(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 813 070**

(51) Int. CI.:

***G06F 21/56*** (2013.01)
***G06Q 50/00*** (2012.01)
***H04L 12/26*** (2006.01)
***G06F 21/57*** (2013.01)
***G06N 99/00*** (2009.01)
***H04L 29/06*** (2006.01)
***H04L 29/08*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **03.10.2008 E 17194191 (7)**

(97) Fecha y número de publicación de la concesión europea: **17.06.2020 EP 3296910**

(54) Título: **Gestión de software intrusivo**

(30) Prioridad:

**05.10.2007 US 868321**
**03.03.2008 US 41309**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**22.03.2021**

(73) Titular/es:

**GOOGLE LLC (100.0%)**
**1600 Amphitheatre Parkway**
**Mountain View, CA 94043, US**

(72) Inventor/es:

**ZHOU, YUNKAI;**
**PROVOS, NIELS;**
**BAVOR JR., CLAYTON W.;**
**DAVIS, ERIC L.;**
**PALATUCCI, MARK;**
**NIGAM, KAMAL P.;**
**MONSON, CHRISTOPHER K.;**
**MAVROMMATIS, PANAYIOTIS y**
**NAKAUCHI, RACHEL**

(74) Agente/Representante:

**VALLEJO LÓPEZ, Juan Pedro**

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

## DESCRIPCIÓN

Gestión de software intrusivo

**Referencia cruzada a solicitudes relacionadas**

Esta solicitud reclama prioridad a la solicitud de EE. UU. Número de serie 11/868.321, presentada el 5 de octubre de 2007 y la solicitud de EE. UU. número de serie 12/041.309, presentada el 3 de marzo de 2008.

**Campo técnico**

El documento se refiere a la gestión de software intrusivo.

**Antecedentes**

Los medios interactivos (por ejemplo, Internet) tienen un gran potencial para mejorar la orientación del contenido patrocinado, por ejemplo, comerciales ("anuncios"), para audiencias receptivas. Por ejemplo, algunos sitios web ofrecen una característica de búsqueda de información basada en palabras clave ingresadas por el usuario que busca información. Esta consulta de usuario puede ser un indicador del tipo de información de interés para el usuario. Al comparar la consulta del usuario con una lista de palabras clave especificadas por un anunciante, es posible proporcionar anuncios dirigidos al usuario.

Otra forma de publicidad en línea es la distribución de anuncios, lo que permite a los anunciantes ampliar su alcance de marketing mediante la distribución de anuncios a socios adicionales. Por ejemplo, los editores en línea de terceros pueden colocar anuncios gráficos o de texto de un anunciante en propiedades web con contenido deseable para atraer clientes en línea al sitio web del anunciante.

Los anuncios, como creatividades que incluyen varias líneas de texto, imágenes o videoclips, incluyen enlaces a páginas de destino. Estas páginas de destino son páginas de sitios web de anunciantes o sitios web de editores sindicados a los que se dirige a los usuarios cuando hacen clic en los anuncios. Algunas de estas páginas de destino, sin embargo, puede incluir software intrusivo, por ejemplo, software, textos, o cualquier otra entidad que sea engañosa, instalado subrepticia y/o automáticamente. Estas entidades de software que se instalan de forma intrusiva se pueden caracterizar generalmente como "malware", un acrónimo de las palabras "malicioso" y "software". Sin embargo, no es necesario que el software realice acciones maliciosas para convertirse en malware; cualquier software que se instale de forma intrusiva puede considerarse malware, independientemente de si las acciones realizadas por el software son maliciosas. Por lo tanto, además de los caballos de Troya, virus y programas intrusos del navegador, otro software, como el software de supervisión, puede considerarse malware. El malware puede estar presente en la página de destino de forma intencionada o no. Por ejemplo, el sitio de un anunciante puede ser pirateado y el malware insertado directamente en la página de destino; un anunciante malintencionado puede insertar malware en una página de destino; un rastreador de clics puede insertar malware a través de una cadena de redireccionamientos que conducen al localizador uniforme de recursos (URL) final de la página de destino; un anunciante puede colocar anuncios o artilugios en una página poblada por terceros que insertan malware en la página de destino; etc.

Una vez que se sabe que una página de destino tiene malware, un editor de publicidad puede impedir la publicación de la página de destino. Sin embargo, un editor de publicidad, por ejemplo, Google, Inc., puede tener acceso a cientos de millones de anuncios y las correspondientes páginas de destino asociadas a los anuncios. Como podría entenderse, puede ser difícil comprobar o volver a comprobar cada página de destino en profundidad para detectar la presencia de malware. El documento de patente US2006253584 describe el suministro a un usuario de un indicador de la reputación de una entidad asociada a un elemento de contenido.

**Sumario**

En el presente documento se describen aparatos, métodos y sistemas para la detección y procesamiento de malware en contenido patrocinado. En una implementación, se identifican las características de intrusión de una página de destino asociadas a contenido patrocinado. Se genera una puntuación de característica para la página de destino basada en las características de intrusión identificadas y, si la puntuación de característica de la página de destino supera un umbral de característica, la página de destino se clasifica como una página de destino candidata. La página de destino candidata se puede proporcionar a un detector de malware para determinar si hay malware presente en la página de destino. En algunas implementaciones, se puede suspender una cuenta de patrocinador asociada a la página de destino del candidato. En algunas implementaciones, un anuncio asociado a la página de destino candidata puede suspenderse.

En otra implementación, un método incluye dividir las páginas de destino asociadas a los anuncios en páginas de destino de entrenamiento y probar las páginas de destino. Un modelo de clasificación se entrena de forma iterativa en las características de intrusión de las páginas de destino de entrenamiento y se prueba de forma iterativa en las características de intrusión de las páginas de destino de prueba. El entrenamiento y las pruebas continúan hasta que

ocurre un evento de cesación. Una asociación de ponderaciones de características y características de intrusión que se derivan del entrenamiento y las pruebas iterativas se almacenan en el modelo de clasificación en respuesta al evento de cesación.

En otra implementación, un sistema incluye un motor de puntuación que incluye instrucciones de software almacenadas en un medio legible por ordenador y ejecutables por un sistema de procesamiento. Tras la ejecución, el sistema de procesamiento identifica una página de destino asociada a contenido patrocinado e identifica las características de intrusión de la página de destino. Se genera una puntuación de característica para la página de destino en característica de las características de intrusión identificadas y, si la puntuación de característica de la página de destino supera un umbral de característica, la página de destino se clasifica como una página de destino candidata. La página de destino candidata se puede proporcionar a un detector de malware para determinar si hay malware presente en la página de destino. En algunas implementaciones, se puede suspender una cuenta de patrocinador asociada a la página de destino del candidato. En algunas implementaciones, un anuncio asociado a la página de destino candidata puede suspenderse.

Los detalles de una o más realizaciones de la materia objeto descrita en la presente memoria descriptiva se exponen en los dibujos adjuntos y en la descripción a continuación. Otras características, aspectos y ventajas del tema en cuestión se harán evidentes a partir de la descripción, los dibujos y las reivindicaciones.

**Breve descripción de los dibujos**

La figura 1 es un diagrama de bloques de un ejemplo de sistema de publicidad en línea.
La figura 2 es un diagrama de flujo de un ejemplo de subsindicación de contenido patrocinado.
La figura 3 es un diagrama de bloques de un ejemplo de sistema de procesamiento de contenido patrocinado.
La figura 4 es un diagrama de bloques de un proceso de entrenamiento de ejemplo para construir un modelo de clasificación.
La figura 5 es un diagrama de bloques de otro ejemplo de sistema de procesamiento de contenido patrocinado que utiliza el modelo de clasificación.
La figura 6 es un diagrama de bloques de otro ejemplo de sistema de procesamiento de contenido patrocinado.
La figura 7 es un diagrama de flujo de un proceso de ejemplo para identificar una página de destino candidata para la detección de intrusos.
La figura 8 es un diagrama de flujo de un proceso de ejemplo para enviar una página de destino candidata a un motor de detección de intrusos.
La figura 9 es un diagrama de flujo de un proceso de ejemplo para manejar una solicitud de apelación.
La figura 10 es un diagrama de flujo de otro proceso de ejemplo para manejar una solicitud de apelación.
La figura 11 es un diagrama de flujo de un proceso de ejemplo para generar un modelo de clasificación.

**Descripción detallada**

La figura 1 es un diagrama de bloques de un ejemplo de sistema 100 de publicidad en línea. En algunas implementaciones, uno o más anunciantes 102 pueden, directa o indirectamente, entrar, mantener y rastrear información de publicidad ("anuncio") en un sistema de gestión de publicidad 104. Aunque se hace referencia a la publicidad, otras formas de contenido, incluyendo otras formas de contenido patrocinado, pueden ser entregadas por el sistema 100. Los anuncios pueden tener forma de anuncios gráficos, como anuncios de banner, anuncios de solo texto, anuncios gráficos, anuncios de audio, anuncios de vídeo, anuncios que combinan uno o más de dichos componentes, etc. Los anuncios también pueden incluir información incrustada, como enlaces, metainformación y/o instrucciones ejecutables por una máquina. Uno o más editores 106 pueden enviar solicitudes de anuncios al sistema 104. El sistema 104 responde enviando anuncios al editor 106 solicitante para colocarlos en una o más de las propiedades web del editor (por ejemplo, sitios web y otro contenido distribuido en la red). Los anuncios pueden incluir la incorporación de enlaces a páginas de destino, por ejemplo, páginas en los sitios web de los anunciantes 102, al que se dirige un usuario cuando el usuario hace clic en un anuncio presentado en un sitio web de un editor.

Otras entidades, como los usuarios 108 y los anunciantes 102, puede proporcionar información de uso al sistema 104, tal como, por ejemplo, si se ha producido o no una conversión o un clic relacionado con un anuncio. Esta información de uso puede incluir el comportamiento del usuario medido u observado relacionado con los anuncios que se han publicado. El sistema 104 realiza transacciones financieras, como acreditar a los editores 106 y cobrar a los anunciantes 102 basándose en la información de uso.

Una red informática 110, como una red de área local (LAN), red de área amplia (WAN), Internet, o una combinación de los mismos, conecta a los anunciantes 102, el sistema 104, los editores 106 y los usuarios 108.

Un ejemplo de un editor 106 es un servidor de contenido general que recibe solicitudes de contenido (por ejemplo, artículos, hilos de discusión, música, vídeo, gráficos, resultados de la búsqueda, listados de páginas web, fuentes de información, etc.) y recupera el contenido solicitado en respuesta a la solicitud. El servidor de contenido puede enviar una solicitud de anuncios a un servidor de anuncios en el sistema 104. La solicitud de anuncio puede incluir varios anuncios deseados. La solicitud de anuncio también puede incluir información de solicitud de contenido. Esta

información puede incluir el contenido en sí (por ejemplo, página u otro documento de contenido), una categoría correspondiente al contenido o la solicitud de contenido (por ejemplo, artes, negocios, ordenadores, artes-películas, artes-música, etc.), parte o la totalidad de la solicitud de contenido, edad del contenido, tipo de contenido (por ejemplo, texto, gráficos, vídeo, audio, medios mixtos, etc.), información de ubicación geográfica, etc.

En algunas implementaciones, el servidor de contenido puede combinar el contenido solicitado con uno o más de los anuncios proporcionados por el sistema 104. Este contenido y anuncios combinados se pueden enviar al usuario 108 que solicitó el contenido para su presentación en un visor (por ejemplo, un navegador u otro sistema de visualización de contenido). El servidor de contenido puede transmitir información sobre los anuncios al servidor de anuncios, incluyendo información que describe cómo, cuándo y/o dónde se mostrarán los anuncios (por ejemplo, en HTML o JavaScript™).

Otro ejemplo de editor 106 es un servicio de búsqueda. Un servicio de búsqueda puede recibir consultas de resultados de búsqueda. En respuesta, el servicio de búsqueda puede recuperar resultados de búsqueda relevantes de un índice de documentos (por ejemplo, de un índice de páginas web). Un servicio de búsqueda a modo de ejemplo se describe en el artículo S. Brin y L. Page, "The Anatomy of a Large-Scale Hypertextual Search Engine", Séptima Conferencia Internacional World Wide Web, Brisbane, Australia y en la Patente de Estados Unidos n.º 6.285.999. Los resultados de la búsqueda pueden incluir, por ejemplo, listas de títulos de páginas web, fragmentos de texto extraídos de esas páginas web y enlaces de hipertexto a esas páginas web, y pueden agruparse en un número predeterminado de (por ejemplo, diez) resultados de búsqueda.

El servicio de búsqueda puede enviar una solicitud de anuncios al sistema 104. La solicitud puede incluir varios anuncios deseados. Este número puede depender de los resultados de la búsqueda, la cantidad de espacio de pantalla o página que ocupan los resultados de la búsqueda, el tamaño y la forma de los anuncios, etc. En algunas implementaciones, el número de anuncios deseados será de uno a diez, o de tres a cinco. La solicitud de anuncios también puede incluir la consulta (tal como se ingresó o analizó), información basada en la consulta (como información de ubicación geográfica, si la consulta provino de un afiliado y un identificador de dicho afiliado), y/o información asociada a, o basada en, los resultados de la búsqueda. Dicha información puede incluir, por ejemplo, identificadores relacionados con los resultados de la búsqueda (por ejemplo, identificadores de documento o "ID de documento"), puntuaciones relacionadas con los resultados de la búsqueda (por ejemplo, puntuaciones de recuperación de información ("IR")), fragmentos de texto extraídos de documentos identificados (por ejemplo, páginas web), texto completo de los documentos identificados, vectores de características de documentos identificados, etc. En algunas implementaciones, Las puntuaciones de IR se pueden calcular a partir de, por ejemplo, productos de puntos de vectores de características correspondientes a una consulta y un documento, puntuaciones de rango de página y/o combinaciones de puntuaciones de IR y puntuaciones de rango de página, etc.

El servicio de búsqueda puede combinar los resultados de la búsqueda con uno o más de los anuncios proporcionados por el sistema 104. Esta información combinada puede enviarse luego al usuario 108 que solicitó el contenido. Los resultados de la búsqueda se pueden mantener a diferencia de los anuncios, para no confundir al usuario entre anuncios pagados y resultados de búsqueda presuntamente neutrales. Por último, el servicio de búsqueda puede transmitir información sobre el anuncio y cuándo, dónde y/o cómo se iba a mostrar el anuncio al sistema 104.

Como se puede apreciar de lo anterior, el sistema de gestión de publicidad 104 puede servir a los editores 106, como servidores de contenido y servicios de búsqueda. El sistema 104 permite servir anuncios dirigidos a documentos servidos por servidores de contenido. Por ejemplo, una red o entre redes puede incluir un servidor de anuncios que sirva anuncios dirigidos en respuesta a las solicitudes de un servicio de búsqueda con espacios publicitarios a la venta. Suponga que la interred es la World Wide Web. El servicio de búsqueda rastrea gran parte o todo el contenido. Parte de este contenido incluirá espacios publicitarios (también denominados "inventario") disponibles. Más específicamente, uno o más servidores de contenido pueden incluir uno o más documentos. Los documentos pueden incluir páginas web, correo electrónico, contenidos, información incorporada (por ejemplo, medios integrados), metainformación e instrucciones ejecutables por máquina, y espacios publicitarios disponibles. Los anuncios insertados en los espacios publicitarios de un documento pueden variar cada vez que se sirve el documento o, alternativamente, puede tener una asociación estática con un documento determinado.

En una implementación, el sistema de gestión de anuncios 104 puede incluir un proceso de subasta para seleccionar anuncios de los anunciantes 102. A los anunciantes 102 se les puede permitir seleccionar, u ofertar, una cantidad que los anunciantes están dispuestos a pagar por cada clic en un anuncio, por ejemplo, una cantidad de coste por clic que paga un anunciante cuando, por ejemplo, un usuario hace clic en un anuncio. El coste por clic puede incluir un coste por clic máximo, por ejemplo, la cantidad máxima que el anunciante está dispuesto a pagar por cada clic en un anuncio basado en una palabra clave, por ejemplo, una palabra o palabras en una consulta. Otros tipos de oferta, sin embargo, también pueden ser usados. Según estas ofertas, los anuncios se pueden seleccionar y clasificar para su presentación.

En algunas implementaciones, el sistema 104 incluye un sistema de detección de malware en la página de anuncios que puede determinar la probabilidad de que el contenido patrocinado (por ejemplo, la página de destino de un anuncio) contiene software malicioso. El malware puede incluir cualquier tipo de contaminante informático, como adware deshonesto, virus informáticos, software espía, caballos de Troya, gusanos informáticos u otros tales como

software, malicioso, no seleccionado y/o no deseado. Concretamente, El malware puede incluir cualquier instalación de software sospechoso que ocurra automáticamente al aterrizar en una página web, como la página de destino de un anuncio. En algunas implementaciones, el sistema de detección de malware de la página de anuncios puede cubrir el caso en el que un usuario debe hacer clic en un enlace de la página (como "descarga gratuita") para que se instale el malware. Sin embargo, no es necesario que el software realice acciones maliciosas para convertirse en malware; cualquier software que se instale de forma intrusiva puede considerarse malware, independientemente de si las acciones realizadas por el software son maliciosas. Por lo tanto, además de los caballos de Troya, virus, gusanos y programas intrusos del navegador, otro software que no daña necesariamente un sistema informático, como software de monitoreo, secuestros de la página de inicio, etc., puede considerarse malware.

El sistema de detección de malware puede, por ejemplo, probar automáticamente las páginas de destino (por ejemplo, una página web definida por una URL incrustada o asociada a contenido patrocinado) para malware y tome las medidas adecuadas cuando se detecte malware. Tales acciones pueden seguir políticas predeterminadas, como suspender la cuenta de un anunciante (por ejemplo, la cuenta de un anunciante con Google Ad-Sense o AdWords), "marcar" el anuncio o los anuncios asociados a la página de destino como relacionados con malware y ayudar al usuario final a evitar los efectos negativos de dichos anuncios en el futuro. El sistema de detección de malware puede proporcionar un proceso para que un anunciante vuelva a comprobar sus anuncios "marcados" y anule la suspensión de sus cuentas. Además, si el sistema de detección de malware vuelve a comprobar las páginas de destino del anuncio o anuncios marcados de un anunciante y determina que las páginas de destino asociadas están limpias (por ejemplo, libre de malware), la cuenta del anunciante se puede restablecer (o borrar). En algunas implementaciones, los anuncios asociados a la página de destino se pueden suprimir por completo, por ejemplo, la publicación del anuncio puede excluirse.

En algunas implementaciones, el sistema de detección de malware puede tener la flexibilidad de suspender grupos de anuncios, como todos los anuncios de un grupo de anuncios o una campaña publicitaria, o todos los anuncios con una URL común. Por ejemplo, el sistema de detección de malware puede determinar que solo un subconjunto de los anuncios de un anunciante contiene malware y, por lo tanto, suspender solo esos anuncios. Tal determinación puede basarse en características comunes compartidas por la página de destino de los anuncios.

El malware se puede encontrar en la página de destino de un anuncio o en la cadena de redireccionamiento, o puede originarse de varias formas. Concretamente, la cadena de redireccionamiento puede incluir la serie de URL que incluyen el anuncio en el que se hizo clic (o URL de destino), URL de las que se crean instancias mediante textos, etc., como resultado del clic en el anuncio y la URL final de la página de destino del anuncio. En algunos casos, el sitio de un anunciante puede ser pirateado e insertado malware directamente en la página de destino. En otro ejemplo, un anunciante malintencionado puede instalar o habilitar a propósito malware en su página de destino de anuncios. En un tercer ejemplo, un rastreador de clics puede insertar malware a través de la cadena de redireccionamientos antes de que se llegue a la URL final. En un cuarto ejemplo, un anunciante puede instalar anuncios y/o artilugios en su página de destino que pueden estar llenos de terceros que insertan software malicioso. En estos y otros ejemplos de malware, cuando un usuario hace clic en un anuncio de este tipo, el ordenador del usuario puede verse comprometida por la instalación de software intrusivo.

Por ejemplo, la figura 2 es un diagrama de flujo de un ejemplo de subsindicación de contenido patrocinado. Considere un anuncio 202 en un sitio web popular 204. Por ejemplo, el sitio web o la página web en cuestión puede incluir un anuncio publicitario de una empresa de publicidad de confianza 206a. El usuario puede hacer clic en el anuncio 202, por ejemplo, en un navegador web que se ejecuta en el ordenador personal del usuario, PDA o similar. La URL de destino del anuncio 202 puede apuntar o iniciar una sola línea de texto (por ejemplo, un primer JavaScript) que hace referencia a la empresa de anuncios 206a en una primera región geográfica 208. El primer JavaScript, a su vez, puede generar un segundo JavaScript para redirigir a través de la URL de una empresa de anuncios 206b (por ejemplo, otra empresa de publicidad). El segundo JavaScript, a su vez, puede generar aún más JavaScript apuntando a otra empresa de anuncios 206c que puede, por ejemplo, utilizar la orientación geográfica para sus anuncios. El anuncio con orientación geográfica puede dar como resultado una única línea de HTML que contiene un iFrame que apunta a una empresa de anuncios 206d en otra región geográfica 210.

Al intentar recuperar el iFrame, el navegador puede ser redirigido, como a través de un encabezado de ubicación, hacia una dirección IP de un servidor programa intruso. Por ejemplo, la dirección IP puede ser, por ejemplo, de la forma xx.xx.xx.xx/<servidor programa intruso> /, como la dirección IP de un servidor de programa intruso 212. La dirección IP servida puede incluir JavaScript cifrado que puede permitir que el servidor de programa intruso 212 intente múltiples programas intrusos contra el navegador del usuario. Como resultado, se pueden instalar varios binarios de malware en el ordenador del usuario. El malware encontrado y/o instalado en este escenario puede ser desconocido para la empresa de anuncios inicial 206a. Sin embargo, cada redirección de la URL de destino (por ejemplo, empresa de anuncios 206a) a la página de destino asociada al contenido patrocinado (por ejemplo, en el servidor de programa intruso 212) puede otorgar a otra parte el control sobre el contenido de la página web original. De esta forma, la subsindicación de contenido patrocinado, caracterizado aquí por varios redireccionamientos de URL, puede llevar al usuario a un encuentro no deseado con malware.

La detección de malware puede incluir el uso de software de detección de malware disponible comercialmente u otro

software o sistemas de detección de virus. El software malicioso también puede detectarse mediante la supervisión del comportamiento del sistema, como monitorear el uso del registro y los archivos del sistema después de visitar una URL. Por ejemplo, un motor de detección de intrusiones puede monitorear el comportamiento de un navegador en una máquina virtual para determinar si hay malware presente.

La figura 3 es un diagrama de bloques de un ejemplo de sistema de procesamiento de contenido patrocinado 300. Los datos relacionados con el contenido patrocinado se pueden almacenar en una base de datos de anuncios 302. Por ejemplo, la base de datos de anuncios 302 puede contener varias formas de contenido patrocinado, como anuncios gráficos, publicidad, anuncios de solo texto, anuncios gráficos, anuncios de audio, anuncios de vídeo, anuncios que combinan uno o más de dichos componentes, etc. Los anuncios pueden estar organizados, por ejemplo, por palabra clave, campaña publicitaria, URL u otro contenido.

El sistema 300 incluye un evaluador de malware 304 que se puede utilizar para detectar malware en una página de destino asociada a un anuncio o en el propio anuncio. Por ejemplo, el evaluador de malware 304 puede evaluar inicialmente la página de destino de un anuncio para ver si es probable que incluya malware, y si se considera que es probable que la página de destino incluya malware, el evaluador de malware 304 puede enviar el anuncio a un proceso de evaluación más exhaustivo. Este proceso de evaluación de dos pasos puede generar eficiencias obtenidas mediante el uso de un proceso de evaluación de malware más completo solo en los anuncios candidatos que se considera que tienen más probabilidades de incluir malware.

La evaluación inicial realizada por el evaluador de malware 304 puede identificar características de intrusión de la página de destino del anuncio o URL en la cadena de redireccionamiento. La evaluación puede inspeccionar el anuncio en busca de características de iFrame, características de URL, características del texto, etc. y comparar dichas características con un repositorio de características que se sabe que están asociadas a páginas de destino que incluyen malware. Como resultado de la evaluación inicial de las características de la página de destino del anuncio, el evaluador de malware 304 puede generar una puntuación de característica que indique la probabilidad de que la página de destino del anuncio incluya malware. Por ejemplo, una puntuación más alta puede significar que es más probable que la página de destino del anuncio incluya software malicioso. Las páginas de destino de cualquier anuncio que tengan una puntuación de características que supere un umbral de características se pueden clasificar como candidatas para un proceso de evaluación de malware más exhaustivo. De esta forma, la identificación de características puede facilitar la heurística de reducción, permitiendo que el sistema reduzca significativamente el número de páginas de destino a un conjunto más pequeño de páginas de destino candidatas que pueden ser evaluadas posteriormente por el proceso de evaluación de malware más completo.

En algunas implementaciones, el evaluador de malware 304 puede utilizar un motor de detección de intrusos 305 que implementa un proceso de evaluación de malware más completo. Por ejemplo, el evaluador de malware 304 puede proporcionar al motor de detección de intrusos 305 una página web (por ejemplo, la página de destino de un anuncio) y recibir una puntuación de intrusión para la página web. En otras implementaciones, el evaluador de malware 304 puede incluir el motor de detección de intrusos 305.

El evaluador de malware 304 puede iniciar el proceso más completo cuando el evaluador de malware envía la página de destino candidata al motor de detección de intrusos 305. El motor de detección de intrusos 305 puede incluir, por ejemplo, una máquina virtual a través de la cual el sistema 300 puede cargar el anuncio en un navegador, navegar a la página de destino del anuncio (por ejemplo, a través de uno o más redireccionamientos de URL) y ejecutar uno o más sistemas de detección de malware, como los sistemas de detección de virus y malware informático disponibles comercialmente. Durante el proceso, la máquina virtual también puede, por ejemplo, monitorear el uso de archivos del sistema y la creación de procesos no autorizados. El motor de detección de intrusiones 305 puede generar una puntuación de intrusión y proporcionar la puntuación de intrusión al evaluador de malware 304. La puntuación de intrusión puede indicar el nivel de malware en la página de destino del anuncio. Si la puntuación de intrusión es suficientemente alta, como por encima de un umbral de intrusión predefinido, el sistema 300 puede marcar el anuncio (por ejemplo, en la base de datos de anuncios 302) como probable que contenga malware en su página de destino.

Los anuncios que están marcados en la base de datos de anuncios 302 pueden no ser servidos a los usuarios, o los anuncios pueden estar anotados de alguna manera para indicar su probabilidad de que la página de destino del anuncio incluya malware. En algunas implementaciones, las anotaciones pueden incluir una puntuación de intrusión que califique la probabilidad de que cada uno de los anuncios esté relacionado con malware. Como resultado de determinar que cualquier parte del contenido patrocinado de un anunciante (por ejemplo, la página de destino de un solo anuncio) incluye software malicioso, el sistema 300 puede marcar algunos o todos los anuncios del anunciante. El sistema 300 también puede suspender la cuenta del anunciante, como para evitar que el anunciante envíe nuevos anuncios. El sistema 300 puede realizar algunas acciones automáticamente, como cuando está claro que los anuncios están relacionados con software malicioso, por ejemplo, una puntuación de intrusión relativamente alta. Otras acciones pueden basarse en decisiones del usuario, como después de revisar los resultados de las evaluaciones de malware.

Un administrador de cuentas 306 puede recibir los resultados de las evaluaciones de malware del evaluador de malware 304. Las evaluaciones pueden incluir, por ejemplo, la información de la cuenta del patrocinador, las URL de las páginas de destino y de destino y cualquier página de la cadena de redireccionamiento. Las evaluaciones también

pueden incluir información que identifique las razones por las que el evaluador de malware 304 identificó el anuncio como relacionado con malware. Un usuario del administrador de cuentas 306 puede facilitar la disposición manual de anuncios y/o cuentas basada en la evaluación. Por ejemplo, un usuario puede suspender la cuenta de un anunciante si se descubre que una o más de las páginas de destino del anuncio del anunciante incluyen software malicioso. En otro ejemplo, un usuario puede decidir marcar uno o más anuncios en la campaña publicitaria de un anunciante.

Puede existir una interfaz 308 de representante de servicio al cliente (CSR) dentro del sistema 300 que permite a los anunciantes iniciar un proceso de apelación para anuncios marcados. Por ejemplo, un cliente (por ejemplo, un anunciante) puede tener una o más páginas de destino correspondientes al contenido patrocinado que el evaluador de malware 304 ha determinado que incluye malware. Después de limpiar dichos sitios del malware, por ejemplo, el anunciante puede iniciar una apelación del anuncio. Tal apelación puede ser, por ejemplo, en una comunicación entre la interfaz CSR 308 y el evaluador de malware 304 y/o el administrador de cuentas 306. La comunicación puede incluir, por ejemplo, el nombre del anunciante y las URL de las páginas de destino que serán reevaluadas por el evaluador de malware 304. Si la apelación de un anunciante de un anuncio marcado tiene éxito, el sistema 300 puede desmarcar el anuncio. En algunas implementaciones, el sistema 300 también puede restablecer la cuenta del anunciante como resultado de una apelación exitosa. En algunas implementaciones, cuando un anunciante apela un anuncio, el sistema 300 puede verificar todos los anuncios del anunciante y solo restablecer la cuenta del anunciante (y desmarcar el anuncio) si todos los anuncios del anunciante están limpios.

En algunas implementaciones, el sistema 300 puede incluir un modelo de cuenta de suspensión escalonada. Por ejemplo, según la probabilidad de presencia de software malicioso en una página de destino, la página de destino se puede clasificar en varias categorías o niveles, de infección de malware. Dichas categorías pueden incluir, por ejemplo, "OK" (por ejemplo, determinado que probablemente esté libre de malware), "sospechoso" (por ejemplo, puede contener malware) o "confirmado" (por ejemplo, muy probable o seguro que contenga malware). La categoría sospechosa se puede categorizar más, como con una calificación basada en una puntuación de intrusión.

En algunas implementaciones, los puntajes de detección de malware se pueden acumular con respecto a una cuenta, y una cuenta en sí puede "clasificarse" en categorías de riesgo, cada una de las cuales se maneja de manera diferente, que van desde la revisión automática, revisión manual y suspensión automática. Por ejemplo, el sistema 300 puede suspender automáticamente una cuenta cuando uno o más anuncios están en la categoría de malware "confirmado", o puede suspender una cuenta cuando el 5 % o más de los anuncios son "sospechosos", etc.

En una implementación, por ejemplo, el evaluador de malware 308 puede identificar páginas de destino asociadas a una cuenta de patrocinador que tienen puntuaciones de características que exceden un umbral de características. Las puntuaciones de las características de estas páginas de destino se pueden acumular para obtener una puntuación de la cuenta, y se puede asignar una categoría de riesgo a la cuenta del patrocinador según la puntuación de la cuenta. Se puede seleccionar uno de varios procesos de corrección de cuentas para la cuenta del patrocinador en característica de la categoría de riesgo, por ejemplo, revisión automática, revisión manual, suspensión automática, suspensión parcial de solo las páginas de destino candidatas, etc.

La detección de malware potencial puede ocurrir de forma continua, periódicamente o de forma aperiódica. Por ejemplo, el evaluador 304 de malware puede comprobar continuamente la base de datos 302 de anuncios. En otro ejemplo, la base de datos de anuncios 302 puede ser revisada periódicamente por el evaluador de malware, por ejemplo, mensual o semanal. En otro ejemplo más, cada anuncio que se añade a la base de datos de anuncios 302 puede comprobarse cuando el anuncio se añade a la base de datos de anuncios 302. También se pueden utilizar otros programas de detección.

La figura 4 es un diagrama de bloques de un ejemplo de proceso de entrenamiento 400 para construir un modelo de clasificación 402. El modelo de clasificación 402 se puede utilizar para evaluar características en una página de destino asociada al anuncio, como características que pueden indicar la probabilidad de que haya malware presente, por ejemplo, pequeños iFrames, texto ofuscado, etc. En algunas implementaciones, a las características se les puede asignar ponderaciones durante el proceso de entrenamiento. Estas evaluaciones basadas en características se pueden utilizar para reducir la cantidad de URL que se evaluarán mediante un proceso de evaluación más sólido, tal como un proceso implementado por el motor de detección de intrusos 305.

El proceso de entrenamiento 400 puede usarse para entrenar iterativamente el modelo de clasificación 402 usando características de intrusión del contenido de las páginas de destino de "entrenamiento". Al mismo tiempo, el proceso 400 puede probar iterativamente el modelo de clasificación 402 usando características de intrusión del contenido de las páginas de destino de "prueba". El proceso iterativo 400 puede continuar hasta que ocurra un evento de cese de prueba, como la determinación de que las asociaciones entre las ponderaciones de las características y las características de intrusión se están estabilizando. Tal determinación puede hacerse, por ejemplo, mediante la implementación de un modelo basado en regresión lineal.

En un ejemplo de flujo general del proceso de entrenamiento 400 para producir el modelo de clasificación 402, el procesamiento puede comenzar con el uso de los anuncios 302. La información utilizada para el proceso de formación 400 se puede identificar en las páginas de destino y las URL 404. El proceso 400 puede dividir aún más las páginas

de destino y las URL 404 en páginas de destino de "entrenamiento" y páginas de destino de "prueba". Por ejemplo, un mayor número de páginas de destino (por ejemplo, 10.000) pueden usarse como ejemplos de entrenamiento para entrenar el modelo de clasificación 402, mientras que un número menor (por ejemplo, 1.000) se puede utilizar para probar el modelo de clasificación 402.

Un motor de extracción de características 406 puede extraer características de las páginas de destino y las URL 404. Las características pueden, por ejemplo, ser indicativo de la probabilidad de que una página de destino asociada a un anuncio incluya software malicioso. Por ejemplo, una o más características relacionadas con malware (o intrusión) pueden corresponder a pequeños iFrames que pueden ser indicativos de un intento de incrustar otros documentos HTML (por ejemplo, relacionado con malware) dentro de un documento principal. Otro ejemplo de una característica de intrusión es una URL incorrecta o sospechosa, como una URL que coincida con una URL de una lista conocida de dominios infectados con malware. Un tercer ejemplo de una característica de intrusión es el lenguaje de texto sospechoso. Por ejemplo, JavaScript u otros lenguajes de secuencias de comandos pueden tener ciertas llamadas a características o elementos de lenguaje que se sabe que se utilizan para atender malware. Pueden existir varios otros tipos de características de intrusión, como la existencia de múltiples marcos, textos o iFrames que aparecen en lugares inusuales (por ejemplo, después del final del HTML), o cualquier otra característica que el proceso de entrenamiento 400 determine que con el tiempo es un marcador de probables infecciones de malware.

En algunas implementaciones, el motor de extracción de características 406 puede incluir una lista de características ponderadas. Por ejemplo, una característica de intrusión particular para una URL que es un sitio de malware conocido puede recibir una ponderación mayor que una característica de intrusión que es menos probable que esté asociada a malware. Las ponderaciones de las características pueden ajustarse con el tiempo, ya que el modelo de clasificación 402 se utiliza para clasificar las páginas de destino en cuanto a su probabilidad de incluir malware.

Las ponderaciones pueden ser acumulativas, de modo que la probabilidad general de que una página de destino incluya malware se pueda determinar agregando o combinando las ponderaciones correspondientes a las características detectadas. En algunas implementaciones, la ponderación de una característica se puede incluir en la suma de cada aparición de la característica correspondiente que se puede detectar en una página de destino. En otras implementaciones, la ponderación de una característica se puede agregar a la puntuación total una vez, independientemente del número de apariciones de la característica en el anuncio. También se pueden utilizar otras evaluaciones basadas en ponderaciones de características.

Si bien muchas características pueden tener una ponderación positiva correspondiente, otras características pueden tener una ponderación negativa. Por ejemplo, característica A, (por ejemplo, correspondiente a una posible llamada a característica relacionada con malware), puede tener una ponderación de 2,5. Al mismo tiempo, la presencia de la característica X puede anular parcialmente la probabilidad de que la característica A sea maliciosa, solicitando al sistema 400 que asigne una ponderación negativa a la característica X.

Se puede utilizar una evaluación de control 408 en la fase de formación del proceso de formación 400. La evaluación de control 408 puede incluir una evaluación humana de las páginas de destino del anuncio. Por ejemplo, la revisión humana de la página de destino de un anuncio en particular puede incluir un examen de las características del anuncio. La revisión también puede proporcionar una calificación general de la probabilidad de que la página de destino incluya malware, como extremadamente infectado con malware, semi-infectado con malware, etc.

La información generada por la evaluación de control 408 puede ser referenciada durante una fase de entrenamiento que asigna ponderaciones de características a las características extraídas por el motor de extracción de características 406. Por ejemplo, un motor de aprendizaje automático 410 puede asignar ponderaciones de características a las características para probar los resultados de la evaluación de control 408, por ejemplo, examinando características similares en otras URL (por ejemplo, URL de las páginas de destino de "prueba"). Concretamente, el motor de aprendizaje automático 410 puede usar características de las páginas de destino de prueba para refinar iterativamente las asociaciones de ponderaciones de características y características de intrusión.

Tal refinamiento se puede realizar, por ejemplo, por un modelo basado en regresión lineal. Por ejemplo, el motor 410 de aprendizaje automático puede usar páginas de destino de entrenamiento y prueba divididas en las páginas de destino y las URL 404. El motor de aprendizaje automático 410 puede, por ejemplo, ajustar las ponderaciones de las características en característica de las páginas de destino de entrenamiento y prueba para generar puntuaciones de características para las páginas de destino de prueba. Si los puntajes de las características arrojan resultados de detección de malware cercanos a los resultados de la evaluación de control, el modelo de clasificación puede considerarse entrenado. A la inversa, si las puntuaciones de las características arrojan resultados de detección de malware sustancialmente diferentes a los resultados de la evaluación de control, el motor de aprendizaje automático 410 puede reajustar las ponderaciones de las características. Por ejemplo, a lo largo de varias iteraciones, el motor 410 de aprendizaje automático puede determinar que la característica X tiene una ponderación demasiado alta y, por lo tanto, puede disminuir la ponderación de la característica asociada a la característica X.

El entrenamiento iterativo y las pruebas del modelo de clasificación 402 sobre las características de intrusión de las páginas de destino de entrenamiento y prueba pueden continuar hasta que ocurra un evento de cese de pruebas, por

ejemplo, una convergencia de los resultados de la prueba con la evaluación de control 408, o hasta que se alcance un límite de iteración. Después del evento de cesación, la asociación de ponderaciones de características y características de intrusión puede persistir en el modelo de clasificación 402.

También se pueden utilizar otros procesos para entrenar el modelo de clasificación 402.

La figura 5 es un diagrama de bloques de otro ejemplo de sistema de procesamiento de contenido patrocinado 500 que utiliza el modelo de clasificación 402. El sistema 500 incluye un motor de puntuación 502 que usa el modelo de clasificación 402 para puntuar anuncios de una base de datos de anuncios 504. Por ejemplo, utilizando las ponderaciones de características almacenadas en el modelo de clasificación 402, el motor de puntuación 502 puede puntuar características de las páginas de destino de los anuncios que procesó desde la base de datos de anuncios 504. Cualquier anuncio que se califique por encima de un umbral predefinido puede identificarse como URL candidatas 506.

Las URL candidatas 506 pueden incluir información asociada al anuncio que puede ser necesaria para un examen exhaustivo por parte de un evaluador 508 de malware. Por ejemplo, las URL candidatas 506 pueden incluir la URL del anuncio y la información de la cuenta del anunciante que proporciona el contenido patrocinado. Se puede utilizar la URL del anuncio (o algún otro identificador del anuncio), por ejemplo, para identificar información adicional para el anuncio en la base de datos de anuncios 504 que puede ser necesaria para el evaluador de malware 506. El evaluador de malware 506 también puede utilizar la URL del anuncio para simular la selección del anuncio en el navegador de un usuario. Por ejemplo, el evaluador de malware 506 puede proporcionar la página de inicio al motor de detección de intrusos 305 que puede cargar la URL en una máquina virtual que incluye software de detección de virus y que monitorea el uso de archivos del sistema y la creación de procesos no autorizados.

En algunas implementaciones, cuando el evaluador de malware 508 determina que una URL candidata está infectada con malware (por ejemplo, basado en una alta puntuación de intrusión recibida del motor de detección de intrusiones 305), a otras URL candidatas 506 relacionadas se les puede asignar una puntuación similar. Por ejemplo, puede estar claro que las URL candidatas 506 que tienen el mismo nombre de dominio también tienen la misma probabilidad de estar infectadas. Dicha determinación puede basarse parcialmente en factores geográficos, por ejemplo, si el dominio es de Rusia, China o cualquier otro país que se sepa estadísticamente por tener tasas más altas de dominios infectados.

La figura 6 es un diagrama de bloques de otro ejemplo de sistema 600 de procesamiento de contenido patrocinado. El sistema 600 incluye un sistema de detección de malware publicitario 602 que puede detectar la probabilidad de malware asociado a anuncios en la base de datos 604 de anuncios. El sistema de detección de malware publicitario 602 también puede facilitar un proceso de apelación mediante el cual los anunciantes pueden solicitar la reevaluación de los anuncios que se han marcado como asociados a malware. En algunas implementaciones, el sistema de detección de malware publicitario 602 puede comprender instrucciones de software que se ejecutan continuamente, por ejemplo, utilizar información de los anuncios 604 para identificar malware en las páginas de destino de los anuncios de forma continua. Por ejemplo, el proceso de identificación puede implicar el seguimiento de los comportamientos del sistema, como monitorear el uso del registro y los archivos del sistema después de que un usuario visita una URL. En otro ejemplo, el proceso de identificación puede implicar un examen programado de las URL de la página de destino de cada anunciante, o puede incluir una o las URL de la página de destino individuales que se considera probable que contengan malware. Dichos procesos pueden monitorear características particulares de la página de destino del anuncio que pueden indicar la probabilidad de que haya malware presente. En otras implementaciones, uno o más componentes del sistema de detección de malware publicitario 602 pueden usarse en un proceso de fuerza bruta para rastrear la base de datos publicitaria 604 para examinar las URL de la página de destino en busca de posibles asociaciones con malware. La determinación de que los anuncios tienen software malicioso asociado puede basarse en anuncios individuales, grupos de anuncios, palabra clave, una o más URL relacionadas, grupos de anuncios dentro de la cuenta de un anunciante, o alguna combinación de los mismos.

En una implementación, la información de la base de datos de anuncios 604 se puede proporcionar a una base de datos de características de criterios de grupo de anuncios 606 y una base de datos de características de URL 608. Por ejemplo, la información en las bases de datos 606 y 608 puede incluir información pertinente de los anuncios, como las URL, palabras clave de los anuncios, los nombres de los anunciantes asociados, la información de la cuenta de los anunciantes y similares. El suministro de esta información puede, por ejemplo, obviar la necesidad de almacenar imágenes, vídeo, audio u otra información relacionada con los anuncios. Tener la información del anuncio local para los criterios del grupo de anuncios presenta la base de datos 606 y la URL presenta la base de datos 608 también puede proporcionar la ventaja de organizar y/o indexar los datos para un uso más eficiente dentro del sistema de detección de malware publicitario 602. Dicha información almacenada en las bases de datos 606 y 608 puede ser suficiente para determinar asociaciones basadas en características de malware con un anuncio en particular sin tener que rastrear la página de destino del anuncio. En otra implementación, el sistema 600 puede rastrear las páginas de destino de los anuncios y utilizar la información disponible en las páginas de destino en lugar de (o además de) utilizar las bases de datos 606 y 608.

La base de datos de características de criterios de grupo de anuncios 606 puede contener información para uno o más

grupos de anuncios para un anunciante, palabras clave asociadas a los anuncios, información de categorización de productos, información de la cuenta del anunciante y otra información relacionada con la publicidad utilizada por el sistema de detección de malware publicitario 602. La base de datos de características de URL 608 puede contener la URL (por ejemplo, la URL de la página de destino) de cada anuncio individual, el nombre del anunciante y cualquier otra información o índices que puedan permitir el acceso a los datos asociados en la base de datos de características de criterios del grupo de anuncios 606.

El sistema de detección de malware publicitario 602 incluye un muestreador 610 que puede servir como primer filtro para identificar anuncios que pueden contener malware. Concretamente, el muestreador 610 puede identificar anuncios para los que se recomienda la detección de malware. El proceso de identificación puede utilizar información relacionada con anuncios almacenada en la base de datos de características de criterios de grupo de anuncios 606 y la base de datos de características de URL 608. Por ejemplo, el muestreador 610 puede buscar en un anuncio cualquiera de un conjunto de características de contenido publicitario determinadas identificadas en la base de datos 606 de características de criterios de grupo de anuncios.

El muestreador 610 puede utilizar el modelo de clasificación 402 descrito en referencia a la figura 4. Por ejemplo, el muestreador 610 puede comparar características de anuncios que procesa de las bases de datos 606 y 608 con características ponderadas representadas en el modelo de clasificación 402. Según las ponderaciones de características acumuladas o combinadas de una o más características en la página de destino de un anuncio, el muestreador 610 puede determinar que la página de destino del anuncio excede un umbral de características. Como tal, la URL del anuncio puede considerarse una URL candidata para una detección de malware más completa.

En algunas implementaciones, la base de datos de características de URL 608 puede incluir información de ofuscación que un detector de ofuscación en el muestreador 610 puede usar para examinar páginas HTML en busca de textos ofuscados, como textos escritos en JavaScript, VBScript y similares. Tales textos pueden contener a menudo una colección aparentemente galimatizada de caracteres que, cuando el usuario hace clic en el anuncio, se reescribirá a sí mismo en otra cadena de URL, luego de nuevo a otra cadena, y así sucesivamente hasta que el código de explotación se escriba o descargue en un dispositivo informático. Este nivel o la reescritura que puede ocurrir a lo largo de la cadena de redireccionamiento puede dificultar la identificación del código HTML malicioso.

En algunas implementaciones, la base de datos 608 de características de URL puede incluir información de ubicación geográfica. Dicha información se puede utilizar, por ejemplo, para categorizar geográficamente las URL utilizadas para los anuncios. A menudo, se puede proporcionar malware desde ciertos países y, por lo tanto, analizar la información de ubicación de los enlaces incrustados puede ayudar a identificar un sitio de malware potencial. Por ejemplo, un dominio US-.com tiene un iFrame a un sitio en una ubicación geográficamente remota conocida por una alta incidencia de malware puede proporcionar una fuerte señal de malware potencial.

Cuando el muestreador 610 ha identificado anuncios candidatos que se sospecha que contienen malware, el muestreador 610 puede enviar las URL candidatas y la información de la cuenta a un centro de malware 612. El concentrador de malware 612 puede servir como una interfaz central para recibir anuncios que se verifican más a fondo en busca de malware y, como se describirá a continuación, para recibir apelaciones de anuncios marcados como que contienen software malicioso. Para cualquier anuncio que el muestreador 610 solicite el centro de malware 612 para revisar, el centro de malware 612 puede actualizar una base de datos de estado 614 con la URL del anuncio y la información de seguimiento correspondiente, como la información de la cuenta del anunciante asociado al anuncio. En algunas implementaciones, la información almacenada en la base de datos de estado 614 puede incluir información que el muestreador 614 consideró el motivo de la detección de malware más avanzada. En algunas implementaciones, los motivos pueden usarse para agrupar estados de anuncios en la base de datos de estado 614 con el fin de agruparlos para un procesamiento más eficiente.

En algunas implementaciones, el muestreador 610 también puede evaluar la antigüedad relativa de dominios y URL para (o enlaces a) esos dominios. La antigüedad de un dominio se puede utilizar para identificar sitios sospechosos de malware, ya que el malware a menudo se distribuye desde nuevos sitios. Por ejemplo, se crean constantemente nuevos sitios de distribución y pueden existir solo durante varias semanas antes de que se eliminen. Para determinar la edad de los dominios, el muestreador 610 puede usar listas públicas o privadas de nombres de dominio recientemente activados que pueden estar disponibles, por ejemplo, de las cámaras de compensación del registro de dominio.

En algunas implementaciones, el concentrador de malware 612 puede servir como una interfaz central para recibir solicitudes de detección de malware publicitario de otros sistemas de gestión de publicidad 104. Por ejemplo, mientras que el sistema de detección de malware publicitario 602 puede ser un componente del sistema Ad-Sense de Google, los sistemas de gestión de publicidad de la competencia 104 pueden pagar una tarifa para que los anuncios bajo su control sean examinados en busca de malware. Como tal, el sistema de detección de malware publicitario 602 puede servir como cámara de compensación para la detección de malware para varios sistemas de gestión de publicidad 104.

Un detector de malware 616 puede procesar los anuncios representados por entradas en la base de datos de estado

614. Por ejemplo, el detector de malware 616 puede procesar uno o más anuncios, utilizando la URL y el ID de cuenta de cada anuncio. Si se necesita información adicional para un anuncio (por ejemplo, que no está almacenado en la base de datos de estado 614), el detector de malware 616 puede extraer información adicional para el anuncio de la base de datos de anuncios 604. Dicha información puede incluir, por ejemplo, información de cuenta, o partes del anuncio en sí que pueden no haber sido proporcionadas al muestreador 610 para la selección inicial del primer filtro.

El detector de malware 616 puede entonces hacer que se lleve a cabo una exploración más completa. Además, el detector de malware 616 puede enviar la URL a un motor de detección de intrusos, por ejemplo, motor de detección de intrusos 305, que realiza una evaluación de malware más detallada, como examinar de cerca la URL de "destino", URL "final", URL en la cadena de redireccionamiento y la página de destino del anuncio (por ejemplo, identificado por la URL final).

El detector de malware 616 puede recibir una puntuación de intrusión para la URL de destino del motor de detección de intrusiones 305. Para cada página de destino con una puntuación de intrusión por encima de un umbral predefinido, el sistema de detección de malware publicitario 602 puede realizar una o más acciones predefinidas, como marcar automáticamente los anuncios como relacionados con malware y suspender la cuenta de un anunciante, o proporcionar dicha información a un usuario que puede suspender manualmente las cuentas de anunciantes maliciosos y/o bloquear sus anuncios. El umbral de puntuación de intrusión que puede aplicar el detector de malware 616 puede establecerse de forma conservadora alta para no producir falsos positivos significativos.

En algunas implementaciones, se puede implementar o integrar un motor de detección de intrusos con el detector de malware 305.

Las acciones que ocurren cuando se detecta malware publicitario pueden seguir una política predefinida. Por ejemplo, la cuenta del anunciante puede suspenderse manualmente y el anunciante puede ser notificado. El anuncio asociado con software malicioso se puede marcar para evitar mostrar el anuncio a los usuarios. El detector de malware 616 puede proporcionar información sobre anuncios marcados, cuentas suspendidas y similares a la base de datos de estado 614. En algunas implementaciones, se puede ejecutar un proceso de forma regular para utilizar dicha información en la base de datos de estado 614 para actualizar la base de datos de anuncios 604.

Una interfaz de cliente 618 puede servir como interfaz gráfica de usuario (GUI) para un usuario, por ejemplo, un representante de servicio al cliente, para revisar los resultados de las detecciones de malware publicitario realizadas por el detector de malware 616. Por ejemplo, los resultados pueden enumerar instancias de páginas de destino específicas y las razones por las que se determina que contienen malware. Las instancias pueden agruparse o clasificarse de diversas formas, como por cuenta de anunciante, URL, etc.

Un proceso de apelación puede permitir que el sistema de detección de malware publicitario 602 vuelva a verificar el anuncio que tiene un anuncio marcado. Por ejemplo, el anunciante puede eliminar la URL final del anuncio o todas las URL de la cadena de redireccionamiento, de malware después de recibir una notificación de que la página de destino del anuncio contiene malware y, a continuación, póngase en contacto con un representante de servicio al cliente como parte del proceso de apelación. El representante de servicio al cliente puede utilizar la interfaz del cliente 618 para enviar solicitudes de apelación al centro de malware 612. Cada solicitud de apelación puede representar uno o más anuncios para los que el anunciante solicita al sistema de detección de malware publicitario 602 que vuelva a evaluar el contenido de malware. Por ejemplo, si el sistema de detección de malware publicitario 602 ha marcado previamente el anuncio del anunciante como relacionado con malware, y el anunciante ha limpiado las URL de la página de destino asociadas al anuncio, la solicitud puede ser reevaluar ese anuncio específico.

El centro de malware 612 puede recibir la solicitud de apelación y actualizar una base de datos de apelaciones 620. Concretamente, las solicitudes de apelación pendientes y completadas pueden almacenarse en la base de datos de apelaciones 620. La información para cada anuncio almacenado en la base de datos de apelaciones 620 puede incluir, por ejemplo, el nombre del anunciante, la información de la cuenta del anunciante, las URL asociadas a las páginas de destino del anuncio y las URL en la cadena de redireccionamiento, y cualquier otra información que pueda usarse para procesar la apelación.

Para procesar como apelación, el detector de malware 616 puede utilizar un proceso similar al proceso descrito anteriormente para evaluar inicialmente la página de destino de un anuncio en busca de malware. En algunas implementaciones, el proceso de apelación también puede incluir automáticamente la reevaluación de las páginas de destino de todos los anuncios para el anunciante, todos los anuncios de un grupo de anuncios, o cualquier otro grupo similar que pueda usarse para buscar otros anuncios relacionados con software malicioso que el anunciante pueda tener.

Al procesar una apelación, el detector de malware 616 puede usar información para cada anuncio que se almacena en la base de datos 620 de apelaciones. El detector de malware 616 puede utilizar un proceso similar al descrito anteriormente para evaluar la página de destino de un anuncio, generar una puntuación de intrusión y aplicar un umbral para determinar si es probable que la página de destino del anuncio se haya eliminado de malware. Los resultados de las reevaluaciones de la página de destino de los anuncios se pueden almacenar en la base de datos de apelaciones

620. En algunas implementaciones, se puede ejecutar un proceso de forma regular para usar dicha información en la base de datos de apelaciones 620 para actualizar la base de datos de anuncios 604.

En un escenario de ejemplo de una apelación de malware, un cliente puede recibir una notificación, como un correo electrónico, indicando que la cuenta del cliente ha sido suspendida por malware. La notificación puede incluir detalles de dónde se encontró el malware (por ejemplo, URL de destino, información de la cuenta, etc.). La notificación también puede proporcionar consejos sobre cómo eliminar el malware y puede dirigir seguimientos, por ejemplo, con representantes de soporte al cliente de malware. Luego, el cliente puede limpiar su página de destino y/u otras URL asociadas al malware, y usar la interfaz del cliente 618 para iniciar el proceso de apelación. Si el detector de malware 616 determina que la página de destino del anuncio ahora está libre de malware, el cliente puede recibir una notificación de que la apelación fue exitosa y que la cuenta ahora se restableció. Sin embargo, si el detector de malware 616 determina que la página de destino del anuncio aún incluye malware, el cliente puede recibir una notificación de que se rechazó la apelación, incluida información detallada sobre el malware detectado. En algunas implementaciones, el proceso de notificación para las detecciones de malware y los resultados de las apelaciones se puede realizar en grupos, por ejemplo, como no abrumar al cliente con una gran cantidad de notificaciones por correo electrónico.

En algunas implementaciones, los anuncios asociados a una cuenta de patrocinador se excluyen por anuncio, por ejemplo, solo los anuncios que tengan una puntuación de intrusión que supere un umbral de intrusión no podrán publicarse. Tras una apelación, la página de destino candidata se vuelve a enviar al motor de detección de intrusos y el motor de detección de intrusiones recibe otra puntuación de intrusión para la página de destino candidata. El anuncio permanece suspendido o se restablece según la puntuación de intrusión recibida durante la apelación.

En algunas implementaciones, los anuncios asociados a una cuenta de patrocinador se excluyen por cuenta si se determina que algún anuncio en la cuenta tiene una puntuación de intrusión que excede el umbral de intrusión. Tras una apelación, todos los anuncios de la cuenta del patrocinador se identifican y se comprueban en busca de malware. La cuenta permanece suspendida si se determina que cualquiera de las páginas de destino asociadas a la cuenta del patrocinador tiene una puntuación de intrusión que excede el umbral de intrusión.

La figura 7 es un diagrama de flujo de un proceso de ejemplo 700 para identificar una página de destino candidata para la detección de intrusos. Por ejemplo, el proceso 700 puede implementarse usando instrucciones de software almacenadas en un medio legible por ordenador y ejecutadas por un sistema de procesamiento. Las páginas de destino candidatas identificadas por el proceso 700 pueden ser identificadas por el motor de puntuación 502 (véase la figura 5) y utilizadas por el detector 508 de malware. Estas páginas candidatas pueden ser un número de páginas significativamente menor que la colección total de páginas de destino que utiliza el proceso 700 para identificar las páginas de destino candidatas.

La etapa 702 identifica una página de destino asociada a contenido patrocinado. Por ejemplo, la página de destino puede ser la página de destino de un anuncio que un usuario puede ver en un navegador web después de hacer clic en un anuncio. En general, el contexto de "páginas de destino" puede incluir cualquier contenido o encabezados, incluidas las redirecciones que puede encontrar o ver el usuario de un navegador web después de hacer clic en un anuncio.

La etapa 704 identifica las características de intrusión de la página de destino. Por ejemplo, el proceso 700 puede usar el motor de puntuación 502 en la figura 5 para identificar las características de la página de destino, como una o más características de iFrame, una o más características de URL y/o una o más características de texto. En otro ejemplo, el muestreador 610 descrito en referencia a la figura 6 puede identificar características de la base de datos de características de criterios de grupo de anuncios 606 y la base de datos de características de URL 608.

La etapa 706 genera una puntuación de características para la página de destino en característica de las características de intrusión identificadas. Por ejemplo, el motor de puntuación 502 (véase la figura 5) puede generar una puntuación de características para la página de destino de un anuncio a partir de la base de datos de anuncios 504 utilizando puntuaciones ponderadas del modelo de clasificación 402. En otro ejemplo, el muestreador 610 puede generar un puntaje de características basado en características de la página de inicio del anuncio usada de la base de datos de características 606 y la base de datos de características de URL 608.

La etapa 708 determina si la puntuación de la característica de la página de destino supera un umbral de característica. Por ejemplo, el motor de puntuación 502 puede determinar si la puntuación de característica generada para la página de destino del anuncio supera un umbral de característica predefinido. En otro ejemplo, el muestreador 610 puede determinar si la puntuación de características generada para el anuncio excede un umbral de características predefinido. Los umbrales de características pueden ser numéricos, por ejemplo. En algunas implementaciones, pueden existir diferentes umbrales de características para diferentes niveles de anunciantes, como niveles basados en el riesgo de malware. Por ejemplo, los anunciantes que se sabe que tienen pocos o ningún anuncio relacionado con malware pueden tener un umbral más alto; o los anunciantes pueden solicitar que se establezca un umbral más bajo para identificar anuncios potencialmente infectados más fácilmente para protegerse contra una mala experiencia del cliente; etc.

La etapa 710 clasifica la página de destino como una página de destino candidata si la puntuación de la característica para la página de destino supera el umbral de la característica. Por ejemplo, si el motor de puntuación 502 determina que la puntuación de característica generada para la página de destino del anuncio supera el umbral de característica predefinido, el motor de puntuación 502 puede generar los correspondientes URL candidatos 506. En otro ejemplo, si el muestreador 610 determina que la puntuación de característica generada para la página de destino del anuncio supera el umbral de característica predefinido, el muestreador 610 puede proporcionar la URL candidata al centro de malware 612.

La figura 8 es un diagrama de flujo de un proceso de ejemplo 800 para enviar una página de destino candidata a un motor de detección de intrusos. Por ejemplo, la página de destino candidata enviada por el proceso 800 puede ser identificada por el proceso 700. El proceso 800 puede implementarse usando instrucciones de software almacenadas en un medio legible por ordenador y ejecutadas por un sistema de procesamiento.

La etapa 802 envía la página de destino candidata a un motor de detección de intrusos. Por ejemplo, haciendo referencia a la figura 5, el sistema 500 puede proporcionar URL candidatas 506 al evaluador de malware 508, que puede proporcionarlos al motor de detección de intrusos 305. En otro ejemplo, las URL candidatas representadas en la base de datos de estado 614 pueden proporcionarse al detector de malware 616 (véase la figura 6).

La etapa 804 recibe una puntuación de intrusión para la página de destino candidata del motor de detección de intrusiones. Por ejemplo, haciendo referencia a la figura 6, la base de datos de estado 614 puede recibir la puntuación de intrusión del detector de malware 616. La puntuación de intrusión puede corresponder a la página de destino del anuncio que el detector de malware 616 procesó desde la base de datos de estado 614.

La etapa 806 excluye la publicación del anuncio asociado a la página de destino candidata si la puntuación de intrusión supera un umbral de intrusión. Por ejemplo, si la puntuación de intrusión de la página de destino del anuncio procesada por el detector de malware 616 supera un umbral de intrusión, el detector de malware 616 puede actualizar la base de datos de estado 614 con información de que el anuncio correspondiente debe ser marcado. Tal información en la base de datos de estado 614 se puede usar más tarde para actualizar la base de datos de anuncios 604. Los anuncios que están marcados en la base de datos de anuncios 604 pueden excluirse de varias formas, por ejemplo, marcando los anuncios publicados (por ejemplo, en el navegador de un usuario) por contener malware potencial o por evitar que se publiquen los anuncios. La exclusión en la etapa 806 también puede incluir la suspensión de la cuenta del anunciante, o en un sistema de cuentas por niveles, elevar la calificación de riesgo de malware para el anunciante.

La figura 9 es un diagrama de flujo de un proceso 900 de ejemplo para gestionar una solicitud de apelación. Por ejemplo, la solicitud de apelación puede realizarla un anunciante después de que uno o más de los anuncios del anunciante hayan sido excluidos, como a través del proceso 800. El proceso 900 puede implementarse usando instrucciones de software almacenadas en un medio legible por ordenador y ejecutadas por un sistema de procesamiento.

La etapa 902 recibe una solicitud de apelación para la cuenta del patrocinador. Por ejemplo, la apelación puede originarse en el interfaz del cliente 618 de la figura 6. La solicitud de apelación se puede recibir, por ejemplo, por el centro de malware 612 que puede almacenar información sobre la solicitud de apelación en la base de datos de apelaciones 620.

La etapa 904 vuelve a enviar la página de destino candidata a un motor de detección de intrusos. Por ejemplo, el sistema 600 puede usar información correspondiente a la apelación que está almacenada en la base de datos de apelaciones 620 para volver a enviar la página de destino candidata al detector de malware 616, que puede incluir o comunicarse con un motor de detección de intrusos.

La etapa 906 recibe otra puntuación de intrusión de la página de destino candidata del motor de detección de intrusos. Por ejemplo, como resultado de la remisión de la etapa 904, se puede generar y recibir una nueva puntuación de intrusión para el anuncio. En general, esta puntuación de intrusión puede ser más baja para la página de destino del anuncio, por ejemplo, si el anunciante que apeló el anuncio eliminó el software malicioso de la página de destino del anuncio o proporcionó una nueva página de destino para el anuncio, por ejemplo, contratando a un nuevo editor.

La etapa 908 determina si la puntuación de intrusión supera un umbral de intrusión. Si la puntuación de intrusión supera el umbral de intrusión, la etapa 910 excluye la publicación del anuncio asociado a la página de destino candidata si otra puntuación de intrusión supera el umbral de intrusión. Por ejemplo, si la nueva puntuación de intrusión de la página de destino del anuncio procesada por el detector de malware 616 supera el umbral de intrusión, el detector de malware 616 puede actualizar la base de datos de apelaciones 620 con información de que el anuncio correspondiente todavía está asociado a malware.

Si la puntuación de intrusión no supera el umbral de intrusión, entonces la etapa 912 permite la publicación del anuncio asociado a la página de destino candidata si otra puntuación de intrusión no excede el umbral de intrusión. Por ejemplo, si la nueva puntuación de intrusión de la página de destino del anuncio procesada por el detector de malware 616 no supera el umbral de intrusión, el detector de malware 616 puede actualizar la base de datos de apelaciones 620 con

información de que el anuncio correspondiente ahora está limpio y puede ser servido sin restricción.

La figura 10 es un diagrama de flujo de otro proceso de ejemplo 1000 para manejar una solicitud de apelación. Por ejemplo, la solicitud de apelación puede realizarla un anunciante después de que uno o más de los anuncios del anunciante hayan sido excluidos, como a través del proceso 800. El proceso 1000 puede implementarse usando instrucciones de software almacenadas en un medio legible por ordenador y ejecutadas por un sistema de procesamiento.

La etapa 1002 identifica una cuenta de patrocinador asociada al anuncio, la cuenta del patrocinador que incluye anuncios adicionales. Por ejemplo, haciendo referencia a la figura 6, la cuenta del patrocinador puede estar asociada a un anuncio que el detector de malware 616 determina que la página de destino del anuncio está infectada con malware. La cuenta puede estar identificada, por ejemplo, en los criterios del grupo de anuncios presenta la base de datos 606 para la base de datos de características URL 608.

La etapa 1004 excluye la publicación de anuncios adicionales asociados a la cuenta del patrocinador si la puntuación de intrusión de la página de destino candidata supera el umbral de intrusión. Por ejemplo, utilizando la información de la cuenta del patrocinador identificada en la etapa 1002, el detector de malware 616 puede impedir la publicación de anuncios adicionales del anunciante. En particular, bajo la política comercial representada por el proceso 1000, una vez que se determina que un anuncio de un anunciante está asociado a software malicioso, ese anuncio y todos los demás del anunciante se pueden marcar (y excluir).

La etapa 1006 recibe una solicitud de apelación para la cuenta del patrocinador. Por ejemplo, la apelación puede originarse en un usuario que ejecuta el interfaz del cliente 618 (véase la figura 6). La solicitud de apelación se puede recibir, por ejemplo, por el centro de malware 612 que puede almacenar información sobre la solicitud de apelación en la base de datos de apelaciones 620.

La etapa 1008 envía la página de destino candidata y las páginas de destino adicionales asociadas a los anuncios adicionales al motor de detección de intrusos. Por ejemplo, el sistema 600 puede usar información correspondiente a la apelación que está almacenada en la base de datos de apelaciones 620 para enviar todas las páginas de destino candidatas del anunciante al detector de malware 616, que puede incluir un motor de detección de intrusos o proporcionar la información de la página de destino a un motor de detección de intrusos. Como parte del proceso, la información de la cuenta correspondiente a la página de destino candidata puede usarse para identificar otros anuncios en la base de datos de anuncios 604 que corresponden a la cuenta del anunciante. Concretamente, las páginas de destino candidatas pueden incluir la página de destino candidata original y páginas de destino adicionales asociadas a los anuncios adicionales del anunciante.

La etapa 1010 recibe otra puntuación de intrusión de la página de destino candidata y puntuaciones de intrusión adicionales para las páginas de destino adicionales del motor de detección de intrusiones. Por ejemplo, como resultado de que el detector de malware 616 evalúa todas las páginas de destino candidatas para el anunciante, Se pueden generar puntuaciones de intrusión correspondientes a las páginas de destino. En particular, las puntuaciones de intrusión se pueden almacenar (o recibir) en la base de datos de apelaciones 620. En algunas implementaciones, las puntuaciones de intrusión de las páginas de destino adicionales pueden almacenarse en la base de datos de estado 614.

La etapa 1012 determina si las puntuaciones de intrusión de las páginas de destino superan el umbral de intrusión. Por ejemplo, el detector de malware 616 puede determinar cuál, si alguna, de las puntuaciones de intrusión de las páginas de destino recibidas en la etapa 1010 superan el umbral de intrusión.

La etapa 1014 excluye la publicación de anuncios asociados a la cuenta del patrocinador si una puntuación de intrusión para cualquiera de las páginas de destino supera el umbral de intrusión. Por ejemplo, si el detector de malware 616 determina que alguna de las puntuaciones de intrusión supera el umbral de intrusión, el detector de malware 616 puede actualizar la base de datos de apelaciones 620 con información de que los anuncios del patrocinador (como un todo) todavía incluyen malware y se puede impedir que se sirvan.

La figura 11 es un diagrama de flujo de un proceso de ejemplo 1100 para generar un modelo de clasificación. Por ejemplo, el proceso 1100 puede usarse para generar el modelo de clasificación 402. El proceso 1100 puede implementarse usando instrucciones de software almacenadas en un medio legible por ordenador y ejecutadas por un sistema de procesamiento.

La etapa 1102 divide las páginas de destino asociadas a los anuncios en páginas de destino de entrenamiento y páginas de destino de prueba. Por ejemplo, haciendo referencia a la figura 4, las páginas de destino y las URL 404 pueden dividirse en páginas de destino de entrenamiento que pueden usarse como ejemplos de entrenamiento para entrenar el modelo de clasificación 402, y páginas de destino que pueden usarse para probar el modelo de clasificación 402.

La etapa 1104 entrena iterativamente un modelo de clasificación sobre las características de intrusión de las páginas

de destino de entrenamiento. Por ejemplo, utilizando características extraídas por el motor de extracción de características 406 de las páginas de destino de entrenamiento obtenidas de las páginas de destino y las URL 404, el sistema 400 puede entrenar iterativamente el modelo de clasificación 402. El entrenamiento se puede realizar mediante una combinación de la evaluación de control 408 y el motor de aprendizaje automático 410.

La etapa 1106 prueba iterativamente el modelo de clasificación en las características de intrusión de las páginas de destino de prueba hasta que ocurre un evento de cese de prueba. Por ejemplo, utilizando características extraídas por el motor de extracción de características 406 de las páginas de destino de prueba obtenidas de las páginas de destino y las URL 404, el sistema 400 puede probar iterativamente el modelo de clasificación 402. La prueba puede ser realizada por el motor de aprendizaje automático 410. Durante la prueba, las asociaciones entre las ponderaciones de las características y las características de intrusión se pueden ajustar, como mediante el uso de un modelo de regresión lineal. Las etapas 1104 y 1106 se pueden repetir iterativamente, por ejemplo, hasta que ocurra un evento de cese de pruebas, como la determinación de que las ponderaciones de las características son lo suficientemente buenas.

La etapa 1108 almacena una asociación de ponderaciones de características y características de intrusión en el modelo de clasificación, la asociación de ponderaciones de características y características de intrusión derivadas del entrenamiento y las pruebas iterativas. Por ejemplo, las asociaciones entre las ponderaciones de las características y las características de intrusión que se generan iterativamente por las etapas 1104 y 1106 pueden almacenarse en el modelo de clasificación 402.

El aparato, métodos, Los diagramas de flujo y los diagramas de bloques de estructura descritos en este documento de patente pueden implementarse en sistemas de procesamiento informático que incluyen código de programa que comprende instrucciones de programa que son ejecutables por el sistema de procesamiento informático. También pueden usarse otras implementaciones. Adicionalmente, los diagramas de flujo y los diagramas de bloques de estructura descritos en este documento de patente, que describen métodos particulares y/o actos correspondientes en apoyo de pasos y características correspondientes en apoyo de los medios estructurales descritos, también se puede utilizar para implementar estructuras de software y algoritmos correspondientes, y equivalentes de los mismos.

Esta descripción escrita establece el mejor modo de la invención y proporciona ejemplos para describir la invención y permitir que una persona con conocimientos ordinarios en la técnica haga y utilice la invención. Esta descripción escrita no limita la invención a los términos precisos establecidos. Por lo tanto, mientras que la invención se ha descrito en detalle con referencia a los ejemplos expuestos anteriormente, los expertos en la materia pueden efectuar alteraciones, modificaciones y variaciones de los ejemplos sin apartarse del ámbito de la invención. El ámbito de la invención se define por las reivindicaciones adjuntas.

**REIVINDICACIONES**

1. Un método, que comprende:

dividir páginas de destino asociadas a anuncios en páginas de destino de entrenamiento y probar las páginas de destino;
entrenar iterativamente un modelo de clasificación sobre características de intrusión de las páginas de destino de entrenamiento; probar iterativamente el modelo de clasificación en las características de intrusión de las páginas de destino de prueba hasta que ocurra un evento de cese de prueba; y
almacenar una asociación de ponderaciones de características y características de intrusión en el modelo de clasificación en respuesta al evento de cese, derivándose la asociación de ponderaciones de características y características de intrusión a partir del entrenamiento y las pruebas iterativas;
identificar una página de destino asociada a un anuncio;
identificar características de intrusión de la página de destino;
generar una puntuación de característica para la página de destino basada en las características de intrusión identificadas y ponderaciones de características;
determinar si la puntuación de característica para la página de destino supera un umbral de característica; y
clasificar la página de destino como una página de destino candidata si la puntuación de característica para la página de destino supera el umbral de característica;
enviar la página de destino candidata a un motor de detección de intrusos; recibir una puntuación de intrusión de la página de destino candidata del motor de detección de intrusos; y
excluir la publicación del anuncio asociado a la página de destino candidata si la puntuación de intrusión supera un umbral de intrusión.

2. El método de la reivindicación 1, en el que el modelo de clasificación comprende un modelo basado en regresión lineal.

3. El método de la reivindicación 1, que comprende adicionalmente:
recibir una solicitud de apelación para la cuenta del patrocinador y en respuesta a recibir la solicitud de apelación:

volver a enviar la página de destino candidata al motor de detección de intrusos;
recibir otra puntuación de intrusión de la página de destino candidata del motor de detección de intrusos;
excluir la publicación del anuncio asociado a la página de destino candidata si la otra puntuación de intrusión supera el umbral de intrusión; y permitir la publicación del anuncio asociado a la página de destino candidata si la otra puntuación de intrusión no supera el umbral de intrusión.

4. El método de la reivindicación 1, que comprende adicionalmente:

identificar una cuenta de patrocinador asociada al anuncio, incluyendo la cuenta de patrocinador anuncios adicionales; y
excluir la publicación de anuncios adicionales asociados a la cuenta de patrocinador si la puntuación de intrusión de la página de destino candidata supera el umbral de intrusión.

5. El método de la reivindicación 1, en el que las características de intrusión comprenden una o más características de iFrame, una o más características de URL y/o una o más características de texto.

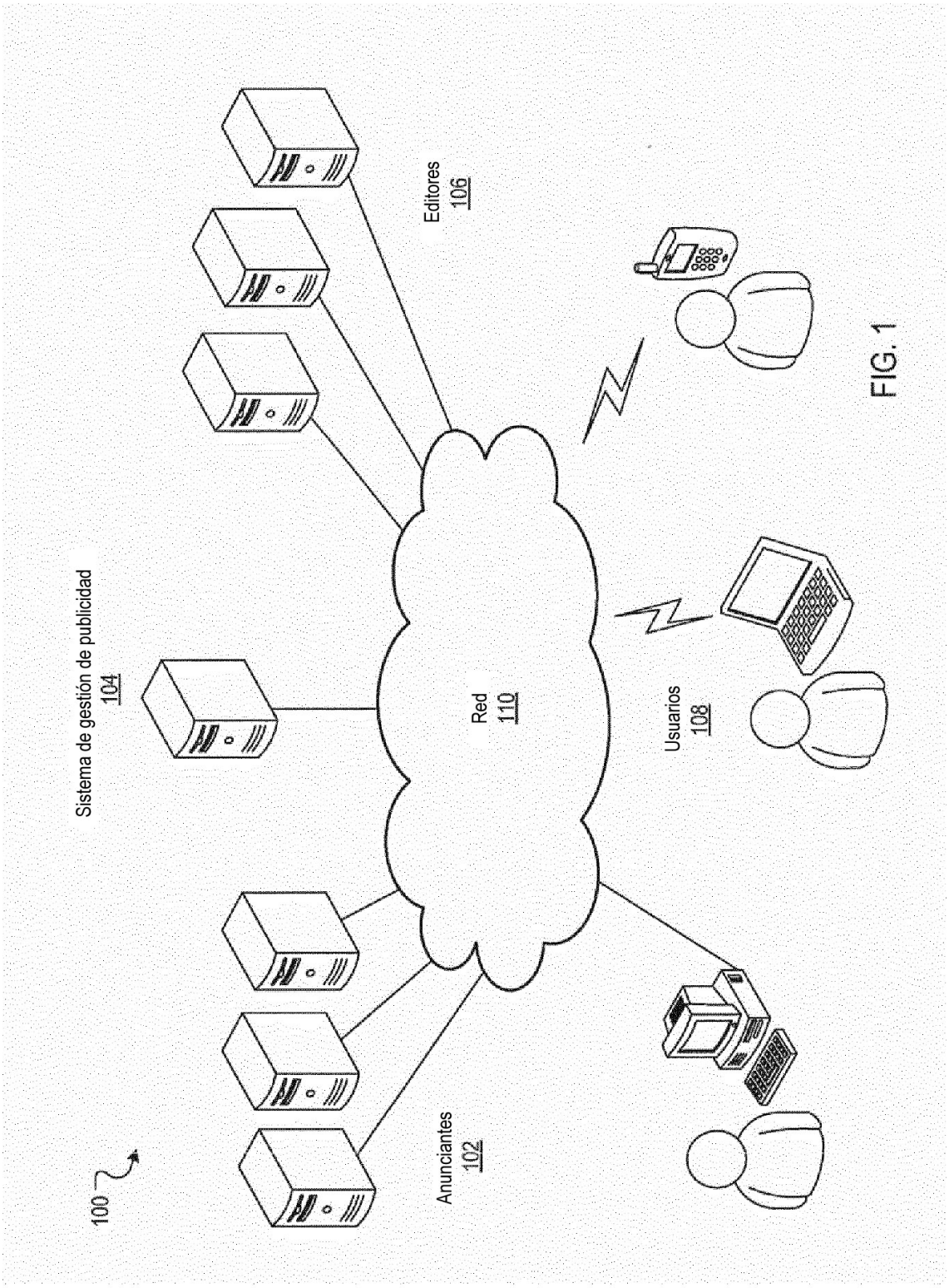
100
Sistema de gestión de publicidad
104
Anunciantes
102
Editores
106
Red
110
Usuarios
108

FIG. 1

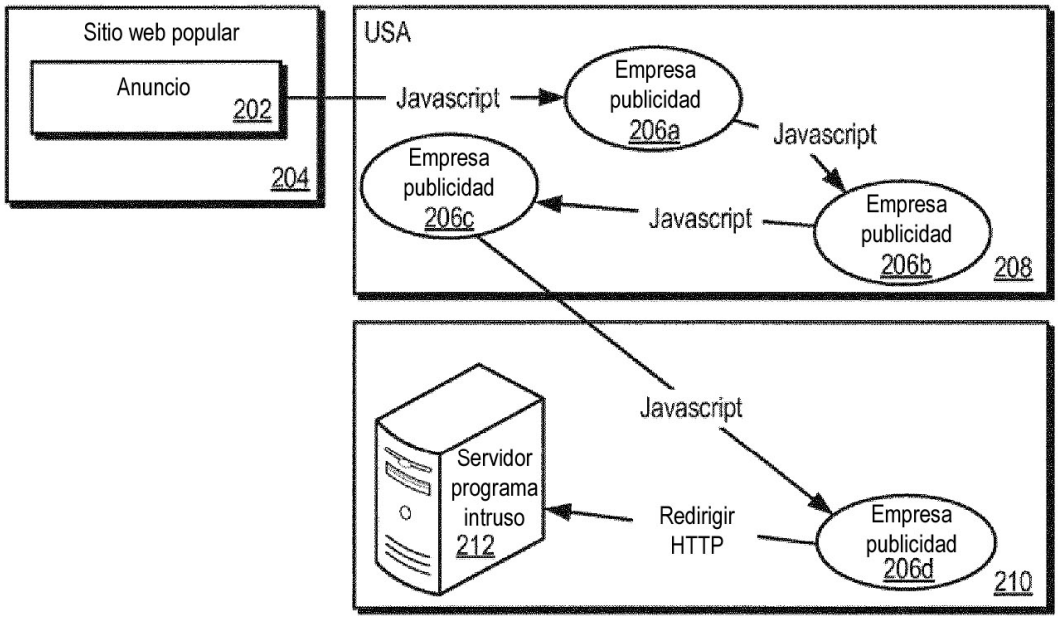
Sitio web popular
Anuncio
202
204
USA
Javascript
Empresa publicidad 206a
Javascript
Empresa publicidad 206c
Javascript
Empresa publicidad 206b
208
Javascript
Servidor programa intruso 212
Redirigir HTTP
Empresa publicidad 206d
210

FIG. 2

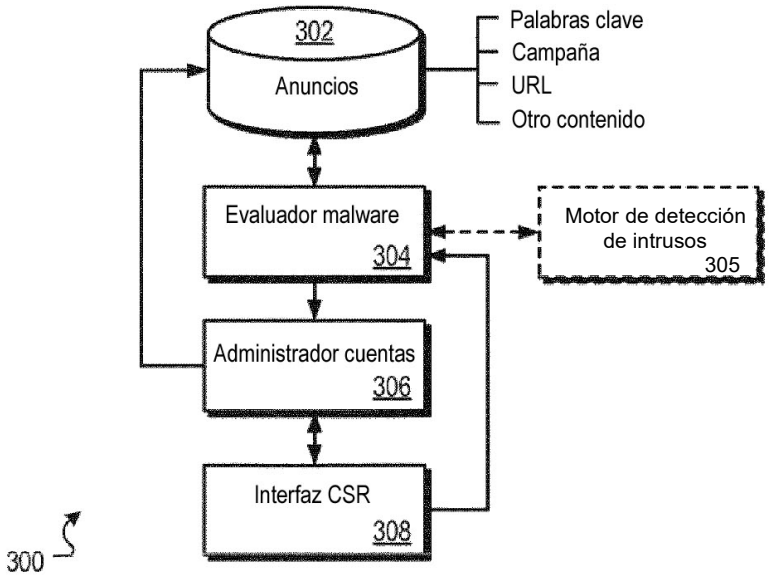
302
Anuncios
Palabras clave
Campaña
URL
Otro contenido
Evaluador malware
304
Motor de detección de intrusos
305
Administrador cuentas
306
Interfaz CSR
308
300

FIG. 3

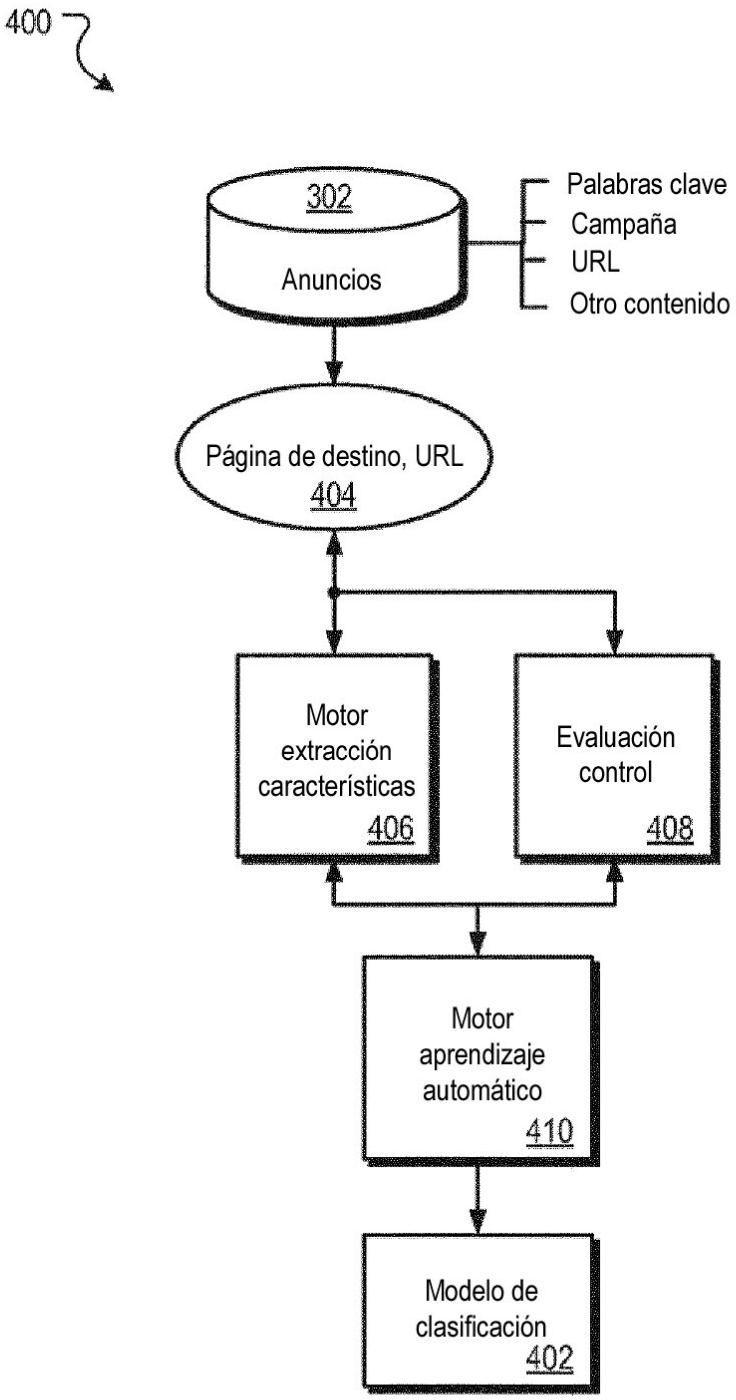
400
302
Anuncios
Palabras clave
Campaña
URL
Otro contenido
Página de destino, URL
404
Motor extracción características
406
Evaluación control
408
Motor aprendizaje automático
410
Modelo de clasificación
402

FIG. 4

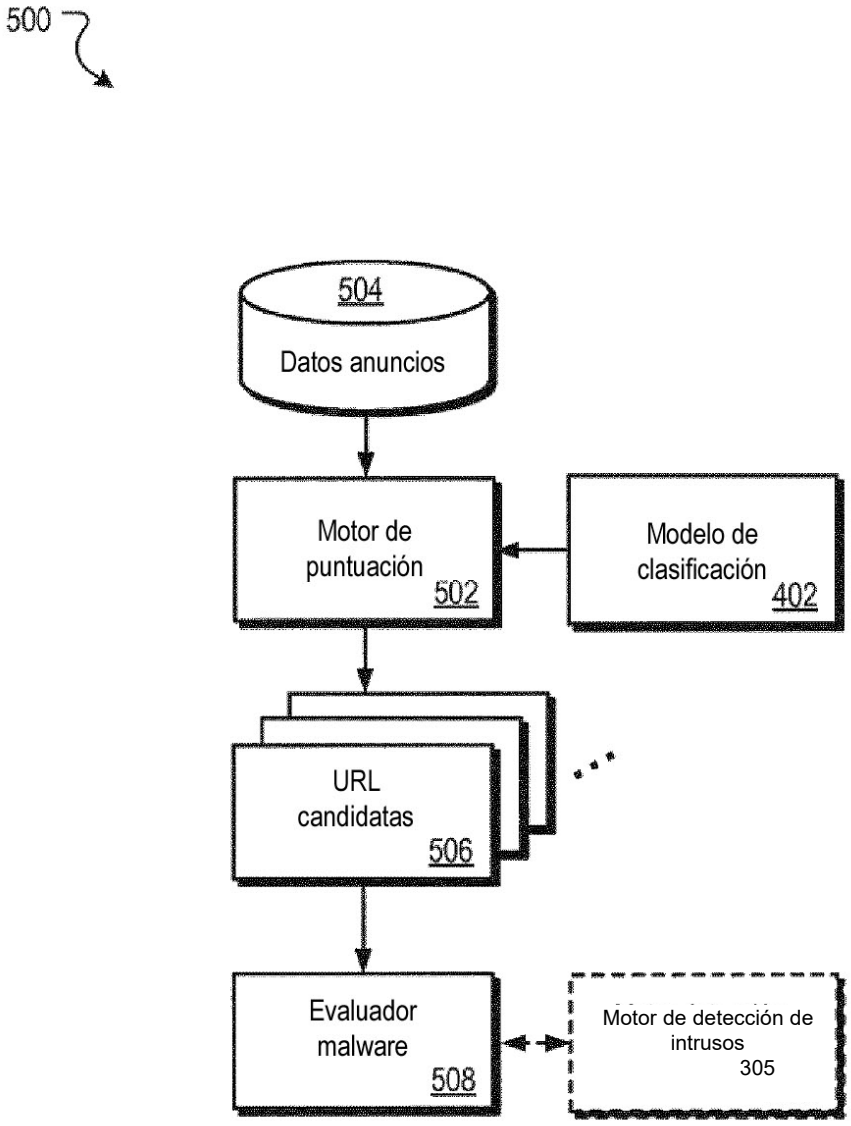
500
504
Datos anuncios
Motor de puntuación
502
Modelo de clasificación
402
URL candidatas
506
Evaluador malware
508
Motor de detección de intrusos
305

FIG. 5

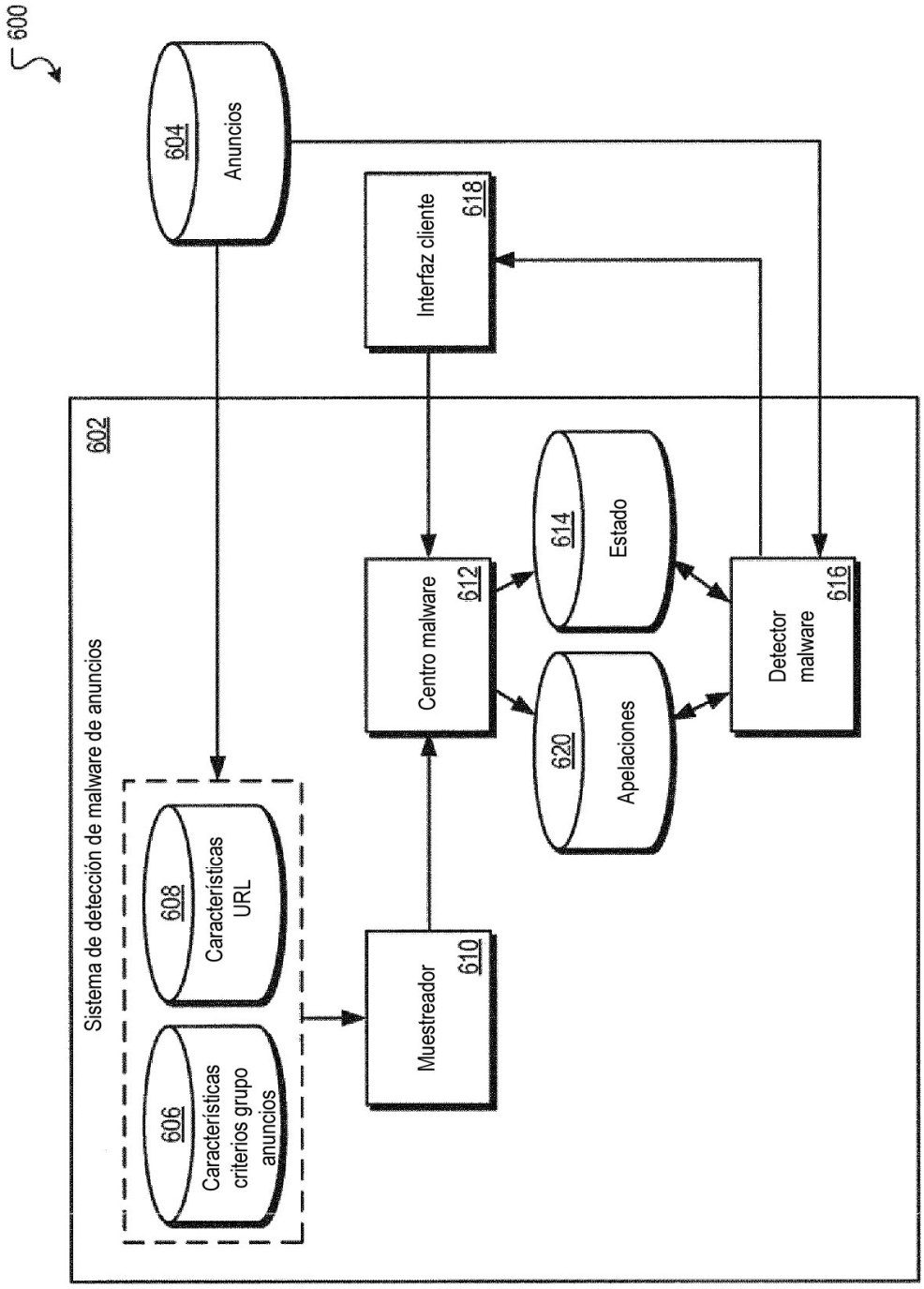
600
604
Anuncios
Interfaz cliente
618
602
Sistema de detección de malware de anuncios
614
Estado
Centro malware
612
Detector malware
616
620
Apelaciones
608
Características URL
606
Características criterios grupo anuncios
Muestreador
610

FIG. 6

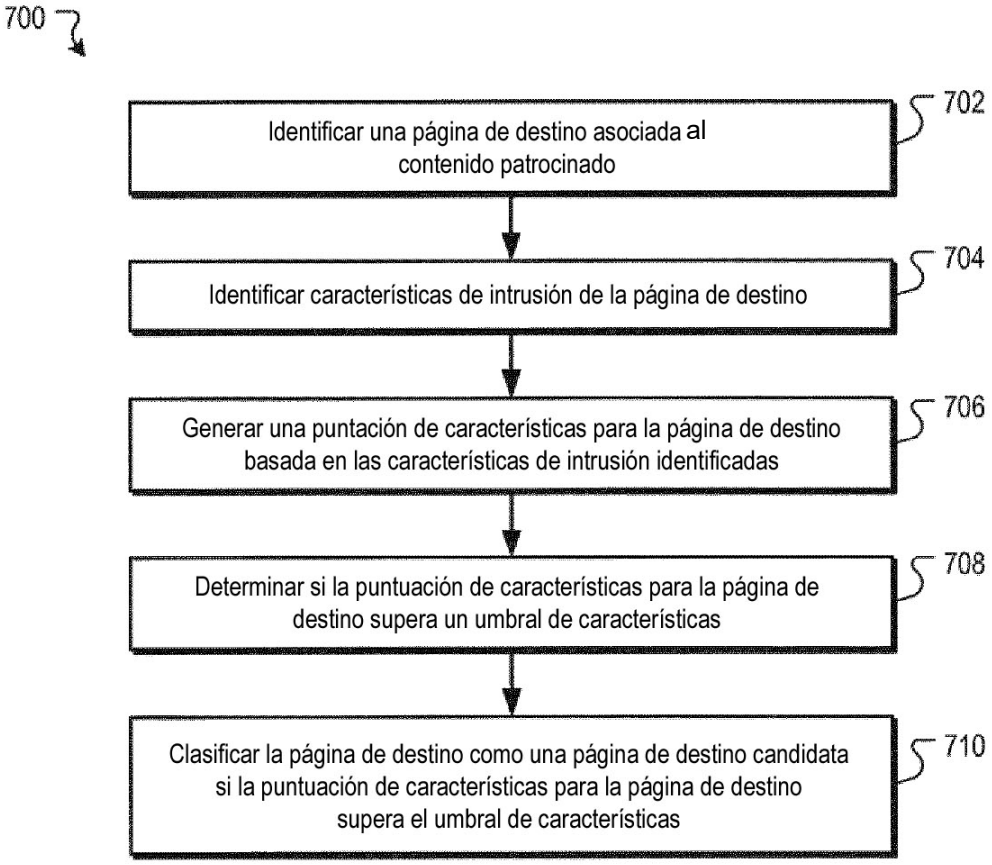
700
Identificar una página de destino asociada al contenido patrocinado
702
Identificar características de intrusión de la página de destino
704
Generar una puntación de características para la página de destino basada en las características de intrusión identificadas
706
Determinar si la puntuación de características para la página de destino supera un umbral de características
708
Clasificar la página de destino como una página de destino candidata si la puntuación de características para la página de destino supera el umbral de características
710

FIG. 7

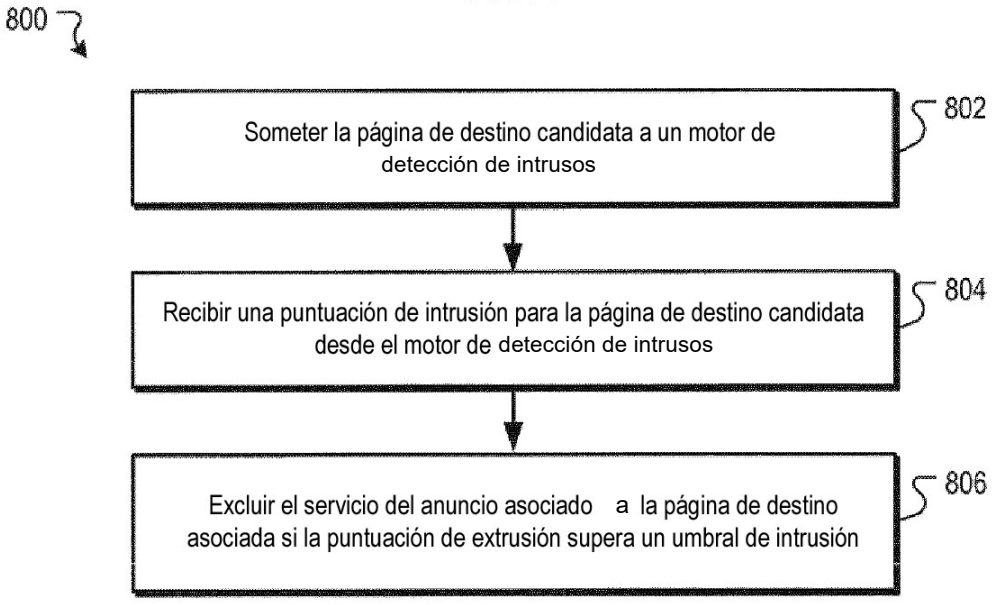
800
Someter la página de destino candidata a un motor de detección de intrusos
802
Recibir una puntuación de intrusión para la página de destino candidata desde el motor de detección de intrusos
804
Excluir el servicio del anuncio asociado a la página de destino asociada si la puntuación de extrusión supera un umbral de intrusión
806

FIG. 8

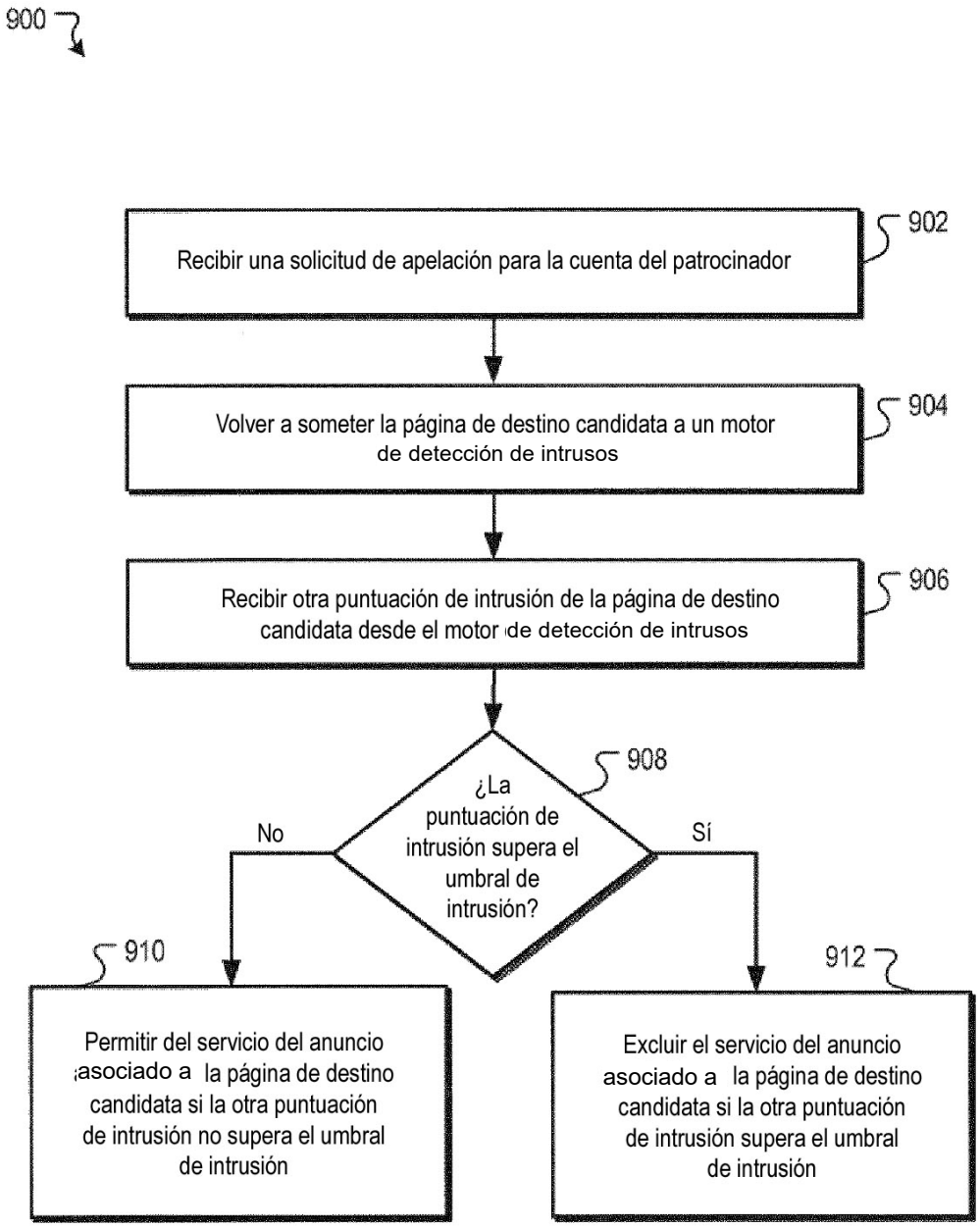
900
Recibir una solicitud de apelación para la cuenta del patrocinador
902
Volver a someter la página de destino candidata a un motor de detección de intrusos
904
Recibir otra puntuación de intrusión de la página de destino candidata desde el motor de detección de intrusos
906
¿La puntuación de intrusión supera el umbral de intrusión?
908
No
Sí
910
Permitir del servicio del anuncio asociado a la página de destino candidata si la otra puntuación de intrusión no supera el umbral de intrusión
912
Excluir el servicio del anuncio asociado a la página de destino candidata si la otra puntuación de intrusión supera el umbral de intrusión

FIG. 9

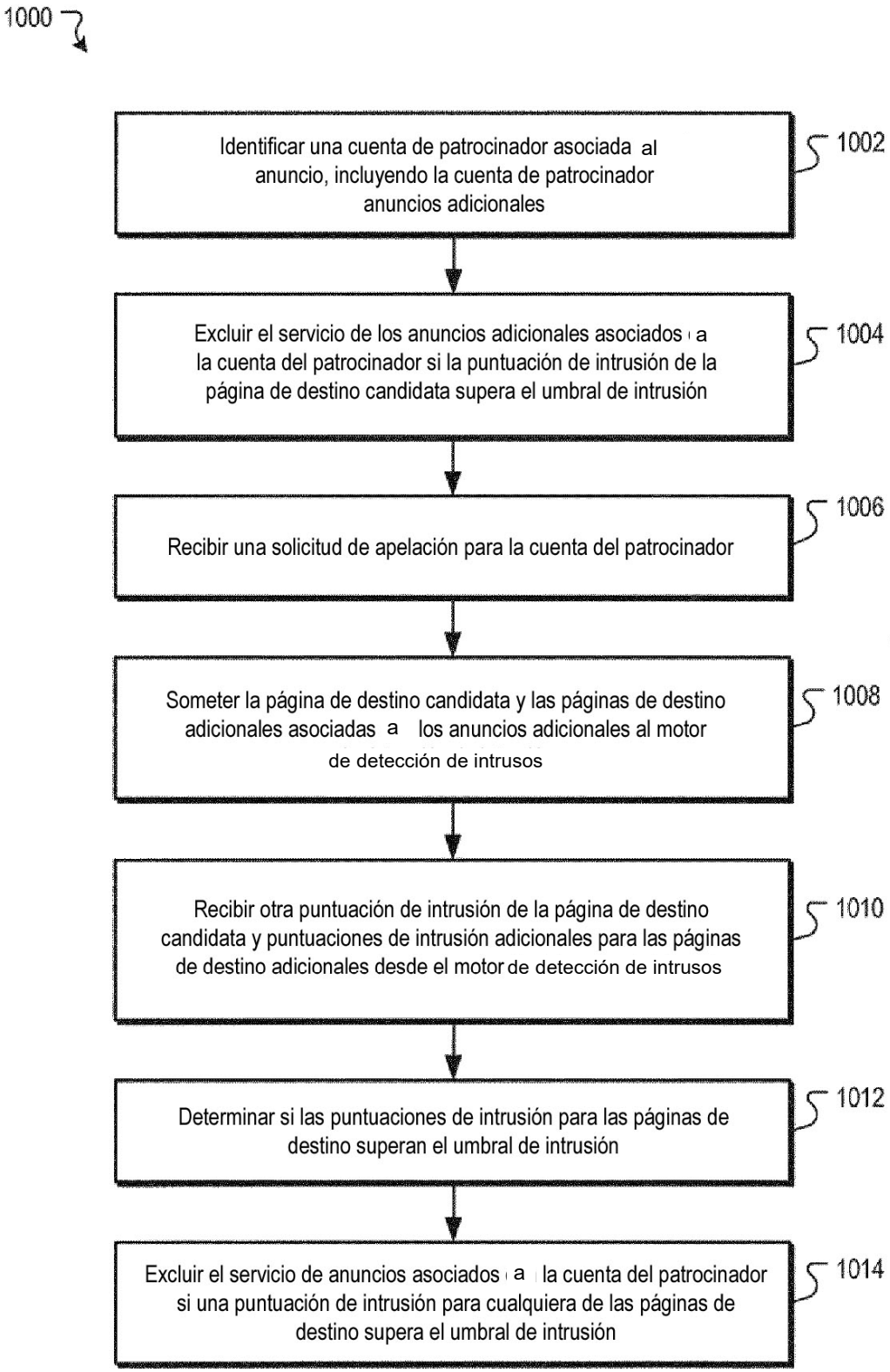
1000
Identificar una cuenta de patrocinador asociada al anuncio, incluyendo la cuenta de patrocinador anuncios adicionales
1002
Excluir el servicio de los anuncios adicionales asociados a la cuenta del patrocinador si la puntuación de intrusión de la página de destino candidata supera el umbral de intrusión
1004
Recibir una solicitud de apelación para la cuenta del patrocinador
1006
Someter la página de destino candidata y las páginas de destino adicionales asociadas a los anuncios adicionales al motor de detección de intrusos
1008
Recibir otra puntuación de intrusión de la página de destino candidata y puntuaciones de intrusión adicionales para las páginas de destino adicionales desde el motor de detección de intrusos
1010
Determinar si las puntuaciones de intrusión para las páginas de destino superan el umbral de intrusión
1012
Excluir el servicio de anuncios asociados a la cuenta del patrocinador si una puntuación de intrusión para cualquiera de las páginas de destino supera el umbral de intrusión
1014

FIG. 10

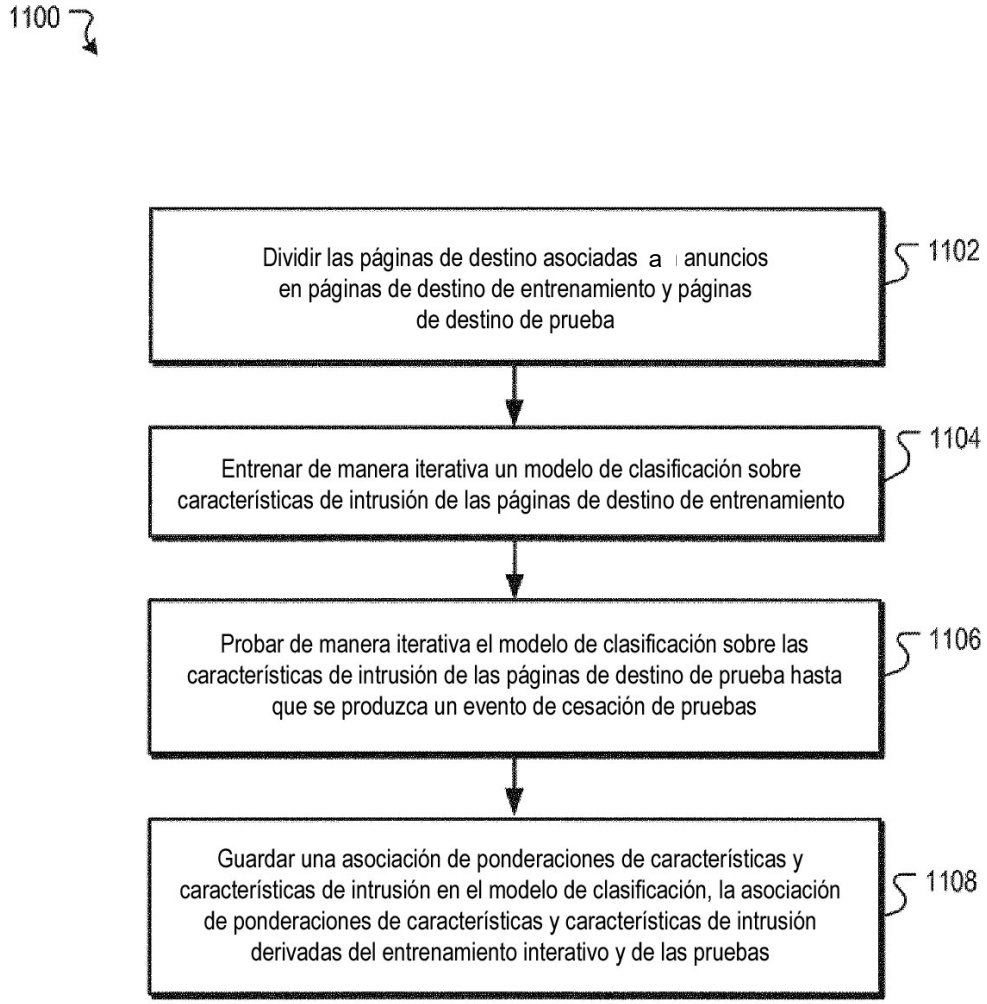
1100
Dividir las páginas de destino asociadas a anuncios en páginas de destino de entrenamiento y páginas de destino de prueba
1102
Entrenar de manera iterativa un modelo de clasificación sobre características de intrusión de las páginas de destino de entrenamiento
1104
Probar de manera iterativa el modelo de clasificación sobre las características de intrusión de las páginas de destino de prueba hasta que se produzca un evento de cesación de pruebas
1106
Guardar una asociación de ponderaciones de características y características de intrusión en el modelo de clasificación, la asociación de ponderaciones de características y características de intrusión derivadas del entrenamiento interativo y de las pruebas
1108

FIG. 11