(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 764 672**

(51) Int. CI.:

G06F 21/53 (2013.01)
G06F 21/12 (2013.01)
G06F 21/56 (2013.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **13.01.2017 PCT/CN2017/071149**

(87) Fecha y número de publicación internacional: **16.11.2017 WO17193626**

(96) Fecha de presentación y número de la solicitud europea: **13.01.2017 E 17795253 (8)**

(97) Fecha y número de publicación de la concesión europea: **30.10.2019 EP 3306510**

(54) Título: **Método y aparato de detección de amenazas y sistema de red**

(30) Prioridad:

10.05.2016 CN 201610305868

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.06.2020

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building, Bantian, Longgang District
Shenzhen, Guangdong 518129, CN

(72) Inventor/es:

CHEN, JIA

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método y aparato de detección de amenazas y sistema de red

Campo técnico

Esta solicitud se relaciona con el campo de las tecnologías informáticas y, en particular, con un método y aparato de detección de amenazas, y un sistema de red.

Antecedentes

Con el desarrollo y la popularidad de las tecnologías de red informática, más usuarios comienzan a centrarse en los problemas de seguridad de la red, y los ataques a la red implementados mediante el uso de una aplicación de red (Web) aparecen con frecuencia. Por ejemplo, para lograr un propósito de ataque, un atacante generalmente incrusta, mediante diversos medios, el código de ataque en forma de secuencia de comandos, un enlace, una imagen, una animación flash, un complemento o similar en una base de datos utilizada por una página dinámica. Cuando un usuario navega a través del código de ataque utilizando un navegador, el atacante puede lograr el propósito.

Considerando las ventajas de una tecnología de entorno de pruebas en la detección de códigos de ataque, por ejemplo, se puede descubrir un ataque desconocido y no se provoca ninguna amenaza a la seguridad de un ordenador que ejecuta un entorno de pruebas, se desarrolla un entorno de pruebas de Web combinando la tecnología de entorno de pruebas y la tecnología de un navegador, y el entorno de pruebas de Web se utiliza para garantizar la seguridad de una página Web a la que accede el navegador. El entorno de pruebas es un entorno de ejecución virtual creado en el ordenador y puede considerarse como una copia de un sistema operativo. Independientemente de un archivo sospechoso que se abra en el entorno de pruebas, todas las operaciones del archivo sospechoso en un disco duro en el ordenador o en un registro en el sistema operativo se asignan direccionalmente a una carpeta temporal. De esta manera, incluso si el archivo sospechoso lleva un código de ataque como un virus troyano o un complemento de publicidad, un rango afectado se limita al entorno virtual y un sistema operativo real no se ve afectado. Cuando se elimina el entorno de pruebas, un archivo que se ejecuta en el entorno de pruebas se borra automáticamente y el ordenador no está envenenada. Por lo tanto, el usuario puede ejecutar un archivo desconocido en el entorno de pruebas, para determinar si el archivo desconocido lleva un código de ataque. Un principio de detección del entorno de pruebas de Web es: simular un entorno real de un navegador de usuario, detectar y analizar una acción que tiene lugar en un proceso de carga de una página actual, y finalmente determinar si la página actual provoca una amenaza a un entorno de sistema del usuario.

Debido a que una tecnología de carga diferida se usa ampliamente en una página Web existente, un efecto de detección se ve muy afectado cuando el entorno de pruebas de Web realiza la detección de seguridad en una página Web, y un fenómeno de detección omitido es especialmente común. La tecnología de carga diferida significa que cuando el usuario usa el navegador para cargar un localizador uniforme de recursos (en inglés, Uniform/Universal Resource Locator - URL), un servidor Web no devuelve, a la vez, todo el contenido identificado por la URL, sino que obtiene solo una parte del contenido de una base de datos y devuelve la parte del contenido al usuario. En este caso, el usuario puede ver, en una interfaz de navegador, solo la parte del contenido devuelto por el servidor Web en este momento. La descarga de recursos de una página posterior (en adelante denominada página de carga de retado), la carga de la página y el procesamiento de presentación solo se activan cuando el usuario continúa navegando por la siguiente página Web. Después de utilizar la tecnología de carga diferida, se puede reducir el rendimiento de la red, se puede aumentar la velocidad de carga del navegador del usuario y se puede acortar el tiempo de espera del usuario, para mejorar la experiencia del usuario. Por lo tanto, la tecnología de carga diferida es una tecnología ampliamente utilizada. Sin embargo, cuando el entorno de pruebas de Web se usa para realizar la detección de seguridad en la página Web, el código de ataque incrustado en la página de carga retardada no se puede detectar y se produce un problema de detección perdido del entorno de pruebas de Web.

ALEXANDER MOSHCHUK ET AL: “SpyProxy: Execution-based Detection of Malicious Web Content”, USENIX, 15 de agosto de 2007 (2007-8-15), páginas 1-16, XP061011093, proporciona una herramienta antimalware basada en proxy llamada SpyProxy. SpyProxy intercepta y evalúa el contenido Web en tránsito desde los servidores Web al navegador. Un navegador en el trabajador VM de SpyProxy recupera y presenta la página Web completa, incluida la página raíz y todo el contenido incorporado.

Sumario

Las realizaciones de esta solicitud proporcionan un método y un aparato de detección de amenazas, y un sistema de red, para que se pueda resolver un problema de detección perdido de un entorno de pruebas de Web en un escenario de carga de retardo.

Para lograr el objetivo anterior, las siguientes soluciones técnicas se utilizan en las realizaciones de esta solicitud.

De acuerdo con un primer aspecto, una realización de esta solicitud proporciona un método de detección de amenazas que se aplica a un escenario de carga de retardo. Primero, cuando se carga un localizador uniforme de recursos URL en un navegador de un entorno de pruebas de Web, un aparato de detección de amenazas obtiene, desde un servidor

Web, el código de página de un primer grupo de páginas de visualización identificado por la URL y un tamaño total ocupado por el primer mostrar grupo de páginas en un área de visualización del navegador, donde el código de página del primer grupo de páginas de visualización incluye código de monitorización, el código de monitorización se usa para obtener y monitorear un valor de una variable de visualización, y se usa el valor de la variable de visualización para representar un tamaño ocupado, en el área de visualización del navegador, por páginas de visualización que se han visualizado desde una ubicación de inicio de una primera página de visualización a una página de visualización actual en el primer grupo de páginas de visualización. Luego, el aparato de detección de amenazas inyecta código dinámico preestablecido en el código de página obtenido del primer grupo de páginas de visualización, analiza y ejecuta el código de página que es del primer grupo de páginas de visualización y que incluye el código dinámico preestablecido y muestra, en una forma secuencial, visualice las páginas en el primer grupo de páginas de visualización, donde el código dinámico preestablecido se usa para activar el cambio de la página de visualización actual a la siguiente página de visualización de la página de visualización actual. Luego, cuando el aparato de detección de amenazas detecta que el valor de la variable de visualización es mayor o igual que un valor preestablecido, el aparato de detección de amenazas envía, al servidor Web, un mensaje de solicitud que lleva un identificador de grupo de páginas de visualización, para solicitar obtener el código de página de un segundo grupo de páginas de visualización del servidor Web, donde una primera página de visualización en el segundo grupo de páginas de visualización es la siguiente página de visualización de una última página de visualización en el primer grupo de páginas de visualización, y el valor predeterminado es mayor o igual a un tamaño ocupado por la primera página de visualización en el primer grupo de páginas de visualización en el área de visualización del navegador y menor que el tamaño total ocupado por el primer grupo de páginas de visualización en el área de visualización del navegador. Finalmente, el aparato de detección de amenazas recibe un mensaje de respuesta enviado por el servidor Web en respuesta al mensaje de solicitud, donde el mensaje de respuesta incluye el código de página del segundo grupo de páginas de visualización y detecta, en el entorno de pruebas, si el código de página obtenido de El segundo grupo de páginas de visualización lleva el código de ataque.

En esta realización de esta solicitud, el código dinámico preestablecido se usa para activar el aparato de detección de amenazas para cambiar de la página de visualización actual a la siguiente página de visualización de la página de visualización actual, es decir, el código dinámico preestablecido puede implementar una función de desplazamiento de forma automática desde la página de visualización actual a la siguiente página de visualización de la página de visualización actual, y la función es equivalente a un proceso de interacción hombre-máquina. El código dinámico preestablecido se usa para implementar el desplazamiento automático desde la página de visualización actual a la siguiente página de visualización de la página de visualización actual. Por lo tanto, en esta realización de esta solicitud, cuando el aparato de detección de amenazas muestra la última página de visualización en el primer grupo de páginas de visualización, bajo una acción del código dinámico preestablecido, el aparato de detección de amenazas necesita continuar mostrando la primera página de visualización en el segundo grupo de páginas de visualización, para activar el aparato de detección de amenazas para obtener el código de página del segundo grupo de páginas de visualización, de modo que el aparato de detección de amenazas detecte, en el entorno de prueba de Web, si el código de página del segundo grupo de páginas de visualización conlleva un código de ataque. De esta forma, en un escenario de carga de retardo, el aparato de detección de amenazas puede detectar, en el entorno de prueba de Web, si el código de página cargado con retardo lleva el código de ataque y si se evita un problema de detección perdido del entorno de prueba de Web.

Opcionalmente, en esta realización de esta solicitud, el aparato de detección de amenazas puede recibir, usando una interfaz de zócalo, el código de página que es del primer grupo de páginas de visualización y que es enviado por el servidor Web.

Específicamente, en este escenario, el aparato de detección de amenazas puede inyectar el código dinámico preestablecido en el código de página del primer grupo de páginas de visualización al recibir el código de página del primer grupo de páginas de visualización utilizando la interfaz de Zócalo.

Opcionalmente, un programa de enganche se configura para enganchar una función de procesamiento de protocolo de capa de red del entorno de pruebas de Web en esta realización de esta solicitud, y el programa de enganche se usa para interceptar el código de página del primer grupo de páginas de visualización. En este caso, el aparato de detección de amenazas inyecta el código dinámico preestablecido en el código de página del primer grupo de páginas de visualización cuando el programa de enganche obtiene el código de página del primer grupo de páginas de visualización.

Opcionalmente, se configura un programa de enganche para enganchar un núcleo del navegador del entorno de prueba de Web en el aparato de detección de amenazas, y el programa de enganche se usa para interceptar el código de página del primer grupo de páginas de visualización. En este caso, el aparato de detección de amenazas inyecta el código dinámico preestablecido en el código de página del primer grupo de páginas de visualización cuando el programa de enganche obtiene el código de página del primer grupo de páginas de visualización.

Se puede aprender de las descripciones anteriores que, en esta realización de esta solicitud, el aparato de detección de amenazas puede inyectar el código dinámico preestablecido en el primer grupo de páginas de visualización en diferentes momentos, y un tiempo de inyección es relativamente flexible.

Opcionalmente, en esta realización de esta solicitud, el código dinámico se coloca al final del código de página del primer grupo de páginas de visualización.

El aparato de detección de amenazas coloca el código dinámico preestablecido al final del código de página del primer grupo de páginas de visualización, de modo que una estructura existente del código de página del primer grupo de páginas de visualización no se ve afectada, es fácil para un desarrollador identificar, y la implementación del código es relativamente simple.

De acuerdo con un segundo aspecto, una realización de esta solicitud proporciona un aparato de detección de amenazas que se aplica a un escenario de carga de retardo, donde el aparato de detección de amenazas incluye una unidad de procesamiento, una unidad de visualización, una unidad de envío y una unidad de recepción.

Específicamente, las funciones implementadas por los módulos de unidad provistos en esta realización de esta solicitud son las siguientes:
La unidad de procesamiento está configurada para: al cargar un localizador uniforme de recursos en un navegador de un entorno de pruebas de Web, obtener, de un servidor Web, el código de página de un primer grupo de páginas de visualización identificado por la URL y un tamaño total ocupado por el primer grupo de páginas de pantalla en un área de visualización del navegador, donde el código de página del primer grupo de páginas de visualización incluye código de monitorización, el código de monitorización se usa para obtener y monitorear un valor de una variable de visualización, y el valor de la variable de visualización se usa para representar un tamaño ocupado, en el área de visualización del navegador, por las páginas de visualización que se han visualizado desde una ubicación de inicio de una primera página de visualización a una página de visualización actual en el primer grupo de páginas de visualización; configurado para inyectar código dinámico preestablecido en el código de página del primer grupo de páginas de visualización, donde el código dinámico preestablecido se usa para activar el cambio de la página de visualización actual a la siguiente página de visualización de la página de visualización actual; y configurado para analizar y ejecutar el código de página que es del primer grupo de páginas de visualización y que incluye el código dinámico preestablecido.

La unidad de visualización está configurada para mostrar, de forma secuencial, las páginas del primer grupo de páginas de visualización de acuerdo con el código de página, analizado y ejecutado por la unidad de procesamiento, que es del primer grupo de páginas de visualización y que incluye el código dinámico preestablecido .

La unidad de envío está configurada para enviar un mensaje de solicitud al servidor Web cuando la unidad de procesamiento detecta que el valor de la variable de visualización es mayor o igual a un valor preestablecido, donde el mensaje de solicitud se utiliza para solicitar obtener el código de página de un segundo grupo de páginas de visualización desde el servidor Web, una primera página de visualización en el segundo grupo de páginas de visualización es la siguiente página de visualización de una última página de visualización en el primer grupo de páginas de visualización, y el valor predeterminado es mayor o igual a un tamaño ocupado por la primera página de visualización en el primer grupo de páginas de visualización en el área de visualización del navegador y menor que el tamaño total ocupado por el primer grupo de páginas de visualización en el área de visualización del navegador.

La unidad de recepción está configurada para recibir un mensaje de respuesta enviado por el servidor Web, donde el mensaje de respuesta incluye el código de página del segundo grupo de páginas de visualización.

La unidad de procesamiento está configurada además para detectar, en el entorno de prueba de Web, si el código de página que es del segundo grupo de páginas de visualización y que es recibido por la unidad de recepción lleva un código de ataque.

En esta realización de esta solicitud, el código dinámico preestablecido se usa para activar el cambio de la página de visualización actual a la siguiente página de visualización de la página de visualización actual, es decir, el código dinámico preestablecido puede implementar una función de desplazamiento automático desde la página de visualización actual a la siguiente página de visualización de la página de visualización actual. En esta realización de esta solicitud, el aparato de detección de amenazas inyecta el código dinámico preestablecido en el código de página obtenido del primer grupo de páginas de visualización, de modo que el aparato de detección de amenazas puede mostrar automáticamente todas las páginas de visualización en el primer grupo de páginas de visualización secuencialmente. Cuando el valor de la variable de visualización es mayor o igual que el valor preestablecido, el aparato de detección de amenazas se activa para interactuar con el servidor Web para obtener el código de página del segundo grupo de páginas de visualización, de modo que el aparato de detección de amenazas pueda detectar, en el entorno de pruebas de Web, si el código de página del segundo grupo de páginas de visualización contiene código de ataque y se evita un problema de detección perdido del entorno de pruebas de Web.

Opcionalmente, la unidad de procesamiento está configurada específicamente para recibir, mediante una interfaz de Zócalo, el código de página que es del primer grupo de páginas de visualización identificado por la URL y que envía el servidor Web.

Opcionalmente, se configura un programa de enganche para enganchar una función de procesamiento de protocolo de capa de red del entorno de pruebas de Web, y el programa de enganche se utiliza para interceptar el código de página del primer grupo de páginas de visualización. La unidad de procesamiento está configurada específicamente

para inyectar el código dinámico preestablecido en el código de página del primer grupo de páginas de visualización cuando el programa de enganche obtiene el código de página del primer grupo de páginas de visualización.

Opcionalmente, se configura un programa de enganche para enganchar un núcleo del navegador del entorno de prueba de Web, y el programa de enganche se utiliza para interceptar el código de página del primer grupo de páginas de visualización. La unidad de procesamiento está configurada específicamente para inyectar el código dinámico preestablecido en el código de página del primer grupo de páginas de visualización cuando el programa de enganche obtiene el código de página del primer grupo de páginas de visualización.

Opcionalmente, en esta realización de esta solicitud, el código dinámico preestablecido se coloca al final del código de página del primer grupo de páginas de visualización.

De acuerdo con un tercer aspecto, otra realización de esta solicitud proporciona un medio de almacenamiento legible por ordenador, y el medio de almacenamiento legible por ordenador incluye una o más piezas de código de programa. Cuando el procesador en el aparato de detección de amenazas ejecuta el código del programa, el aparato de detección de amenazas ejecuta el método de detección de amenazas de acuerdo con cualquiera de los aspectos anteriores y varias implementaciones opcionales de los mismos.

Para un efecto técnico del medio de almacenamiento legible por ordenador provisto en esta realización de esta solicitud, refiérase a un efecto técnico correspondiente de cualquiera de los aspectos anteriores y varias implementaciones opcionales de los mismos. Los detalles no se describen aquí nuevamente.

De acuerdo con un cuarto aspecto, otra realización de esta solicitud proporciona un sistema de red que se aplica a un escenario de carga de retardo, que incluye al menos un aparato de detección de amenazas de acuerdo con cualquiera de los aspectos anteriores y varias implementaciones opcionales de los mismos y un servidor Web. Cada aparato de detección de amenazas del al menos un aparato de detección de amenazas está conectado al servidor Web mediante una red.

Específicamente, el servidor Web está configurado para enviar el código de página correspondiente al aparato de detección de amenazas de acuerdo con una solicitud enviada por el aparato de detección de amenazas, de modo que el aparato de detección de amenazas detecte, en un entorno de pruebas de Web, si el código de página recibido de una página de visualización grupo lleva el código de ataque.

Opcionalmente, el servidor Web envía, al aparato de detección de amenazas de acuerdo con un localizador uniforme de recursos URL enviado por el aparato de detección de amenazas, el código de página de un primer grupo de páginas de visualización identificado por la URL. El servidor Web envía el código de página de un segundo grupo de páginas de visualización al aparato de detección de amenazas de acuerdo con un mensaje de solicitud enviado por el aparato de detección de amenazas y que se utiliza para solicitar obtener el código de página del segundo grupo de páginas de visualización.

Para un efecto técnico del sistema de red provisto en esta realización de esta solicitud, consulte el efecto técnico del aparato de detección de amenazas descrito en el método de detección de amenazas ejecutado por el aparato de detección de amenazas de acuerdo con cualquiera de los aspectos anteriores y diversas implementaciones opcionales de estos. Los detalles no se describen aquí nuevamente.

Breve descripción de los dibujos

Para describir las soluciones técnicas en las realizaciones de esta solicitud o en la técnica anterior más claramente, a continuación, se describen brevemente los dibujos adjuntos necesarios para describir las realizaciones o la técnica anterior. Aparentemente, los dibujos que se acompañan en la siguiente descripción muestran simplemente algunas realizaciones de esta solicitud.

La figura 1 es un primer diagrama estructural esquemático de composición de un sistema de red de acuerdo con una realización de esta solicitud;

La figura 2 es un segundo diagrama estructural esquemático de composición de un sistema de red de acuerdo con una realización de esta solicitud;

La figura 3 es un tercer diagrama estructural esquemático de composición de un sistema de red de acuerdo con una realización de esta solicitud;

La figura 4 es un diagrama de flujo esquemático de un método de detección de amenazas de acuerdo con una realización de esta solicitud;

La figura 5 es un primer diagrama estructural esquemático de un aparato de detección de amenazas de acuerdo con una realización de esta solicitud;

La figura 6 es un segundo diagrama estructural esquemático de un aparato de detección de amenazas de acuerdo con una realización de esta solicitud; y

La figura 7 es un diagrama estructural esquemático de un sistema de red de acuerdo con una realización de esta solicitud.

Descripción de realizaciones

Lo siguiente describe en detalle las soluciones técnicas en las realizaciones de esta solicitud con referencia a los dibujos adjuntos en las realizaciones de esta solicitud.

En la siguiente descripción, para ilustrar en lugar de limitar, se proporcionan detalles específicos como una estructura de sistema particular, una interfaz y una tecnología para comprender a fondo esta solicitud. Sin embargo, un experto en la materia debería saber que esta solicitud se puede practicar en otras realizaciones sin estos detalles específicos. En otros casos, se omiten descripciones detalladas de aparatos, circuitos y métodos conocidos, de modo que esta solicitud se describe sin ser observada por detalles innecesarios.

Además, los términos “incluir”, “tener”, o cualquier otra variante de la misma mencionada en la especificación, las reivindicaciones y los dibujos adjuntos de esta solicitud, están destinados a cubrir una inclusión no excluyente. Por ejemplo, un proceso, un método, un sistema, un producto o un dispositivo que incluye una serie de pasos o unidades no se limita a los pasos o unidades enumerados, sino que opcionalmente incluye además un paso o unidad no incluido en la lista, u opcionalmente incluye otro paso inherente o unidad del proceso, el método, el producto o el dispositivo.

Las realizaciones de esta solicitud pueden implementarse como un proceso (método) de implementación de ordenador, un sistema informático o un producto tal como un producto de programa de ordenador o un medio legible por ordenador. El producto de programa de ordenador puede ser un medio de almacenamiento de ordenador que es legible en un sistema de ordenador y que está codificado para incluir un programa de ordenador que se utiliza para permitir que un ordenador o un sistema de ordenador ejecute una instrucción de un proceso de ejemplo. Un medio de almacenamiento legible por ordenador es un dispositivo de almacenamiento legible por ordenador no transitorio. Por ejemplo, el medio de almacenamiento legible por ordenador puede implementarse usando una o más de una memoria de ordenador volátil, una memoria no volátil, un disco duro y una unidad flash, un disquete, un disco compacto o un medio similar.

El término “y/o” en las realizaciones de esta solicitud describe solo una relación de asociación para describir objetos asociados y representa que pueden existir tres relaciones. Por ejemplo, A y/o B pueden representar los siguientes tres casos: solo existe A, existen A y B, y solo B existe. Además, el carácter “/” en esta especificación generalmente indica una relación “o” entre los objetos asociados.

En la especificación, las reivindicaciones y los dibujos adjuntos de esta solicitud, los términos “primero”, “segundo”, etc., tienen la intención de distinguir entre diferentes objetos, pero no indican un orden particular.

En un escenario de carga de retardo, para resolver un problema de detección omitida de un entorno de pruebas de Web que existe cuando el entorno de pruebas de Web realiza la detección de seguridad en una página Web, las realizaciones de esta solicitud proporcionan un método de detección de amenazas. Un aparato de detección de amenazas inyecta, en el código de página que es de un primer grupo de páginas de visualización identificado por una URL y que es obtenido por el aparato de detección de amenazas, código dinámico preestablecido que se utiliza para activar el cambio de una página de visualización actual a una página de visualización siguiente de la página de visualización actual, de modo que el aparato de detección de amenazas puede mostrar automáticamente todas las páginas de visualización en el primer grupo de páginas de visualización secuencialmente. Bajo la acción de una función de desplazamiento automático a una página de visualización siguiente, se implementa la interacción entre el aparato de detección de amenazas y un servidor Web, y se obtiene el código de página de un segundo grupo de páginas de visualización, de modo que el aparato de detección de amenazas detecta, en el entorno de pruebas de Web, si el código de página del segundo grupo de páginas de visualización lleva código de ataque, y se evita el problema de detección perdido del entorno de pruebas de Web.

El aparato de detección de amenazas en las realizaciones de esta solicitud puede ser un terminal de usuario en el que se establece un entorno de pruebas de Web, o puede ser un dispositivo de detección de seguridad en el que se establece un entorno de pruebas de Web, donde el dispositivo de detección de seguridad está ubicado entre un servidor Web y un terminal de usuario, o puede ser un dispositivo de detección de derivación dedicado en el que se establece un entorno de pruebas de Web. Se puede establecer un entorno de pruebas de Web en un sistema operativo virtual del dispositivo de detección de derivación dedicado, o se puede establecer en un sistema operativo real del dispositivo de detección de derivación dedicado.

El terminal de usuario puede ser un terminal inalámbrico o un terminal cableado. El terminal inalámbrico puede ser un dispositivo que proporciona conectividad de voz y/o datos para un usuario, un dispositivo portátil con una función de conexión inalámbrica u otro dispositivo de procesamiento conectado a un módem inalámbrico. El terminal inalámbrico puede comunicarse con una o más redes centrales mediante una red de acceso de radio (en inglés, Radio Access Network RAN). El terminal inalámbrico puede ser un terminal móvil, como un teléfono móvil (o denominado teléfono “celular”) o un ordenador con un terminal móvil, o puede ser un ordenador portátil, de bolsillo, de mano, incorporada, o aparatos móviles en el vehículo, e intercambia voz y/o datos con la red de acceso por radio. Por ejemplo, el terminal inalámbrico puede ser un dispositivo como un teléfono de servicio de comunicación personal (en inglés, Personal

Communication Service - PCS), un teléfono inalámbrico, un teléfono de Protocolo de Inicio de Sesión (SIP, por sus siglas en inglés), una estación de Bucle Local Inalámbrico (en inglés, Wireless Local Loop - WLL) o un asistente digital personal (en inglés, Personal Digital Assistant - PDA). El terminal inalámbrico también puede denominarse agente de usuario (en inglés, User Agent), dispositivo de usuario (en inglés, User Device) o equipo de usuario (en inglés, User Equipment).

El método de detección de amenazas proporcionado en las realizaciones de esta solicitud se aplica a un sistema de red. El sistema de red incluye al menos un aparato de detección de amenazas y un servidor Web.

Opcionalmente, con referencia a las descripciones anteriores, si el aparato de detección de amenazas es un terminal de usuario en el que se establece un entorno de pruebas de Web, en la figura 1 se muestra una estructura de un sistema de red al que se aplica el método de detección de amenazas proporcionado en las realizaciones de esta solicitud. Con referencia a la figura 1, el sistema de red incluye un servidor 10 Web y al menos un terminal 11 de usuario en el que se establece un entorno 12 de pruebas Web, y el servidor 10 Web está conectado a cada terminal 11 de usuario utilizando una red.

El servidor 10 Web almacena un texto, un medio y otra información, como un audio, un video, una imagen, un gráfico, un diagrama y una tabla. El servidor 10 Web proporciona principalmente contenido o un servicio para el terminal 11 de usuario. Por ejemplo, el servidor 10 Web envía el código de página correspondiente a una URL al terminal 11 de usuario.

Opcionalmente, el servidor 10 Web en esta realización de esta solicitud puede ser un dispositivo informático que ejecuta uno o más programas de software en un entorno de red, o puede considerarse como un servidor Web virtual ejecutado en uno o más dispositivos informáticos de un servidor Web en una red, y el servidor Web virtual se implementa mediante un programa de software.

El entorno 12 de pruebas Web se establece en el terminal 11 de usuario. El terminal 11 de usuario puede comunicarse, utilizando un protocolo de comunicaciones predefinido, con el entorno 12 de pruebas Web establecido en el terminal 11 de usuario. El terminal 11 de usuario puede solicitar, utilizando el entorno 12 de pruebas Web, obtener el código de página del servidor 10 Web. El contenido representado por el código de la página puede incluir componentes de un sitio Web, como una imagen, un componente de texto, un medio o cualquier combinación de los mismos. El terminal 11 de usuario puede detectar, en el entorno 12 de pruebas Web, si el código de página enviado por el servidor 10 Web al terminal 11 de usuario lleva código de ataque.

La red en esta realización de esta solicitud puede ser cualquier arquitectura de red proporcionada mediante el uso de una tecnología cableada o inalámbrica.

Opcionalmente, con referencia a las descripciones anteriores, si el aparato de detección de amenazas es un dispositivo de seguridad en el que se establece un entorno de pruebas de Web, se muestra una estructura de un sistema de red al que se aplica el método de detección de amenazas proporcionado en las realizaciones de esta solicitud como se muestra en la figura 2. Con referencia a la figura 2, el sistema de red incluye un servidor 20 Web, un dispositivo 21 de seguridad en el que se establece un entorno 23 de pruebas Web y al menos un terminal 22 de usuario. El servidor 20 Web está conectado al dispositivo 21 de seguridad mediante una red, y el dispositivo 21 de seguridad está conectado a cada terminal 22 de usuario utilizando una red.

Una función que puede ser implementada por el servidor 20 Web en esta realización de esta solicitud es la misma que la función implementada por el servidor 10 Web en el ejemplo anterior, y los detalles no se describen aquí nuevamente.

El entorno 23 de pruebas Web se establece en el dispositivo 21 de seguridad. El dispositivo 21 de seguridad puede comunicarse, mediante un protocolo de comunicaciones predefinido, con el entorno 23 de pruebas Web establecido en el dispositivo 21 de seguridad. El dispositivo 21 de seguridad puede solicitar, utilizando entorno 23 de pruebas Web, para obtener el código de página del servidor 20 Web. El dispositivo 21 de seguridad puede detectar, en el entorno 23 de pruebas Web, si el código de página enviado por el servidor 20 Web al dispositivo 21 de seguridad lleva un código de ataque.

El terminal 22 de usuario interactúa con el dispositivo 21 de seguridad, y puede obtener un resultado de detección al detectar, mediante el dispositivo 21 de seguridad, si el código de página lleva el código de ataque.

Opcionalmente, con referencia a las descripciones anteriores, si el aparato de detección de amenazas es un dispositivo de detección de derivación dedicado en el que se establece un entorno de pruebas de Web, se aplica una estructura de un sistema de red al que se aplica el método de detección de amenazas proporcionado en las realizaciones de esta solicitud como se muestra en la figura 3. Con referencia a la figura 3, el sistema de red incluye un servidor 30 Web, un conmutador 31, un dispositivo 32 de detección de derivación dedicado en el que se establece un entorno de pruebas de Web, y al menos un terminal 33 de usuario. El servidor 30 Web está conectado al conmutador 31 al utilizar una red, el conmutador 31 está conectado al dispositivo 32 de detección de derivación dedicado utilizando una red, y el conmutador 31 está conectado a cada terminal 33 de usuario utilizando una red.

Una función que puede ser implementada por el servidor 30 Web en esta realización de esta solicitud es la misma que

la función implementada por el servidor 10 Web en el ejemplo anterior, y los detalles no se describen aquí nuevamente.

Al detectar un mensaje de solicitud que incluye una URL y que es enviado por el terminal 33 de usuario al servidor 30 Web, el conmutador 31 refleja la solicitud, es decir, copia el mensaje de solicitud que incluye la URL y envía el mensaje de solicitud al dispositivo 32 dedicado de detección de derivación. El conmutador 31 en esta realización de esta solicitud puede reemplazarse con un enrutador.

El entorno de pruebas de Web en el dispositivo 32 de detección de derivación dedicado puede establecerse en un sistema operativo virtual del dispositivo de detección de derivación dedicado, o puede establecerse en un sistema operativo real del dispositivo de detección de derivación dedicado. El dispositivo 32 de detección de derivación dedicado puede comunicarse, mediante un protocolo de comunicaciones predefinido, con el entorno de pruebas de Web establecido en el dispositivo 32 de detección de derivación dedicado. Después de obtener el mensaje de solicitud que incluye la URL, el dispositivo 32 de detección de derivación dedicado puede solicitar, utilizando el entorno de pruebas de Web en el dispositivo 32 de detección de derivación dedicado, obtener el código de página correspondiente a la URL del servidor 30 Web. El dispositivo 32 de detección de derivación dedicado puede detectar, en el entorno de pruebas de Web, si el código de página enviado por el servidor 30 Web al dispositivo 32 de detección de derivación dedicado lleva un código de ataque.

El método y el aparato de detección de amenazas y el sistema de red proporcionado en las realizaciones de esta solicitud son aplicables a un escenario de carga retardada.

La figura 4 es un diagrama de flujo esquemático de un método de detección de amenazas de acuerdo con una realización de esta solicitud. El método de detección de amenazas puede aplicarse al sistema de red que se muestra en cualquier dibujo adjunto de la figura 1 a la figura 3)

Con referencia a la figura 4, el método de detección de amenazas incluye los siguientes pasos.

S400. Al cargar una URL en un navegador de un entorno de pruebas de Web, un aparato de detección de amenazas obtiene, de un servidor Web, el código de página de un primer grupo de páginas de visualización identificado por la URL y un tamaño total ocupado por el primer grupo de páginas de visualización en un área de visualización del navegador.

El código de página del primer grupo de páginas de visualización incluye el código de monitorización, y el código de monitorización se utiliza para obtener y monitorizar un valor de una variable de visualización. El valor de la variable de visualización se utiliza para representar un tamaño ocupado, en el área de visualización del navegador, por las páginas de visualización que se han mostrado desde una ubicación de inicio de una primera página de visualización a una página de visualización actual en el primer grupo de página de visualización.

S401. El aparato de detección de amenazas inyecta código dinámico preestablecido en el código de página del primer grupo de páginas de visualización.

El código dinámico preestablecido se usa para activar el cambio de la página de visualización actual a la siguiente página de visualización de la página de visualización actual, es decir, el código dinámico preestablecido puede implementar una función de desplazamiento automático desde la página de visualización actual hasta la página de siguiente página de visualización de la página de visualización actual, y la función es equivalente a un proceso de interacción hombre-máquina.

S402. El aparato de detección de amenazas analiza y ejecuta el código de página del primer grupo de páginas de visualización y que incluye el código dinámico preestablecido, y muestra, de forma secuencial, las páginas de visualización en el primer grupo de páginas de visualización.

S403. El aparato de detección de amenazas envía un mensaje de solicitud al servidor Web cuando detecta que el valor de la variable de visualización es mayor o igual que un valor preestablecido, donde el mensaje de solicitud se utiliza para solicitar obtener el código de página de un segundo grupo de páginas de visualización del servidor Web.

Una primera página de visualización en el segundo grupo de páginas de visualización es la siguiente página de visualización de una última página de visualización en el primer grupo de páginas de visualización. Es decir, el aparato de detección de amenazas primero muestra todas las páginas de visualización del primer grupo de páginas de visualización, y luego muestra todas las páginas de visualización del segundo grupo de páginas de visualización.

El valor predeterminado es mayor o igual a un tamaño ocupado por la primera página de visualización en el primer grupo de páginas de visualización en el área de visualización del navegador y menor que el tamaño total ocupado por el primer grupo de páginas de visualización en el área de visualización del navegador .

S404. El servidor Web envía, al aparato de detección de amenazas, un mensaje de respuesta que lleva el código de página del segundo grupo de páginas de visualización.

S405. El aparato de detección de amenazas detecta, en el entorno de pruebas de la Web, si el código de página del segundo grupo de páginas de visualización lleva código de ataque.

En esta realización de esta solicitud, un cliente que puede analizar una página Web se construye en el entorno de pruebas de Web del aparato de detección de amenazas, y el cliente es un navegador común u otro programa de aplicación que integra un navegador incorporado.

El programa de aplicación es un programa informático desarrollado para completar una o más tareas específicas y que se ejecuta en un sistema operativo. En esta realización de esta solicitud, el programa de aplicación que puede analizar una página Web es un programa de aplicación que es compatible con un sistema transportado por el entorno de pruebas de Web del aparato de detección de amenazas.

Para facilitar la comprensión, en esta realización de esta solicitud, se utiliza un navegador en el entorno de pruebas de Web del aparato de detección de amenazas como un ejemplo para la descripción.

En general, un proceso en el que el aparato de detección de amenazas abre una página Web utilizando el navegador en un sistema operativo real del aparato de detección de amenazas puede considerarse como un proceso de comunicación entre el navegador en el aparato de detección de amenazas y el servidor Web. Específicamente, en un escenario de carga retardada, cuando el navegador carga una URL, el primer navegador obtiene, del servidor Web, una parte de todo el código de página correspondiente a la URL, y carga el código de página obtenido. El navegador en el aparato de detección de amenazas continúa, solo cuando un usuario arrastra una barra de desplazamiento hacia abajo o activa la página de visualización para deslizarse hacia abajo, para comunicarse con el servidor Web y obtener y cargar el código de página posterior.

Se puede aprender que, en el escenario de carga de retardo, el servidor Web divide todo el código de página correspondiente a la URL en varios segmentos de código de página. Para facilitar la descripción, en esta realización de esta solicitud, cada segmento de código de página dividido se denomina código de página. El servidor Web devuelve, de acuerdo con el mensaje de solicitud enviado por el aparato de detección de amenazas, el código de página correspondiente al mensaje de solicitud al aparato de detección de amenazas. El contenido representado por el código de página devuelto por el servidor Web cada vez se puede mostrar en al menos una página de visualización. Por lo tanto, el código de página devuelto por el servidor Web cada vez es el código de página de un grupo de páginas de visualización. El grupo de páginas de visualización en esta realización de esta solicitud incluye al menos una página de visualización.

En el escenario de carga de retardo, que el servidor Web divida todo el código de página correspondiente a la URL pertenece a la técnica anterior. Para obtener detalles, consulte las descripciones de la técnica anterior, y los detalles no se describen en esta realización de esta solicitud.

En esta realización de esta solicitud, cuando se carga la URL en el navegador del entorno de pruebas de Web, el aparato de detección de amenazas obtiene, del servidor Web, el código de página del primer grupo de páginas de visualización identificado por la URL. El código de página del primer grupo de páginas de visualización es una parte de todo el código de página correspondiente a la URL, y el código de página del primer grupo de páginas de visualización es el código de página obtenido por el aparato de detección de amenazas por primera vez cuando el navegador en esta realización de esta solicitud carga la URL.

Específicamente, en esta realización de esta solicitud, al cargar la URL en el navegador del entorno de pruebas de Web, el aparato de detección de amenazas obtiene, del servidor Web, el código de página del primer grupo de páginas de visualización identificado por la URL y el tamaño total ocupado por el primer grupo de páginas de visualización en el área de visualización del navegador, es decir, el aparato de detección de amenazas realiza S400.

Un método mediante el cual el aparato de detección de amenazas obtiene, desde el servidor Web, el código de página del primer grupo de páginas de visualización identificado por la URL es que el aparato de detección de amenazas envía, al servidor Web, el mensaje de solicitud que lleva la URL, y el servidor Web envía el código de página del primer grupo de páginas de visualización al aparato de detección de amenazas de acuerdo con la URL.

Opcionalmente, el código de página del primer grupo de páginas de visualización puede expresarse utilizando un lenguaje de secuencia de comandos JavaScript, o puede expresarse utilizando un lenguaje de secuencia de comandos VBScript (en inglés, Visual Basic Script), o puede expresarse utilizando cualquier otro lenguaje de secuencia de comandos utilizado para admitir contenido de la página Web. Esto no está específicamente limitado en esta realización de esta solicitud.

Después de obtener el código de página del primer grupo de páginas de visualización del servidor Web, el aparato de detección de amenazas obtiene además el tamaño total ocupado por el primer grupo de páginas de visualización en el área de visualización del navegador.

Opcionalmente, en esta realización de esta solicitud, el tamaño total ocupado por el primer grupo de páginas de visualización en el área de visualización del navegador puede ser un valor de altura de un área de página Web visible ocupada por el primer grupo de páginas de visualización en el área de visualización del navegador, o puede ser un valor de ancho de un área de página Web visible ocupada por el primer grupo de páginas de visualización en el área de visualización del navegador, o puede ser un valor de ancho de un texto de página Web completo ocupado por el primer grupo de páginas de visualización en el área de visualización del navegador. Esto no está específicamente

limitado en esta realización de esta solicitud.

Por ejemplo, si el código de página del primer grupo de páginas de visualización se expresa usando el lenguaje de secuencia de comandos JavaScript, el aparato de detección de amenazas puede obtener, usando una interfaz de documento *body. clientWidth*, el valor de ancho del área visible de la página Web ocupada por el primer grupo de páginas de visualización en el área de visualización del navegador; obtener, mediante el uso de una interfaz de documento *body. clientHeight*, el valor de altura del área visible de la página Web ocupada por el primer grupo de páginas de visualización en el área de visualización del navegador; y obtener, mediante el uso de una interfaz de documento *body. scrollWidth*, el valor de ancho de todo el texto de la página Web ocupado por el primer grupo de páginas de visualización en el área de visualización del navegador. Para definiciones de la interfaz de documento *body. clientWidth*, la interfaz de documento *body. clientHeight* y la interfaz de documento *body. scrollWidth*, consulte el protocolo de comunicaciones del navegador y los detalles no se describen en este documento.

En esta realización de esta solicitud, se puede establecer un sistema de coordenadas rectangulares en cualquier ubicación en una pantalla de visualización del aparato de detección de amenazas, y el sistema de coordenadas rectangulares incluye un eje X y un eje Y. Una dirección que está en cualquier página de visualización en el primer grupo de páginas de visualización y que es paralela al eje X del sistema de coordenadas rectangular puede definirse como ancho (o alto), y una dirección que está en la página de visualización y que es paralela al eje Y del sistema de coordenadas rectangular puede definirse como altura (o ancho).

Además, después de que el aparato de detección de amenazas obtiene el código de página del primer grupo de páginas de visualización, el aparato de detección de amenazas inyecta el código dinámico preestablecido en el código de página obtenido del primer grupo de páginas de visualización, es decir, el aparato de detección de amenazas realiza S401.

En esta realización de esta solicitud, un lenguaje de secuencia de comandos utilizado por el código dinámico preestablecido puede ser el mismo o diferente del lenguaje de secuencia de comandos utilizado por el código de página del primer grupo de páginas de visualización. Esto no está específicamente limitado en esta realización de esta solicitud. En esta realización de esta solicitud, solo necesita asegurarse de que tanto el código de página del primer grupo de páginas de visualización como el código dinámico preestablecido puedan ser identificados por el aparato de detección de amenazas.

Por ejemplo, si el código dinámico preestablecido se expresa utilizando el lenguaje de secuencia de comandos JavaScript, el código dinámico preestablecido puede ser el siguiente código:

```
<script type="text/javascript">        // código de carácter de inicio //
var pageHeight;                        // define una variable pageHeight //
var currentLocate=0;                   // define a variable currentLocate, utilizada para representar el tamaño ocupado por la página de visualización visualizada en el área de visualización del navegador //
var scrollTimer;                       // define a un temporizador scrollTimer //
scrollTimer=setInterval ("autoScrollDown(),10); // ejecuta una función autoScrollDown cada 10 milisegundos //
window.onload = function () {          // ejecuta si se abre una página Web //
pageHeight=document. body. scrollHeight;   // obtiene un valor alto de un área visible de la página Web ocupada por el código de página obtenido en el área de visualización del navegador, y asigna un valor de un pageHeight variable al valor de altura del área de la página Web visible //
}
función autoScrollDown ()              // define la función autoScrollDown //
{
If(currentLocate<pageHeight)
        {
currentLocate ++;
scroll(0,currentLocate));              // si un valor del currentLocate variable es menor que el valor de altura del área de página Web visible, desplácese automáticamente a la siguiente página de visualización //
```

```
        } else {
clearInterval(scrollTimer));        // de lo contrario, elimine el temporizador scrollTimer //
        }
}
</script>                           // carácter de fin de código //
```

Específicamente, bajo la premisa de que la correspondencia de etiquetas en el código de página del primer grupo de páginas de visualización no se ve afectada, en esta realización de esta solicitud, el aparato de detección de amenazas puede colocar el código dinámico preestablecido después de cualquier párrafo de secuencia de comandos en el código de página del primer grupo de páginas de visualización.

Opcionalmente, el aparato de detección de amenazas coloca el código dinámico preestablecido al final del código de página del primer grupo de páginas de visualización. De esta manera, una estructura original del código de página del primer grupo de páginas de visualización no se ve afectada, y es fácil de identificar para un desarrollador. Además, en una aplicación real, la implementación del código es elativamente simple.

Además, opcionalmente, en esta realización de esta solicitud, un proceso en el que el aparato de detección de amenazas inyecta el código dinámico preestablecido en el código de página del primer grupo de páginas de visualización puede ser que el aparato de detección de amenazas inyecte el código dinámico preestablecido en el código de página del primer grupo de páginas de visualización al recibir, mediante una interfaz de zócalo (Zócalo), el código de página que es del primer grupo de páginas de visualización y que envía el servidor Web.

Un proceso en el que el aparato de detección de amenazas carga la URL en el navegador en el entorno de pruebas de Web puede considerarse como un proceso de comunicación entre el navegador en el aparato de detección de amenazas y el servidor Web. Específicamente, el navegador crea una interfaz de Zócalo entre el navegador y el servidor Web, y envía un paquete de solicitud HTTP al servidor Web de acuerdo con las especificaciones del Protocolo de transferencia de hipertexto (en inglés, Hypertext Transfer Protocol - HTTP). El servidor Web analiza, de acuerdo con las especificaciones HTTP, el paquete de solicitud HTTP enviado por el navegador, y envía un mensaje de respuesta al navegador, donde el mensaje de respuesta incluye código de página, como un documento JavaScript. El navegador analiza el código de la página en el mensaje de respuesta y procesa, mediante representación, el código de la página en una página correspondiente del lenguaje de marcado de hipertexto (en inglés, HyperText Markup Language - HTML).

Específicamente, en esta realización de esta solicitud, al recibir, mediante el uso de la interfaz de Zócalo, el mensaje de respuesta enviado por el servidor Web, el aparato de detección de amenazas primero determina si el mensaje de respuesta incluye el código de página del primer grupo de páginas de visualización. Si el mensaje de respuesta incluye el código de página del primer grupo de páginas de visualización, el aparato de detección de amenazas inyecta el código dinámico preestablecido en el código de página del primer grupo de páginas de visualización.

Opcionalmente, en esta realización de esta solicitud, se establece un programa de enganche en el aparato de detección de amenazas. El programa de enganche conecta una función de procesamiento de protocolo de capa de red del entorno de pruebas de Web del aparato de detección de amenazas, y el programa de enganche se utiliza para interceptar el código de página del primer grupo de páginas de visualización. En esta realización de esta solicitud, un proceso en el que el aparato de detección de amenazas inyecta el código dinámico preestablecido en el código de página del primer grupo de páginas de visualización puede ser que el aparato de detección de amenazas inyecte el código dinámico preestablecido en el código de páginas del primer grupo de páginas de visualización cuando el programa de enganche obtiene el código de página del primer grupo de páginas de visualización.

Puede entenderse que el entorno de pruebas de Web es equivalente a una copia de un sistema operativo del aparato de detección de amenazas. Por lo tanto, el entorno de pruebas de Web también incluye capas de protocolo de comunicaciones. En esta realización de esta solicitud, una capa de red del entorno de pruebas de Web es una capa de protocolo que tiene una función de una capa de red en un modelo de Protocolo de Control de Transmisión/Protocolo de Internet (en inglés, Transmission Control Protocol/Internet Protoco – TCP/IP).

Por ejemplo, si el entorno de pruebas de Web del aparato de detección de amenazas se ejecuta en un sistema Linux, se establece un programa de enganche NF_IP_LOCAL_IN de un mecanismo de filtro de red Linux en el aparato de detección de amenazas, y el programa de enganche NF_IP_LOCAL_IN engancha la función de procesamiento del protocolo de capa de red del entorno de prueba de Web. El aparato de detección de amenazas inyecta el código dinámico preestablecido en el código de página del primer grupo de páginas de visualización cuando el programa de enganche NF_IP_LOCAL_IN obtiene el código de página del primer grupo de páginas de visualización.

Opcionalmente, en esta realización de esta solicitud, se establece un programa de enganche en el aparato de detección de amenazas. El programa de enganche engancha un núcleo del navegador del entorno de pruebas de Web y el programa de enganche se utiliza para interceptar el código de página del primer grupo de páginas de

visualización. En esta realización de esta solicitud, un proceso en el que el aparato de detección de amenazas inyecta el código dinámico preestablecido en el código de página del primer grupo de páginas de visualización puede ser que el aparato de detección de amenazas inyecte el código dinámico preestablecido en el código de páginas del primer grupo de páginas de visualización cuando el programa de enganche obtiene el código de página del primer grupo de páginas de visualización.

Específicamente, el aparato de detección de amenazas inyecta el código dinámico preestablecido en el código de página del primer grupo de páginas de visualización después de que el entorno de pruebas de Web del aparato de detección de amenazas obtenga el código de página del primer grupo de páginas de visualización, antes de que el navegador en el entorno de pruebas de Web comience a analizar y representar el código de página del primer grupo de páginas de visualización, y cuando el programa de enganche que engancha el núcleo del navegador del entorno de pruebas de Web intercepta el código de página del primer grupo de páginas de visualización.

Por ejemplo, si el navegador en el entorno de pruebas de Web es un navegador Webkit, un núcleo del navegador del navegador Webkit tiene una interfaz de Cargador de Recurso vacío::ha Recibido Datos (Manipulador de Recurso*, datos de carácter* constante, longitud de enteros, Longitud de Datos de enteros codificados), y se establece un programa de enganche en el aparato de detección de amenazas para enganchar el núcleo del navegador del navegador Webkit. Cuando el programa de enganche obtiene el código de página del primer grupo de páginas de visualización desde un parámetro de datos en la interfaz Cargador de Recurso vacío:: ha Recibido Datos (Manipulador de Recurso*, datos de carácter* constante, longitud de enteros, Longitud de Datos de enteros codificados), el aparato de detección de amenazas inyecta el código dinámico preestablecido en el código de página que es del primer grupo de páginas de visualización y que se indica mediante el parámetro de datos.

Independientemente de un momento en el que el aparato de detección de amenazas inyecte el código dinámico preestablecido en el código de página del primer grupo de páginas de visualización, el aparato de detección de amenazas puede obtener el código de página que es del primer grupo de páginas de visualización y que incluye el código dinámico preestablecido.

Después de que el aparato de detección de amenazas obtiene el código de página que es del primer grupo de páginas de visualización y que incluye el código dinámico preestablecido, el aparato de detección de amenazas analiza y ejecuta el código de página que es del primer grupo de páginas de visualización y que incluye el código dinámico preestablecido, y muestra secuencialmente las páginas de visualización en el primer grupo de páginas de visualización, es decir, el aparato de detección de amenazas realiza S402.

En esta realización de esta solicitud, el código dinámico preestablecido se usa para activar el cambio de la página de visualización actual a la siguiente página de visualización de la página de visualización actual, es decir, el código dinámico preestablecido puede implementar la función de desplazamiento automático desde página de visualización actual a la siguiente página de visualización de la página de visualización actual, y la función es equivalente a un proceso de interacción hombre-máquina.

De las descripciones anteriores se puede aprender que el primer grupo de páginas de visualización incluye al menos una página de visualización. Por lo tanto, cuando el aparato de detección de amenazas analiza y ejecuta el código de página que es del primer grupo de páginas de visualización y que incluye el código dinámico preestablecido, el aparato de detección de amenazas muestra secuencialmente las páginas de visualización en el primer grupo de páginas de visualización.

Además, cuando el aparato de detección de amenazas analiza y ejecuta el código de página que es del primer grupo de páginas de visualización y que incluye el código dinámico preestablecido, el aparato de detección de amenazas supervisa un cambio del valor de la variable de visualización.

Se puede aprender de las descripciones anteriores que el valor de la variable de visualización se usa para representar el tamaño ocupado, en el área de visualización del navegador, por las páginas de visualización que se han mostrado desde la ubicación de inicio de la primera página de visualización la a la página de visualización actual en el primer grupo de páginas de visualización. Se entiende fácilmente que cuando el aparato de detección de amenazas muestra secuencialmente las páginas de visualización en el primer grupo de páginas de visualización, el valor de la variable de visualización aumenta gradualmente.

El valor de la variable de visualización puede representar un valor de ancho de un área de página Web visible ocupada por una página de visualización visualizada en el área de visualización del navegador, o puede representar un valor de altura de un área de página Web visible ocupada por una página de visualización visualizada en el área de visualización del navegador.

Específicamente, cuando el aparato de detección de amenazas detecta que el valor de la variable de visualización es mayor o igual que el valor preestablecido, el aparato de detección de amenazas envía el mensaje de solicitud al servidor Web, es decir, el aparato de detección de amenazas realiza S403.

El mensaje de solicitud enviado por el aparato de detección de amenazas lleva un identificador de grupo de páginas de visualización, y el servidor Web determina, de acuerdo con el identificador de grupo de páginas de visualización, el

código de página que es de un grupo de páginas de visualización y que debe obtener el aparato de detección de amenazas.

El identificador del grupo de páginas de visualización puede ser un identificador del primer grupo de páginas de visualización, o puede ser un identificador del segundo grupo de páginas de visualización. Esto no está específicamente limitado en esta realización de esta solicitud. En esta realización de esta solicitud, si el mensaje de solicitud lleva el identificador del primer grupo de páginas de visualización, el servidor Web busca, de acuerdo con el identificador del primer grupo de páginas de visualización, el código de página del segundo grupo de páginas de visualización después del primer grupo de páginas de visualización identificado por el identificador del primer grupo de páginas de visualización y devuelve el código de página del segundo grupo de páginas de visualización. En esta realización de esta solicitud, si el mensaje de solicitud lleva el identificador del segundo grupo de páginas de visualización, el servidor Web busca, de acuerdo con el identificador del segundo grupo de páginas de visualización, el código de página del segundo grupo de páginas de visualización identificado por el identificador del segundo grupo de páginas de visualización y devuelve el código de página del segundo grupo de páginas de visualización.

En esta realización de esta solicitud, si el identificador del grupo de páginas de visualización incluido en el mensaje de solicitud es el identificador del segundo grupo de páginas de visualización, el identificador del grupo de páginas de visualización puede ser un orden de visualización del segundo grupo de páginas de visualización en todos los grupos de páginas de visualización, o puede ser información de índice del segundo grupo de páginas de visualización. Esto no está específicamente limitado en esta realización de esta solicitud.

Por ejemplo, si el orden de visualización del segundo grupo de páginas de visualización en todos los grupos de páginas de visualización es 2, el mensaje de solicitud puede llevar el código de operación “*get page2*”.

Además, después de que el aparato de detección de amenazas envía el mensaje de solicitud al servidor Web, el servidor Web envía el mensaje de respuesta al aparato de detección de amenazas en respuesta al mensaje de solicitud, donde el mensaje de respuesta lleva el código de página del segundo grupo de páginas de visualización, es decir, se realiza S404.

En consecuencia, el aparato de detección de amenazas puede obtener el código de página del segundo grupo de páginas de visualización.

Además, el aparato de detección de amenazas detecta, en el entorno de pruebas de la Web, si el código de página del segundo grupo de páginas de visualización lleva código de ataque, es decir, el aparato de detección de amenazas realiza S405.

Para un proceso en el que el aparato de detección de amenazas detecta, en el entorno de prueba de Web, si el código de página del segundo grupo de páginas de visualización contiene código de ataque, consulte un principio de detección existente de un entorno de pruebas de Web, y los detalles no se describen en este documento.

El código de página del segundo grupo de páginas de visualización es el código de página cargado con retardo. Por lo tanto, de acuerdo con el método de detección de amenazas provisto en esta solicitud, el aparato de detección de amenazas puede detectar si una página de carga de retardo lleva un código de ataque y si se evita un problema de detección perdido del entorno de pruebas de la Web.

Después de que el aparato de detección de amenazas obtiene el código de página del segundo grupo de páginas de visualización, el código de página del primer grupo de páginas de visualización y el código de página del segundo grupo de páginas de visualización se combinan en una sola pieza de código de página. En este caso, el aparato de detección de amenazas continúa ejecutando el código dinámico preestablecido. Por lo tanto, el aparato de detección de amenazas continúa cambiando automáticamente la página de visualización. Cuando el aparato de detección de amenazas cambia automáticamente la página de visualización, el aparato de detección de amenazas se activa para continuar interactuando con el servidor Web, obtener el código de página de un grupo de páginas de visualización posterior y detectar el código de página del grupo de páginas de visualización posterior, hasta que todas las páginas de visualización se carguen correspondientemente a la URL y luego finaliza el proceso.

Por ejemplo, si el código dinámico preestablecido es el código que se muestra en el ejemplo anterior, en el código dinámico preestablecido que se muestra en el ejemplo anterior, si el valor de la variable *currentLocate* es menor que el valor de la variable *pageHeight*, la página de visualización actual automáticamente se desplaza a la siguiente página de visualización. Después de que el aparato de detección de amenazas obtiene el código de página del segundo grupo de páginas de visualización, el valor de la *pageHeight* variable obtenida por el aparato de detección de amenazas aumenta en consecuencia. Por lo tanto, el aparato de detección de amenazas continúa cambiando automáticamente la página de visualización.

De las descripciones anteriores se puede aprender que, de acuerdo con el método de detección de amenazas provisto en esta realización de esta solicitud, el aparato de detección de amenazas puede obtener un código de página cargado con retardo en el entorno de pruebas de Web, y puede detectar, en el entorno de pruebas de Web, si el retardo El código de página cargado lleva el código de ataque. De esta forma, se evita el problema de detección perdida del entorno de pruebas de Web.

Una realización de esta solicitud proporciona un aparato 1 de detección de amenazas. El aparato 1 de detección de amenazas está configurado para realizar los pasos realizados por el aparato de detección de amenazas en el método de detección de amenazas anterior. El aparato 1 de detección de amenazas puede incluir módulos correspondientes a los pasos correspondientes.

Como se muestra en la figura 5, el aparato 1 de detección de amenazas incluye una unidad 50 de procesamiento, una unidad 51 de visualización, una unidad 52 de envío y una unidad 53 de recepción.

La unidad 50 de procesamiento está configurada para: al cargar un localizador uniforme de recursos URL en un navegador de un entorno de pruebas de Web, obtener, desde un servidor Web, el código de página de un primer grupo de páginas de visualización identificado por la URL y un tamaño total ocupado por el primer grupo de páginas de visualización en un área de visualización del navegador, donde el código de página del primer grupo de páginas de visualización incluye código de monitorización, el código de monitorización se usa para obtener y monitorear un valor de una variable de visualización, y el valor de la variable de visualización se usa para representar un tamaño ocupado, en el área de visualización del navegador, por páginas de visualización que se han visualizado desde una ubicación de inicio de una primera página de visualización a una página de visualización actual en el primer grupo de páginas de visualización; configurado para inyectar código dinámico preestablecido en el código de página del primer grupo de páginas de visualización, donde el código dinámico preestablecido se usa para activar el cambio de la página de visualización actual a la siguiente página de visualización de la página de visualización actual; y configurado para analizar y ejecutar el código de página que es del primer grupo de páginas de visualización y que incluye el código dinámico preestablecido.

La unidad 51 de visualización está configurada para mostrar, de manera secuencial, páginas de visualización en el primer grupo de páginas de visualización de acuerdo con el código de página, analizado y ejecutado por la unidad 50 de procesamiento, que es del primer grupo de páginas de visualización y que incluye el preajuste código dinámico

La unidad 52 de envío está configurada para enviar un mensaje de solicitud al servidor Web cuando la unidad 50 de procesamiento detecta, utilizando el código de monitorización, que el valor de la variable de visualización es mayor o igual a un valor preestablecido, donde el mensaje de solicitud es utilizado para solicitar obtener el código de página de un segundo grupo de páginas de visualización del servidor Web, una primera página de visualización en el segundo grupo de páginas de visualización es una página de visualización siguiente de una última página de visualización en el primer grupo de páginas de visualización, y el valor predeterminado el valor es mayor o igual que un tamaño ocupado por la primera página de visualización en el primer grupo de páginas de visualización en el área de visualización del navegador y menor que el tamaño total ocupado por el primer grupo de páginas de visualización en el área de visualización del navegador.

La unidad 53 de recepción está configurada para recibir un mensaje de respuesta enviado por el servidor Web, donde el mensaje de respuesta incluye el código de página del segundo grupo de páginas de visualización.

La unidad 50 de procesamiento está configurada además para detectar, en el entorno de prueba de Web, si el código de página que es del segundo grupo de páginas de visualización y que es recibido por la unidad 53 de recepción lleva un código de ataque.

Además, la unidad 50 de procesamiento está configurada específicamente para recibir, usando una interfaz de Zócalo, el código de página que es del primer grupo de páginas de visualización identificado por la URL y que es enviado por el servidor Web.

Opcionalmente, en esta realización de esta solicitud, se establece un programa de enganche en el aparato 1 de detección de amenazas para enganchar una función de procesamiento de protocolo de capa de red del entorno de pruebas de Web, y el programa de enganche se usa para interceptar el código de página del primer grupo de páginas de visualización. La unidad 50 de procesamiento está configurada específicamente para inyectar el código dinámico preestablecido en el código de página del primer grupo de páginas de visualización cuando el programa de enganche obtiene el código de página del primer grupo de páginas de visualización.

Opcionalmente, en esta realización de esta solicitud, se establece un programa de enganche en el aparato 1 de detección de amenazas para enganchar un núcleo del navegador del entorno de prueba de Web, y el programa de enganche se usa para interceptar el código de página del primer grupo de páginas de visualización. La unidad 50 de procesamiento está configurada específicamente para inyectar el código dinámico preestablecido en el código de página del primer grupo de páginas de visualización cuando el programa de enganche obtiene el código de página del primer grupo de páginas de visualización.

Opcionalmente, el código dinámico preestablecido se coloca al final del código de página del primer grupo de páginas de visualización.

Puede entenderse que el aparato 1 de detección de amenazas en esta realización de esta solicitud está simplemente dividido lógicamente de acuerdo con las funciones implementadas por el aparato 1 de detección de amenazas. En una aplicación real, las unidades anteriores pueden superponerse o dividirse.

La función implementada por el aparato 1 de detección de amenazas provisto en esta realización de esta solicitud está en una correspondencia uno a uno con el método de detección de amenazas provisto en la realización anterior. Un proceso de procesamiento más detallado implementado por el aparato 1 de detección de amenazas se ha descrito en detalle en la realización del método anterior, y los detalles no se describen aquí nuevamente.

Otra realización de esta solicitud proporciona un aparato de detección de amenazas. Como se muestra en la figura 6, el aparato de detección de amenazas incluye un circuito 60 de interfaz, un procesador 61, una memoria 62, un bus 63 de sistema y una pantalla 64.

El circuito 60 de interfaz, el procesador 61, la memoria 62 y la pantalla 64 se conectan utilizando el bus 63 del sistema y se completa la comunicación mutua.

Un experto en la materia puede comprender que una estructura del aparato de detección de amenazas que se muestra en la figura 6 no constituye ninguna limitación al aparato de detección de amenazas. El aparato de detección de amenazas puede incluir componentes más o menos que los mostrados en la figura 6, o combinar algunos componentes, o tener diferentes arreglos de componentes.

Específicamente, cuando el aparato de detección de amenazas funciona, el aparato de detección de amenazas ejecuta el método de detección de amenazas en la realización mostrada en la figura 4. Para el método de detección de amenazas específico, consulte las descripciones relacionadas en la realización mostrada en la figura 4, y los detalles no se describen aquí nuevamente.

En esta realización de esta solicitud, se establece un entorno de pruebas de Web en el aparato de detección de amenazas.

Con referencia a la realización anterior, el circuito 60 de interfaz en esta realización de esta solicitud puede ser la unidad 52 de envío en la realización anterior, y puede ser la unidad 53 de recepción en la realización anterior.

Específicamente, el circuito 60 de interfaz está configurado para implementar una conexión de comunicación entre el aparato de detección de amenazas y un servidor Web.

Con referencia a la realización anterior, la memoria 62 en esta realización de esta solicitud puede ser la unidad 50 de procesamiento en la realización anterior.

Específicamente, la memoria 62 puede configurarse para almacenar un programa de software y un módulo de aplicación. Al ejecutar el programa de software y el módulo de aplicación que están almacenados en la memoria 62, el procesador 61 ejecuta varias aplicaciones funcionales del aparato de detección de amenazas y procesa datos.

La memoria 62 puede incluir principalmente un área 620 de almacenamiento de programas y un área 621 de almacenamiento de datos. El área 620 de almacenamiento de programas puede almacenar un sistema operativo, un programa de aplicación requerido por al menos una función, tal como la función de enviar un mensaje de solicitud. El área 621 de almacenamiento de datos puede almacenar el código de página enviado por el servidor Web, por ejemplo, guardar el código de página de un primer grupo de páginas de visualización y el código de página de un segundo grupo de páginas de visualización.

La memoria 62 puede incluir una memoria volátil, tal como una memoria de acceso aleatorio de alta velocidad (en inglés, Random Access Memory - RAM). La memoria 62 también puede incluir una memoria no volátil, tal como al menos un componente de almacenamiento de disco magnético, un componente de memoria flash u otro componente de almacenamiento de estado sólido volátil. Esto no está específicamente limitado en esta realización de esta solicitud.

Con referencia a la realización anterior, el procesador 61 en esta realización de esta solicitud puede ser la unidad 50 de procesamiento en la realización anterior.

Específicamente, el procesador 61 es un centro de control del aparato de detección de amenazas.

El procesador 61 está conectado a todas las partes de todo el aparato de detección de amenazas mediante el uso de varias interfaces y líneas. El procesador 62 corre o ejecuta el programa de software y/o el módulo de aplicación almacenado en la memoria 62, e invoca los datos almacenados en la memoria 62, para ejecutar diversas funciones del aparato de detección de amenazas y procesar datos, para monitorear todo el aparato de detección de amenazas.

Opcionalmente, el procesador 61 puede ser una unidad de procesamiento central (en inglés, Central Processing Unit - CPU). El procesador 61 también puede ser otro procesador general, un procesador de señal digital (en inglés, Digital Signal Processor - DSP) u otro dispositivo lógico programable o dispositivo lógico de transistor, un componente de hardware discreto o similar. Esto no está específicamente limitado en esta realización de esta solicitud.

El procesador general puede ser un microprocesador, o el procesador puede ser cualquier procesador convencional o similar.

El bus 63 del sistema puede incluir un bus de datos, un bus de alimentación, un bus de control, un bus de estado de

señal o similar.

En esta realización de esta solicitud, para una descripción clara, varios buses están representados por el bus 63 de sistema en la figura 6)

Con referencia a la realización anterior, la pantalla 64 en esta realización de esta solicitud puede ser la unidad 51 de visualización en la realización anterior.

Esta realización de esta solicitud proporciona el aparato de detección de amenazas. El aparato de detección de amenazas almacena código dinámico preestablecido, y el código dinámico preestablecido se usa para activar el aparato de detección de amenazas para cambiar de una página de visualización actual a una página de visualización siguiente de la página de visualización actual. Por lo tanto, cuando se ejecuta el código de página del primer grupo de páginas de visualización y el código dinámico preestablecido, el aparato de detección de amenazas muestra, de manera secuencial, páginas de visualización en el primer grupo de páginas de visualización. Cuando el aparato de detección de amenazas detecta que el valor de una variable de visualización es mayor o igual que un valor preestablecido, el aparato de detección de amenazas interactúa con el servidor Web para obtener el código de página del segundo grupo de páginas de visualización. De esta manera, en un escenario de carga de retardo, el aparato de detección de amenazas puede obtener el código de página cargado con retardo en el entorno de pruebas de Web, de modo que el aparato de detección de amenazas detecta, en el entorno de pruebas de Web, si el código de página cargado con retardo lleva código de ataque, y se evita la detección perdida en el entorno de prueba de Web por parte del aparato de detección de amenazas en el código de página cargado con retardo.

Cuando el método de detección de amenazas en la realización mostrada en la figura 4 se implementa en forma de un módulo funcional de software y se vende o utiliza como un producto independiente, el método de detección de amenazas puede almacenarse en un medio de almacenamiento legible por ordenador. En base a tal comprensión, una persona experta en la técnica debe comprender que las realizaciones de esta solicitud pueden proporcionarse como un método, un dispositivo electrónico o un producto de programa de ordenador. Por lo tanto, esta solicitud puede usar una forma de realizaciones solo de hardware, realizaciones solo de software o realizaciones con una combinación de software y hardware. Además, esta solicitud puede usar una forma de un producto de programa de ordenador implementado en uno o más medios de almacenamiento legibles por ordenador que incluyen código de programa. El medio de almacenamiento del ordenador incluye, entre otros, una memoria flash USB, un disco duro extraíble, una memoria de solo lectura (en inglés, Read Only Memory - ROM), una memoria de disco magnético, un CD-ROM, una memoria óptica o similares.

En consecuencia, esta realización de esta solicitud proporciona además un medio de almacenamiento legible por ordenador, y el medio de almacenamiento legible por ordenador incluye una o más piezas de código de programa. Cuando el procesador en el aparato de detección de amenazas ejecuta el código del programa, el aparato de detección de amenazas ejecuta el método de detección de amenazas que se muestra en la figura 4)

Una realización de esta solicitud proporciona además un sistema de red. Como se muestra en la figura 7, el sistema de red incluye al menos un aparato de detección de amenazas de acuerdo con las realizaciones anteriores y un servidor Web.

Específicamente, el servidor Web está configurado para enviar el código de página correspondiente al aparato de detección de amenazas de acuerdo con una solicitud enviada por el aparato de detección de amenazas, de modo que el aparato de detección de amenazas detecte, en un entorno de pruebas de Web, si el código de página recibido de un grupo de página de visualización lleva el código de ataque.

Opcionalmente, el servidor Web envía, al aparato de detección de amenazas de acuerdo con un localizador uniforme de recursos URL enviado por el aparato de detección de amenazas, el código de página de un primer grupo de páginas de visualización identificado por la URL. El servidor Web envía el código de página de un segundo grupo de páginas de visualización al aparato de detección de amenazas de acuerdo con un mensaje de solicitud enviado por el aparato de detección de amenazas y que se utiliza para solicitar obtener el código de página del segundo grupo de páginas de visualización.

Un proceso de procesamiento más detallado implementado por el servidor Web se ha descrito en detalle en la realización anterior, y los detalles no se describen aquí nuevamente.

Un proceso de procesamiento más detallado implementado por el aparato de detección de amenazas se ha descrito en detalle en la realización anterior, y los detalles no se describen aquí nuevamente.

Esta realización de esta solicitud proporciona el sistema de red. El aparato de detección de amenazas en el sistema de red almacena el código dinámico preestablecido, y el código dinámico preestablecido se usa para activar el aparato de detección de amenazas para cambiar de una página de visualización actual a una página de visualización siguiente de la página de visualización actual. Por lo tanto, cuando se ejecuta el código de página del primer grupo de páginas de visualización y el código dinámico preestablecido, el aparato de detección de amenazas muestra, de manera secuencial, páginas de visualización en el primer grupo de páginas de visualización. Cuando el aparato de detección de amenazas detecta que el valor de una variable de visualización es mayor o igual que un valor preestablecido, el

aparato de detección de amenazas interactúa con el servidor Web para obtener el código de página del segundo grupo de páginas de visualización. De esta manera, en un escenario de carga de retardo, el aparato de detección de amenazas puede obtener el código de página cargado con retardo en el entorno de pruebas de Web, de modo que el aparato de detección de amenazas detecta, en el entorno de pruebas de Web, si el código de página cargado con retardo lleva código de ataque, y si se evita la detección perdida en el entorno de prueba de Web por parte del aparato de detección de amenazas en el código de página cargado con retardo.

Las descripciones anteriores sobre implementaciones permiten a una persona experta en la técnica comprender que, con el propósito de una descripción conveniente y breve, la división de los módulos de funciones anteriores se toma como un ejemplo a modo de ilustración. En la aplicación real, las funciones anteriores pueden asignarse a diferentes módulos e implementarse de acuerdo con un requisito, es decir, una estructura interna de un aparato se divide en diferentes módulos de función para implementar todas o parte de las funciones descritas anteriormente. Para un proceso de trabajo detallado del sistema, aparato y unidad anteriores, se puede hacer referencia a un proceso correspondiente en las realizaciones del método anterior, y los detalles no se describen aquí nuevamente.

En las diversas realizaciones proporcionadas en esta solicitud, debe entenderse que el sistema, el aparato y el método divulgados pueden implementarse de otras maneras.

Por ejemplo, la realización del aparato descrito es simplemente un ejemplo. Por ejemplo, la división de unidad o módulo es meramente una división de función lógica y puede ser otra división en la implementación real. Por ejemplo, una pluralidad de unidades o componentes pueden combinarse o integrarse en otro sistema, o algunas características pueden ignorarse o no realizarse. Además, los acoplamientos mutuos mostrados o discutidos o los acoplamientos directos o las conexiones de comunicación pueden implementarse utilizando algunas interfaces. Los acoplamientos indirectos o las conexiones de comunicación entre los aparatos o unidades pueden implementarse en forma electrónica, mecánica u otras formas.

Las unidades descritas como partes separadas pueden o no estar físicamente separadas, y las partes mostradas como unidades pueden o no ser unidades físicas, pueden estar ubicadas en una posición o pueden distribuirse en una pluralidad de unidades de red. Algunas o todas las unidades pueden seleccionarse de acuerdo con los requisitos reales para lograr los objetivos de las soluciones de las realizaciones.

Además, las unidades funcionales en las realizaciones de esta solicitud pueden integrarse en una unidad de procesamiento, o cada una de las unidades puede existir solo físicamente, o dos o más unidades están integradas en una unidad. La unidad integrada puede implementarse en forma de hardware, o puede implementarse en forma de una unidad funcional de software.

Cuando la unidad integrada se implementa en forma de una unidad funcional de software y se vende o utiliza como un producto independiente, la unidad integrada puede almacenarse en un medio de almacenamiento legible por ordenador.

Sobre la base de tal comprensión, las soluciones técnicas de la presente invención esencialmente, o la parte que contribuye a la técnica anterior, o la totalidad o parte de las soluciones técnicas pueden implementarse en forma de un producto de software. El producto de software se almacena en un medio de almacenamiento e incluye varias instrucciones para instruir a un dispositivo informático (que puede ser un ordenador personal, un servidor o un dispositivo de red) o un procesador para realizar todos o parte de los pasos de los métodos descritos. en las realizaciones de la presente invención. El medio de almacenamiento anterior incluye: cualquier medio que pueda almacenar código de programa, como una memoria flash USB, un disco duro extraíble, una memoria de solo lectura (en inglés, Read Only Memory - ROM), una memoria de acceso aleatorio (en inglés, Random Access Memory - RAM), un disco magnético o un disco óptico.

Aunque se han descrito algunas realizaciones de esta solicitud, una persona experta en la técnica puede hacer cambios y modificaciones a estas realizaciones una vez que aprenden el concepto inventivo básico. Por lo tanto, las siguientes reivindicaciones están destinadas a ser interpretadas para cubrir las realizaciones y todos los cambios y modificaciones que caen dentro del alcance de esta solicitud.

Obviamente, una persona experta en la técnica puede realizar diversas modificaciones y variaciones a esta solicitud sin apartarse del alcance de esta solicitud. Esta solicitud está destinada a cubrir estas modificaciones y variaciones de esta solicitud, siempre que entren dentro del alcance de protección definido por las siguientes afirmaciones y sus tecnologías equivalentes.

REIVINDICACIONES

1. Un método de detección de amenazas que se aplica a un escenario de carga de retardo, el método comprende:

al cargar un localizador uniforme de recursos, URL, en un navegador de un entorno de pruebas de Web, obteniendo, mediante un aparato de detección de amenazas de un servidor Web, el código de página de un primer grupo de páginas de visualización identificado por la URL y un tamaño total ocupado por el primer grupo de páginas de visualización en un área de visualización del navegador, en donde el código de página del primer grupo de páginas de visualización comprende un código de monitorización, el código de monitorización se utiliza para obtener y monitorizar un valor de una variable de visualización, y el valor de la variable de visualización se utiliza para representar un tamaño ocupado, en el área de visualización del navegador, por páginas de visualización que se han visualizado desde una ubicación inicial de una primera página de visualización a una página de visualización actual en el primer grupo de páginas de visualización;

inyectar, mediante el aparato de detección de amenazas, código dinámico preestablecido en el código de página del primer grupo de páginas de visualización, en donde el código dinámico preestablecido se usa para activar el cambio de la página de visualización actual a una página de visualización siguiente de la página de visualización actual;

analizar y ejecutar, mediante el aparato de detección de amenazas, el código de página que es del primer grupo de páginas de visualización y que comprende el código dinámico preestablecido, y mostrar, de manera secuencial, páginas de visualización en el primer grupo de páginas de visualización;

enviar un mensaje de solicitud al servidor Web si el aparato de detección de amenazas detecta, utilizando el código de monitorización, que el valor de la variable de visualización es mayor o igual a un valor preestablecido, en donde el mensaje de solicitud se utiliza para solicitar obtener el código de página de un segundo grupo de páginas de visualización desde el servidor Web, una primera página de visualización en el segundo grupo de páginas de visualización es la siguiente página de visualización de una última página de visualización en el primer grupo de páginas de visualización, y el valor preestablecido es mayor o igual a un tamaño ocupado por la primera página de visualización en el primer grupo de páginas de visualización en el área de visualización del navegador y menor que el tamaño total ocupado por el primer grupo de páginas de visualización en el área de visualización del navegador;

recibir, por el aparato de detección de amenazas, un mensaje de respuesta enviado por el servidor Web, en donde el mensaje de respuesta lleva el código de página del segundo grupo de páginas de visualización; y

detectar, mediante el aparato de detección de amenazas en el entorno de prueba de Web, si el código de página del segundo grupo de páginas de visualización lleva código de ataque.

2. El método de detección de amenazas según la reivindicación 1, en donde la obtención, por un aparato de detección de amenazas de un servidor Web, el código de página de un primer grupo de páginas de visualización identificado por la URL comprende:

recibir, mediante el aparato de detección de amenazas usando una interfaz de Zócalo, el código de página que es del primer grupo de páginas de visualización identificado por la URL y que es enviado por el servidor Web.

3. El método de detección de amenazas de acuerdo con la reivindicación 1 o 2, en donde un programa de enganche está configurado para enganchar una función de procesamiento de protocolo de capa de red del entorno de prueba de Web, y el programa de enganche se usa para interceptar el código de página del primer grupo de páginas de visualización; y

la inyección, mediante el aparato de detección de amenazas, del código dinámico preestablecido en el código de página del primer grupo de páginas de visualización comprende:

inyectar, mediante el aparato de detección de amenazas, el código dinámico preestablecido en el código de página del primer grupo de páginas de visualización cuando el programa de enganche obtiene el código de página del primer grupo de páginas de visualización.

4. El método de detección de amenazas de acuerdo con la reivindicación 1 o 2, en donde un programa de enganche está configurado para enganchar un núcleo del navegador del entorno de prueba de Web, y el programa de enganche se usa para interceptar el código de página del primer grupo de páginas de visualización; y

la inyección, mediante el aparato de detección de amenazas, del código dinámico preestablecido en el código de página del primer grupo de páginas de visualización comprende:

inyectar, mediante el aparato de detección de amenazas, el código dinámico preestablecido en el código de página del primer grupo de páginas de visualización cuando el programa de enganche obtiene el código de página del primer grupo de páginas de visualización.

5. El método de detección de amenazas de acuerdo con una cualquiera de las reivindicaciones 1 a 4, en donde el código dinámico se coloca al final del código de página del primer grupo de páginas de visualización.

6. Un aparato de detección de amenazas que se aplica a un escenario de carga de retardo, el aparato de detección de amenazas comprende:

una unidad de procesamiento, configurada para: al cargar un localizador uniforme de recursos, URL, en un navegador de un entorno de pruebas de Web, obtenga, de un servidor Web, el código de página de un primer grupo de páginas de visualización identificado por la URL y un tamaño total ocupado por el primer grupo de páginas de visualización en un área de visualización del navegador, en donde el código de página del primer grupo de páginas de visualización comprende un código de monitorización, el código de monitorización se utiliza para obtener y monitorizar un valor de una variable de visualización, y el valor de la variable de visualización se utiliza para representar un tamaño ocupado, en el área de visualización del navegador, por páginas de visualización que se han visualizado desde una ubicación de inicio de una primera página de visualización a una página de visualización actual en el primer grupo de páginas de visualización; configurado para inyectar código dinámico preestablecido en el código de página del primer grupo de páginas de visualización, en donde el código dinámico preestablecido se usa para activar el cambio de la página de visualización actual a la siguiente página de visualización de la página de visualización actual; y configurado para analizar y ejecutar el código de página que es del primer grupo de páginas de visualización y que comprende el código dinámico preestablecido;

una unidad de visualización, configurada para mostrar, de manera secuencial, páginas de visualización en el primer grupo de páginas de visualización de acuerdo con el código de página, analizado y ejecutado por la unidad de procesamiento, que es del primer grupo de páginas de visualización y que comprende el código dinámico preestablecido;

una unidad de envío, configurada para enviar un mensaje de solicitud al servidor Web cuando la unidad de procesamiento detecta, utilizando el código de monitorización, que el valor de la variable de visualización es mayor o igual que un valor preestablecido, en donde el mensaje de solicitud se utiliza para solicitar obtener el código de página de un segundo grupo de páginas de visualización del servidor Web, una primera página de visualización en el segundo grupo de páginas de visualización es una siguiente página de visualización de una última página de visualización en el primer grupo de páginas de visualización, y el valor predeterminado es mayor o igual que un tamaño ocupado por la primera página de visualización en el primer grupo de páginas de visualización en el área de visualización del navegador y menor que el tamaño total ocupado por el primer grupo de páginas de visualización en el área de visualización del navegador; y

una unidad de recepción, configurada para recibir un mensaje de respuesta enviado por el servidor Web, en donde el mensaje de respuesta comprende el código de página del segundo grupo de páginas de visualización, en donde

la unidad de procesamiento está configurada adicionalmente para detectar, en el entorno de pruebas de la Web, si el código de página que es del segundo grupo de páginas de visualización y que es recibido por la unidad de recepción lleva un código de ataque.

7. El aparato de detección de amenazas según la reivindicación 6, en donde

la unidad de procesamiento está configurada específicamente para recibir, mediante una interfaz de Zócalo, el código de página que es del primer grupo de páginas de visualización identificado por la URL y que es enviado por el servidor Web.

8. El aparato de detección de amenazas de acuerdo con la reivindicación 6 o 7, en donde un programa de enganche está configurado para enganchar una función de procesamiento de protocolo de capa de red del entorno de prueba Web, y el programa de enganche se usa para interceptar el código de página del primer grupo de páginas de visualización; y

la unidad de procesamiento está configurada específicamente para inyectar el código dinámico preestablecido en el código de página del primer grupo de páginas de visualización cuando el programa de enganche obtiene el código de página del primer grupo de páginas de visualización.

9. El aparato de detección de amenazas de acuerdo con la reivindicación 6 o 7, en donde un programa de enganche está configurado para enganchar un núcleo del navegador del entorno de prueba de Web, y el programa de enganche se usa para interceptar el código de página del primer grupo de páginas de visualización; y

la unidad de procesamiento está configurada específicamente para inyectar el código dinámico preestablecido en el código de página del primer grupo de páginas de visualización cuando el programa de enganche obtiene el código de página del primer grupo de páginas de visualización.

10. El aparato de detección de amenazas de acuerdo con una cualquiera de las reivindicaciones 6 a 9, en donde

el código dinámico preestablecido se coloca en un final del código de página del primer grupo de páginas de visualización.

11. Un sistema de red que se aplica a un escenario de carga retardada, el sistema de red comprende al menos un

aparato de detección de amenazas de acuerdo con una cualquiera de las reivindicaciones 6 a 10 y un servidor Web, en donde cada aparato de detección de amenazas del al menos un aparato de detección de amenazas es conectado al servidor Web mediante una red.

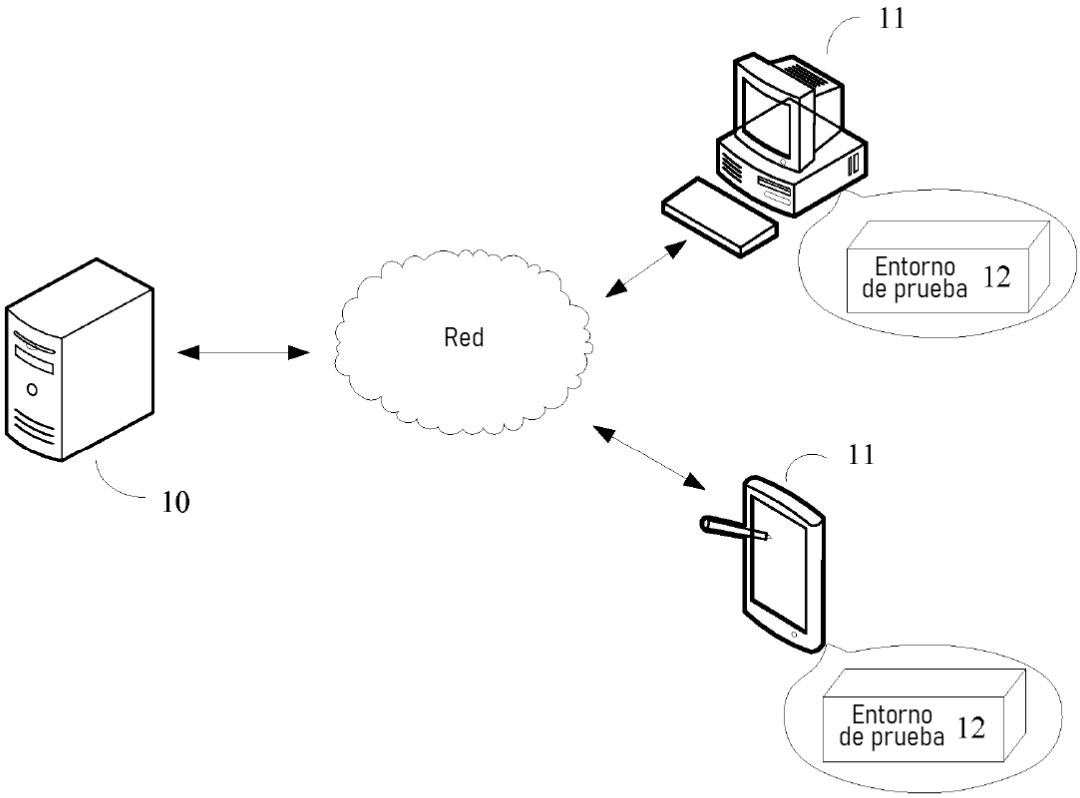

FIG. 1

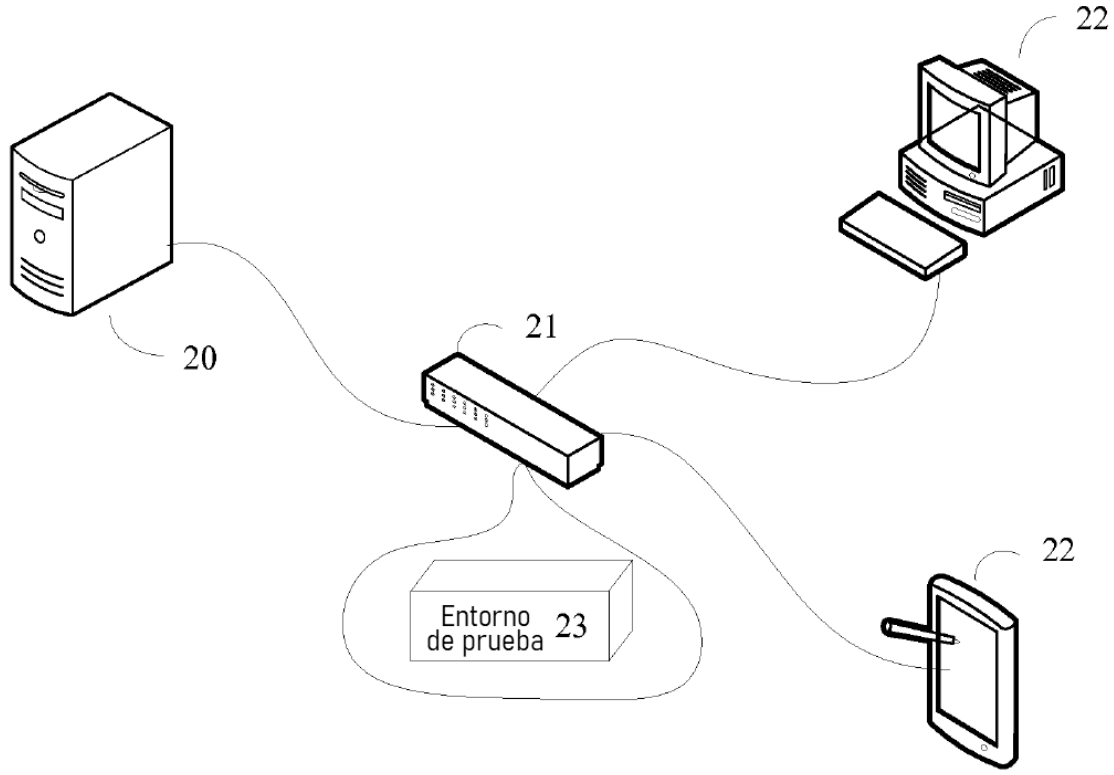

FIG. 2

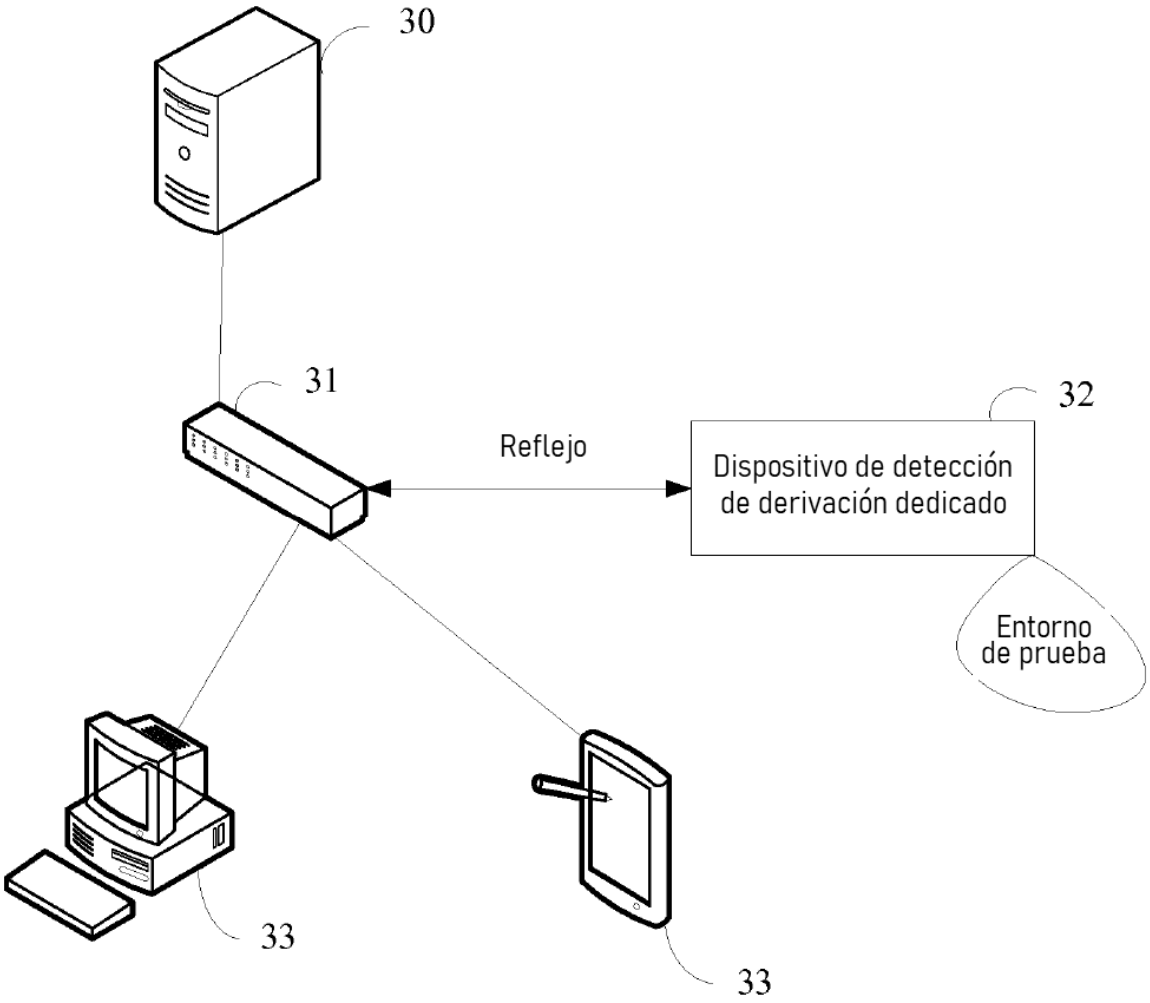
30
31
32
Reflejo
Dispositivo de detección de derivación dedicado
Entorno de prueba
33
33

FIG. 3

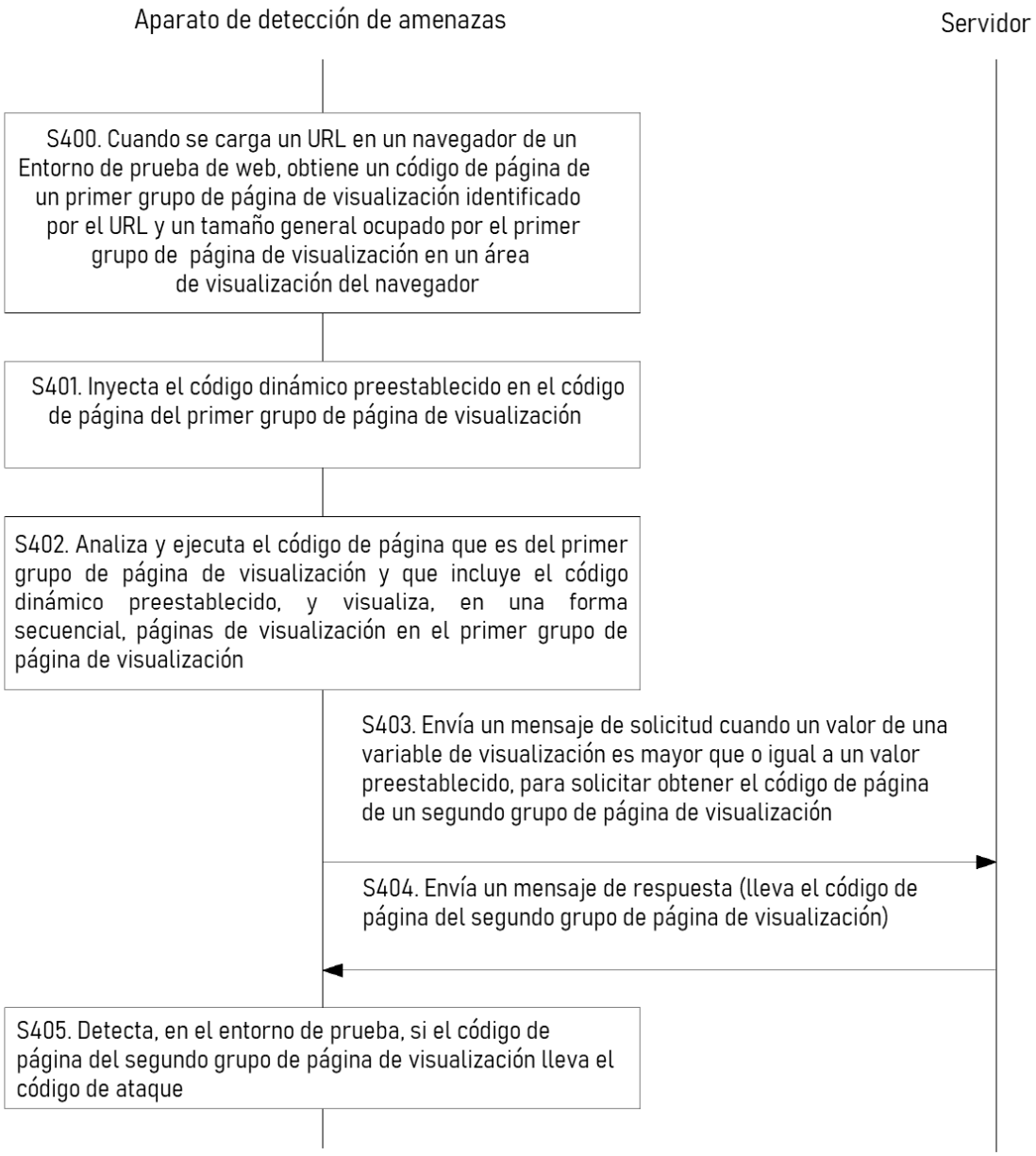
Aparato de detección de amenazas
Servidor
S400. Cuando se carga un URL en un navegador de un Entorno de prueba de web, obtiene un código de página de un primer grupo de página de visualización identificado por el URL y un tamaño general ocupado por el primer grupo de página de visualización en un área de visualización del navegador
S401. Inyecta el código dinámico preestablecido en el código de página del primer grupo de página de visualización
S402. Analiza y ejecuta el código de página que es del primer grupo de página de visualización y que incluye el código dinámico preestablecido, y visualiza, en una forma secuencial, páginas de visualización en el primer grupo de página de visualización
S403. Envía un mensaje de solicitud cuando un valor de una variable de visualización es mayor que o igual a un valor preestablecido, para solicitar obtener el código de página de un segundo grupo de página de visualización
S404. Envía un mensaje de respuesta (lleva el código de página del segundo grupo de página de visualización)
S405. Detecta, en el entorno de prueba, si el código de página del segundo grupo de página de visualización lleva el código de ataque

FIG. 4

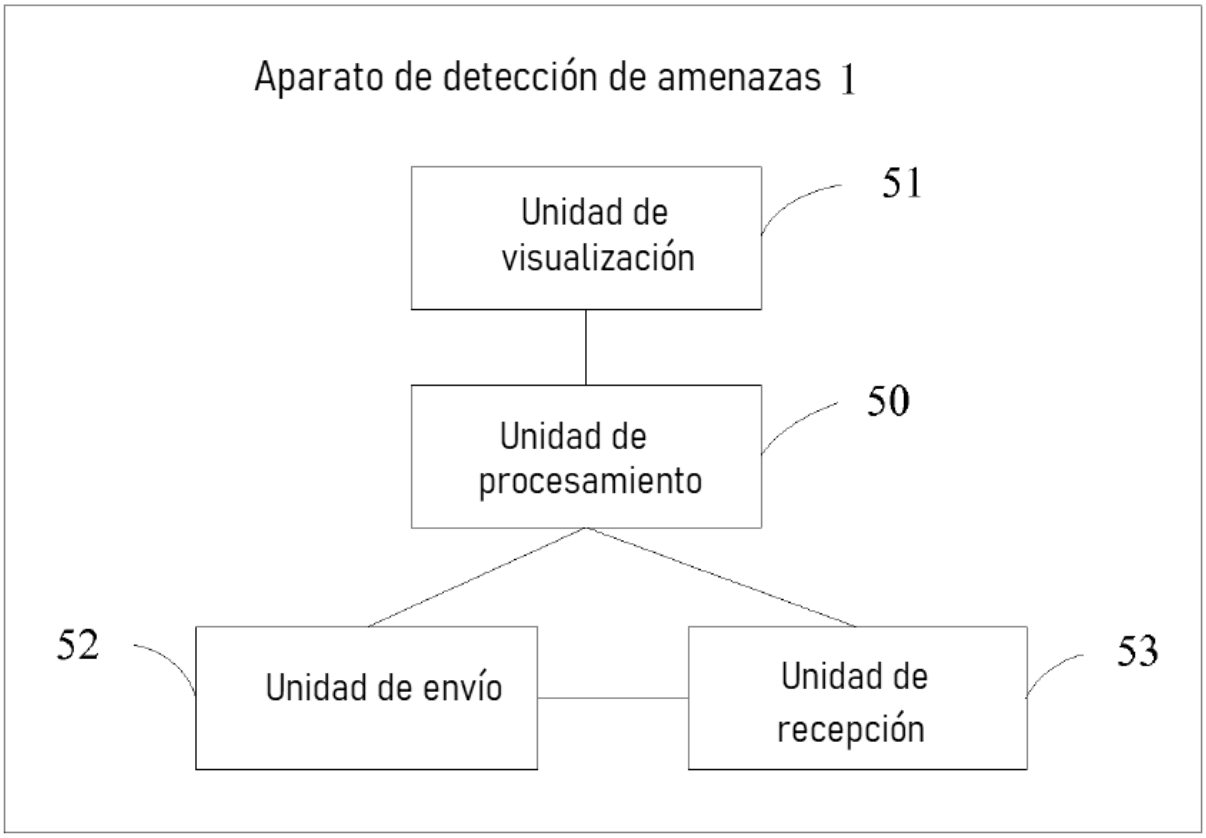
Aparato de detección de amenazas 1
Unidad de visualización
51
Unidad de procesamiento
50
52
Unidad de envío
Unidad de recepción
53

FIG. 5

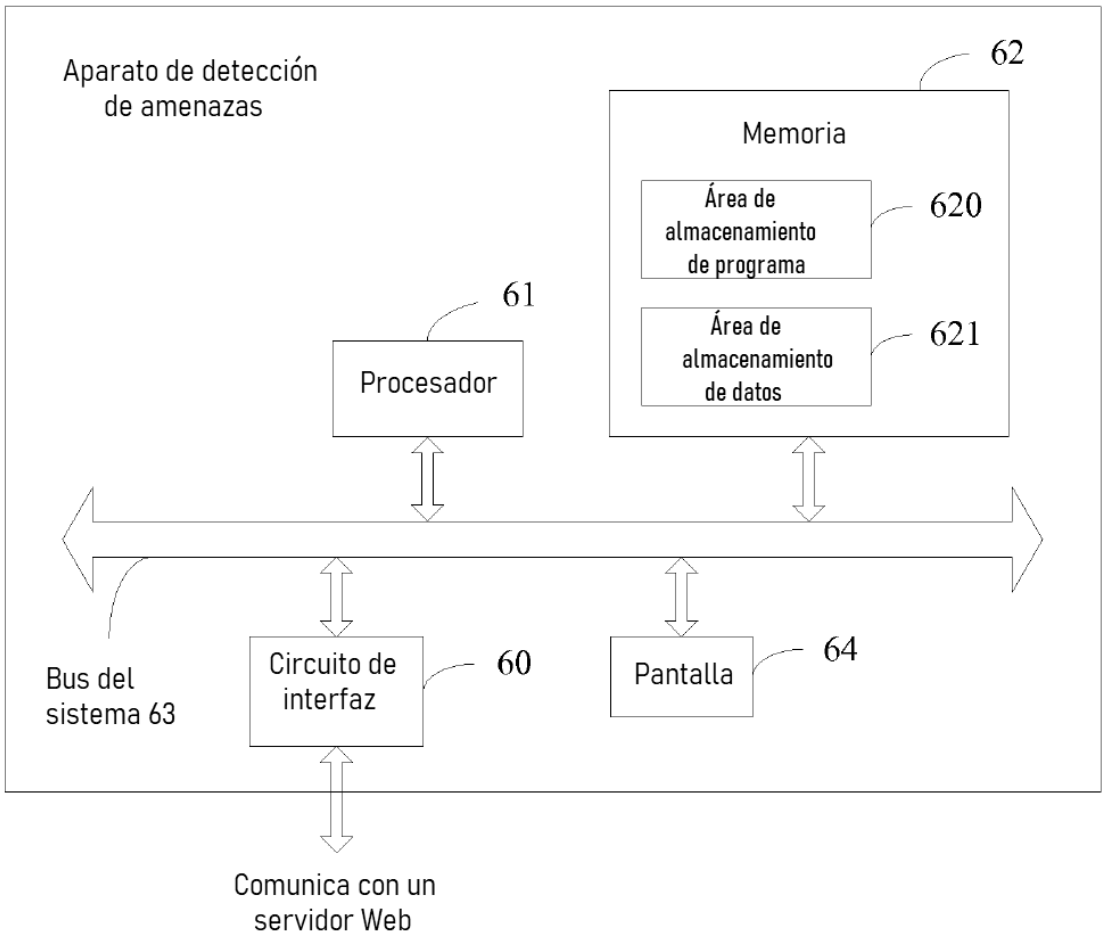
Aparato de detección de amenazas
62
Memoria
Área de almacenamiento de programa
620
Área de almacenamiento de datos
621
61
Procesador
Bus del sistema 63
Circuito de interfaz
60
Pantalla
64
Comunica con un servidor Web

FIG. 6

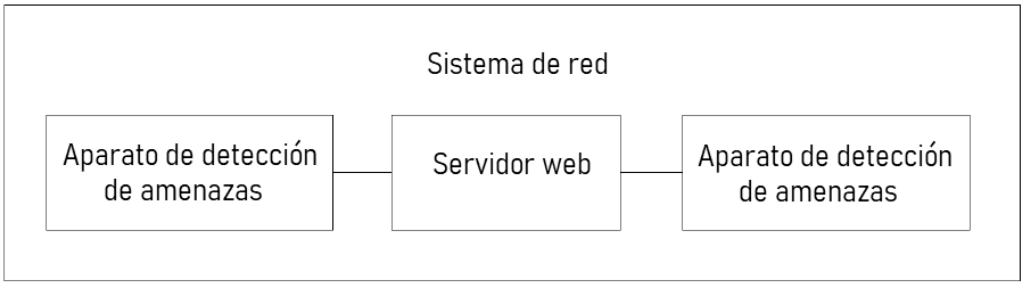
Sistema de red
Aparato de detección de amenazas
Servidor web
Aparato de detección de amenazas

FIG. 7