(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 775 250**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 16/951 (2009.01)
H04L 12/58 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **01.08.2014 E 14179540 (1)**

(97) Fecha y número de publicación de la concesión europea: **11.12.2019 EP 2849404**

(54) Título: **Procedimiento de detección de intrusiones no solicitadas en una red de información, dispositivo, producto programa de ordenador y medio de almacenamiento correspondientes**

(30) Prioridad:

28.08.2013 FR 1301993

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.07.2020

(73) Titular/es:

AIRBUS CYBERSECURITY SAS (100.0%)
1 Boulevard Jean Moulin, ZAC de la Clef Saint Pierre
78990 Elancourt, FR

(72) Inventor/es:

LORIOT, NICOLAS y
FONTARENSKY, IVAN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento de detección de intrusiones no solicitadas en una red de información, dispositivo, producto programa de ordenador y medio de almacenamiento correspondientes

1. Ámbito técnico de la invención

El ámbito técnico de la invención es el de los procedimientos y sistemas de detección de intrusiones no solicitadas en una red de información, especialmente una red informática. En particular, la invención concierne a los métodos de detección de los ataques dirigidos del tipo de « Amenazas Persistentes Avanzadas », más conocido con la denominación inglesa de Advanced Persitents Threads o con el acrónimo APT.

2. Antecedentes tecnológicos

En todo el texto que sigue, los términos « ataque dirigido » e « intrusión no solicitada » se utilizan para definir la misma práctica que consiste en penetrar en una red de información sin autorización de su responsable.

En todo el texto, los términos « red de información » designan una red de intercambios de información por cualesquiera tipos de medios de comunicación, tal como por ejemplo una red Ethernet, una red radio, etc. Dicha red de información es por ejemplo una red informática, una red radio, una red radio móvil profesional (más conocida con el acrónimo PMR), y de manera general una red que conecta entre sí un conjunto de equipos para intercambiar informaciones. Una red de información designa tanto a un conjunto de máquinas conectadas entre sí para intercambiar informaciones como a una máquina individual. En otras palabras, un procedimiento de detección de intrusiones no solicitadas en una red formada según la invención, especialmente una red informática, tiene por objetivo tanto la detección de intrusiones en una red de información formada por varias máquinas conectadas entre sí como la detección de intrusiones en una máquina única que recibe informaciones, ya sea por intermedio de una red de tipo Internet, Ethernet, Radio o equivalente, o por la conexión de un dispositivo de almacenamiento de informaciones tal como una llave USB, un disco de almacenamiento, una antena radio, etc.

Los ataques dirigidos representan una amenaza muy importante para todos los organismos, se trate de administraciones públicas, de empresas privadas o de órganos gubernamentales. Dicho ataque dirigido o intrusión no solicitada tiene por objetivo en general recoger informaciones sensibles de cualquier naturaleza (secretos industriales, informaciones políticas sensibles, datos bancarios, etc.), o tomar el control total de la red de información, especialmente de la red informática, de una organización. Se trata a menudo de un ataque silencioso que se extiende en el tiempo y del que a veces es difícil medir todas las consecuencias. Estos ataques emanan de grupos individuales coordinados, organizados, financiados que van dirigidos a los activos de gran valor. La principal dificultad para detectar estos ataques dirigidos reside en el hecho de que estos grupos se concentran en ataques lentos y discretos, pasan de un anfitrión a otro, sin generar tráfico de red regular o previsible, y establecen procedimientos para asegurarse de que sus acciones no sean percibidas por los operadores legítimos de los sistemas. Para hacer esto, utilizan todo un panel de herramientas, que van de la utilización de softwares maliciosos a las técnicas de ingeniería social, pasando por la captura de informaciones específicas de ciertos individuos objetivos.

Las medidas de defensa tradicionales contra este tipo de ataque, en el caso de una red informática, consisten en utilizar cortafuegos, sistemas de prevención de intrusión, antivirus y herramientas de vigilancia de la red informática de la entidad considerada. Estas técnicas son a menudo imperfectas hasta el punto de que es frecuente que los ataques elaborados no sean detectados antes de 400 días de presencia en la red atacada.

Entre las técnicas utilizadas para las medidas de defensa, el documento US 2008/126493 describe un dispositivo y un procedimiento de detección de archivos maliciosos en el seno de correos electrónicos. El documento US 2008/0222177 describe un dispositivo y un procedimiento de detección de virus en un repertorio de un ordenador. El documento US 2007/0208822 describe un procedimiento para probar sitios de internet y determinar si una visita a estos sitios es susceptible de generar una intrusión no solicitada.

Otro inconveniente de estas medidas tradicionales es que permiten identificar eventos individuales, no asocian los eventos entre sí, impidiendo de esta manera un análisis global de los ataques de la red.

Otro inconveniente de las medidas actuales es que no permiten tratar rápidamente las cantidades de datos transportadas por las redes de información, especialmente las redes informáticas.

Existe por tanto una necesidad real de disponer de un método de detección de intrusiones no solicitadas en una red que permita tratar rápidamente un gran número de datos con miras a facilitar una visión global de la situación de la red y a detectar rápidamente la presencia de intrusiones no solicitadas, para erradicarlas antes de que las mismas pongan en peligro la organización objetivo.

3. Objetivos de la invención

La invención tiene por objetivo paliar al menos algunos de los inconvenientes de los procedimientos de detección de intrusiones no solicitadas en una red de información, especialmente una red informática.

En particular, la invención tiene por objetivo también facilitar, al menos en un modo de realización de la invención, un procedimiento de detección de intrusiones no solicitadas, que permita tratar un gran número de datos de cualquier naturaleza.

La invención tiene por objetivo también facilitar, al menos en un modo de realización, un procedimiento que relacione entre sí las diferentes detecciones de intrusiones no solicitadas detectadas.

La invención tiene por objetivo también facilitar, al menos en un modo de realización, un procedimiento que permita obtener en un instante t, el estado del tratamiento en curso.

La invención tiene por objetivo también facilitar, al menos en un modo de realización, un procedimiento que no necesite una interrogación de la red estudiada (y por tanto potencialmente corrompida) para recuperar datos adicionales.

La invención tiene por objetivo también facilitar, al menos en un modo de realización, un procedimiento que facilite un informe legible por un operador humano y directamente explotable.

La invención tiene por objetivo igualmente, según diferentes aspectos de la invención, facilitar un dispositivo, un producto programa de ordenador y un medio de almacenamiento correspondientes.

4. Exposición de la invención

Para hacer esto, la invención concierne a un procedimiento de detección de intrusiones no solicitadas en una red de información que comprende una etapa de recepción de una pluralidad de datos brutos procedentes de esta red, caracterizado por que comprende para cada dato recibido:

- una etapa de atribución de al menos un motor de búsqueda de un indicio de intrusión adaptado para tratar este tipo de dato bruto,
- una etapa de tratamiento(s) de este dato bruto, en paralelo por cada motor de búsqueda atribuido a este dato bruto, estando configurado cada motor de búsqueda para buscar en el citado dato al menos un indicio de intrusión, y extraer eventuales nuevos datos que haya que analizar, denominados datos derivados, potencialmente corrompidos,
- una etapa de reenvío de cada dato derivado como nuevo dato bruto hacia la citada etapa de atribución, si este dato derivado no ha sido ya tratado por el citado(los citados) mismo(s) motor(es) de búsqueda atribuido(s) a este dato, de manera que se asegure un análisis recurrente de cada dato bruto procedente de la red.

En todo el texto que sigue, los términos « dato bruto » o « dato derivado » designan un conjunto de códigos numéricos adaptados para poder ser interpretados directamente por una máquina, tal como un ordenador. En otras palabras, se trata de cualquier información digitalizada transportada por una red informática elaborada por un usuario, un programa o una máquina. Típicamente, se trata de un documento de texto, imagen, audio, vídeo, de un documento comprimido, de un documento de visualización tridimensional, de un programa ejecutable, de un archivo de máquina, de un archivo histórico, de una base de datos, de una dirección URL, una dirección URI, una dirección IP, un nombre de dominio, etc.

Un procedimiento según la invención permite analizar de manera recurrente todos los datos procedentes de la red y especialmente los datos encapsulados en otro dato. Un procedimiento según la invención puede por tanto analizar en detalle todos los datos procedentes de la red y recuperar todos los indicios de ataques de la red.

Además, un procedimiento según la invención somete cada dato a un motor de búsqueda adaptado específicamente al tipo del dato, ya sea para extraer del mismo otro dato, o para recuperar un indicio de que el dato es un dato no solicitado y representa un peligro para la seguridad de la red.

Los motores de búsqueda pueden ser de tipos cualesquiera, tales como herramientas de descompresión, herramientas de descifrado, herramientas « cajas de arena » más conocidas con su denominación inglesa de sandbox, que permiten la ejecución de softwares con menos riesgos para el sistema de explotación, analizadores de softwares maliciosos tales como antivirus, analizadores de redes, etc.

La recurrencia del análisis a partir de un dato bruto se detiene únicamente cuando cada dato derivado facilitado por cada motor de búsqueda ya ha sido puesto en evidencia por un motor de búsqueda idéntico. Esto significa especialmente que el motor de búsqueda ya ha permitido poner en evidencia el mismo dato. Si la versión del motor de búsqueda es diferente de la utilizada para la detección previa del dato derivado, el bucle recurrente continúa. Esto permite por ejemplo, en el caso de un antivirus y de un dato de tipo archivo, garantizar que el archivo ya ha sido analizado por la última versión del antivirus. Si este dato ya ha sido tratado, pero únicamente por una versión antigua del antivirus, entonces será analizado de nuevo por la última versión disponible. Esto permite por ejemplo detectar un virus en el archivo que no estaba presente en la versión anterior del antivirus y por tanto no detectable con la versión precedente del antivirus, aunque el archivo hubiera sido ya detectado.

En todo el texto, el análisis completo de un dato hace referencia al paso del dato por al menos las etapas sucesivas de atribución de los motores de búsqueda, de tratamiento(s) del dato por los motores de búsqueda y de reenvío de los datos derivados hacia la etapa de atribución. Salvo mención en contrario, los términos de « tratamiento del dato » corresponden a las etapas específicas de tratamiento(s) de este dato por los motores de búsqueda atribuidos. En cambio, el análisis del dato corresponde a la sucesión de etapas, incluidas las etapas de tratamiento. El término « análisis » se utiliza por tanto para definir el conjunto del proceso al cual es sometido el dato mientras que el término « tratamiento » se utiliza para aludir a la extracción por los motores de búsqueda.

Un procedimiento según la invención permite por tanto analizar automáticamente un gran número de datos, teniendo siempre la garantía de que los datos son tratados con las últimas versiones disponibles de los motores de búsqueda utilizados.

Un procedimiento según la invención permite un análisis automatizado y rápido de todos los datos procedentes de la red. Permite por tanto detectar rápidamente la presencia en la red de datos no solicitados, permitiendo a los equipos de seguridad actuar rápidamente para establecer las medidas correctivas necesarias.

Ventajosamente, un procedimiento según la invención comprende una etapa de comunicación de cada indicio de intrusión y cada dato derivado facilitado por cada motor de búsqueda en el transcurso de la citada etapa de tratamiento(s). Cada dato derivado y cada indicio de intrusión son comunicados a un módulo, denominado en lo que sigue módulo administrador. Esto permite a este módulo administrador especialmente controlar el procedimiento de detección teniendo un conocimiento del resultado de cada tratamiento de cada dato analizado, y por tanto determinar las etapas siguientes del análisis. Esto permite igualmente relacionar entre sí diferentes direcciones de intrusiones no solicitadas.

Ventajosamente, un procedimiento según la invención comprende una etapa de elaboración de un informe, denominado informe individual, en el cual los resultados de los tratamientos por los motores de búsqueda son posteriormente salvaguardados conjuntamente con una identificación de los motores de búsqueda atribuidos.

Esto permite salvaguardar los resultados en informes que son posteriormente explotables para controlar el procedimiento de detección, o para relacionar entre sí las diferentes detecciones, o bien para facilitar en un instante t el estado del procedimiento de detección.

Ventajosamente, la elaboración de cada informe individual es realizada por el mismo módulo que el módulo al cual son comunicados los resultados de los tratamientos, dicho de otro modo el citado módulo administrador.

Según esta variante ventajosa, en el transcurso de la etapa de atribución se elabora un informe individual para cada dato analizado. Los resultados de los tratamientos por los motores de búsqueda atribuidos a este dato son salvaguardados en este informe individual. En el marco del análisis recurrente, si en el transcurso de un tratamiento por un motor de búsqueda se pone en evidencia un dato derivado, este dato puede ser reenviado por la etapa de reenvío hacia la etapa de atribución y ser asimilado a un nuevo dato bruto. Así pues, el módulo administrador elabora un informe individual para este dato derivado, en el cual se salvaguardan los resultados de los tratamientos por los motores de búsqueda atribuidos a este dato derivado. Ei mecanismo de elaboración de los informes individuales continúa así, para cada dato bruto inicial, hasta el final del análisis recurrente para este dato. Esto genera por tanto un árbol de informes individuales, conteniendo este árbol en cada nudo el informe individual del tratamiento del dato considerado. Es por tanto posible posteriormente, leyendo el árbol de informes individuales, conocer el mecanismo que ha permitido detectar un dato derivado y/o un indicio de intrusión no solicitada y así comprender el mecanismo de ataque puesto en práctica por el atacante.

Cada informe individual elaborado por un procedimiento según esta variante puede contener una variedad de informaciones relativas a los tratamientos realizados por los motores de búsqueda atribuidos a este dato y al propio dato.

Ventajosamente, cada informe individual es elaborado de modo que contenga una o varias de las informaciones siguientes: fecha de la elaboración de la informe individual; fecha de los diferentes tratamientos realizados en el dato; nombre y versión de cada motor de búsqueda atribuido a este dato; nombre del dato analizado; tamaño de memoria del dato analizado; código de comprobación del dato; fuente del dato.

Ventajosamente, un procedimiento según la invención comprende una etapa de compilación, para cada dato bruto procedente de la red, de los citados informes individuales en un informe final cuando el análisis recurrente de este dato bruto haya terminado.

El informe final permite acceder al árbol de los informes individuales y saber lo que ha pasado en cada etapa del análisis.

Ventajosamente, un procedimiento según la invención comprende una etapa de salvaguarda de cada informe individual y de cada informe final en una base de salvaguarda.

Esto permite constituir una base de conocimientos de los diferentes tratamientos realizados por los motores de búsqueda. Esto permite igualmente relacionar entre sí detecciones de intrusiones realizadas en períodos diferentes, lo que permite por ejemplo determinar que ataques distintos provienen de la misma fuente.

Ventajosamente, un procedimiento según la invención comprende una etapa de interrogación a la citada base de salvaguarda para determinar si un dato derivado ha sido tratado ya por un motor de búsqueda idéntico.

Un procedimiento según esta variante interroga a la base de salvaguarda para determinar si el dato derivado detectado por un motor de búsqueda ha sido ya objeto de un tratamiento por un mismo motor de búsqueda. El recurso a la base de salvaguarda permite por tanto un acceso rápido y ordenado del conjunto de las informaciones obtenidas en el transcurso de los tratamientos precedentes.

Ventajosamente y según la invención, en la etapa de atribución, cada motor de búsqueda de un indicio de intrusión es seleccionado entre una pluralidad de motores de búsqueda.

Se facilita una lista predeterminada de motores de búsqueda, por ejemplo antes de la ejecución del procedimiento y la etapa de atribución selecciona para cada tipo de dato recibido, al menos un motor de búsqueda adaptado para tratar este dato.

Esta lista de motores de búsqueda puede ser actualizada desde la aparición, ya sea de un nuevo tipo de dato, o de un nuevo tratamiento posible que haya que efectuar en un tipo de dato.

Ventajosamente, un procedimiento según la invención comprende una etapa de notificación, por un motor de búsqueda específico, denominado motor por defecto, de que el citado dato no puede ser tratado si el dato es de un tipo no reconocido en el transcurso de la etapa de atribución.

Si la etapa de atribución no permite asociar un motor de búsqueda adaptado para tratar el tipo de dato recibido (sea un dato bruto procedente directamente de la red cuyos datos son analizados, o un dato derivado, procedente de un tratamiento precedente por otro motor de búsqueda), el dato es transmitido a un motor de búsqueda por defecto que solamente hace notificar que el dato es de un tipo no reconocido que el mismo no puede tratar. Se elabora sin embargo un informe en el transcurso de la etapa de elaboración y la información según la cual el dato no puede ser tratado, es salvaguardada en el informe.

La invención tiene por objetivo igualmente un dispositivo de detección de intrusión no solicitada en una red de información, especialmente una red informática, que comprende un módulo de recepción de los datos brutos procedentes de esta red, caracterizado por que el mismo comprende:

- una pluralidad de motores de búsqueda de un indicio de intrusión configurados para buscar en el seno de al menos un tipo de dato bruto, al menos un indicio de ataque y extraer eventuales nuevos datos que haya que analizar, denominados datos derivados, potencialmente corrompidos,

- un módulo repartidor adaptado para atribuir a cada dato bruto recibido por el citado módulo de recepción, al menos un motor de búsqueda de la citada pluralidad de motores de búsqueda adaptado para tratar este tipo de dato bruto,

- un módulo administrador conectado con los motores de búsqueda y con un módulo repartidor y configurado para transmitir al citado módulo repartidor cada dato derivado como nuevo dato bruto si éste no ha sido tratado ya por los citados mismos motores de búsqueda, de manera que se asegure un análisis recurrente de cada dato bruto recibido por el citado módulo de recepción.

En todo el texto, se designa por módulo, un elemento informático, un subconjunto de un programa informático, que puede ser compilado separadamente, para una utilización independiente, o para ser ensamblado con otros módulos de un programa, o un elemento material, o una combinación de un elemento material y de un sub-programa informático. Dicho elemento material puede comprender un circuito integrado apropiado para una aplicación (más conocido con el acrónimo ASIC de la denominación inglesa Application-Specific Integrated Circuit) o un circuito lógico programable o cualquier material equivalente. De manera general, un módulo es por tanto un elemento (de software y/o material) que permita asegurar una función.

Según la invención, un módulo de recepción recibe una pluralidad de datos brutos procedentes de una red que haya que analizar. Cada dato es analizado después por el módulo repartidor para asignar a este dato bruto uno o varios motores de búsqueda adaptados para tratar este tipo de dato bruto. Los resultados de estos diferentes tratamientos son transmitidos después al módulo administrador el cual determina si ha terminado o no el análisis recurrente de este dato bruto. Si deben ser analizados nuevos datos brutos, estos datos son transmitidos al módulo repartidor para una reiteración del proceso de análisis.

Los motores de búsqueda pueden ser de tipos cualesquiera. Los mismos pueden comprender herramientas de descompresión, herramientas de descifrado, herramientas « cajas de arena » más conocidas con la denominación

inglesa sandbox, analizadores de softwares maliciosos tales como antivirus, analizadores de redes, etc. Estos pueden presentarse en forma de productos materiales, de softwares o incluso de servicios ofrecidos por un tercero.

Preferentemente, el módulo de recepción de los datos procedentes de la red que haya que analizar y el módulo administrador forman uno y un solo módulo de tal modo que el módulo administrador es el que recibe los datos procedentes de la red que deben ser analizados.

El módulo repartidor pone en práctica ventajosamente la etapa de atribución de un procedimiento según la invención y la etapa de atribución de un procedimiento según la invención es puesta en práctica ventajosamente por un módulo repartidor según la invención.

El módulo administrador pone en práctica ventajosamente la etapa de reenvío de un procedimiento según la invención y la etapa de reenvío de un procedimiento según la invención es puesta en práctica ventajosamente por un módulo administrador según la invención.

Ventajosamente y según la invención, cada motor de búsqueda está configurado para transmitir al citado módulo administrador cada indicio de intrusión y cada dato derivado que el mismo haya detectado.

Según esta variante, el módulo administrador es el que recibe los resultados de los tratamientos. El mismo desempeña por tanto la función de módulo de control y de mando del dispositivo puesto que, por una parte, recibe los datos que haya que analizar y, por otra, recibe los resultados de los tratamientos por los diferentes motores de búsqueda. El mismo es por tanto capaz de determinar si el análisis recurrente debe continuar o si este dato ha sido extensivamente analizado.

El módulo administrador pone en práctica ventajosamente la etapa de comunicación de un procedimiento según la invención y la etapa de comunicación de un procedimiento según la invención es puesta en práctica ventajosamente por un módulo administrador según la invención.

Ventajosamente y según esta variante, el módulo administrador está configurado para elaborar para cada dato trasmitido al módulo repartidor, un informe de tratamiento, denominado informe individual, en el cual los resultados de los tratamientos por los citados motores de búsqueda transmitidos al módulo administrador son posteriormente salvaguardados en combinación con la identificación de los motores de búsqueda atribuidos.

El módulo administrador elabora, según esta variante, un informe individual para cada dato transmitido al módulo repartidor.

El módulo administrador pone en práctica ventajosamente la etapa de elaboración de un informe individual de un procedimiento según la invención y la etapa de elaboración de un informe individual según la invención es ventajosamente puesta práctica por un módulo administrador según la invención.

Ventajosamente, un dispositivo según la invención comprende un módulo de elaboración de un informe final, para cada dato bruto procedente de la red, compilando los informes individuales, una vez terminado el análisis recurrente de este dato bruto.

El módulo de elaboración pone en práctica ventajosamente la etapa de compilación de los informes individuales de un procedimiento según la invención y la etapa de compilación de los informes individuales según la invención es ventajosamente puesta en práctica por un módulo de elaboración según la invención.

Ventajosamente, un dispositivo según la invención comprende una base de salvaguarda accesible por el citado módulo administrador en la cual son salvaguardados cada informe individual y cada informe final.

El módulo administrador pone en práctica ventajosamente la etapa de interrogación a la base de salvaguarda de un procedimiento según la invención y la etapa de interrogación a la base de salvaguarda según la invención es puesta en práctica ventajosamente por un módulo administrador según la invención.

Según una variante ventajosa de la invención, la base de salvaguarda comprende además informaciones relativas a tratamientos de datos brutos procedentes de otras redes de información desempeñando así la función de base de conocimiento.

Según esta variante, la base de salvaguarda comprende informaciones que provienen por ejemplo de análisis de otras redes de información o de análisis precedentes de la misma red de información. Es por tanto posible hacer correlaciones entre los diferentes análisis y caracterizar los ataques detectados. Así pues, informaciones de diferentes ataques permiten determinar un perfil de un atacante por ejemplo reagrupando informaciones diferentes, pero que presentan entre las mismas un vínculo, como por ejemplo, el mismo tipo de archivo corrompido detectado o una firma idéntica de un atacante, etc.

Ventajosamente y según la invención, el módulo de recepción de los datos brutos no está conectado con la citada red de información en la cual se pone en práctica la detección de ataques dirigidos.

Preferentemente, el análisis completo de los datos brutos procedentes de una red se realiza mientras se está totalmente desconectado de la red en cuestión. Esto asegura que los eventuales ataques no tengan conocimiento de las búsquedas que son efectuadas en su contra. La idea es permanecer lo más discreto posible en el análisis que se hace para no alertar a los atacantes de que está en curso una detección, lo que permite posteriormente contrarrestar mejor al atacante. Esto permite por ejemplo, a partir del momento en que se haya detectado una intrusión no solicitada, observar lo que hace el atacante, determinar lo que éste intenta extraer de la red y eventualmente obtener informaciones sobre el atacante para cercarle y actualizarle. Así pues, no se efectúa ninguna interrogación a la red informática estudiada en el transcurso del análisis de los datos procedentes de la red.

Dicho esto, según otras variantes, el análisis completo de los datos puede ser hecho en línea y/o analizando el flujo continuo de los datos dirigidos a la red.

Un dispositivo según la invención puede presentar diferentes arquitecturas. Puede tratarse de una arquitectura distribuida o de una arquitectura autónoma e independiente.

Según una variante ventajosa, el dispositivo comprende una pluralidad de máquinas distintas, alojando cada máquina al menos un módulo del dispositivo, estando las máquinas conectadas una a otra por intermedio de al menos una red alámbrica y/o inalámbrica.

La invención tiene por objetivo igualmente un producto programa de ordenador descargable desde una red de comunicación y/o registrado en un soporte legible por ordenador y/o ejecutable por un procesador, caracterizado por que el mismo comprende instrucciones de código de programa para la puesta en práctica del procedimiento de detección de intrusiones no solicitadas de una red informática según la invención.

Dicho producto programa de ordenador puede ser ejecutado por ejemplo en una máquina única para analizar el contenido de los datos almacenados en este ordenador y detectar eventuales intrusiones no solicitadas.

La invención tiene por objetivo igualmente un medio de almacenamiento legible por un ordenador total o parcialmente desmontable, que almacene un programa de ordenador que comprende un juego de instrucciones ejecutables por un ordenador para poner en práctica el procedimiento de detección de intrusiones no solicitadas de una red de información según la invención.

La invención concierne igualmente a un procedimiento, un dispositivo, un producto programa de ordenador y un dispositivo de almacenamiento, caracterizados en combinación por todas o parte de las características mencionadas anteriormente o en lo que sigue.

5. Lista de las figuras

Otros objetivos, características y ventajas de la invención se pondrán de manifiesto en la lectura de la descripción que sigue dada a modo únicamente no limitativo y que se refiere a las figuras anejas, en las cuales:

- la figura 1 es una vista esquemática en forma de etapas de un procedimiento de detección de intrusiones no solicitadas según un modo de realización de la invención,
- la figura 2 es una vista esquemática de un dispositivo de detección de intrusiones no solicitadas en una red de información según un modo de realización de la invención,
- la figura 3 es una vista esquemática del principio del análisis recurrente puesto en práctica en un procedimiento y por un dispositivo según un modo de realización de la invención,
- la figura 4 es una vista esquemática de la sucesión de etapas de elaboración de los informes individuales puestas en práctica por un dispositivo y en un procedimiento de detección de un modo de realización de la invención,
- la figura 5 es una vista esquemática en forma de etapas de un procedimiento según un modo de realización de la invención puesto en práctica por un módulo administrador de un dispositivo según un modo de realización de la invención,
- la figura 6 es una vista esquemática de un dispositivo de detección de intrusiones no solicitadas según un modo de realización de la invención, en el cual el tratamiento de los datos se realiza estando desconectado de la red analizada,
- la figura 7 es una vista esquemática de un dispositivo de detección de intrusiones no solicitadas según un modo de realización de la invención, en el cual motores de búsqueda de un indicio de intrusión están distribuidos en diferentes sitios de tratamiento

6. Descripción detallada de un modo de realización de la invención

En toda la descripción que sigue en referencia a las figuras, salvo indicación en contrario, un dispositivo y un procedimiento de detección de intrusiones no solicitadas en una red de información según la invención se describen tomando el ejemplo de una red de información de tipo red informática. Dicha red informática permite el reparto entre diferentes usuarios y/o máquinas de datos digitales de tipos cualesquiera, elaborados por usuarios, programas o máquinas (ordenadores, teléfonos móviles, tabletas digitales, etc.). Se trata por ejemplo de un documento de texto, imagen, audio, vídeo, de un documento comprimido, de un documento de visualización tridimensional, de un programa ejecutable, de un archivo de máquina, de un archivo histórico, de una base de datos, de una dirección URL, una dirección URI, una dirección IP, un nombre de dominio, etc.

En referencia a la figura 1, un procedimiento de detección de intrusiones no solicitadas en una red de información según la invención comprende una etapa 10 de recepción de una pluralidad de datos brutos procedentes de esta red. En la figura 1, un dato bruto 40 recibido en el transcurso de la etapa de recepción está representado como correo electrónico (denominado en lo que sigue e-mail) que contiene archivos adjuntos.

Un procedimiento según la invención comprende además, para cada dato 40 bruto, una etapa 11 de atribución de al menos un motor 32, 33, 34, 35 de búsqueda de un indicio de intrusión adaptado para tratar este tipo de dato bruto.

En el caso de un dato 40 bruto de tipo e-mail, los motores 32, 33, 34, 35 de búsqueda son por ejemplo antivirus adaptados para detectar eventuales virus en los archivos adjuntos del e-mail, herramientas de descifrado para descifrar datos cifrados en archivo adjunto del e-mail, herramientas de descompresión, etc.

De manera general, los motores de búsqueda pueden ser de tipos cualesquiera, tales como herramientas de descompresión, herramientas de descifrado, sandbox de los analizadores de softwares maliciosos tales como antivirus, analizadores de redes, etc. Los motores de búsqueda son determinados en función de los datos brutos que haya que analizar. Si aparecen nuevos datos en la red que haya que analizar, pueden ser integrados a la invención nuevos motores de búsqueda para permitir el tratamiento de estos nuevos datos. La invención se describe con cuatro motores de búsqueda distintos, pero es evidente de que el número de motores de búsqueda no está imitado a este número. Según un modo de realización de la invención, los motores de búsqueda son seleccionados entre una lista predeterminada de motores de búsqueda.

Si el dato que haya que tratar es de tipo no reconocido, hay una notificación por un motor de búsqueda atribuido por defecto a este dato no reconocido de que el dato no puede ser tratado.

Según la invención, un procedimiento comprende además una etapa 12 de tratamientos de este dato bruto 40, en paralelo por cada motor 32, 33, 34, 35 de búsqueda atribuido a este dato 40 bruto.

Cada motor 32, 33, 34, 35 de búsqueda está configurado para buscar en este dato 40 al menos un indicio de intrusión y extraer eventuales datos 41 derivados, potencialmente corrompidos.

Un procedimiento según la invención comprende una etapa 13 de reenvío de cada dato 41 derivado como nuevo dato bruto hacia la etapa de atribución, si este dato derivado no ha sido tratado ya por los mismos motores de búsqueda atribuidos a este dato, de manera que se asegure un análisis recurrente de cada dato bruto procedente de la red.

El análisis es recurrente y se detiene únicamente cuando ya no se detecte ningún dato derivado o cuando los datos derivados puestos en evidencia hayan sido tratados ya por motores de búsqueda idénticos, Los motores de búsqueda atribuidos a un dato derivado no son necesariamente los mismos que los motores de búsqueda atribuidos al dato bruto inicial. Esto depende del tipo de dato derivado y del tipo de dato bruto inicial.

Un procedimiento según el modo de realización de la figura 1 es puesto en práctica ventajosamente por un dispositivo según la figura 2.

Dicho dispositivo comprende un módulo 30 administrador, un módulo 31 repartidor y un pluralidad de motores 32, 33, 34, 35 de búsqueda.

El módulo 30 administrador desempeña la función de módulo de recepción de los datos que haya que analizar.

Los motores 32, 33, 34, 35 de búsqueda está adaptados para buscar en el seno de al menos un tipo de dato bruto, al menos un indicio de ataque y extraer eventuales nuevos datos derivados, potencialmente corrompidos, que haya que analizar.

El módulo 31 repartidor está adaptado para atribuir a cada dato bruto recibido por el módulo 30 administrador, al menos un motor de búsqueda adaptado para tratar este tipo de dato bruto.

Si el dato que haya que tratar por los motores de búsqueda es de un tipo no reconocido, se atribuye a este dato un motor de búsqueda, denominado motor por defecto.

El módulo 30 administrador desempeña la función de unidad de control y de mando del dispositivo. Es el que recibe los datos que haya que analizar, el que los dirige hacia el módulo repartidor. Es también el que determina si un eventual dato derivado detectado por un motor de búsqueda debe ser a su vez analizado o no.

Según un modo de realización de la invención, comprende además un módulo 36 de elaboración de los informes. Este módulo elabora informes individuales al final de cada tratamiento, bajo el impulso del módulo administrador, y el informe final, al final del análisis completo del dato.

El módulo 30 administrador salvaguarda los resultados de los diferentes tratamientos en una base 37 de salvaguarda.

La consulta a esta base de salvaguarda permite conocer el estado del análisis de la red en un instante t, no solamente por los operadores que efectúan el análisis de la red, sino igualmente por operadores que analicen otras redes, desempañando de esta manera la base 37 de salvaguarda la función de base de conocimiento para recuperar informaciones de ataques ya detectados. Esto permite especialmente conectar entre sí diferentes detecciones con el fin de caracterizar lo mejor posible a un atacante.

Según el modo de realización de la figura 2, los diferentes módulos son elementos de software.

Según otros modos de realización, al menos ciertos módulos pueden ser subconjuntos de un programa informático, que pueden ser compilados separadamente. Los mismos pueden también tomar la forma de un elemento material, o de una combinación de un elemento material y de un subprograma informático.

En la figura 3, el principio del análisis recurrente está ilustrado a partir de un dato bruto que toma la forma de un correo electrónico 50 (denominado en lo que sigue e-mail). Con fines de ilustración y de claridad, los módulos utilizados en el transcurso del análisis están representados para cada bucle recurrente. El análisis representado en la figura 3 cuenta con cinco ciclos, indicados respectivamente por A, B, C, D y E.

En el transcurso de ciclo A, el e–mail 50 es recibido por el módulo 30 administrador en el transcurso de la etapa 10 de recepción, y transmitido después a módulo 31 repartidor en el transcurso de la etapa 11 de atribución, el cual le redirige hacia un motor 32 de búsqueda adaptado para tratar un e-mail en el transcurso de la etapa 12 de tratamientos. La etapa 12 de tratamientos pone en evidencia dos datos derivados, respectivamente un archivo de texto 51 y un archivo comprimido 52 de tipo archivo « zip ». Estos dos datos derivados son reenviados cada uno, en el transcurso de una etapa 13 de reenvío, hacia el módulo 30 administrador para experimentar un nuevo ciclo de análisis.

En el transcurso del ciclo B de análisis, el archivo de texto 51 es examinado por el módulo 30, administrador, y después transmitido al módulo 31, repartidor. El módulo 31, repartidor atribuye a este archivo de texto 51, en el transcurso de la etapa recurrente 11 de atribución, el motor 33 de búsqueda adaptado para tratar archivos de texto. Según el modo de realización representado en la figura 3, el motor 33 de búsqueda no detecta ningún nuevo dato derivado en el transcurso de la etapa 12 de tratamiento. En cambio, este motor de búsqueda puede haber detectado un indicio de ataque, por ejemplo si el archivo contiene un virus y si el motor 33 de búsqueda es un antivirus. En la hipótesis en que no se haya detectado ningún nuevo dato derivado por el motor 33 de búsqueda y que este motor 33 de búsqueda sea idéntico al motor de búsqueda previamente utilizado para analizar un archivo de texto, el bucle recurrente para este archivo de texto ha terminado.

En el transcurso del ciclo C de análisis, el archivo comprimido 52 es examinado por el módulo 30 administrador y después transmitido al módulo 31 repartidor. El módulo 31 repartidor atribuye a este archivo comprimido 52, en el transcurso de la etapa recurrente 11 de atribución, el motor 34 de búsqueda adaptado para tratar archivos comprimidos. Esta etapa 12 de tratamiento por el motor 34 de búsqueda pone en evidencia dos nuevos datos derivados, respectivamente un archivo de texto 53 y una base de datos 54. Estos dos nuevos datos son por tanto a su vez reenviados hacia el módulo 30 administrador en el transcurso de una etapa recurrente de reenvío.

En el transcurso del ciclo D de análisis, el archivo de texto 53 es examinado por el módulo 30 administrador y transmitido después al módulo 31 repartidor. El módulo 31 repartidor atribuye a este archivo de texto 53, en el transcurso de la etapa recurrente 11 de atribución, el motor 33 de búsqueda adaptado para tratar archivos de texto. En el modo de realización de la figura 3, se trata del mismo motor de búsqueda que el utilizado en el transcurso del ciclo B puesto que se trata de un archivo de texto del mismo tipo. Según el modo de realización representado en la figura 3, el motor 33 de búsqueda no detecta ningún nuevo dato derivado en el transcurso de la etapa 12 de tratamiento. En la hipótesis en que no haya sido detectado ningún nuevo dato derivado por el motor 33 de búsqueda y que este motor 33 de búsqueda sea idéntico al motor de búsqueda previamente utilizado para analizar un archivo de texto, el bucle recurrente para este archivo de texto ha terminado.

Finalmente, en el transcurso del ciclo E de análisis, la base de datos 54 es examinada por el módulo 30 administrador y transmitida después al módulo 31 repartidor. El módulo 31 repartidor atribuye a esta base de datos 54, en el transcurso de la etapa recurrente 11 de atribución, el motor 35 de búsqueda adaptado para tratar bases de datos. En la hipótesis en que no haya sido detectado ningún nuevo dato derivado por el motor 35 de búsqueda y que este motor 35 de búsqueda sea idéntico al motor de búsqueda previamente utilizado para analizar un archivo del mismo tipo, el bucle recurrente para este dato ha terminado.

De esta manera, el dato bruto 50 es analizado totalmente por los ciclos sucesivos A, B, C, D y E, los cuales han permitido poner en evidencia los datos derivados 51, 52, 53, 54 y los eventuales indicios de ataques en el transcurso de los tratamientos por los diferentes motores de búsqueda. Como se indicó anteriormente, estos indicios de ataque son por ejemplo detecciones de un virus por un software antivirus.

Según un modo ventajoso de realización de la invención, se elaboran informes individuales para contener los resultados de los tratamientos por los motores de búsqueda y la identificación de los motores de búsqueda atribuidos a este dato.

En la figura 3, se elabora un informe 61 para contener los resultados del análisis del e-mail 50 obtenidos durante el ciclo inicial A de análisis del e-mail 50. El archivo de texto 51, derivado del e-mail 50 pasa después por las etapas sucesivas de recepción, de atribución y de tratamientos. Los resultados de este bucle B de análisis son salvaguardados en un informe 62. El archivo comprimido 52, derivado del e-mail 50, pasa igualmente por las etapas sucesivas de recepción, de atribución y de tratamientos. Los resultados de este bucle C de análisis son salvaguardados en un informe 63. Habiendo puesto en evidencia estos análisis dos nuevos datos derivados, respectivamente el archivo de texto 53 y la base de datos 54, cada uno de estos nuevos datos pasa por el bucle de análisis. Los resultados del bucle D de análisis del archivo de texto 53 son salvaguardados en un informe 64 y los resultados del bucle E de análisis de la base de datos son salvaguardados en un informe 65.

Esto permite generar un árbol de informes tal como está representado en la figura 4.

Cuando haya terminado el análisis completo del dato, según una variante ventajosamente de la invención, en el transcurso de una etapa 25 de compilación, se elabora un informe final que compila el conjunto de los informes individuales. Cada informe individual y el informe final son preferentemente salvaguardados en una base 37 de salvaguarda.

La figura 5 ilustra las diferentes etapas puestas en práctica en un módulo 30 administrador según un modo preferente de realización de la invención.

En la etapa 10, se recibe un dato 40 que hay que analizar. En la etapa 14 de elaboración de un informe individual se elabora un informe individual 60. Este informe individual 60 es completado posteriormente, pero se elabora desde la recepción del dato 40 que hay que analizar para indicar por ejemplo la hora de recepción del dato y la proveniencia.

En la etapa 15 siguiente, el módulo 30 administrador determina si el dato 40 es conocido. Para hacer esto, el módulo 30 administrador consulta la base 37 de salvaguarda.

Si el dato 40 es conocido, el módulo 30 administrador extrae de la base 37 de salvaguarda, en el transcurso de una etapa 16, los informes elaborados durante el análisis precedente de este dato 40 para listar en los mismos los diferentes motores de búsqueda utilizados precedentemente para tratar este dato 40. Si los motores de búsqueda han sido actualizados, el dato 40 es enviado al módulo 31 repartidor para tratamiento. Si los motores de búsqueda no han sido actualizados, el dato 40 no será tratado de nuevo y se pasa directamente a la etapa 19 de interrogación a la base 37 de salvaguarda para recuperar los resultados facilitados por los motores de búsqueda.

Si el dato 40 no es conocido, éste es enviado al módulo 31 repartidor en el transcurso de una etapa 18 de transmisión del dato al módulo 31 repartidor.

En el transcurso de una etapa 19, los resultados de los tratamientos por los diferentes motores de búsqueda son recuperados por el módulo 30 administrador.

El informe 60 individual es actualizado en el transcurso de una etapa 20.

Este informe 60 es salvaguardado en la base 37 de salvaguarda en el transcurso de una etapa 21 de salvaguarda.

En la etapa 22, el módulo 30 administrador determina si se ha puesto en evidencia un dato derivado. Si se ha puesto en evidencia un dato derivado, entonces éste es reenviado hacia la etapa 10 de recepción para análisis recurrente de este dato derivado. Según el modo de realización de la figura 5, el final del análisis recurrente es determinado por dos pruebas sucesivas separadas. Por una parte, está la determinación en la etapa 22 de la existencia de un nuevo dato y, por otra, la determinación de un eventual nuevo motor de búsqueda en la etapa 17. Según otros modos de realización, estas dos etapas son concomitantes.

Si ningún nuevo dato es puesto en evidencia por los motores de búsqueda, se elabora un informe final en la etapa 25 de compilación de los informes individuales.

En la etapa 26, se actualiza la base de salvaguarda 27.

Un dispositivo según la invención puede estar conectado físicamente a la red informática de la cual analiza los datos o estar separado de esta última. Para hacer esto, el módulo 10 de recepción recibe los datos directamente de la red analizada o por intermedio de una base de datos previamente almacenada en un soporte de archivos.

La figura 6 ilustra un ejemplo de dispositivo separado de la red analizada. Un conjunto de datos de diferentes tipos procedentes de la red está almacenado en soportes de archivos. En la figura y a modo de ejemplo únicamente no limitativo, los datos están representados como ficheros de texto 70, correos electrónicos 71, archivos sistemas 72, archivos comprimidos 73, bases de datos 74, archivos anuarios 75, archivos procedentes de teléfonos móviles 76 y archivos procedentes de tabletas digitales 77. Evidentemente, cualquier otro tipo de archivo puede ser tenido en cuenta para un dispositivo según la invención.

El conjunto de estos datos que haya que analizar es almacenado después en soportes de archivos tal como un disco óptico 78, una llave USB 79 o un disco duro externo 80. Naturalmente, pueden ser considerados otros tipos de soportes.

El dispositivo 8 de detección de intrusiones no solicitadas analiza el conjunto de los datos almacenados en los soportes de almacenamiento. En otras palabras, el módulo de recepción de un dispositivo según la invención es alimentado por los datos procedentes de uno u otro de estos soportes de archivos de manera que se establezca un informe final 81 de análisis de este conjunto de datos.

Según otros modos de realización, el análisis puede ser efectuado en línea.

Cualquiera que sea el tipo de análisis efectuado (en línea o desconectado de la red), el análisis puede ser local o estar distribuido entre diferentes sitios.

Por ejemplo, según el modo de realización de la figura 7, el análisis está distribuido entre tres localizaciones. Según este modo de realización, el módulo 30 administrador está localizado en una primera máquina 56 de un primer sitio 44. Esta primera máquina 56 del primer sitio 44 alberga igualmente el módulo 31 repartidor, el módulo 36 de elaboración de informes y dos motores de búsqueda 32, 33. En este mismo sitio 44 está albergado, por una segunda máquina 57, un tercer motor de búsqueda 34.

Según el modo de realización de la figura 7, un tercer motor de búsqueda 35 está albergado por una máquina 58 de un segundo sitio 45.

Según el modo de realización de la figura 7, un tercer sitio 46 alberga la base de salvaguarda 37 en una máquina 57.

El conjunto de los sitios están conectados por una red tal como la red 48 Internet.

Según otros modos de realización, los sitios 44, 45, 46 están conectados por una red inalámbrica.

Un procedimiento según la invención puede ser puesto en práctica en forma de una secuencia de instrucciones de un programa informático. El procedimiento puede ser puesto en práctica igualmente en forma material o en una forma mixta material y de software. En el caso en que la invención esté implantada parcial o totalmente en la forma de software, la secuencia de instrucciones correspondiente podrá estar almacenada en un medio de almacenamiento desmontable, tal como un disquete, un CD-ROM, un DVD-ROM, una llave USB, etc., o en un medio de almacenamiento no desmontable, siendo estos diferentes medios legibles parcial o totalmente por un ordenador o por un microprocesador.

La invención no se limita a los únicos modos de realización descritos. En particular, según otros modos de realización, la red de información es una red de tipo PMR o cualquier otro tipo de red que transporte informaciones y susceptible de encontrar datos maliciosos.

REIVINDICACIONES

1. Procedimiento de detección de intrusiones no solicitadas en una red de información que comprende una etapa (10) de recepción de una pluralidad de datos (40, 50) brutos procedentes de esta red, que comprende para cada dato (40, 50) bruto recibido:

- una etapa (11) de atribución de al menos un motor (32, 33, 34, 35) de búsqueda de un indicio de intrusión adaptado para tratar este tipo de dato bruto,

- una etapa (12) de tratamiento de este dato bruto, en paralelo por cada motor (32, 33, 34, 35) de búsqueda atribuido a este dato (40, 50) bruto, estando configurado cada motor (32, 33, 34, 35) de búsqueda para buscar en el citado dato al menos un indicio de intrusión, y extraer eventuales nuevos datos que haya que analizar, denominados datos (41, 51, 52, 53, 54) derivados, potencialmente corrompidos,

- una etapa (13) de reenvío de cada dato (41, 51, 52, 53, 54) derivado como nuevo dato bruto hacia la citada etapa (11) de atribución, si este dato derivado no ha sido tratado ya por el citado mismo motor de búsqueda atribuido a este dato, de manera que se asegure un análisis recurrente de cada dato bruto procedente de la red,

caracterizado por que el análisis recurrente continúa si el citado motor de búsqueda ha sido actualizado y presenta una versión diferente de la utilizada para un tratamiento previo del dato derivado.

2. Procedimiento según la reivindicación 1, caracterizado por que comprende una etapa de comunicación de cada indicio de intrusión y cada dato derivado facilitado por cada motor (32, 33, 34, 35) de búsqueda en el trascurso de la citada etapa (12) de tratamiento.

3. Procedimiento según una de las reivindicaciones 1 o 2, caracterizado por que comprende una etapa (25) de compilación, para cada dato bruto procedente de la red, de los citados informes individuales (60, 61, 62, 63, 64, 65) individuales en un informe final cuando el análisis recurrente de este dato bruto ha terminado.

4. Procedimiento según una de las reivindicaciones 1 a 3, caracterizado por que en la citada etapa (11) de atribución, cada motor de búsqueda de un indicio de intrusión es seleccionado entre una pluralidad predeterminada de motores de búsqueda.

5. Procedimiento según la reivindicación 4, caracterizado por que comprende una etapa de notificación por un motor de búsqueda específico, denominado motor por defecto, de que el citado dato no puede ser tratado si el citado dato es de un tipo no reconocido.

6. Procedimiento según una cualquiera de las reivindicaciones 1 a 5, caracterizado por que comprende:

- una etapa (14) de elaboración de un informe, denominado informe (60, 61, 62, 63, 64, 65) individual, en el cual los resultados de los tratamientos por los motores (32, 33, 34, 35) de búsqueda son posteriormente salvaguardados así como una identificación de los motores de búsqueda atribuidos al dato derivado, de los cuales el nombre y la versión de los citados motores de búsqueda,

- una etapa (21, 26) de salvaguarda de cada informe individual y de cada informe final en una base (37) de salvaguarda,

- una etapa (16, 19) de interrogación a la citada base (37) de salvaguarda para determinar si un dato derivado ha sido tratado ya por un motor de búsqueda idéntico.

7. Procedimiento según una cualquiera de las reivindicaciones 1 a 6, caracterizado por que al menos uno de los motores (32, 33, 34, 35) de búsqueda se presente en forma de una herramienta de descifrado o de una herramienta de tipo « caja de arena ».

8. Dispositivo de detección de intrusiones no solicitadas en una red de información que comprende un módulo de recepción de los datos brutos procedentes de esta red, que comprende:

- una pluralidad de motores (32, 33, 34, 35) de búsqueda de un indicio de intrusión configurados para buscar en el seno de al menos un tipo de dato (40, 50, 70, 71, 72, 73, 74, 75, 76, 77) bruto, al menos un indicio de ataque y extraer eventuales nuevos datos que haya que analizar, denominados datos (51, 52, 53, 54) derivados, potencialmente corrompidos,

- un módulo (31) repartidor adaptado para atribuir a cada dato bruto recibido por el citado módulo de recepción, al menos un motor (32, 33, 34, 35) de búsqueda de la citada pluralidad de motores de búsqueda adaptado para tratar este tipo de dato bruto,

- un módulo (30) administrador conectado con los motores (32, 33, 34, 35) de búsqueda y con el módulo (31) repartidor y configurado para transmitir al citado módulo (31) repartidor cada dato derivado como nuevo dato bruto si éste no ha sido tratado ya por el citado mismo motor de búsqueda, de manera que se asegure un análisis recurrente

de cada dato bruto recibido por el citado módulo de recepción, caracterizado por que el análisis recurrente continúa si el citado motor de búsqueda ha sido actualizado y presenta una versión diferente de la utilizada por un tratamiento previo del dato derivado.

9. Dispositivo según la reivindicación 8, caracterizado por que cada motor (32, 33, 34, 35) de búsqueda está configurado para transmitir al citado módulo (30) administrador cada indicio de intrusión y cada dato derivado que haya detectado.

10. Dispositivo según una cualquiera de las reivindicaciones 8 o 9, caracterizado por que:

- el módulo (30) administrador está configurado para elaborar para cada dato trasmitido al módulo (31) repartidor, un informe de tratamiento, denominado informe (61, 62, 63, 64, 65) individual, en el cual los resultados de los tratamientos por los citados motores de búsqueda transmitidos al módulo (30) administrador son posteriormente salvaguardados en combinación con la identificación de los motores (32, 33, 34, 35) de búsqueda atribuidos, de los cuales el nombre y la versión de los citados motores de búsqueda,

- el dispositivo comprende una base (37) de salvaguarda accesible por el citado módulo (30) administrador en la cual son salvaguardados cada informe individual y cada informe final,

- el módulo (30) administrador está configurado para interrogar la citada base (37) de salvaguarda para determinar si un dato derivado ha sido tratado ya por un motor de búsqueda idéntico.

11. Dispositivo según una cualquiera de las reivindicaciones 8 a 10, caracterizado por que al menos uno de los motores (32, 33, 34, 35) de búsqueda se presenta en forma de una herramienta de descifrado o de una herramienta de tipo «caja de arena ».

12. Dispositivo según una de las reivindicaciones 8 a 11, caracterizado por que un módulo (36) de elaboración de un informe final, para cada dato bruto procedente de la red, compilando los informes (61, 62, 63, 64, 65) individuales, una vez terminado el análisis recurrente de este dato bruto.

13. Dispositivo según una de las reivindicaciones 8 a 12, caracterizado por que comprende una pluralidad de máquinas (56, 57, 58, 59) distintas, alojando cada máquina al menos un módulo del dispositivo, estando conectadas las máquinas (56, 57, 58, 59) una con otra por intermedio de al menos una red (48) alámbrica o inalámbrica.

14. Producto programa de ordenador descargable desde una red de comunicación y/o registrado en un soporte legible por ordenador y/o ejecutable por un procesador, caracterizado por que comprende instrucciones de código de programa para la puesta en práctica del procedimiento de detección de ataques dirigidos de una red de información según al menos una de las reivindicaciones 1 a 7, cuando el programa es ejecutado en un ordenador.

15. Medio de almacenamiento legible por ordenador, total o parcialmente desmontable, que almacena un programa de ordenador que comprende un juego de instrucciones ejecutable por un ordenador para poner en práctica el procedimiento de detección de ataques dirigidos de una red de información según al menos una de las reivindicaciones 1 a 7.

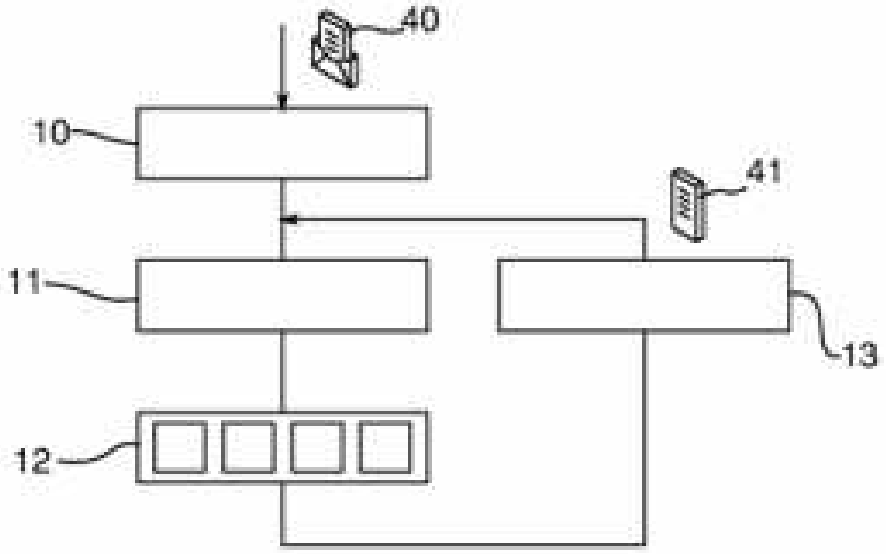

Figura 1

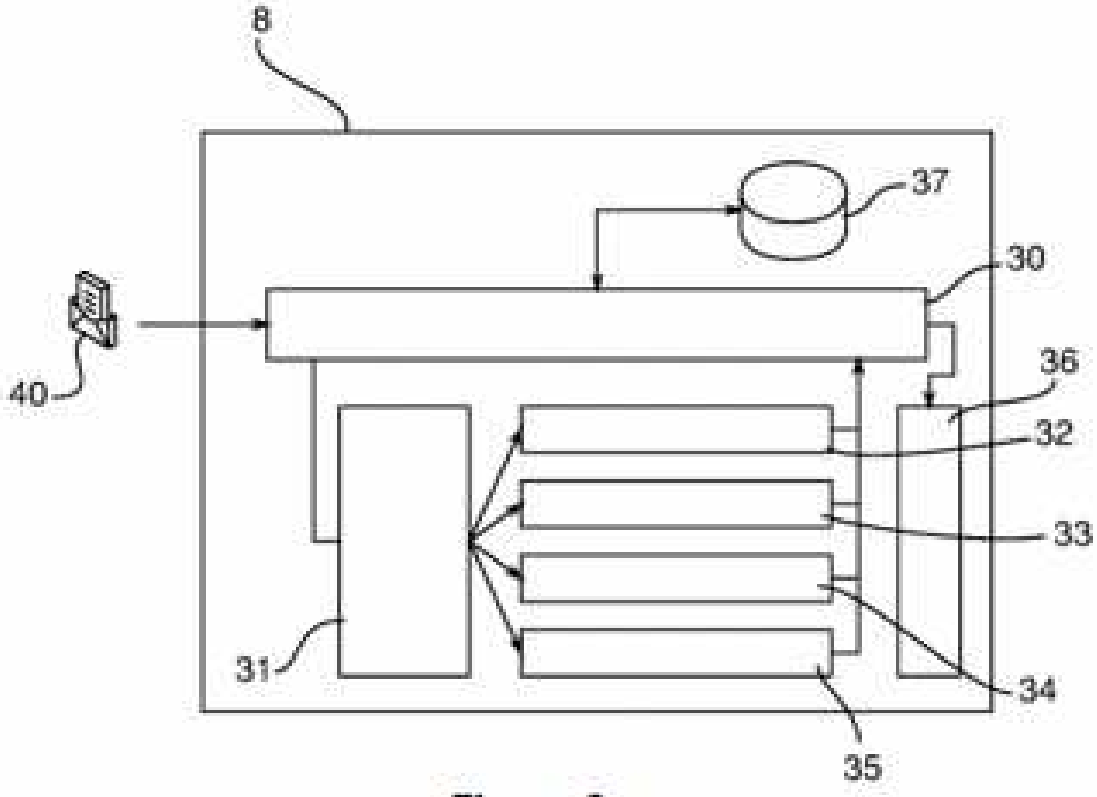

Figura 2

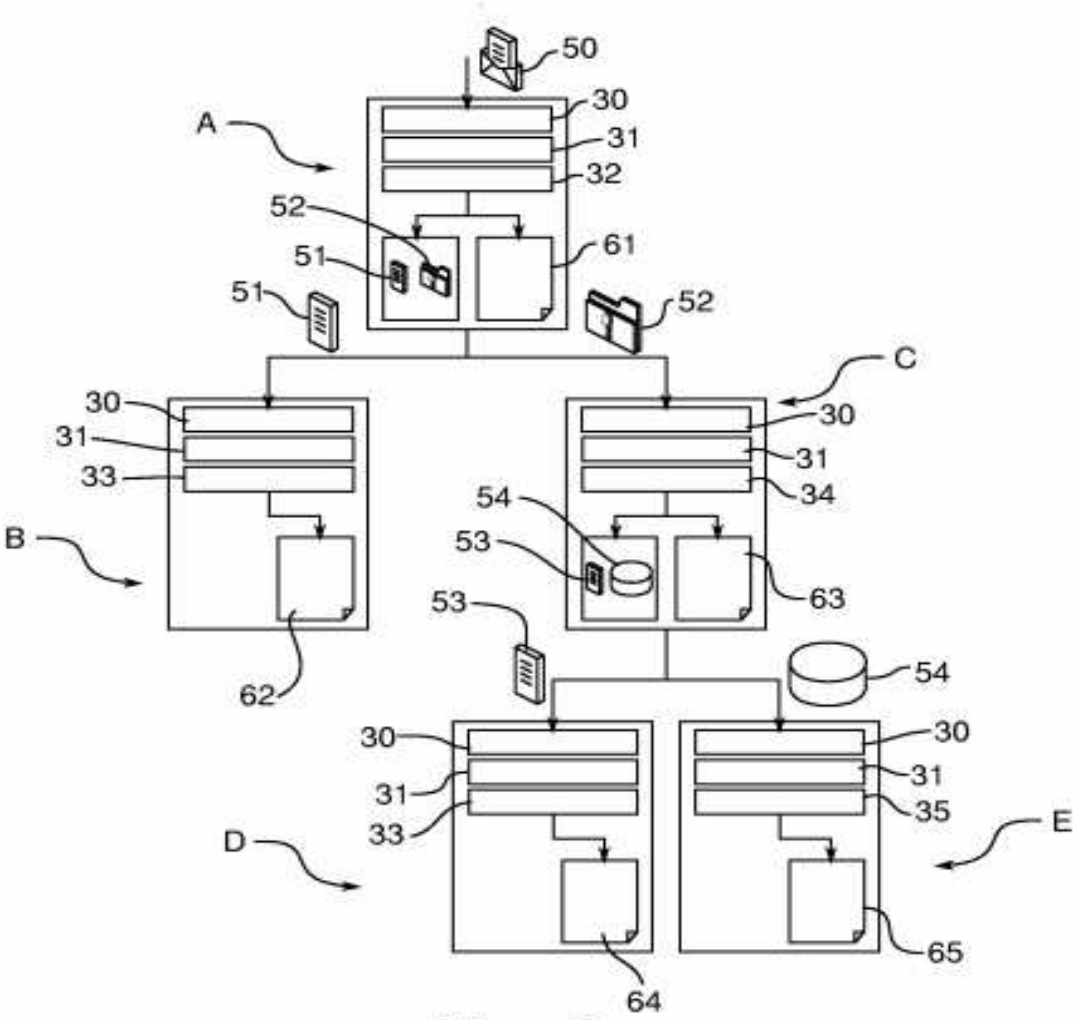

Figura 3

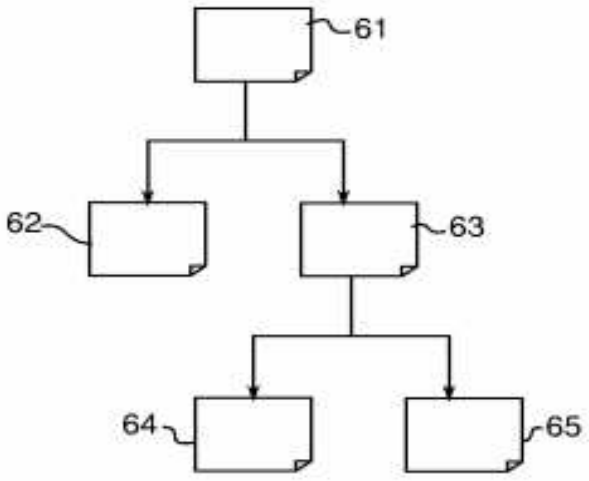

Figura 4

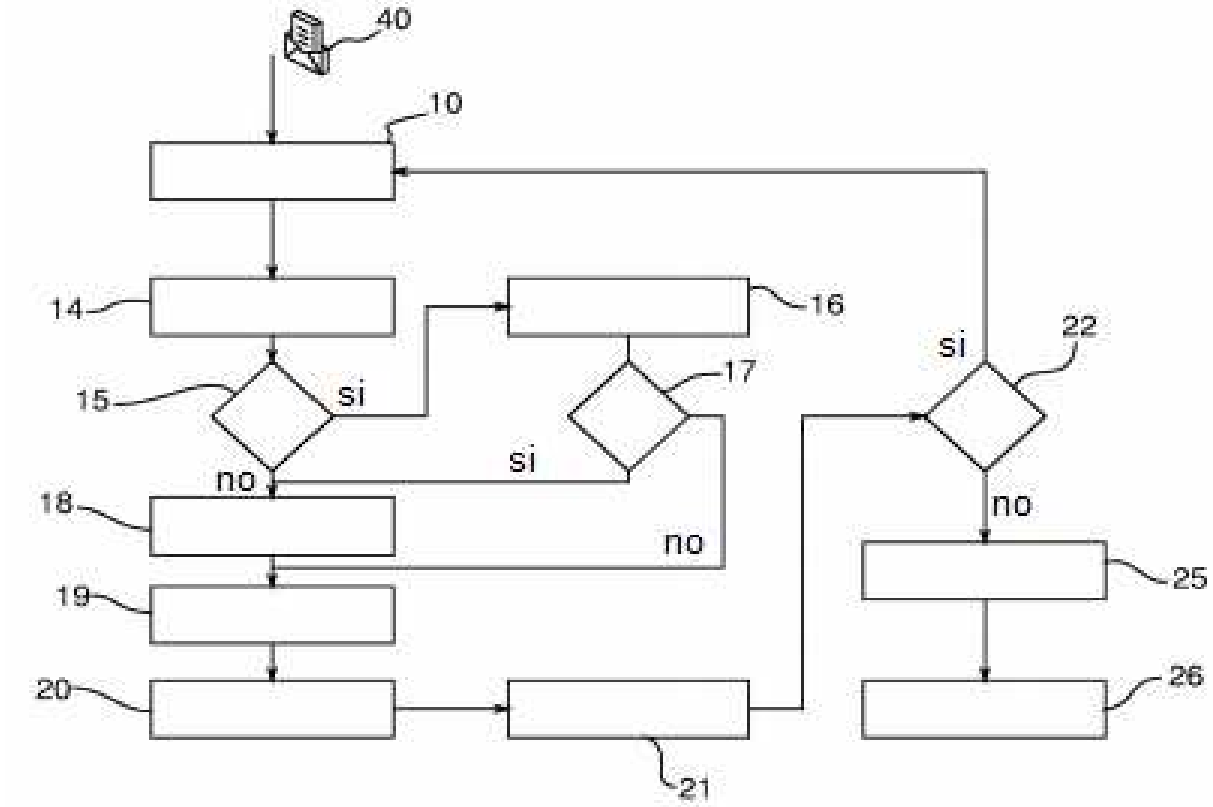

Figura 5

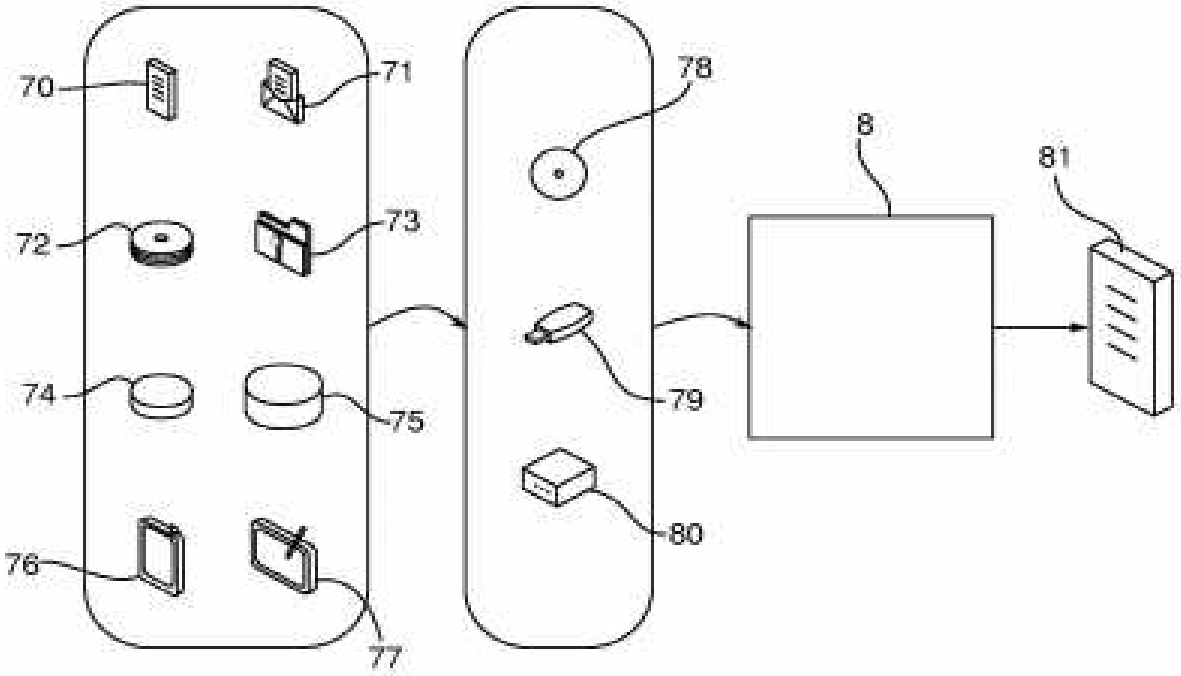

Figura 6

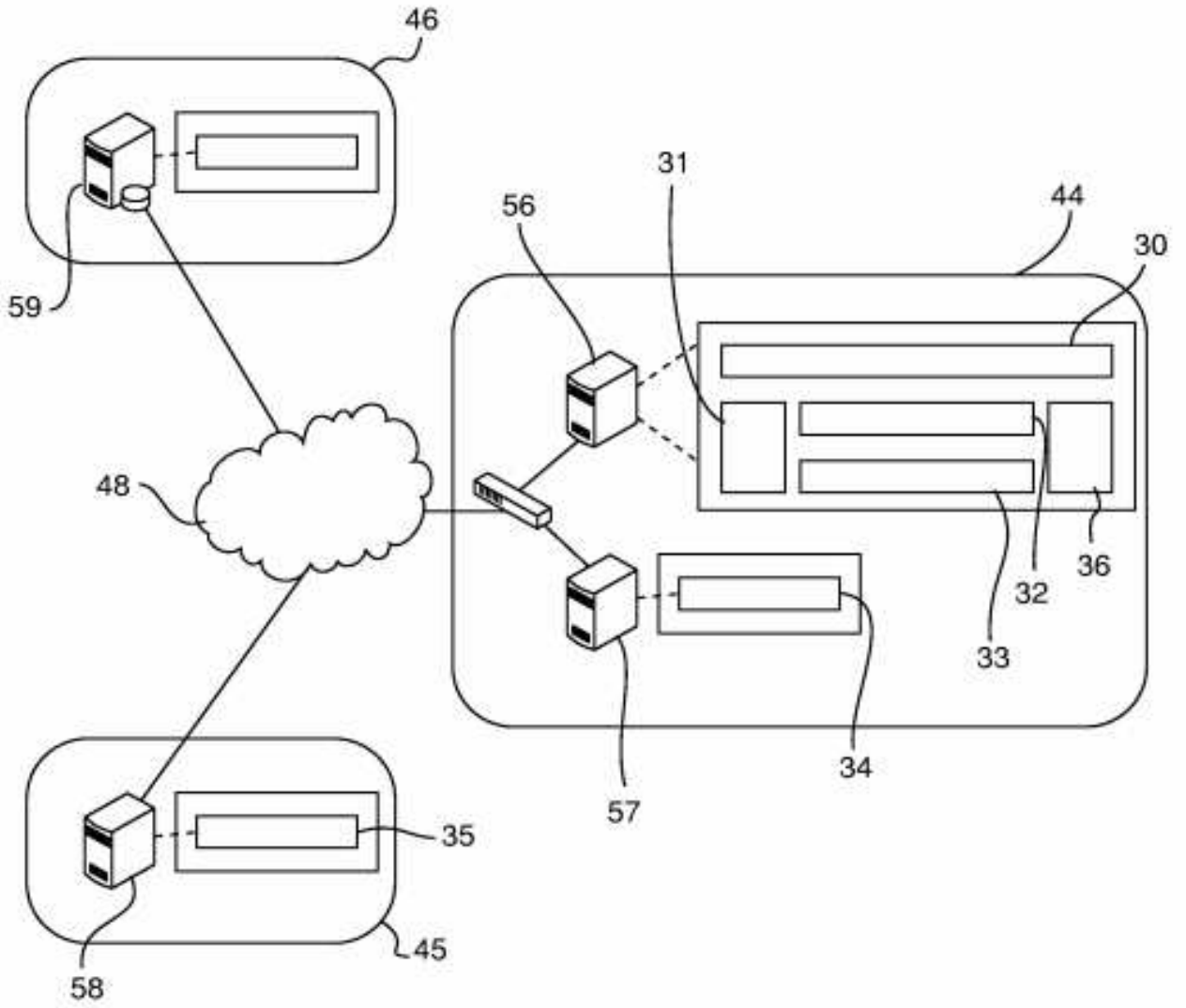

Figura 7