la ocurrencia de diversos eventos dentro del sistema de cliente. Dichos eventos ejemplares pueden incluir, entre otras cosas, la creación de un proceso o hilo, la inyección de código, una llamada de sistema, un intento de crear un nuevo archivo de disco, un intento de escribir a un archivo de disco existente, un intento de editar una clave de registro de OS, y un intento de escribir a una sección de memoria concreta. Algunos de los eventos notificados pueden ser indicativos de malware, mientras que otros eventos pueden no ser en sí indicativos de una amenaza de seguridad, pero indicar una amenaza potencial cuando ocurren junto con otros eventos.

En respuesta a la recepción de notificaciones de eventos, la aplicación de seguridad puede ejecutar un conjunto de procedimientos de detección (por ejemplo, heurísticos) para determinar si los respectivos eventos son indicativos de

malware. En respuesta a la determinación de que un evento es indicativo de malware, un heurístico puede provocar que una puntuación indicativa de malware sea aumentada. Un motor de puntuación puede determinar además si el sistema de cliente está bajo ataque según la puntuación indicativa de malware. Un módulo de limpieza puede tomar además acciones anti malware contra entidades o grupos de entidades consideradas como maliciosas.

Los sistemas convencionales anti malware normalmente asocian una puntuación a cada entidad individual, y aumentan dichas puntuaciones cuando las respectivas entidades se comportan de una manera indicativa de malware. Dichos sistemas convencionales normalmente fallan al detectar el malware evasivo, lo que divide las actividades maliciosas entre una pluralidad de entidades. Cuando el comportamiento de cada entidad participante no es indicativo de malware cuando se considera de manera aislada, dicho comportamiento puede no llevar a la detección en base a puntuaciones individuales. Al contrario, algunas realizaciones de la presente invención abordan el malware evasivo mediante la correlación de los comportamientos de las múltiples entidades relacionadas.

En algunas realizaciones, la aplicación de seguridad divide las entidades monitorizadas en una pluralidad de grupos de entidades, en donde todos los miembros de un grupo están relacionados por filiación o inyección de código. Una entidad puede pertenecer de manera simultánea a múltiples grupos de entidades. La aplicación de seguridad puede además asociar un conjunto de puntuaciones con cada grupo de entidades. Dichas puntuaciones de grupo pueden ser aumentadas cuando un miembro del grupo respectivo realiza ciertas acciones. Por tanto, incluso aunque las acciones realizadas por miembros individuales pueden no ser indicativas de malware per se, la puntuación de grupo puede capturar el comportamiento malicioso colectivo y desencadenar la detección.

En algunas realizaciones de la presente invención, las entidades ejecutables se dividen en al menos dos categorías principales, esto es, los creadores de grupo y los herederos de grupo. La categoría de creadores de grupo puede incluir entidades tales como los procesos de sistema operativo, los gestores de archivos y los navegadores, que pueden realizar a menudo actividades tales como la creación de entidades de una manera legítima. En algunas realizaciones, las entidades creadores de grupo crean nuevos grupos cuando generan entidades hijas. La categoría de herederos de grupo puede complementar los procesos de usuario y los procesos desconocidos. Las entidades herederas de grupo pueden resultar miembros de un grupo de su entidad padre, o puede ser la primera entidad de un grupo, cuando su entidad padre es una creadora de grupo. Tener distintas reglas de pertenencia al grupo para las entidades creadoras y herederas de grupo permite que algunas realizaciones de la presente invención monitoricen las dos categorías de entidades usando distintas estrategias de detección de malware.

Otra manera de abordar el malware evasivo según algunas realizaciones de la presente invención comprende usar heurísticos de detección de malware que detectan una secuencia o combinación concreta de acciones realizada por un grupo de entidades relacionadas, al contrario de las acciones aisladas realizadas por entidades individuales. El heurístico respectivo puede desencadenar un aumento de la puntuación sólo cuando se hayan realizado todas las acciones de la secuencia o combinación respectiva.

Los sistemas de seguridad informática convencionales pueden detectar las entidades maliciosas individuales, y pueden tomar acciones anti malware contra cada una de dichas entidades de manera aislada de otras entidades. Cuando la entidad maliciosa detectada es una pequeña parte de una red coordinada de entidades maliciosas, incapacitar una única entidad puede aún dejar el sistema de cliente vulnerable a, o incluso infectado con malware. Al contrario, en respuesta a la detección de un grupo de entidades maliciosas, algunas realizaciones de la presente invención pueden limpiar o en otro caso incapacitar todo el grupo de entidades maliciosas. Cuando una entidad sospechosa es parte de múltiples grupos de entidades, pero la aplicación de seguridad es incapaz de determinar cual de los respectivos grupos está llevando a cabo las actividades maliciosas, algunas realizaciones de la presente invención toman acciones anti malware sólo contra la respectiva entidad sospechosa, para evitar la identificación de falsos positivos de malware.

Estará claro para alguien experto en la técnica que las realizaciones anteriores se pueden alterar de muchas maneras sin salir del alcance de la invención. Por consiguiente, el alcance de la invención debería estar determinado por las siguientes reivindicaciones y sus equivalentes legales.

REIVINDICACIONES

1. Un sistema de servidor que comprende al menos un procesador de hardware y una unidad de memoria, configurado el al menos un procesador de hardware para ejecutar un gestor de entidades y un motor de heurísticos, en donde:

el gestor de entidades se configura para organizar una colección de entidades ejecutables monitorizadas en una pluralidad de grupos de entidades, en donde organizar la colección comprende:

en respuesta a la detección de que una primera entidad de la colección ha generado una entidad hija, determinar si la primera entidad pertenece a una categoría de entidades creadores de grupos;

en respuesta a la determinación de si la primera entidad pertenece a la categoría de creadores de grupos, cuando la primera entidad pertenece a la categoría de creadores de grupos:

añadir un nuevo grupo de entidades a la pluralidad de grupos de entidades, y

asignar la entidad hija al nuevo grupo de entidades; y

en respuesta a la determinación de si la primera entidad pertenece a la categoría de creadores de grupo, cuando la primera entidad no pertenece a la categoría de creadores de grupo:

seleccionar un primer grupo de entidades de la pluralidad de grupos de entidades de manera que la primera entidad es miembro del primer grupo de entidades, y

asignar la entidad hija al primer grupo de entidades; y

el motor de heurísticos se configura, en respuesta a una primera acción realizada por la entidad hija, para:

seleccionar un segundo grupo de entidades de la pluralidad de grupos de entidades de manera que la entidad hija sea un miembro del segundo grupo de entidades, en donde la entidad hija es un miembro del segundo grupo de entidades mientras que también es un miembro del primer grupo de entidades o del nuevo grupo de entidades; y

en respuesta a seleccionar el segundo grupo de entidades, determinar si la primera acción es indicativa de un ataque de malware según una segunda acción realizada por otro miembro del segundo grupo de entidades.

2. El sistema de servidor de la reivindicación 1, en donde organizar la colección comprende, además, en respuesta a la determinación de si la primera entidad pertenece a la categoría de creadora de grupo, cuando la primera entidad no pertenece a la categoría de creadora de grupo:

seleccionar un tercer grupo de entidades de la pluralidad de grupos de entidades de manera que la primera entidad es un miembro del tercer grupo de entidades, y

asignar la entidad hija al tercer grupo de entidades.

3. El sistema de servidor de la reivindicación 1, en donde organizar la colección comprende, además, en respuesta a la detección de que la entidad hija ha inyectado código dentro de una tercera entidad de la colección:

seleccionar un tercer grupo de entidades de la pluralidad de grupos de entidades de manera que la entidad hija es un miembro del tercer grupo de entidades; y

en respuesta, asignar la tercera entidad al tercer grupo de entidades.

4. El sistema de servidor de la reivindicación 1, en donde organizar la colección comprende, además, en respuesta a la detección de que la primera entidad ha generado la entidad hija:

determinar si la entidad hija pertenece a la categoría de creadora de grupo; y

en respuesta, cuando la entidad hija pertenece a la categoría de creadores de grupo, eliminar la entidad hija de la categoría de creadores de grupo.

5. El sistema de servidor de la reivindicación 1, en donde determinar si la primera entidad pertenece a la categoría de creadores de grupo comprende la determinación de si la primera entidad es un componente de un navegador web que se ejecuta en el sistema de servidor.

6. El sistema de servidor de la reivindicación 1, en donde determinar si la primera entidad pertenece a la categoría de creadores de grupo comprende la determinación de si la primera entidad es un componente de un sistema operativo que se ejecuta en el sistema de servidor.

7. El sistema de servidor de la reivindicación 1, en donde determinar si la primera acción es indicativa de ataque de malware comprende la determinación de si la primera acción ha ocurrido antes de la segunda acción.

8. El sistema de servidor de la reivindicación 1, en donde el motor de heurísticos se configura para determinar si la primera acción es indicativa de ataque de malware además según una tercera acción realizada por una tercera entidad del segundo grupo de entidades.

9. El sistema de servidor de la reivindicación 1, en donde determinar si la primera acción es indicativa de ataque de malware comprende la determinación de si la primera acción es parte de un conjunto de acciones indicativas de malware, en donde todas las acciones del conjunto de acciones indicativas de malware son realizadas por miembros del segundo grupo de entidades.

10. El sistema de servidor de la reivindicación 9, en donde determinar si la primera es parte del conjunto de acciones indicativas de malware comprende la determinación de si un subconjunto del conjunto de acciones indicativas de malware se produce en un orden específico.

11. (original) El sistema de servidor de la reivindicación 1, en donde el al menos un procesador de hardware se configura además para ejecutar un módulo de limpieza configurado, en respuesta a una determinación de que la primera acción es indicativa de un ataque de malware, para terminar una pluralidad de miembros del segundo grupo de entidades.

12. El sistema de servidor de la reivindicación 11, en donde la pluralidad de miembros comprende todos los miembros del segundo grupo de entidades.

13. El sistema de servidor de la reivindicación 1, en donde el al menos un procesador de hardware se configura además para ejecutar un módulo de limpieza configurado, en respuesta a una determinación de que la primera acción es indicativa de un ataque de malware, para deshacer un conjunto de cambios provocados al sistema de servidor por la ejecución de los miembros del segundo grupo de entidades.

14. Un método que comprende:

emplear al menos un procesador de hardware de un sistema de servidor para organizar una colección de entidades ejecutables monitorizadas en una pluralidad de grupos de entidades, en donde organizar la colección comprende:

en respuesta a la detección de que una primera entidad de la colección ha generado una entidad hija, determinar si la primera entidad pertenece a una categoría de entidades creadoras de grupo;

en respuesta a la determinación de si la primera entidad pertenece a la categoría de creadores de grupo, cuando la primera entidad pertenece a la categoría de creadores de grupo:

añadir un nuevo grupo de categorías a la pluralidad de grupos de entidades, y asignar la entidad hija al nuevo grupo de entidades; y

asignar la entidad hija al nuevo grupo de entidades; y

en respuesta a la determinación de si la primera entidad pertenece a la categoría de creadores de grupo, cuando la primera entidad no pertenece a la categoría de creadores de grupo:

seleccionar un primer grupo de entidades de la pluralidad de grupos de entidades de manera que la primera entidad es un miembro del primer grupo de entidades, y

asignar la entidad hija al primer grupo de entidades;

en respuesta a una primera acción realizada por la entidad hija, emplear al menos un procesador de hardware del sistema de servidor para seleccionar un segundo grupo de entidades de la pluralidad de grupos de entidades de manera que la entidad hija sea un miembro del segundo grupo de entidades, en donde la entidad hija es un miembro del segundo grupo de entidades mientras que también es un miembro del primer grupo de entidades o del nuevo grupo de entidades; y

en respuesta a la selección del segundo grupo de entidades, emplear al menos un procesador de hardware del sistema de servidor para determinar si la primera acción es indicativa de un ataque de malware según una segunda acción realizada por otro miembro del segundo grupo de entidades.

15. El método de la reivindicación 14, en donde organizar la colección comprende, además, en respuesta a determinar si la primera entidad pertenece a la categoría de creadores de grupo, cuando la primera entidad no pertenece a la categoría de creadores de grupo;

seleccionar un tercer grupo de entidades de la pluralidad de grupos de entidades de manera que la primera entidad sea un miembro del tercer grupo de entidades, y

asignar la entidad hija al tercer grupo de entidades.

16. El método de la reivindicación 14, en donde organizar la colección comprende, además, en respuesta a la detección de que la entidad hija ha inyectado código en una tercera entidad de la colección:

seleccionar un tercer grupo de entidades de la pluralidad de grupos de entidades de manera que la entidad hija sea un miembro del tercer grupo de entidades; y

en respuesta, asignar la tercera entidad al tercer grupo de entidades.

17. El método de la reivindicación 14, en donde organizar la colección comprende, además, en respuesta a la detección de que la primera entidad ha generado la entidad hija:

determinar si la entidad hija pertenece a la categoría de creadora de grupo; y

en respuesta, cuando la entidad hija pertenece a la categoría de creadores de grupo, eliminar la entidad hija de la categoría de creadores de grupo.

18. El método de la reivindicación 14, en donde determinar si la primera entidad pertenece a la categoría de creadores de grupo comprende la determinación de si la primera entidad es un componente de un navegador web que se ejecuta en el sistema de servidor.

19. El método de la reivindicación 14, en donde determinar si la primera entidad pertenece a la categoría de creadores de grupo comprende determinar si la primera entidad es un componente de un sistema operativo que se ejecuta en el sistema de servidor.

20. El método de la reivindicación 14, en donde determinar si la primera acción es indicativa de ataque de malware comprende determinar si la primera acción ha ocurrido antes de la segunda acción.

21. El método de la reivindicación 14, que comprende además determinar si la primera acción es indicativa de ataque de malware según una tercera acción realizada por una tercera entidad del segundo grupo de entidades.

22. El método de la reivindicación 14, en donde determinar si la primera acción es indicativa de ataque de malware comprende determinar si la primera acción es parte de un conjunto de acciones indicativas de malware, en donde todas las acciones del conjunto de acciones indicativas de malware son realizadas por los miembros del segundo grupo de entidades.

23. El método de la reivindicación 22, en donde determinar si la primera acción es parte del conjunto de acciones indicativas de malware comprende la determinación de si un subconjunto del conjunto de acciones indicativas de malware ocurre en un orden específico.

24. El método de la reivindicación 14 que comprende, además, en respuesta a la determinación de que la primera acción es indicativa de un ataque de malware, el empleo de al menos un procesador de hardware del sistema de servidor para terminar una pluralidad de miembros del segundo grupo de entidades.

25. El método de la reivindicación 24, en donde la pluralidad de miembros comprende todos los miembros del segundo grupo de entidades.

26. El método de la reivindicación 14, que comprende, además, en respuesta a una determinación de que la primera acción es indicativa de un ataque de malware, que emplea al menos un procesador de hardware del sistema de servidor para deshacer un conjunto de cambios en el sistema de servidor provocados por la ejecución de los miembros del segundo grupo de entidades.

27. Un medio legible por ordenador no transitorio que almacena instrucciones que, al ser ejecutadas por al menos un procesador de hardware de un sistema de servidor, provocan que el sistema de servidor cree un gestor de entidades y un motor de heurísticos, en donde:

el gestor de entidades se configura para organizar una colección de entidades ejecutables monitorizadas en una pluralidad de grupos de entidades, en donde organizar la colección comprende:

en respuesta a la detección de que una primera entidad de la colección ha generado una entidad hija, determinar si la primera entidad pertenece a una categoría de entidades creadores de grupo;

en respuesta a la detección de si la primera entidad pertenece a la categoría de creadores de grupo, cuando la primera entidad pertenece a la categoría de creadores de grupo:

añadir un nuevo grupo de entidades a la pluralidad de grupos de entidades, y

asignar la entidad hija al nuevo grupo de entidades; y

en respuesta a la determinación de si la primera entidad pertenece a la categoría de creadores de grupo, cuando la primera entidad no pertenece a la categoría de creadores de grupo:

seleccionar un primer grupo de entidades de la pluralidad de grupos de entidades de manera que la primera entidad es un miembro del primer grupo de entidades, y

asignar la entidad hija al primer grupo de entidades; y

el motor de heurísticos se configura, en respuesta a una primera acción realizada por la entidad hija, para:

seleccionar un segundo grupo de entidades de la pluralidad de grupos de entidades de manera que la entidad hija sea un miembro del segundo grupo de entidades, en donde la entidad hija es un miembro del segundo grupo de entidades mientras que también es un miembro del primer grupo de entidades o del nuevo grupo de entidades; y

en respuesta a la selección del segundo grupo de entidades, determinar si la primera acción es indicativa de ataque de malware según una segunda acción realizada por otro miembro del segundo grupo de entidades.

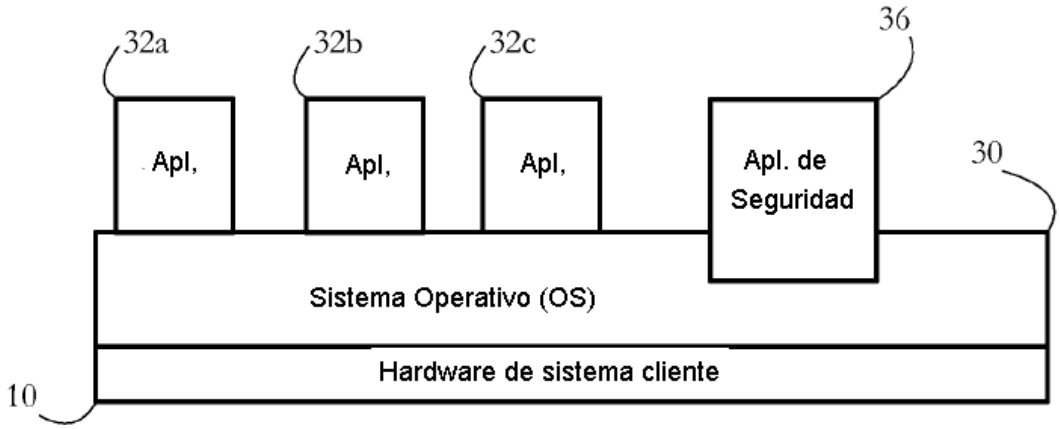
32a
32b
32c
36
Apl,
Apl,
Apl,
Apl. de Seguridad
30
Sistema Operativo (OS)
Hardware de sistema cliente
10

FIG. 1

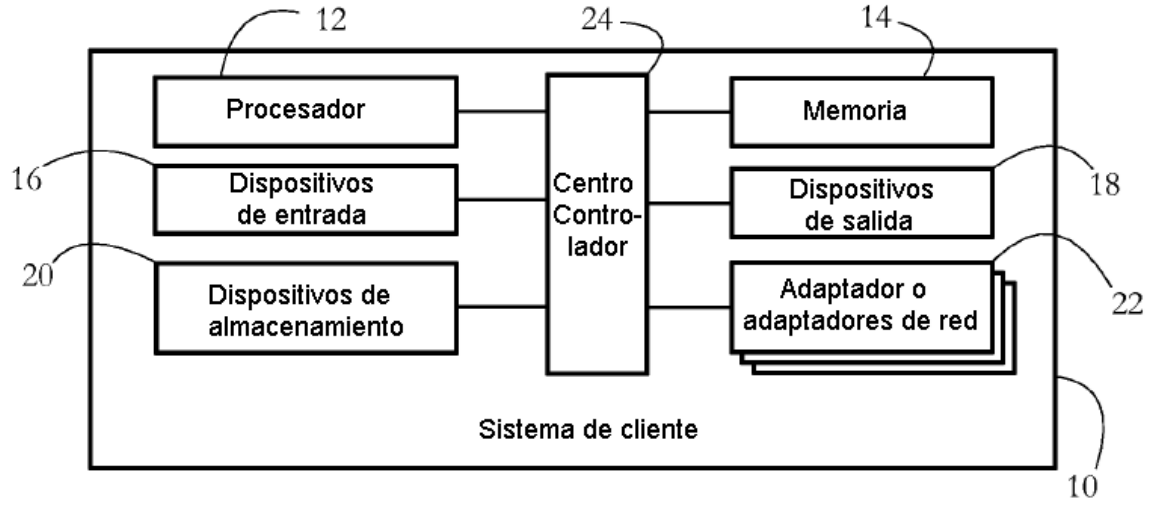
12
24
14
Procesador
Memoria
16
Dispositivos de entrada
Centro Contro-lador
Dispositivos de salida
18
20
Dispositivos de almacenamiento
Adaptador o adaptadores de red
22
Sistema de cliente
10

FIG. 2

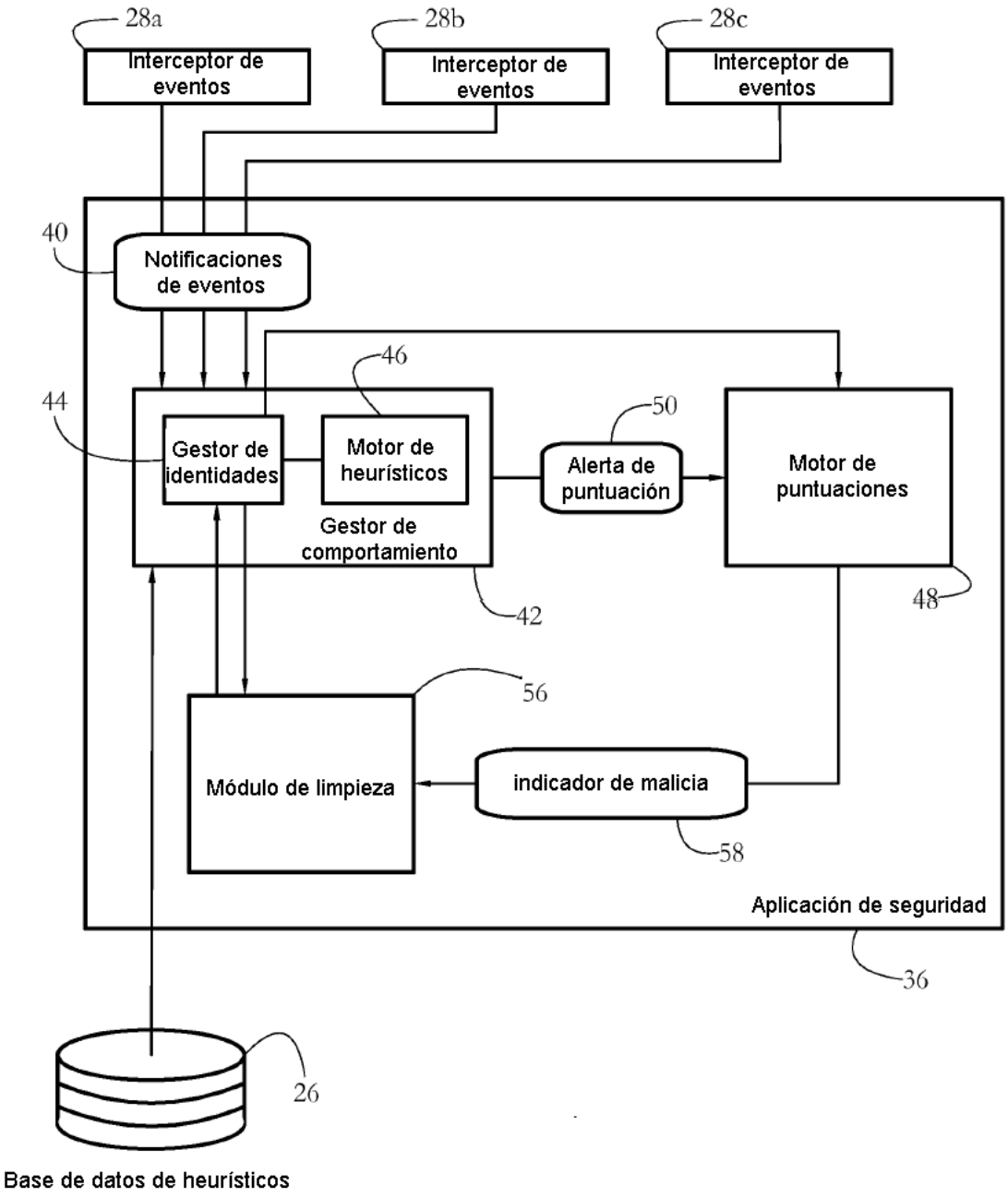
28a
Interceptor de eventos
28b
Interceptor de eventos
28c
Interceptor de eventos
40
Notificaciones de eventos
46
44
Gestor de identidades
Motor de heurísticos
Gestor de comportamiento
42
50
Alerta de puntuación
Motor de puntuaciones
48
56
Módulo de limpieza
indicador de malicia
58
Aplicación de seguridad
36
26
Base de datos de heurísticos

FIG. 3

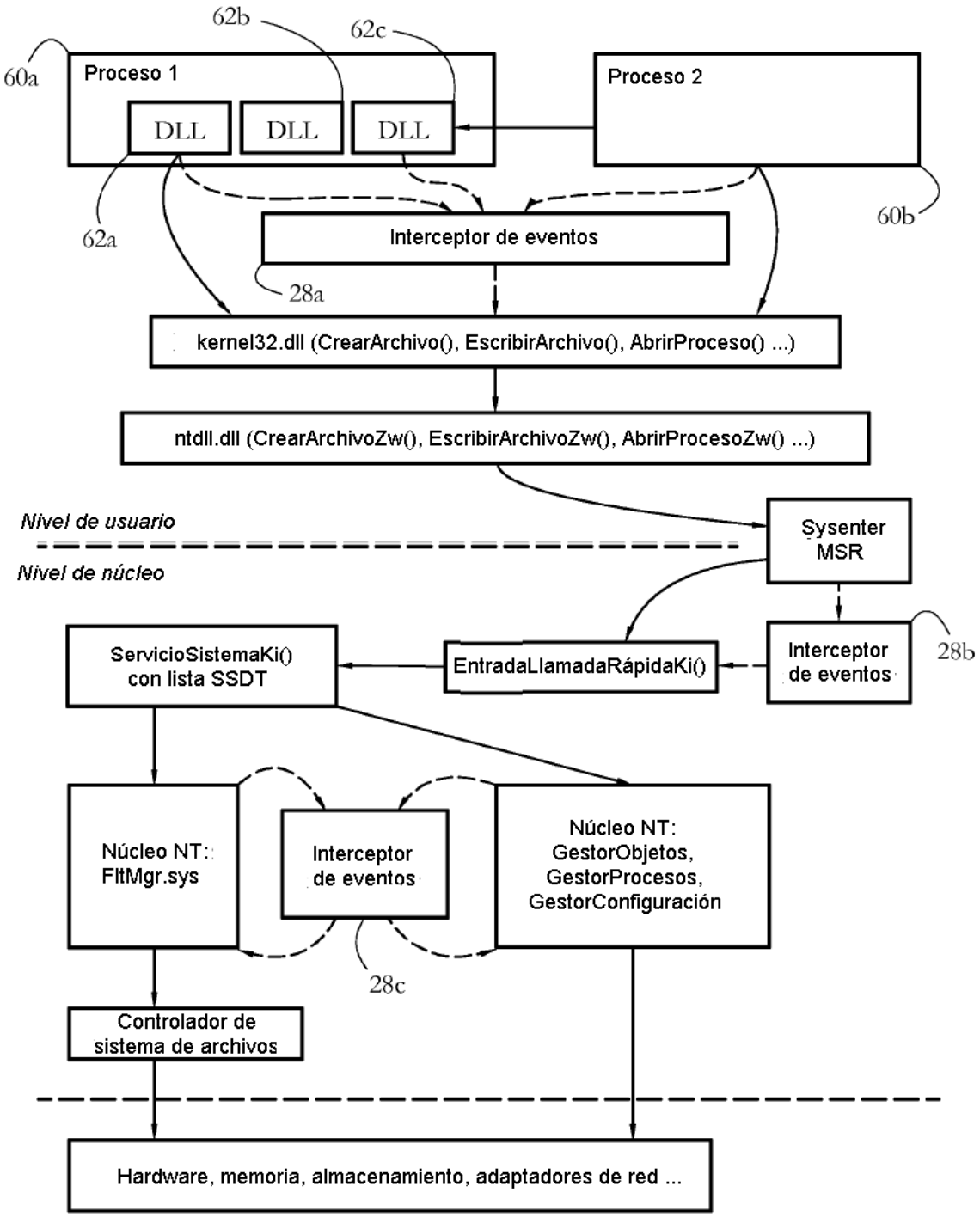
62b
62c
60a
Proceso 1
DLL
DLL
DLL
Proceso 2
62a
60b
Interceptor de eventos
28a
kernel32.dll (CrearArchivo(), EscribirArchivo(), AbrirProceso() ...)
ntdll.dll (CrearArchivoZw(), EscribirArchivoZw(), AbrirProcesoZw() ...)
Nivel de usuario
Nivel de núcleo
Sysenter MSR
ServicioSistemaKi() con lista SSDT
EntradaLlamadaRápidaKi()
Interceptor de eventos
28b
Núcleo NT: FltMgr.sys
Interceptor de eventos
Núcleo NT: GestorObjetos, GestorProcesos, GestorConfiguración
28c
Controlador de sistema de archivos
Hardware, memoria, almacenamiento, adaptadores de red ...

FIG. 4

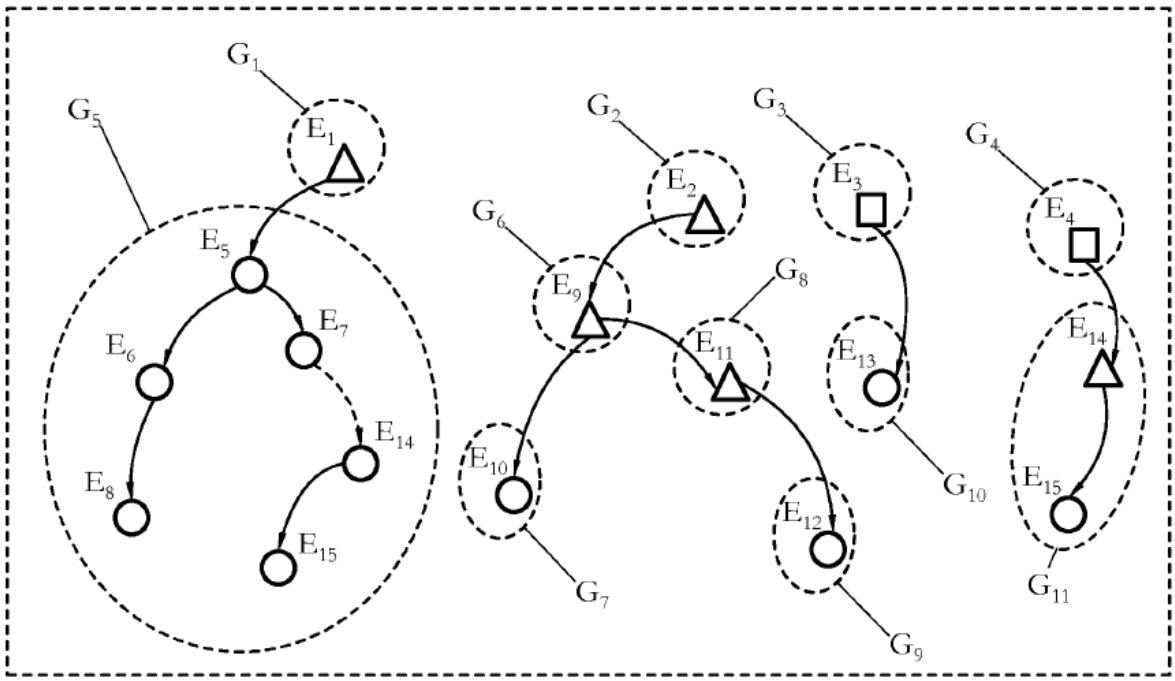
G1
G5
E1
E5
E6
E7
E14
E8
E15
G2
G3
G4
E2
E3
E4
G6
E9
G8
E11
E13
E14
E10
E15
E12
G10
G7
G11
G9

FIG. 5-A

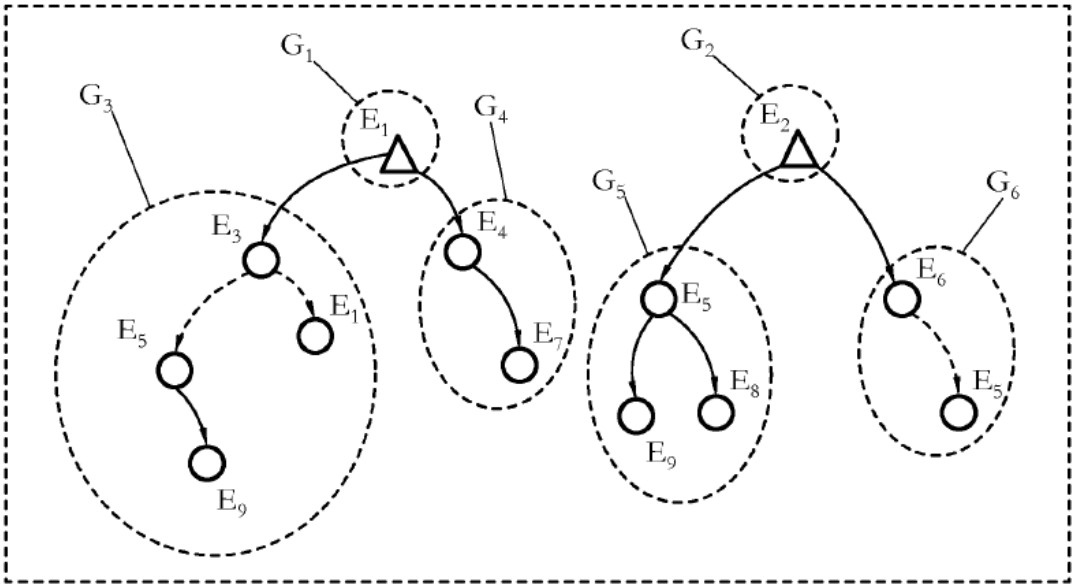
G1
G3
E1
G4
E3
E4
E5
E1
E7
E9
G2
E2
G5
G6
E5
E6
E8
E5
E9

FIG. 5-B

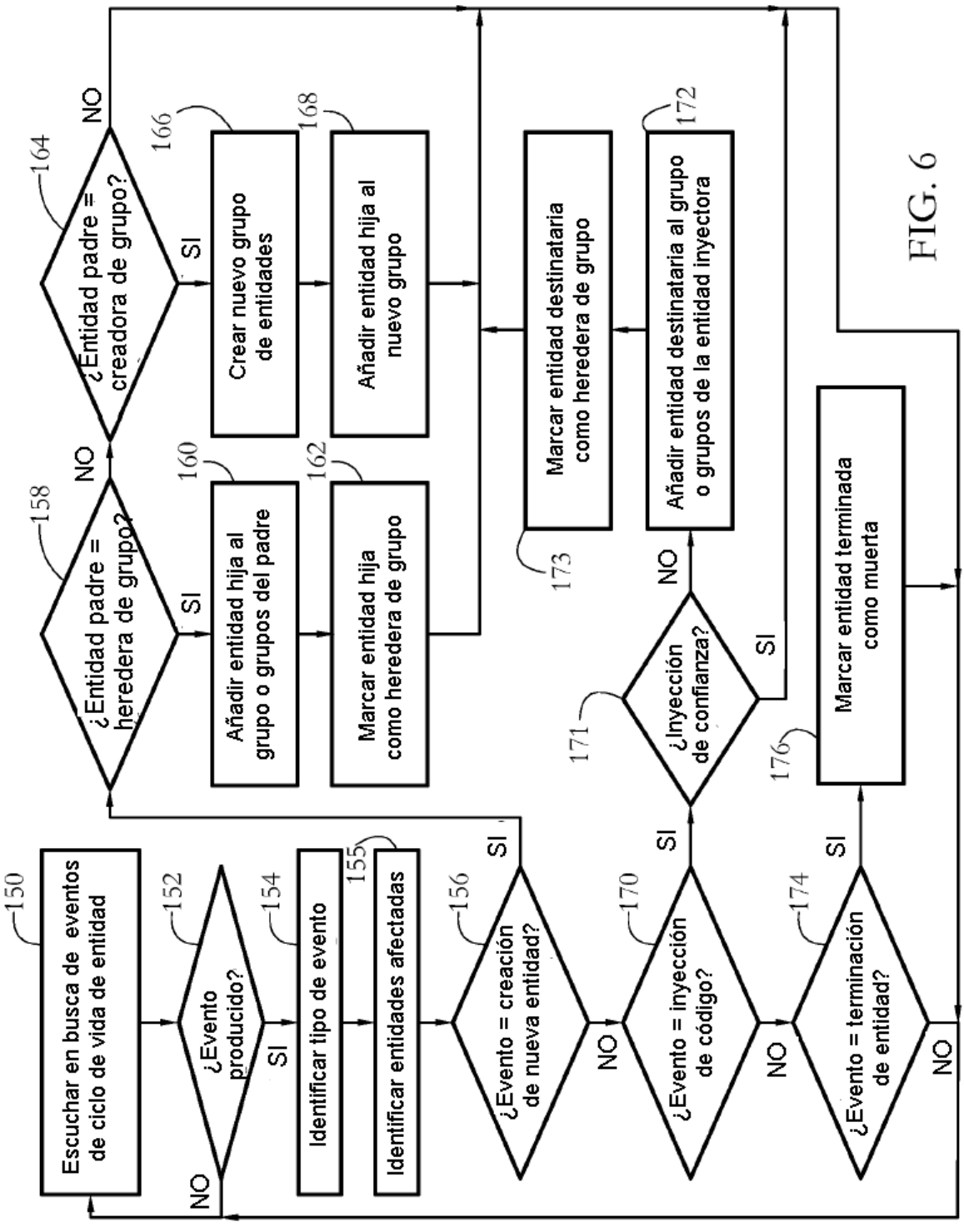
150
Escuchar en busca de eventos de ciclo de vida de entidad
152
¿Evento producido?
NO
SI
154
Identificar tipo de evento
155
Identificar entidades afectadas
156
¿Evento = creación de nueva entidad?
SI
NO
158
¿Entidad padre = heredera de grupo?
SI
NO
160
Añadir entidad hija al grupo o grupos del padre
162
Marcar entidad hija como heredera de grupo
164
¿Entidad padre = creadora de grupo?
SI
NO
166
Crear nuevo grupo de entidades
168
Añadir entidad hija al nuevo grupo
170
¿Evento = inyección de código?
SI
NO
171
¿Inyección de confianza?
SI
NO
172
Añadir entidad destinataria al grupo o grupos de la entidad inyectora
173
Marcar entidad destinataria como heredera de grupo
174
¿Evento = terminación de entidad?
SI
NO
176
Marcar entidad terminada como muerta

FIG. 6

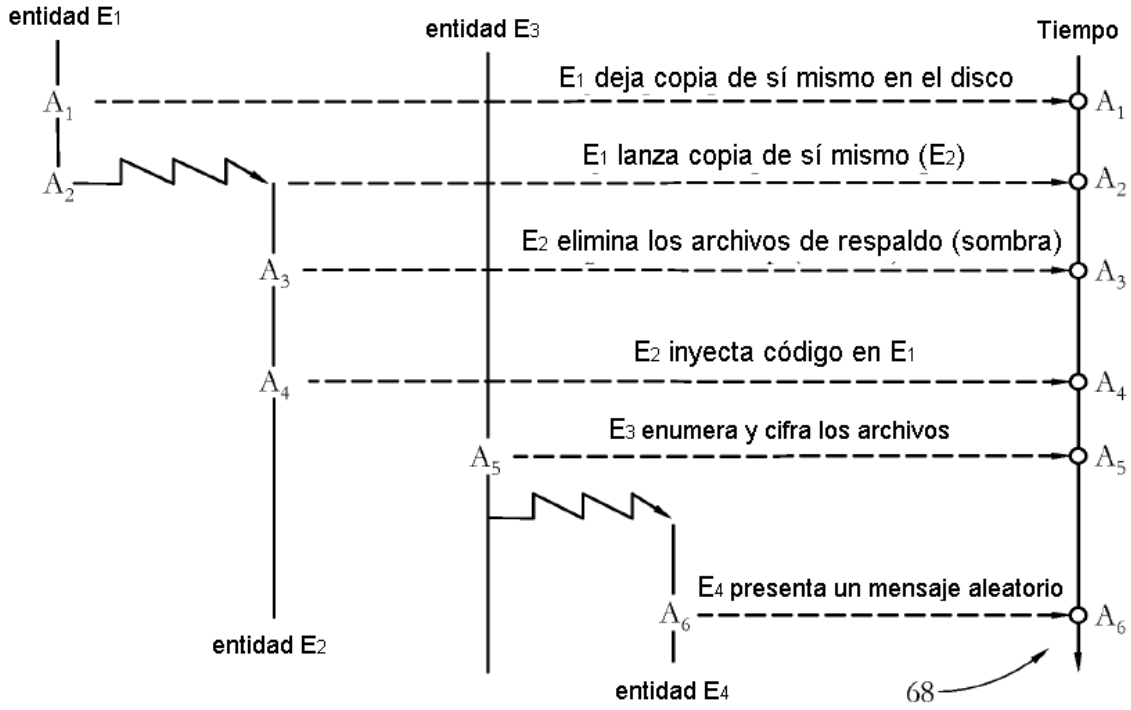

FIG. 7

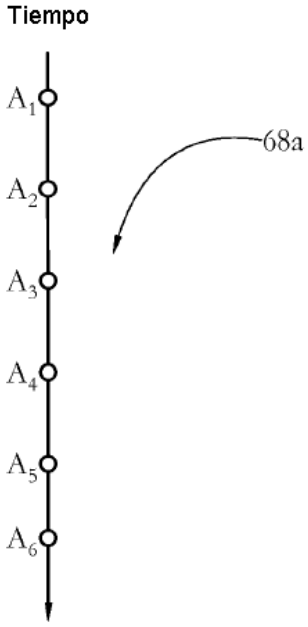

FIG. 8-A

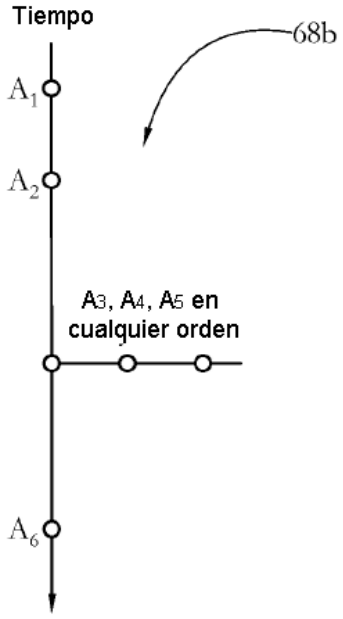

FIG. 8-B

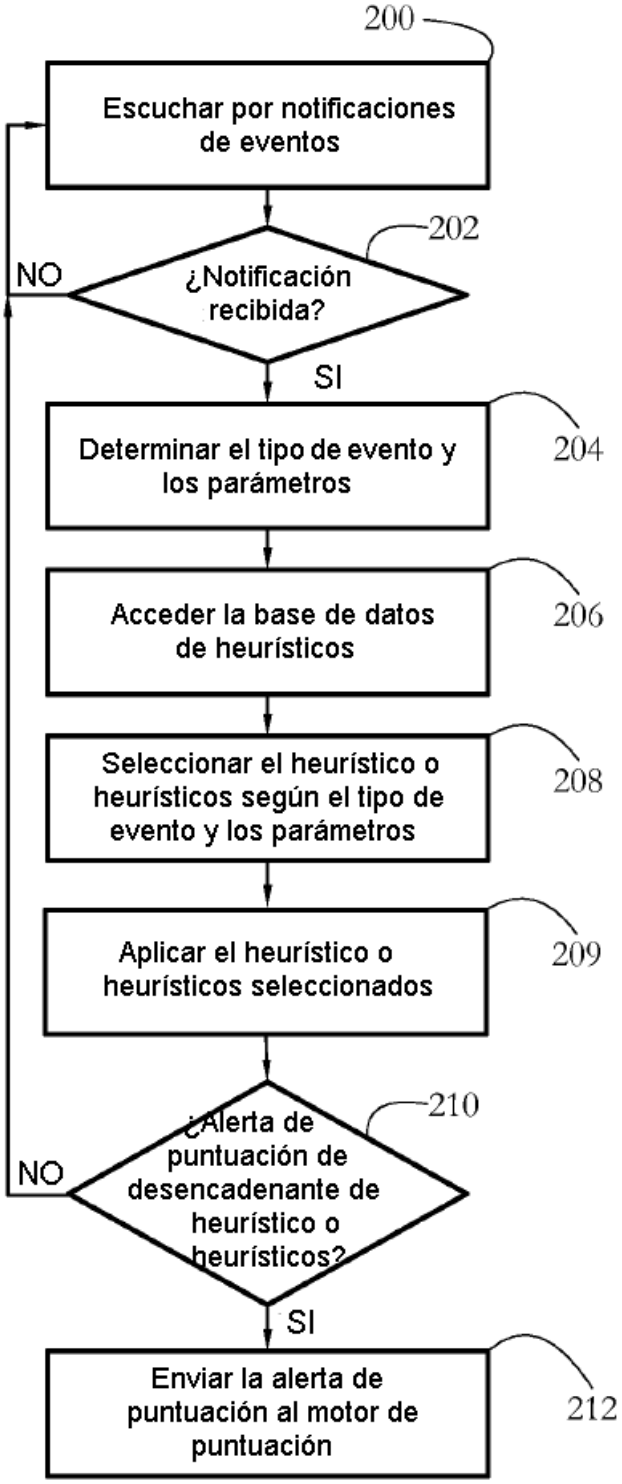
200
Escuchar por notificaciones de eventos
202
¿Notificación recibida?
NO
SI
Determinar el tipo de evento y los parámetros
204
Acceder la base de datos de heurísticos
206
Seleccionar el heurístico o heurísticos según el tipo de evento y los parámetros
208
Aplicar el heurístico o heurísticos seleccionados
209
¿Alerta de puntuación de desencadenante de heurístico o heurísticos?
210
NO
SI
Enviar la alerta de puntuación al motor de puntuación
212

FIG. 9

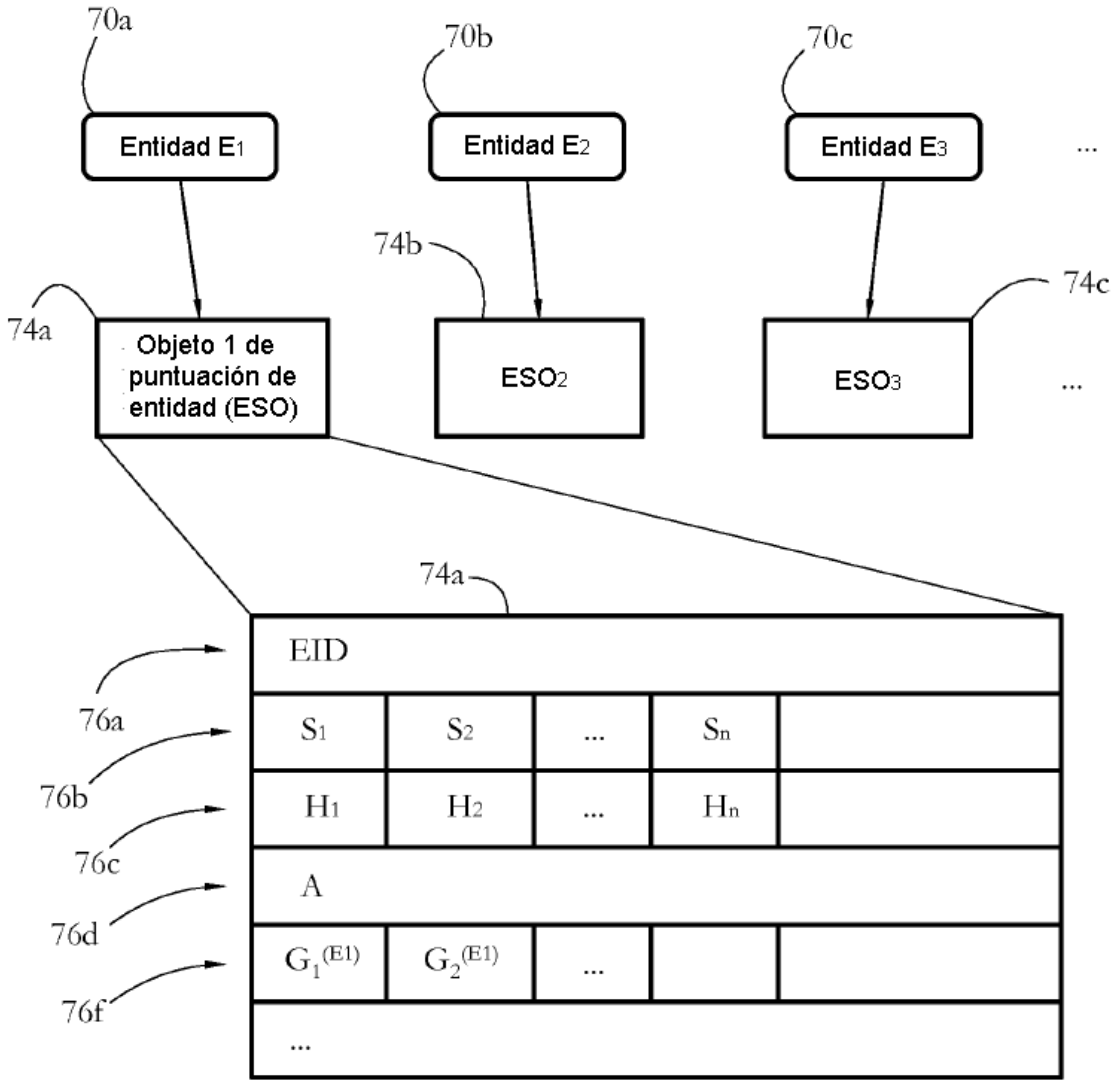
70a
70b
70c
Entidad E1
Entidad E2
Entidad E3
...
74b
74c
74a
Objeto 1 de puntuación de entidad (ESO)
ESO2
ESO3
...
74a
EID
76a
S1
S2
...
Sn
76b
H1
H2
...
Hn
76c
A
76d
G1(E1)
G2(E1)
...
76f
...

FIG. 10-A

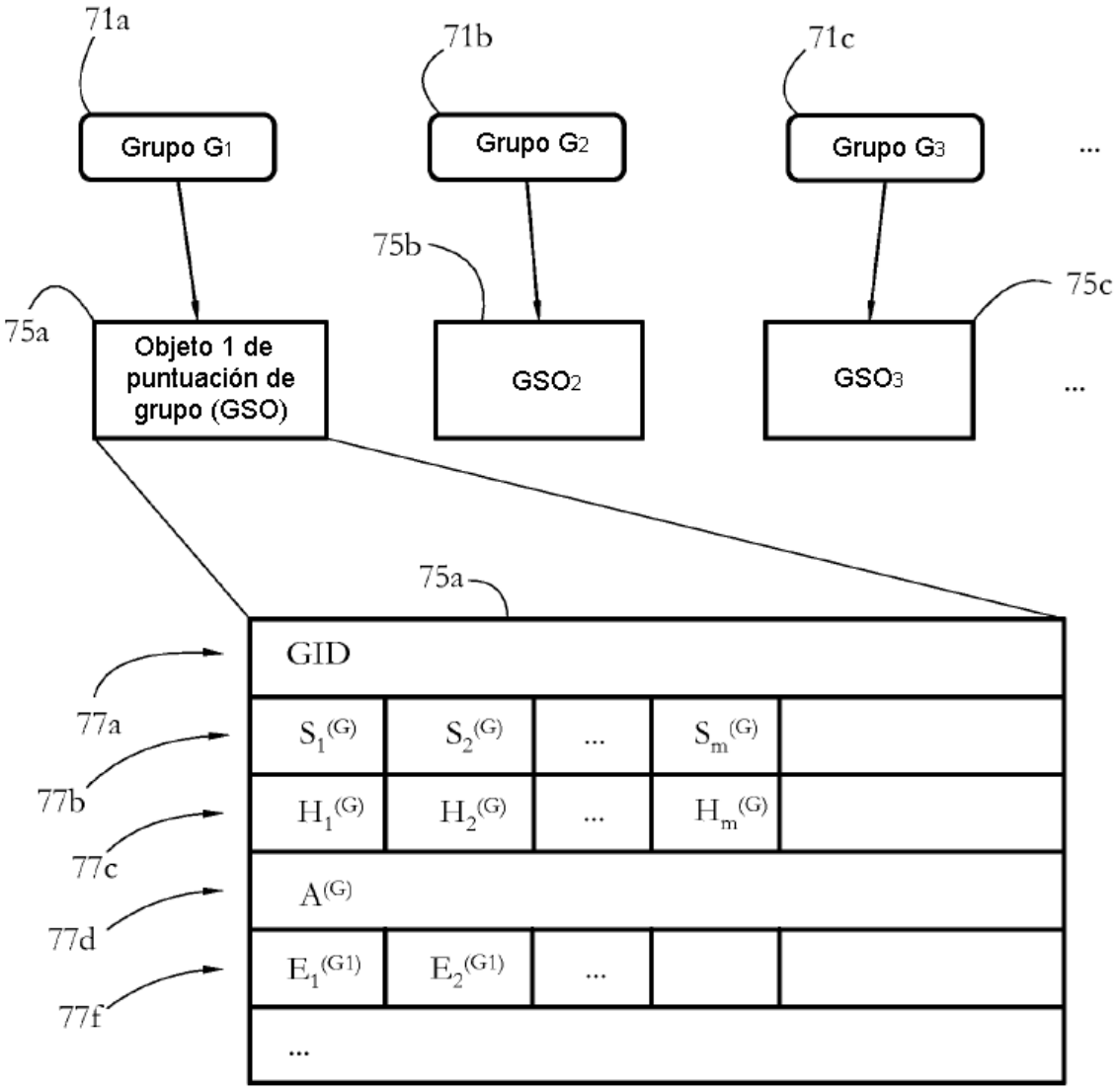
71a
71b
71c
Grupo G1
Grupo G2
Grupo G3
...
75b
75c
75a
Objeto 1 de puntuación de grupo (GSO)
GSO2
GSO3
...
75a
GID
77a
77b
77c
77d
77f
$S_1^{(G)}$
$S_2^{(G)}$
...
$S_m^{(G)}$
$H_1^{(G)}$
$H_2^{(G)}$
...
$H_m^{(G)}$
$A^{(G)}$
$E_1^{(G1)}$
$E_2^{(G1)}$
...
...

FIG. 10-B

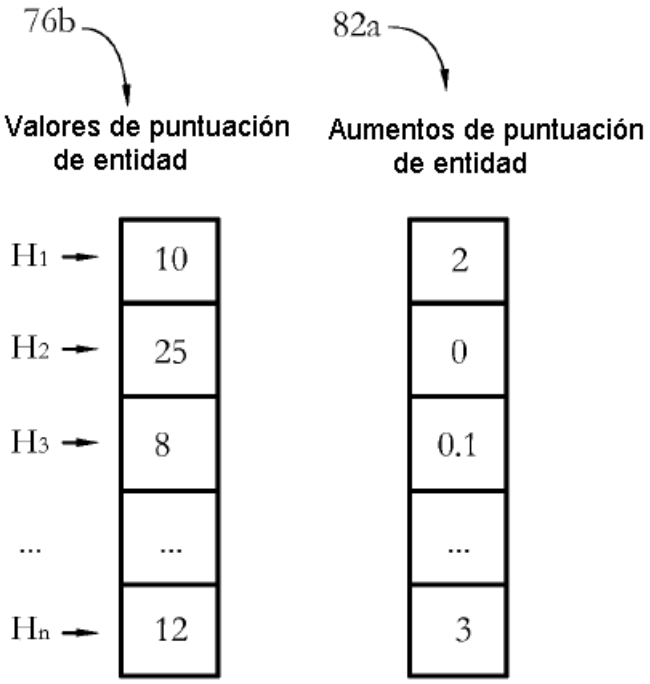

FIG. 11-A

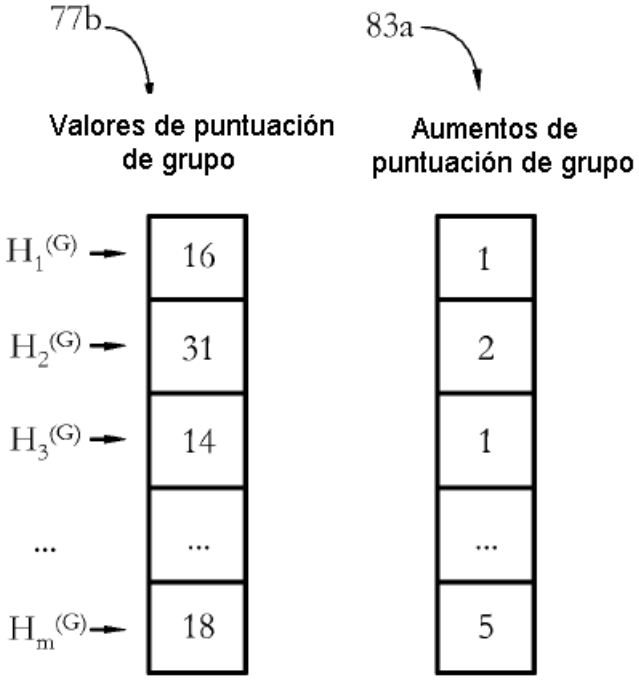

FIG. 11-B

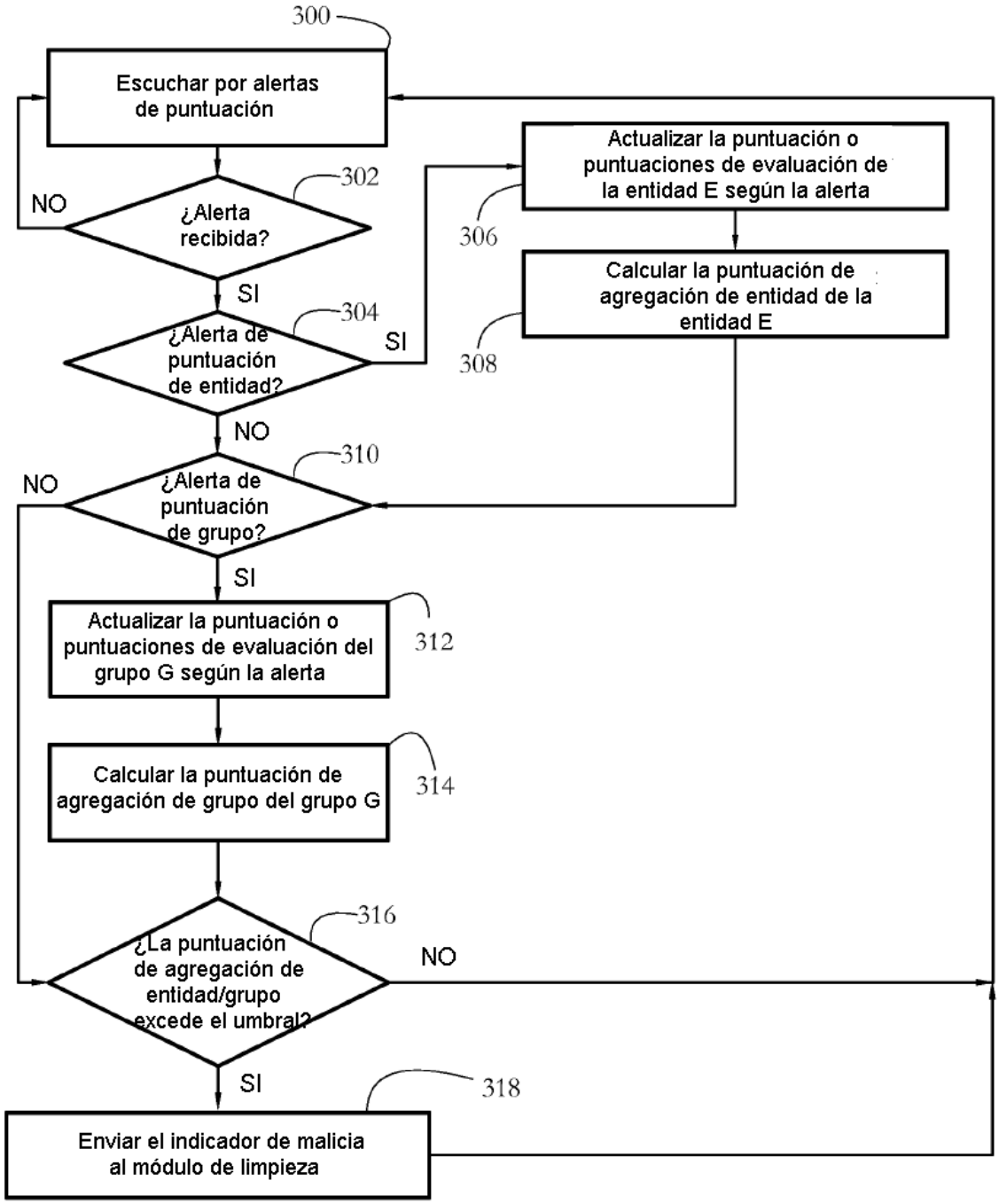
300
Escuchar por alertas de puntuación
302
¿Alerta recibida?
NO
SI
304
¿Alerta de puntuación de entidad?
SI
NO
306
Actualizar la puntuación o puntuaciones de evaluación de la entidad E según la alerta
308
Calcular la puntuación de agregación de entidad de la entidad E
310
¿Alerta de puntuación de grupo?
NO
SI
312
Actualizar la puntuación o puntuaciones de evaluación del grupo G según la alerta
314
Calcular la puntuación de agregación de grupo del grupo G
316
¿La puntuación de agregación de entidad/grupo excede el umbral?
NO
SI
318
Enviar el indicador de malicia al módulo de limpieza

FIG. 12-A

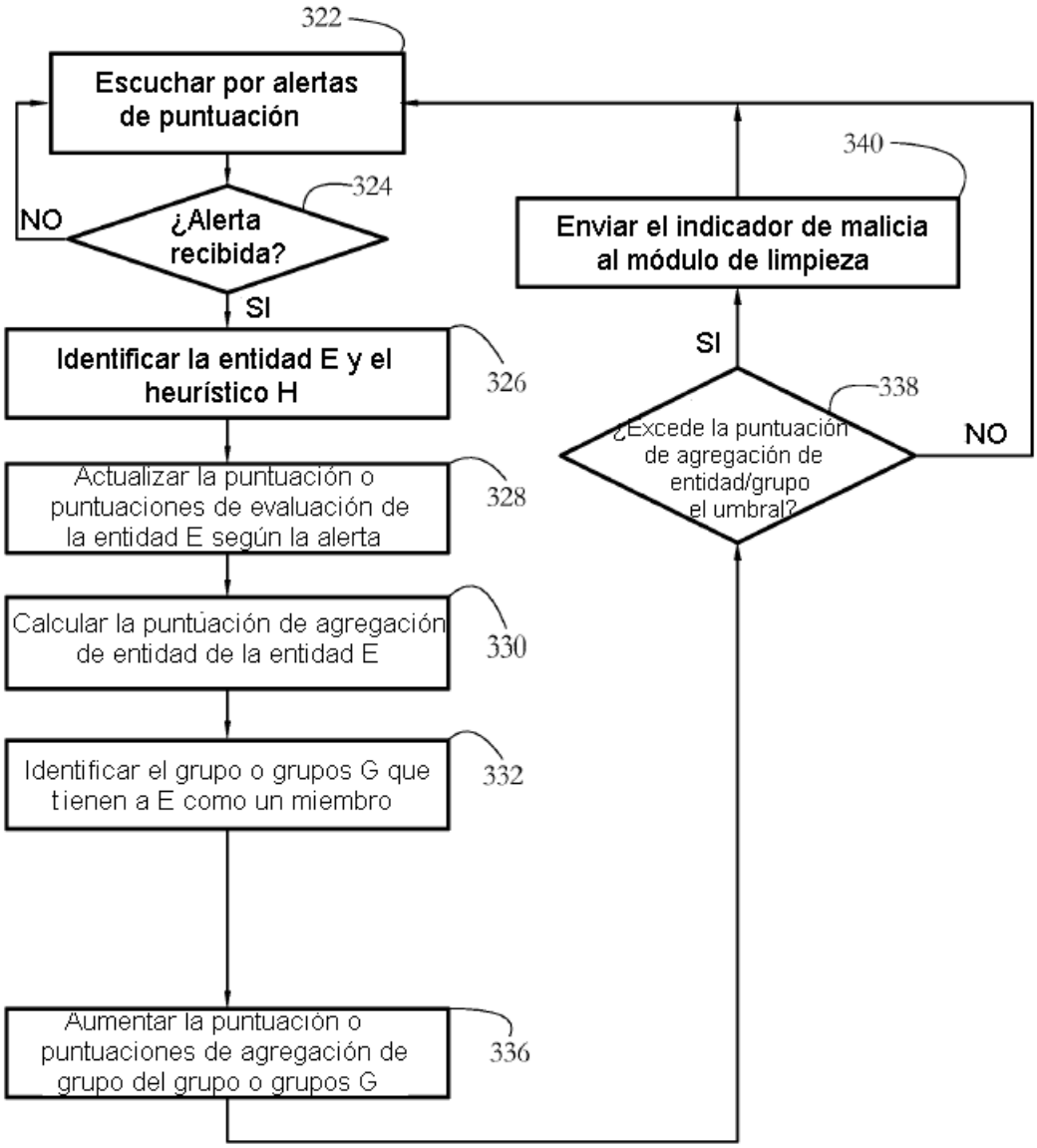
322
Escuchar por alertas de puntuación
324
NO
¿Alerta recibida?
SI
Identificar la entidad E y el heurístico H
326
Actualizar la puntuación o puntuaciones de evaluación de la entidad E según la alerta
328
Calcular la puntuación de agregación de entidad de la entidad E
330
Identificar el grupo o grupos G que tienen a E como un miembro
332
Aumentar la puntuación o puntuaciones de agregación de grupo del grupo o grupos G
336
340
Enviar el indicador de malicia al módulo de limpieza
SI
338
¿Excede la puntuación de agregación de entidad/grupo el umbral?
NO

FIG. 12-B

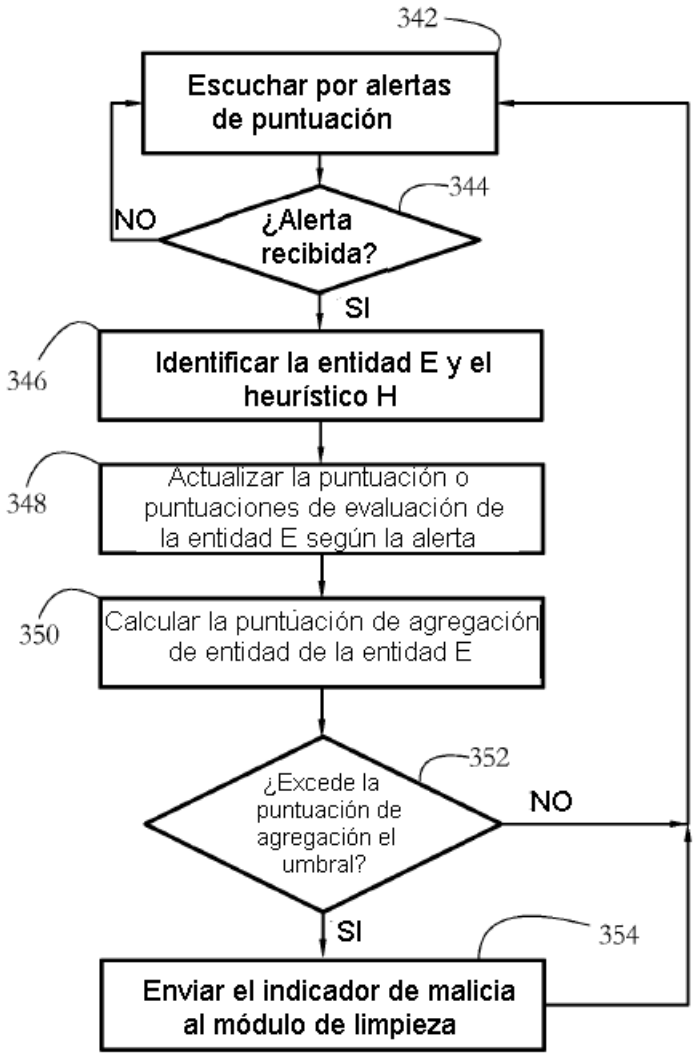
342
Escuchar por alertas de puntuación
344
NO
¿Alerta recibida?
SI
346
Identificar la entidad E y el heurístico H
348
Actualizar la puntuación o puntuaciones de evaluación de la entidad E según la alerta
350
Calcular la puntuación de agregación de entidad de la entidad E
352
¿Excede la puntuación de agregación el umbral?
NO
SI
354
Enviar el indicador de malicia al módulo de limpieza

FIG. 12-C

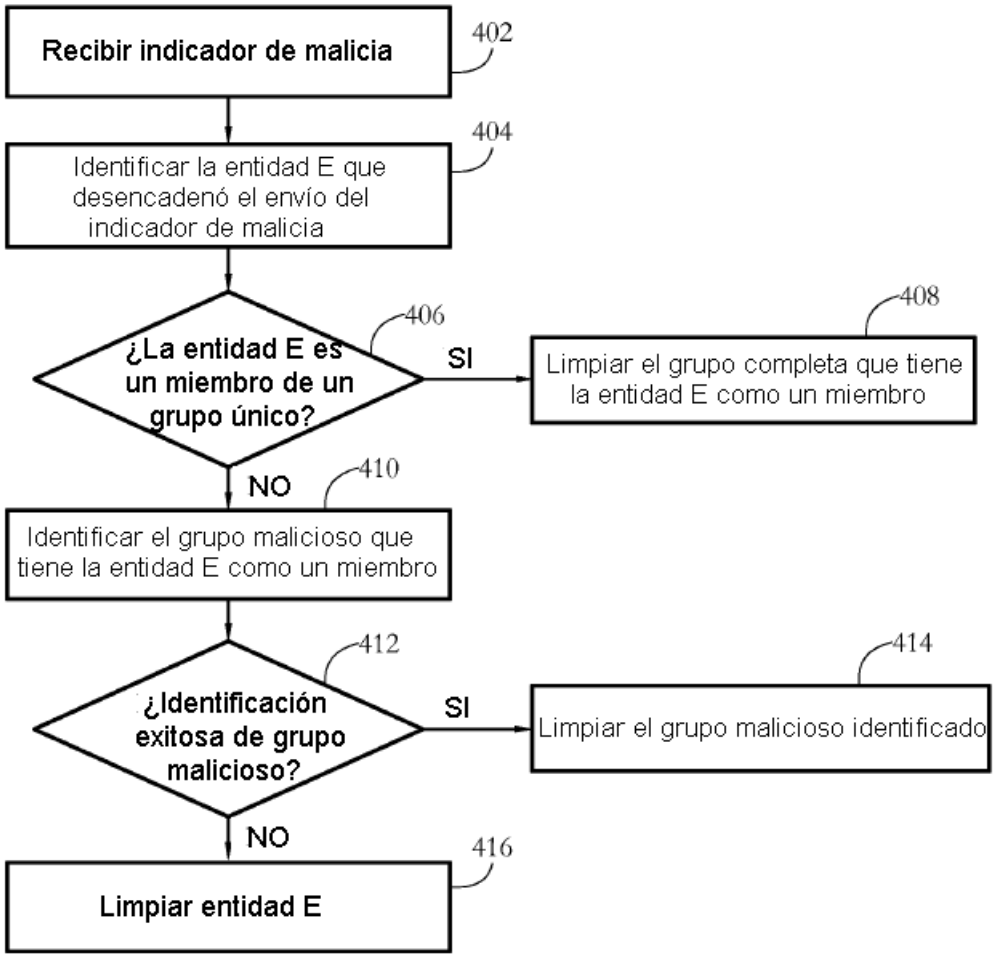
Recibir indicador de malicia
402
Identificar la entidad E que desencadenó el envío del indicador de malicia
404
¿La entidad E es un miembro de un grupo único?
406
SI
Limpiar el grupo completa que tiene la entidad E como un miembro
408
NO
Identificar el grupo malicioso que tiene la entidad E como un miembro
410
¿Identificación exitosa de grupo malicioso?
412
SI
Limpiar el grupo malicioso identificado
414
NO
Limpiar entidad E
416

FIG. 13