(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 829 600**

(51) Int. CI.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **05.06.2017 PCT/CN2017/087170**

(87) Fecha y número de publicación internacional: **03.05.2018 WO18076697**

(96) Fecha de presentación y número de la solicitud europea: **05.06.2017 E 17863527 (2)**

(97) Fecha y número de publicación de la concesión europea: **16.09.2020 EP 3509001**

(54) Título: **Método y aparato para detectar el comportamiento zombi**

(30) Prioridad:

25.10.2016 CN 201610948753

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.06.2021

(73) Titular/es:

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

(72) Inventor/es:

JIANG, WU

(74) Agente/Representante:

SÁNCHEZ SILVA, Jesús Eladio

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

DESCRIPCIÓN

Método y aparato para detectar el comportamiento zombi

Campo técnico

La presente invención se refiere al campo de las tecnologías de seguridad informática y, en particular, a un método y aparato para la detección de la característica de un robot informático.

Antecedentes

Una red de robots informáticos es una red de control de tipo uno a muchos, formada entre un atacante y ordenadores infectados después de que el atacante utiliza uno o varios enfoques de propagación para infectar una gran cantidad de ordenadores con un programa robot informático, por ejemplo, al enviar un archivo malicioso a un gran cantidad de ordenadores para que los ordenadores se infecten con un programa robot informático al recibir y ejecutar el archivo malicioso. Los ordenadores infectados son ordenadores zombis. El atacante puede controlar los ordenadores zombis utilizando la relación de uno a muchos, mediante el uso de canales de comando y control (Comando y Control, C&C). La red de robots informáticos forma una plataforma de ataque y, al utilizar esta plataforma, pueden iniciarse varios comportamientos de ciberataque, lo que trae como resultado una falla en el sistema de aplicación de un objeto atacado, una pérdida de privacidad personal y, similares. Estos comportamientos de ciberataques incluyen, por ejemplo, usar la red de robots informáticos para enviar correos basura a un objeto atacado o robar un secreto. En comparación con un comportamiento convencional según el cual el atacante ataca al objeto atacado utilizando un solo ordenador, la red de robots informáticos puede causar daños más severos al objeto atacado.

En la técnica anterior, después de que se detecta un archivo malicioso, la característica del robot informático se identifica y se extrae del archivo malicioso, generalmente a través de un análisis manual y, el archivo malicioso que se reciba posteriormente se filtra y se bloquea en base a la característica del robot informático. Sin embargo, para evadir la detección, el atacante suele modificar el archivo malicioso con relativa frecuencia y, una gran cantidad de variantes del archivo malicioso puede fácilmente generarse. El método de extracción de la característica del robot informático anterior es relativamente ineficaz y, no puede aplicarse a gran escala.

LINDORFER MARTINA Y OTROS, Detecting Environment-Sensitive Malware, CONFERENCIA INTERNACIONAL SOBRE ANÁLISIS INFORMÁTICO DE IMÁGENES Y PATRONES. CAIP 2017: ANÁLISIS INFORMÁTICO DE IMÁGENES Y PATRONES; [NOTAS DE LA CONFERENCIA EN CIENCIA DE LA INFORMÁTICA; NOTAS DE CONF. DE INFORMÁTICA], SPRINGER, BERLIN, HEIDELBERG, PÁGINA(S) 338 - 357, (20110920), ISBN 978-3-642-17318-9, * Resumen, secciones 2, 3, 4, Figuras 1, 2. * describe técnicas novedosas para detectar muestras de programas maliciosos que exhiben un comportamiento semánticamente diferente en entornos de prueba de análisis diferentes. Estas técnicas son compatibles con cualquier tecnología de monitoreo que pueda utilizarse para el análisis dinámico y, son completamente independientes de la forma en que el programa malicioso logra la evasión. Los autores implementan las técnicas propuestas en una herramienta llamada Desarmar y, demuestran que puede detectar con precisión el programa malicioso evasivo, lo que conlleva al descubrimiento de técnicas de evasión previamente desconocidas.

El documento US 2014/215617 A1 describe un sistema y un método para el análisis avanzado de programas maliciosos. El método filtra los mensajes entrantes con una lista de seguimiento, los mensajes entrantes que incluyen archivos adjuntos, si un mensaje entrante coincide con la lista de seguimiento, reenvía el mensaje a un motor de detección de programas maliciosos, elimina los archivos adjuntos del mensaje reenviado, uno o varios archivos adjuntos que incluyan uno o varios archivos ejecutables, activa una pluralidad de entornos de prueba, ejecuta cada uno de los archivos ejecutables en la pluralidad de entornos de prueba, los entornos de prueba generan resultados de análisis que pueden utilizarse para determinar si cada archivo ejecutable es malicioso, normaliza los resultados del análisis, evalúa el nivel de riesgo de los archivos adjuntos del mensaje reenviado en base a los resultados del análisis normalizado de los archivos ejecutables en los archivos adjuntos del mensaje reenviado y, si el nivel de riesgo de un archivo adjunto del mensaje reenviado se encuentra por encima de cierto nivel, determina que el mensaje reenviado es malicioso y pone en cuarentena permanentemente el mensaje reenviado.

El documento US 2014/137255 A1 describe un método, un sistema y un aparato para detectar un código malicioso, para resolver el problema donde la eficiencia de detección es baja y se ocupan más recursos. El método que incluye: monitorear la ejecución de una instrucción en un supervisor de la máquina virtual de un ordenador central, donde la instrucción se genera en modo de escape cuando una solicitud de lectura-escritura que se genera durante la ejecución del código de programa en la máquina virtual del ordenador central se entrega al supervisor de la máquina virtual; obtener las características de ejecución del código de programa de acuerdo con la ejecución de la instrucción; y comparar las características de ejecución obtenidas con las características de ejecución prealmacenadas de códigos maliciosos conocidos y, determinar que el código de programa es un código malicioso cuando las características de ejecución obtenidas y las características de ejecución prealmacenadas son las mismas. Esto mejora la eficiencia de detección y, ahorra los recursos de almacenamiento y los recursos de procesamiento en el ordenador central.

Resumen

Las modalidades de la presente invención proporcionan un método y aparato para la detección de la característica de un robot informático, para mejorar la eficiencia en la extracción de la característica del robot informático.

De acuerdo con un primer aspecto, una modalidad proporciona un método para la detección de la característica de un robot informático. El método para la detección de la característica de un robot informático incluye las siguientes etapas.

La etapa A. Obtener un primer archivo de comportamiento dinámico y un segundo archivo de comportamiento dinámico.

El primer archivo de comportamiento dinámico es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada a un archivo malicioso en un primer entorno de prueba. El segundo archivo de comportamiento dinámico es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada al archivo malicioso en un segundo entorno de prueba.

La detección de comportamiento dinámico incluye: cuando el archivo malicioso se está ejecutando, obtener una serie de comportamientos iniciados por el archivo malicioso en el sistema operativo durante el tiempo de ejecución, como la solicitud de servicio del sistema, la lectura y escritura de archivos, modificación de registro, llamada a la interfaz de programación de aplicaciones (Interfaz de Programación de Aplicaciones, API) y, acceso a la red; y registrar la información correspondiente a cada comportamiento en un archivo de comportamiento dinámico. Por ejemplo, la información de comportamiento de un archivo de lectura y escritura de comportamiento incluye un operador que ejecuta una acción, una ruta involucrada y similar.

La etapa B. Determinar la característica del robot informático del archivo malicioso en base a una característica común del primer archivo de comportamiento dinámico y del segundo archivo de comportamiento dinámico.

En la solución de la implementación del primer aspecto, se simula el archivo malicioso para que se ejecute en los entornos de prueba y, se recopilan los archivos de comportamiento, para ser específicos, los archivos de comportamiento dinámico, que registran los comportamientos de red del archivo malicioso en este proceso en ejecución, de manera que la característica del robot informático se extrae de los archivos de comportamiento dinámico. Todo este proceso puede automatizarse, lo que mejora, de esta manera, la eficiencia en la extracción de la característica del robot informático. Además, debido a que la detección de comportamiento dinámico se realiza en el mismo archivo malicioso en al menos dos entornos de prueba, durante la extracción de la característica del robot informático, extraer la característica del robot informático de la característica común de los archivos de comportamiento dinámico respectivamente generada mediante al menos los dos entornos de prueba puede evitar que la característica extraída del robot informático incluya cadenas de caracteres rellenadas aleatoriamente mediante diferentes entornos de prueba en los archivos de comportamiento dinámico y una cadena de caracteres utilizada para describir información sobre un entorno de prueba (por ejemplo, una dirección de Protocolo de Internet y una dirección de puerto del entorno de prueba), lo que mejora de esta manera, la precisión de la característica del robot informático.

El primer archivo de comportamiento dinámico incluye un primer paquete de sesión, el segundo archivo de comportamiento dinámico incluye un segundo paquete de sesión, la dirección de destino de Protocolo de Internet (Protocolo de Internet, IP) del primer paquete de sesión es la misma que la dirección de destino IP del segundo paquete de sesión y, el puerto de destino del primer paquete de sesión es el mismo que el puerto de destino del segundo paquete de sesión.

La etapa B incluye:

Etapa B11. Determinar la característica del robot informático del archivo malicioso en base a una característica común del primer paquete de sesión y del segundo paquete de sesión.

En una primera implementación del primer aspecto, la etapa B11 incluye las siguientes etapas.

Etapa B21. Obtener un primer campo preconfigurado. Existe una pluralidad de métodos para obtener el primer campo preconfigurado. Por ejemplo, el primer campo preconfigurado se almacena de antemano en una primera tabla de configuración en un dispositivo de puerta de enlace y, el primer campo preconfigurado se determina mediante la lectura de la primera tabla de configuración. Opcionalmente, el primer campo preconfigurado incluido en la primera tabla de configuración puede actualizarse en cualquier momento. Opcionalmente, cuando un paquete de sesión es un paquete de capa de aplicación que se encapsula utilizando el Protocolo de Transferencia de Hipertexto (Protocolo de Transferencia de Hipertexto, HTTP), el primer campo preconfigurado incluye un campo de carga útil y/o un campo de solicitud.

Etapa B22. Determinar si el contenido en el primer campo preconfigurado en el primer paquete de sesión y el contenido en el primer campo preconfigurado en el segundo paquete de sesión contienen la misma cadena de caracteres; y si el contenido en el primer campo preconfigurado en el primer paquete de sesión y el contenido en el primer campo

preconfigurado en el segundo paquete de sesión contienen una misma cadena de caracteres, determinar que la característica del robot informático del archivo malicioso incluye la cadena de caracteres y una ubicación de la cadena de caracteres en el primer campo preconfigurado.

En una segunda implementación del primer aspecto, la etapa B11 incluye las siguientes etapas.

Etapa B31. Obtener un segundo campo preconfigurado y un contenido preestablecido en el segundo campo preconfigurado.

Existe una pluralidad de métodos de obtención. Opcionalmente, el segundo campo preconfigurado y el contenido preestablecido en el segundo campo preconfigurado se almacenan de antemano en una segunda tabla de configuración en un dispositivo de puerta de enlace y, el segundo campo preconfigurado y el contenido preestablecido en el segundo campo preconfigurado se determinan mediante la lectura de la segunda tabla de configuración. Opcionalmente, el contenido en la segunda tabla de configuración puede actualizarse en cualquier momento. Opcionalmente, cuando un paquete de sesión es un paquete de capa de aplicación que se encapsula mediante el uso de HTTP, el segundo campo preconfigurado incluye un campo de agente y, el contenido preestablecido en el campo de agente incluye información sobre un usuario que envía una solicitud.

Etapa B32. Cuando el segundo campo preconfigurado existe en la característica común del primer paquete de sesión y del segundo paquete de sesión y, el contenido en el segundo campo preconfigurado en la característica común es diferente del contenido preestablecido, determinar que la característica del robot informático incluye el contenido en el segundo campo preconfigurado en la característica común.

En una tercera implementación del primer aspecto, la etapa B11 incluye las siguientes etapas.

Etapa B41. Obtener una regla de operación de preprocesamiento, donde la regla de operación de preprocesamiento ordena que se elimine un carácter especificado en un paquete.

Existe una pluralidad de métodos para obtener la regla de operación de preprocesamiento. Por ejemplo, la regla de operación de preprocesamiento se almacena de antemano en una tercera tabla de configuración en un dispositivo de puerta de enlace y, la regla de operación de preprocesamiento se determina mediante la lectura de la tercera tabla de configuración. Opcionalmente, el contenido en la tercera tabla de configuración puede actualizarse en cualquier momento.

Puede existir una pluralidad de reglas de operación de preprocesamiento. Por ejemplo, cuando un paquete de sesión es un paquete HTTP, la regla de operación de preprocesamiento se utiliza para ordenar que se elimine al menos una de las siguientes cadenas de caracteres: una palabra clave HTTP en el paquete de sesión, una dirección IP del entorno de prueba y un puerto en el paquete de sesión, o un tipo de unidad de procesamiento central (Unidad de Procesamiento Central, CPU) en el paquete de sesión. La palabra clave HTTP puede ser una cadena de caracteres como GET o HTTP1.1.

Etapa B42. Obtener el primer contenido restante del primer paquete de sesión y el segundo contenido restante del segundo paquete de sesión de acuerdo con la regla de operación de preprocesamiento, donde el primer contenido restante es el contenido del paquete en el primer paquete de sesión excepto el carácter especificado y, el segundo contenido restante es el contenido del paquete en el segundo paquete de sesión excepto el carácter especificado.

Etapa B43. Determinar la característica del robot informático del archivo malicioso en base a una característica común del primer contenido restante y del segundo contenido restante.

En una cuarta implementación del primer aspecto, la etapa A incluye las siguientes etapas.

Etapa A11. Obtener un archivo de comportamiento estático y un archivo de comportamiento dinámico que se generan mediante el primer entorno de prueba y, un archivo de comportamiento estático y un archivo de comportamiento dinámico que se generan mediante el segundo entorno de prueba.

El archivo de comportamiento estático generado mediante el primer entorno de prueba es un archivo de comportamiento que resulta de la detección de comportamiento estático realizada en el archivo a detectar en el primer entorno de prueba. El archivo de comportamiento estático generado mediante el segundo entorno de prueba es un archivo de comportamiento que resulta de la detección de comportamiento estático realizada en el archivo a detectar en el segundo entorno de prueba. El archivo de comportamiento dinámico generado mediante el primer entorno de prueba es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada en el archivo a detectar en el primer entorno de prueba. El archivo de comportamiento dinámico generado mediante el segundo entorno de prueba es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada en el archivo a detectar en el segundo entorno de prueba.

Etapa A12. Determinar si el archivo a detectar es un archivo malicioso en base al archivo de comportamiento estático y al archivo de comportamiento dinámico que se generan mediante el primer entorno de prueba y, al archivo de comportamiento estático y al archivo de comportamiento dinámico que se generan mediante el segundo entorno de prueba.

Por ejemplo, la puntuación basada en peso se realiza en al menos un elemento de excepción en los cuatro archivos generados mediante el primer entorno de prueba y el segundo entorno de prueba y, se determina si el archivo a detectar es un archivo malicioso en base a un resultado de puntuación.

Etapa A13. Al determinar que el archivo a detectar es un archivo malicioso, determinar que el archivo de comportamiento dinámico generado mediante el primer entorno de prueba es el primer archivo de comportamiento dinámico y, que el archivo de comportamiento dinámico generado mediante el segundo entorno de prueba es el segundo archivo de comportamiento dinámico.

En una quinta implementación del primer aspecto, la etapa A incluye las siguientes etapas.

Etapa A21. Obtener el archivo malicioso.

Existe una pluralidad de métodos de obtención, por ejemplo, determinar, mediante el análisis manual, que un archivo a detectar es un archivo malicioso, o recibir un archivo malicioso enviado por otro dispositivo.

Etapa A22. Ingresar el archivo malicioso en el primer entorno de prueba y en el segundo entorno de prueba por separado para la detección de comportamiento dinámico.

Etapa A23. Obtener un archivo de comportamiento dinámico generado mediante el primer entorno de prueba y, un archivo de comportamiento dinámico generado mediante el segundo entorno de prueba.

Un segundo aspecto de las modalidades de la presente invención proporciona un aparato para la detección de la característica del robot informático, que incluye:
un módulo de obtención, configurado para obtener un primer archivo de comportamiento dinámico y un segundo archivo de comportamiento dinámico, donde el primer archivo de comportamiento dinámico es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada en un archivo malicioso en un primer entorno de prueba y, el segundo archivo de comportamiento dinámico es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada en el archivo malicioso en un segundo entorno de prueba; y
un módulo de determinación, configurado para determinar una característica del robot informático del archivo malicioso en base a una característica común del primer archivo de comportamiento dinámico y del segundo archivo de comportamiento dinámico.

Debe aclararse que el módulo de obtención proporcionado en esta modalidad se configura para realizar la etapa A en el primer aspecto de las modalidades de la presente invención y, el módulo de determinación proporcionado en esta modalidad se configura para realizar la etapa B en el primer aspecto de las modalidades de la presente invención.

Para obtener detalles sobre los procesos de implementación específicos de la etapa A y de la etapa B, consulte las descripciones en el primer aspecto de las modalidades de la presente invención. Los detalles no se describen de nuevo en esta modalidad.

El primer archivo de comportamiento dinámico incluye un primer paquete de sesión, el segundo archivo de comportamiento dinámico incluye un segundo paquete de sesión, la dirección IP de destino de protocolo de Internet del primer paquete de sesión es la misma que la dirección IP de destino del segundo paquete de sesión y, el puerto de destino del primer paquete de sesión es el mismo que el puerto de destino del segundo paquete de sesión.

El módulo de determinación se configura específicamente para determinar la característica del robot informático del archivo malicioso en base a una característica común del primer paquete de sesión y del segundo paquete de sesión.

Debe aclararse que el módulo de determinación proporcionado en esta modalidad se configura para realizar la etapa B11 en el primer aspecto de las modalidades de la presente invención. Para obtener detalles sobre un proceso de implementación específico de la etapa B11, consulte las descripciones en el primer aspecto de las modalidades de la presente invención. Los detalles no se describen de nuevo en esta modalidad.

En una primera implementación del segundo aspecto, el módulo de determinación se configura específicamente para:
obtener un primer campo preconfigurado; y
determinar si el contenido en el primer campo preconfigurado en el primer paquete de sesión y el contenido en el primer campo preconfigurado en el segundo paquete de sesión contienen una misma cadena de caracteres; y si el contenido en el primer campo preconfigurado en el primer paquete de sesión y el contenido en el primer campo preconfigurado en el segundo paquete de sesión contienen una misma cadena de caracteres, determinar que la

característica del robot informático del archivo malicioso incluye la cadena de caracteres y una ubicación de la cadena de caracteres en el primer campo preconfigurado.

Debe aclararse que el módulo de determinación proporcionado en esta modalidad se configura para realizar la etapa B21 y la etapa B22 en el primer aspecto de las modalidades de la presente invención. Para obtener detalles sobre los procesos de implementación específicos de la etapa B21 y de la etapa B22, consulte las descripciones en el primer aspecto de las modalidades de la presente invención. Los detalles no se describen de nuevo en esta modalidad.

En una segunda implementación del segundo aspecto, el módulo de determinación se configura específicamente para:
obtener un segundo campo preconfigurado y un contenido preestablecido en el segundo campo preconfigurado; y
cuando el segundo campo preconfigurado existe en la característica común del primer paquete de sesión y del segundo paquete de sesión y, el contenido en el segundo campo preconfigurado en la característica común es diferente del contenido preestablecido, determinar que la característica del robot informático incluye el contenido en el segundo campo preconfigurado en la característica común.

Debe aclararse que el módulo de determinación proporcionado en esta modalidad se configura para realizar la etapa B31 y la etapa B32 en el primer aspecto de las modalidades de la presente invención. Para obtener detalles sobre los procesos de implementación específicos de la etapa B31 y de la etapa B32, consulte las descripciones en el primer aspecto de las modalidades de la presente invención. Los detalles no se describen de nuevo en esta modalidad.

En una tercera implementación del segundo aspecto, el módulo de determinación se configura específicamente para:
obtener una regla de operación de preprocesamiento, donde la regla de operación de preprocesamiento ordena que se elimine un carácter especificado en un paquete;
obtener el primer contenido restante del primer paquete de sesión y el segundo contenido restante del segundo paquete de sesión de acuerdo con la regla de operación de preprocesamiento, donde el primer contenido restante es el contenido del paquete en el primer paquete de sesión excepto el carácter especificado y, el segundo contenido restante es el contenido del paquete en el segundo paquete de sesión excepto el carácter especificado; y
determinar la característica del robot informático del archivo malicioso en base a una característica común del primer contenido restante y del segundo contenido restante.

Debe aclararse que el módulo de determinación proporcionado en esta modalidad se configura para realizar la etapa B41, la etapa B42 y la etapa B43 en el primer aspecto de las modalidades de la presente invención. Para obtener detalles sobre los procesos de implementación específicos de la etapa B41, la etapa B42 y la etapa B43, consulte las descripciones en el primer aspecto de las modalidades de la presente invención. Los detalles no se describen de nuevo en esta modalidad.

En una cuarta implementación del segundo aspecto, el módulo de obtención se configura específicamente para:
obtener un archivo de comportamiento estático y un archivo de comportamiento dinámico que se generan mediante el primer entorno de prueba y, un archivo de comportamiento estático y un archivo de comportamiento dinámico que se generan mediante el segundo entorno de prueba, donde el archivo de comportamiento estático generado mediante el primer entorno de prueba es un archivo de comportamiento que resulta de la detección de comportamiento estático realizada en un archivo a detectar en el primer entorno de prueba, el archivo de comportamiento estático generado mediante el segundo entorno de prueba es un archivo de comportamiento que resulta de la detección de comportamiento estático realizada en el archivo a detectar en el segundo entorno de prueba, el archivo de comportamiento dinámico generado mediante el primer entorno de prueba es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada en el archivo a detectar en el primer entorno de prueba y, el archivo de comportamiento dinámico generado mediante el segundo entorno de prueba es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada en el archivo a detectar en el segundo entorno de prueba;
determinar si el archivo a detectar es un archivo malicioso en base al archivo de comportamiento estático y al archivo de comportamiento dinámico que se generan mediante el primer entorno de prueba y, al archivo de comportamiento estático y al archivo de comportamiento dinámico que se generan mediante el segundo entorno de prueba; y
al determinar que el archivo a detectar es un archivo malicioso, determinar que el archivo de comportamiento dinámico generado mediante el primer entorno de prueba es el primer archivo de comportamiento dinámico y, que el archivo de comportamiento dinámico generado mediante el segundo entorno de prueba es el segundo archivo de comportamiento dinámico.

Debe aclararse que el módulo de obtención proporcionado en esta modalidad se configura para realizar la etapa A11, la etapa A12 y la etapa A13 en el primer aspecto de las modalidades de la presente invención. Para obtener detalles sobre los procesos de implementación específicos de la etapa A11, de la etapa A12 y de la etapa A13, consulte las descripciones en el primer aspecto de las modalidades de la presente invención. Los detalles no se describen de nuevo en esta modalidad.

En una quinta implementación del segundo aspecto, el módulo de obtención se configura específicamente para:
obtener el archivo malicioso;

ingresar el archivo malicioso en el primer entorno de prueba y en el segundo entorno de prueba por separado para la detección de comportamiento dinámico; y obtener un archivo de comportamiento dinámico generado mediante el primer entorno de prueba y un archivo de comportamiento dinámico generado mediante el segundo entorno de prueba.

Debe aclararse que el módulo de obtención proporcionado en esta modalidad se configura para realizar la etapa A21, la etapa A22 y la etapa A23 en el primer aspecto de las modalidades de la presente invención. Para obtener detalles sobre los procesos de implementación específicos de la etapa A21, de la etapa A22 y de la etapa A23, consulte las descripciones en el primer aspecto de las modalidades de la presente invención. Los detalles no se describen de nuevo en esta modalidad.

En esta modalidad, el aparato para la detección de la característica del robot informático realiza la detección de comportamiento dinámico en el archivo malicioso en los entornos de prueba, recopila, mediante la utilización de los entornos de prueba, todos los comportamientos de red del archivo malicioso durante un proceso en ejecución, genera los archivos de comportamiento dinámico que registran los comportamientos de red y, extrae la característica del robot informático de los archivos de comportamiento dinámico. De esta forma, puede extraerse una firma de comunicación del robot informático. Esto ayuda a implementar la detección de un archivo malicioso en base a la firma característica de comunicación y, evita los falsos positivos y los falsos negativos informados debido a la interferencia de varias variantes de un archivo de robot informático. Además, debido a que la detección de comportamiento dinámico se realiza en el mismo archivo malicioso en al menos dos entornos de prueba, durante la extracción de la característica del robot informático, extraer la característica del robot informático de la característica común de los archivos de comportamiento dinámico respectivamente generados mediante al menos dos entornos de prueba puede evitar que la característica del robot informático extraída incluya cadenas de caracteres rellenadas aleatoriamente mediante diferentes entornos de prueba en los archivos de comportamiento dinámico y una cadena de caracteres utilizada para describir información sobre un entorno de prueba (por ejemplo, una dirección IP y una dirección de puerto del entorno de prueba), mejorando, de esta manera, la precisión de la característica del robot informático.

Un cuarto aspecto de las modalidades de la presente invención proporciona un medio de almacenamiento legible por ordenador que almacena uno o varios programas. El único o demás programas incluyen una instrucción. Cuando la instrucción se ejecuta mediante un dispositivo de puerta de enlace, el dispositivo de puerta de enlace realiza el método de acuerdo con cualquier primer aspecto de las modalidades de la presente invención de la quinta implementación del primer aspecto de las modalidades de la presente invención.

Breve descripción de los dibujos

La Figura 1 es un diagrama de flujo esquemático de una modalidad de un método para la detección de la característica de un robot informático de acuerdo con la presente invención;
La Figura 2 es un diagrama estructural esquemático de una modalidad de un sistema de comunicación de acuerdo con la presente invención;
La Figura 3 es un diagrama estructural esquemático de módulos, en un dispositivo de puerta de enlace, configurado para realizar la detección de un robot informático Troyano;
La Figura 4 es un diagrama estructural esquemático de una modalidad de un aparato para la detección de la característica de un robot informático de acuerdo con la presente invención; y
La Figura 5 es un diagrama estructural esquemático de una modalidad de un dispositivo de puerta de enlace de acuerdo con la presente invención.

Descripción de las modalidades

A continuación se explica y se describe, mediante la utilización de la Figura 1 como ejemplo, un método para la detección de la característica de un robot informático proporcionado en las modalidades. Con referencia a la Figura 1, la Figura 1 es un diagrama de flujo esquemático de una modalidad de un método para la detección de la característica de un robot informático de acuerdo con la presente invención. Esta modalidad de la presente invención se ejecuta mediante un dispositivo informático. Opcionalmente, el dispositivo informático puede ser un dispositivo de puerta de enlace universal, un dispositivo de puerta de enlace doméstico, un enrutador, un administrador de dispositivos de puerta de enlace o similares. El dispositivo de puerta de enlace universal puede ser un dispositivo de puerta de enlace de red de acceso, un cortafuegos de dispositivo de puerta de enlace empresarial, un conmutador o similar, que no se limita en la presente descripción. Todos los dispositivos anteriores se denominan "dispositivos de puerta de enlace" en esta modalidad.

En esta modalidad, la solución se describe mediante la utilización de un ejemplo en el que el cuerpo de ejecución es un dispositivo de puerta de enlace. Después de recibir los paquetes de servicio, el dispositivo de puerta de enlace determina, a partir de los paquetes de servicio, una serie de paquetes de servicio que se utilizan para transportar un mismo archivo, o en otras palabras, una sesión que se utiliza para transportar un mismo archivo y, reensambla la serie de paquetes de servicio para la restauración, para obtener un archivo transportado por una parte de la carga útil de la serie de paquetes. Cuando se determina que un archivo es un archivo malicioso, el dispositivo de puerta de enlace detecta una característica del robot informático del archivo malicioso mediante la utilización del método para la detección de la característica del robot informático en esta modalidad, para sincronizar la característica del robot

informático obtenida con otro dispositivo cortafuego de hardware en una red o software de antivirus instalado en un ordenador personal, mejorando de esta manera el efecto de detección del archivo malicioso y mejorando el nivel de protección de seguridad de una red.

Como se muestra en la Figura 1, el método para la detección de la característica del robot informático en esta modalidad incluye las siguientes etapas.

101. Un dispositivo de puerta de enlace obtiene un primer archivo de comportamiento dinámico y un segundo archivo de comportamiento dinámico.

En esta modalidad, el primer archivo de comportamiento dinámico es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada en un archivo malicioso en un primer entorno de prueba y, el segundo archivo de comportamiento dinámico es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada en el archivo malicioso en un segundo entorno de prueba. El archivo malicioso es un archivo utilizado por un atacante para infectar a un ordenador atacado como un ordenador zombi en una red de robots informáticos. Un entorno de prueba es un programa de un sistema virtual y, se destina para proporcionar un mecanismo de seguridad, a fin de proporcionar un entorno de prueba para un programa en ejecución. Un programa que se ejecuta en el entorno de prueba no genera un impacto permanente en el hardware. En esta modalidad, la detección de comportamiento dinámico se realiza en el archivo malicioso en los entornos de prueba, para simular los comportamientos de red del archivo malicioso en un ordenador atacado después de que se ejecuta el archivo malicioso y, buscar la característica del robot informático del archivo malicioso en los archivos de comportamiento generados sobre los comportamientos de red.

Existe una pluralidad de métodos para obtener el primer archivo de comportamiento dinámico y el segundo archivo de comportamiento dinámico.

En una posible implementación, el dispositivo de puerta de enlace detecta primero el archivo malicioso. Existe una pluralidad de métodos para detectar el archivo malicioso. A continuación, se describe uno de los métodos mediante la utilización de un ejemplo. El dispositivo de puerta de enlace obtiene un archivo a detectar e ingresa el archivo a detectar en el primer entorno de prueba y en el segundo entorno de prueba por separado. El primer entorno de prueba y el segundo entorno de prueba pueden ubicarse en el dispositivo de puerta de enlace, o pueden ubicarse en un dispositivo distinto al dispositivo de puerta de enlace, que no se limita en la presente descripción.

Existe una pluralidad de métodos para que el dispositivo de puerta de enlace obtenga el archivo a detectar. Por ejemplo, el dispositivo de puerta de enlace reensambla una pluralidad de paquetes de red recibidos de una misma sesión para la restauración, para generar un archivo completo y, utiliza el archivo como el archivo a detectar. El archivo a detectar puede ser un archivo que sirve como adjunto de correo y que se envía mediante la utilización de un paquete de protocolo de correo, o puede ser un archivo que sirve como una extensión de una página web y que se envía mediante la utilización del Protocolo de Transferencia de Hipertexto. Alternativamente, después de generar un archivo completo, el dispositivo de puerta de enlace determina si el archivo es un archivo bajo sospecha de ser malicioso. Si el archivo es un archivo bajo sospecha de ser malicioso, el dispositivo de puerta de enlace determina que el archivo es un archivo a detectar. Existe una pluralidad de métodos para determinar si el archivo es un archivo bajo sospecha de ser malicioso. Por ejemplo, el dispositivo de puerta de enlace determina si el archivo es un archivo ejecutable portátil (Ejecutable Portátil, PE) y, si el archivo es un archivo ejecutable portátil, el dispositivo de puerta de enlace determina que el archivo es un archivo bajo sospecha de ser malicioso. Para otro ejemplo, el dispositivo de puerta de enlace realiza una comparación de coincidencia entre un localizador de recursos uniforme (Localizador de Recursos Uniforme, URL) del archivo y una URL del robot informático prealmacenada localmente. Si la comparación de coincidencia es exitosa, el dispositivo de puerta de enlace puede determinar directamente que el archivo es un archivo malicioso, es decir, excluir el archivo de los archivos a detectar. De esta manera, puede reducirse una cantidad de archivos a detectar y, puede mejorarse la eficiencia en la detección de la característica del robot informático.

Los entornos de prueba realizan dos tipos de detección en el archivo a detectar, concretamente, la detección de comportamiento estático y la detección de comportamiento dinámico. La detección de comportamiento estático se realiza para obtener un parámetro del archivo a detectar mediante el análisis del contenido de código y de la estructura de código del archivo a detectar cuando el archivo a detectar no se está ejecutando. En una manera común de detección de comportamiento estático, se determina un tipo de archivo al que pertenece el código del archivo a detectar y, se leen los datos en una ubicación predeterminada en el archivo a detectar en base a una estructura de datos que corresponde al tipo de archivo. Cuando se utiliza esta manera, puede obtenerse información tal como un nombre de archivo, un tamaño de archivo, información de la versión y, una firma digital del archivo a detectar. En otra manera común de detección de comportamiento estático, la comparación de coincidencia se realiza entre el código del archivo a detectar y una característica conocida prealmacenada y, si la comparación de coincidencia es exitosa, se determina que el archivo a detectar incluye la característica conocida.

La detección de comportamiento dinámico incluye: cuando el archivo a detectar se está ejecutando, obtener una serie de comportamientos iniciados por el archivo a detectar en un sistema operativo durante el tiempo de ejecución, tales como la solicitud de servicio del sistema, la lectura y escritura de archivos, la modificación de registros, llamadas API

y, acceso a la red; y registrar la información correspondiente a cada comportamiento en un archivo de comportamiento dinámico. Por ejemplo, la información de comportamiento de un archivo de lectura y escritura de comportamiento incluye un operador de una acción ejecutada, una ruta involucrada en la acción ejecutada y, similar.

La detección de comportamiento estático se realiza en el archivo a detectar en cada entorno de prueba y, se genera un archivo de comportamiento, para ser específico, un archivo de comportamiento estático, que resulta de la detección de comportamiento estático realizada en el archivo a detectar.

La detección de comportamiento dinámico se realiza además en el archivo a detectar en cada entorno de prueba y, se genera un archivo de comportamiento, para ser específico, un archivo de comportamiento dinámico, que resulta de la detección de comportamiento dinámico realizada en el archivo a detectar. Opcionalmente, un archivo de comportamiento dinámico generado mediante cada entorno de prueba incluye datos de paquetes de red enviados y recibidos por el archivo a detectar. Opcionalmente, el archivo de comportamiento dinámico incluye además otros datos tales como un ID de tarea, un nombre de archivo, una secuencia de comportamiento dinámico y, un objeto operativo de comportamiento dinámico.

Después de que se obtienen un archivo de comportamiento estático y un archivo de comportamiento dinámico que se generan mediante el primer entorno de prueba y, un archivo de comportamiento estático y un archivo de comportamiento dinámico que se generan mediante el segundo entorno de prueba, se determina si el archivo a detectar es un archivo malicioso en base a los cuatro archivos. Específicamente, la puntuación basada en peso se realiza en al menos un elemento de excepción en los cuatro archivos generados mediante el primer entorno de prueba y el segundo entorno de prueba y, se determina si el archivo a detectar es un archivo malicioso en base a un resultado de puntuación. Un método para determinar un archivo malicioso es la técnica anterior, que no se describe en detalle en la presente descripción. Cuando se determina que el archivo a detectar es un archivo malicioso, se determina que el archivo de comportamiento dinámico generado mediante el primer entorno de prueba es el primer archivo de comportamiento dinámico y, que el archivo de comportamiento dinámico generado mediante el segundo entorno de prueba es el segundo archivo de comportamiento dinámico.

En la aplicación real, es posible que un entorno de prueba no genere un archivo de comportamiento dinámico después de realizar la detección de comportamiento dinámico en un archivo malicioso. Esto indica que el archivo malicioso no realiza un comportamiento de red en el entorno de prueba. Por lo tanto, opcionalmente, el archivo a detectar se puede volver a determinar como un archivo no malicioso.

En otra posible implementación de esta modalidad, el dispositivo de puerta de enlace utiliza primero otro método, por ejemplo, análisis manual, para examinar un archivo y determinar si el archivo es un archivo malicioso. Al determinar que el archivo es un archivo malicioso, el dispositivo de puerta de enlace ingresa el archivo malicioso en el primer entorno de prueba y en el segundo entorno de prueba por separado para la detección de comportamiento dinámico, obtiene un archivo de comportamiento dinámico generado mediante el primer entorno de prueba y considera el archivo de comportamiento dinámico como el primer archivo de comportamiento dinámico y, obtiene un archivo de comportamiento dinámico generado mediante el segundo entorno de prueba y considera el archivo de comportamiento dinámico como el segundo archivo de comportamiento dinámico.

102. El dispositivo de puerta de enlace determina una característica del robot informático de un archivo malicioso en base a una característica común del primer archivo de comportamiento dinámico y del segundo archivo de comportamiento dinámico.

En esta modalidad, existe una pluralidad de métodos para determinar la característica del robot informático en base a la característica común del primer archivo de comportamiento dinámico y del segundo archivo de comportamiento dinámico.

Por ejemplo, se obtiene un primer campo preconfigurado y, se determina si el contenido en el primer campo preconfigurado en el primer archivo de comportamiento dinámico y el contenido en el primer campo preconfigurado en el segundo archivo de comportamiento dinámico contienen la misma cadena de caracteres. Si el contenido en el primer campo preconfigurado en el primer archivo de comportamiento dinámico y el contenido en el primer campo preconfigurado en el segundo archivo de comportamiento dinámico contienen la misma cadena de caracteres, se determina que la característica del robot informático del archivo malicioso incluye la misma cadena de caracteres y una ubicación de la cadena de caracteres en el primer campo preconfigurado. Existe una pluralidad de métodos para obtener el primer campo preconfigurado. Por ejemplo, el primer campo preconfigurado se almacena de antemano en una primera tabla de configuración en el dispositivo de puerta de enlace y, el primer campo preconfigurado se determina mediante la lectura de la primera tabla de configuración. Opcionalmente, el primer campo preconfigurado incluido en la primera tabla de configuración puede actualizarse en cualquier momento.

El campo en esta modalidad puede ser una ubicación de almacenamiento especificada en un archivo de comportamiento dinámico con una estructura fija. En un archivo de comportamiento dinámico con una estructura como se muestra en la Tabla 2, el campo puede ser un ID de tarea, una secuencia de comportamiento dinámico, un objeto operativo de comportamiento dinámico o similar en los elementos de nivel 1. Cuando el archivo de comportamiento

dinámico incluye datos de paquetes de red, el campo puede ser alternativamente un campo en un paquete de sesión que se encapsula mediante la utilización de un protocolo especificado.

Por ejemplo, cuando un paquete de sesión es un paquete de capa de aplicación que se encapsula mediante la utilización de HTTP, el primer campo preconfigurado incluye un campo de carga útil y/o un campo de solicitud.

Para otro ejemplo, se obtienen un segundo campo preconfigurado y un contenido preestablecido en el segundo campo preconfigurado. Existe una pluralidad de métodos de obtención. Opcionalmente, el segundo campo preconfigurado y el contenido preestablecido en el segundo campo preconfigurado se almacenan de antemano en una segunda tabla de configuración en el dispositivo de puerta de enlace y, el segundo campo preconfigurado y el contenido preestablecido en el segundo campo preconfigurado se determinan mediante la lectura de la segunda tabla de configuración. Opcionalmente, el contenido en la segunda tabla de configuración puede actualizarse en cualquier momento. Opcionalmente, el segundo campo preconfigurado es un campo que puede modificarse mediante un programa de robot informático y, el contenido preestablecido en el segundo campo preconfigurado es un contenido regular en el segundo campo preconfigurado en un paquete normal.

Cuando el segundo campo preconfigurado existe en la característica común del primer archivo de comportamiento dinámico y del segundo archivo de comportamiento dinámico y, el contenido en el segundo campo preconfigurado en la característica común es diferente del contenido preestablecido, se determina que la característica del robot informático del archivo malicioso incluye el contenido en el segundo campo preconfigurado en la característica común.

Opcionalmente, cuando un paquete de sesión es un paquete de capa de aplicación que se encapsula mediante el uso de HTTP, el segundo campo preconfigurado incluye un campo de agente y, el contenido preestablecido en el campo de agente incluye información sobre un usuario que envía una solicitud.

En una aplicación real, cuando se genera un archivo malicioso en una red de robots informáticos, los campos de carga útil de los archivos maliciosos del mismo tipo son los mismos. Debido a que un pirata informático puede configurar y definir el campo de solicitud y/o el campo de agente, los campos de solicitud y/o los campos de agente en diferentes redes de robots informáticos pueden ser diferentes. Por lo tanto, cuando se realiza la detección de la característica del robot informático, el campo de carga útil puede hacerse coincidir primero para determinar una característica del robot informático y, el campo de solicitud y/o el campo de agente luego se hacen coincidir para agrupar las características de robots informáticos detectadas con las características de robots informáticos de diferentes redes de robots informáticos.

En esta modalidad, el archivo de comportamiento dinámico generado mediante cada entorno de prueba incluye datos de paquetes de red. Los datos de paquetes de red incluyen paquetes de sesión que se encuentran entre el entorno de prueba y diferentes objetos de comunicación y que se generan durante la detección de comportamiento dinámico realizada en el archivo malicioso. Para determinar una característica del robot informático, la característica del robot informático puede buscarse en una pluralidad de paquetes de sesión en los archivos de comportamiento dinámico.

El primer archivo de comportamiento dinámico y el segundo archivo de comportamiento dinámico son archivos de resultados que resultan de la detección de comportamiento dinámico realizada en el mismo archivo malicioso en diferentes entornos de prueba. Por lo tanto, cada paquete de sesión en el primer/segundo archivo de comportamiento dinámico es un paquete de sesión entre el primer/segundo entorno de prueba y un mismo lote de objetos de comunicación. El mismo lote de objetos de comunicación incluye n objetos de comunicación, donde n es un número entero positivo. Para un i-ésimo objeto de comunicación (i es cualquier entero positivo mayor o igual que 1 pero menor o igual que n), el primer archivo de comportamiento dinámico incluye un paquete de sesión entre el primer entorno de prueba y el i-ésimo objeto y, en un quíntuplo del paquete de sesión, una dirección IP de origen y un puerto de origen son una dirección IP y un puerto del primer entorno de prueba, respectivamente y, una dirección IP de destino y un puerto de destino son una dirección IP y un puerto del i-ésimo objeto, respectivamente; y el segundo archivo de comportamiento dinámico incluye un paquete de sesión entre el segundo entorno de prueba y el i-ésimo objeto y, en un quíntuple del paquete de sesión, una dirección IP de origen y un puerto de origen son una dirección IP y un puerto del segundo entorno de prueba, respectivamente y, una dirección IP de destino y un puerto de destino son una dirección IP y un puerto del i-ésimo objeto, respectivamente.

Un paquete de sesión transporta cadenas de caracteres, como una cadena de caracteres rellenada aleatoriamente mediante un entorno de prueba y una cadena de caracteres utilizada para describir información sobre el entorno de prueba (por ejemplo, una dirección IP y una dirección de puerto del entorno de prueba). Estas cadenas de caracteres definitivamente no son una característica del robot informático. Por lo tanto, cuando se busca una característica del robot informático, la característica del robot informático del archivo malicioso se determina en base a la característica común del primer archivo de comportamiento dinámico y del segundo archivo de comportamiento dinámico, lo que evita que la característica del robot informático determinada incluya estas cadenas de caracteres. Específicamente, la característica del robot informático del archivo malicioso se determina en base a una característica común de un primer paquete de sesión en el primer archivo de comportamiento dinámico y de un segundo paquete de sesión en el segundo archivo de comportamiento dinámico. El primer/segundo paquete de sesión es un paquete de sesión entre el primer/segundo entorno de prueba y un mismo objeto de comunicación. En otras palabras, una dirección IP de destino

del primer paquete de sesión es la misma que una dirección IP de destino del segundo paquete de sesión y, un puerto de destino del primer paquete de sesión es el mismo que un puerto de destino del segundo paquete de sesión.

Por lo tanto, antes de que se determine la característica del robot informático del archivo malicioso, los paquetes de sesión en el primer archivo de comportamiento dinámico se emparejan primero con los paquetes de sesión en el segundo archivo de comportamiento dinámico, para determinar los paquetes de sesión, en el primer archivo de comportamiento dinámico y en el segundo archivo de comportamiento dinámico, que corresponden a un mismo objeto de comunicación. Existe una pluralidad de métodos de emparejamiento. Por ejemplo, para el primer paquete de sesión en el primer archivo de comportamiento dinámico, después de que se obtienen la dirección IP de destino y el puerto de destino del primer paquete de sesión, se cruzan todos los paquetes de sesión en el segundo archivo de comportamiento dinámico, para encontrar un paquete de sesión, para ser específicos, el segundo paquete de sesión, que tiene la misma dirección IP de destino y el mismo puerto de destino.

En esta modalidad, existe una pluralidad de métodos para determinar la característica del robot informático del archivo malicioso en base a la característica común del primer paquete de sesión y del segundo paquete de sesión. Por ejemplo, primero se obtiene la característica común del primer paquete de sesión y del segundo paquete de sesión y, luego se busca la característica del robot informático en la característica común. Para otro ejemplo, una ubicación (denominada primera ubicación para facilitar la descripción), en el primer paquete de sesión, en la que se produce una característica del robot informático y, una ubicación (denominada segunda ubicación para facilitar la descripción), en el segundo paquete de sesión, en la que se produce una característica del robot informático se determinan primero, se obtiene entonces una característica común del contenido del paquete en la primera ubicación y del contenido del paquete en la segunda ubicación y, se determina la característica del robot informático en base a la característica común. La primera ubicación y la segunda ubicación pueden ser al menos el campo de carga útil, el campo de solicitud o el campo de agente descrito anteriormente.

En esta modalidad, en un proceso de determinación de la característica del robot informático en base a la característica común del primer paquete de sesión y del segundo paquete de sesión, se incluye una etapa de preprocesamiento del primer paquete de sesión y del segundo paquete de sesión para marcar algunas cadenas de caracteres, en el primer paquete de sesión y en el segundo paquete de sesión, que definitivamente no son una característica del robot informático, de modo que las cadenas de caracteres marcadas no se comparan cuando se comparan el primer paquete de sesión y el segundo paquete de sesión para obtener la característica común de los dos paquetes de sesión, mejorando de esta manera la eficiencia en la obtención de la característica común. A continuación se describe, mediante la utilización de un ejemplo, uno de los métodos para determinar la característica del robot informático en base a la característica común del primer paquete de sesión y del segundo paquete de sesión.

Se obtiene una regla de operación de preprocesamiento. La regla de operación de preprocesamiento ordena que se elimine un carácter especificado en un paquete. De acuerdo con la regla de operación de preprocesamiento, el primer contenido restante se obtiene del primer paquete de sesión y, el segundo contenido restante se obtiene del segundo paquete de sesión. El primer contenido restante es el contenido del paquete en el primer paquete de sesión, excepto el carácter especificado y, el segundo contenido restante es el contenido del paquete en el segundo paquete de sesión, excepto el carácter especificado. La característica del robot informático del archivo malicioso se determina en base a una característica común del primer contenido restante y del segundo contenido restante.

Existe una pluralidad de métodos para obtener la regla de operación de preprocesamiento. Por ejemplo, la regla de operación de preprocesamiento se almacena de antemano en una tercera tabla de configuración en el dispositivo de puerta de enlace y, la regla de operación de preprocesamiento se determina mediante la lectura de la tercera tabla de configuración. Opcionalmente, el contenido en la tercera tabla de configuración puede actualizarse en cualquier momento.

Puede existir una pluralidad de reglas de operación de preprocesamiento. Por ejemplo, cuando un paquete de sesión es un paquete HTTP, la regla de operación de preprocesamiento se utiliza para ordenar que se elimine al menos una de las siguientes cadenas de caracteres: una palabra clave HTTP en el paquete de sesión, una dirección IP del entorno de prueba o un puerto en el paquete de sesión, o un tipo de CPU en el paquete de sesión. La palabra clave HTTP puede ser una cadena de caracteres tal como GET o HTTP1.1, que no se limita en la presente descripción.

Opcionalmente, en esta modalidad, se preestablece además una lista blanca de protocolos en el dispositivo de puerta de enlace. La lista blanca de protocolos almacena al menos un protocolo de capa de transporte. Opcionalmente, la lista blanca de protocolos puede actualizarse en cualquier momento. Antes de que se obtenga la característica común del primer archivo de comportamiento dinámico y del segundo archivo de comportamiento dinámico, cuando se determina que existe un paquete de sesión específico en los dos archivos de comportamiento dinámico, se determina que el paquete de sesión específico no incluye una característica del robot informático y, el paquete de sesión específico se excluye durante la obtención de la característica común del primer archivo de comportamiento dinámico y del segundo archivo de comportamiento dinámico. El paquete de sesión específico es un paquete de sesión en cuyo quíntuple un protocolo de capa de transporte se encuentra en la lista blanca de protocolos. De esta manera, puede reducirse una cantidad de paquetes de sesión utilizados para obtener la característica común y, puede mejorarse la eficiencia en la determinación de la característica del robot informático.

En esta modalidad, se simula el archivo malicioso para que se ejecute en los entornos de prueba y, los archivos de comportamiento, para ser específicos, los archivos de comportamiento dinámico, que registran los comportamientos de red del archivo malicioso en este proceso en ejecución se recopilan, de modo que se extrae la característica del robot informático de los archivos de comportamiento dinámico. Todo este proceso puede automatizarse, lo que mejora, de esta manera, la eficiencia en la extracción de la característica del robot informático. Además, debido a que la detección de comportamiento dinámico se realiza en el mismo archivo malicioso en al menos dos entornos de prueba, durante la extracción de la característica del robot informático, extraer la característica del robot informático de la característica común de los archivos de comportamiento dinámico respectivamente generada mediante al menos los dos entornos de prueba puede evitar que la característica extraída del robot informático incluya cadenas de caracteres rellenadas aleatoriamente mediante diferentes entornos de prueba en los archivos de comportamiento dinámico y una cadena de caracteres utilizada para describir información sobre un entorno de prueba (por ejemplo, una dirección de Protocolo de Internet y una dirección de puerto del entorno de prueba), lo que mejora de esta manera, la precisión de la característica del robot informático.

Para facilitar la comprensión, a continuación se describe el método para la detección de la característica del robot informático en esta modalidad mediante la utilización de un ejemplo con referencia a un escenario de aplicación real.

Con referencia a la Figura 2, la Figura 2 es un diagrama estructural esquemático de una modalidad de un sistema de comunicación de acuerdo con la presente invención. En esta modalidad, el sistema de comunicación incluye al menos un dispositivo de puerta de enlace y un dispositivo de ciberseguridad 202. Para facilitar la descripción, a continuación se utiliza un dispositivo de puerta de enlace 201 en al menos un dispositivo de puerta de enlace como ejemplo para la descripción. Después de recibir los paquetes de servicio, el dispositivo de puerta de enlace 201 determina, a partir de los paquetes de servicio, una serie de paquetes de servicio que se utilizan para transportar un mismo archivo, o en otras palabras, una sesión que se utiliza para transportar un mismo archivo y, reensambla la serie de paquetes de servicio para la restauración, para obtener un archivo transportado por una parte de la carga útil de la serie de paquetes. Cuando se determina que un archivo es un archivo bajo sospecha de ser malicioso, el dispositivo de puerta de enlace 201 utiliza el archivo como un archivo a detectar e ingresa el archivo en al menos dos entornos de prueba locales por separado.

Existe una pluralidad de métodos para que el dispositivo de puerta de enlace 201 determine que un archivo es un archivo bajo sospecha de ser malicioso. Por ejemplo, el dispositivo de puerta de enlace 201 primero realiza la comparación de coincidencia entre una URL de un archivo transportado en una sesión y una URL del robot informático prealmacenada localmente. Si la comparación de coincidencia es exitosa, el dispositivo de puerta de enlace 201 puede determinar directamente que el archivo es un archivo malicioso. Si la comparación de coincidencia no es exitosa, el dispositivo de red 201 determina además si el paquete de red es un archivo ejecutable portátil (Ejecutable Portátil, PE). Si el paquete de red es un archivo ejecutable portátil, el dispositivo de puerta de enlace 201 determina que el archivo es un archivo bajo sospecha de ser malicioso.

Con referencia a la Figura 3, la Figura 3 es un diagrama estructural esquemático de módulos, en el dispositivo de puerta de enlace 201, configurado para realizar la detección de un robot informático Troyano. El dispositivo de puerta de enlace 201 incluye al menos dos entornos de prueba, un módulo de determinación de amenazas, un módulo para la detección de la característica del robot informático, un módulo de gestión y control y, un módulo de gestión de entorno de prueba. Los entornos de prueba, el módulo de determinación de amenazas, el módulo para la detección de la característica del robot informático, el módulo de gestión y control y, el módulo de gestión de entorno de prueba son módulos de función implementados mediante la utilización de un programa de software. El módulo de gestión y control se configura para gestionar el módulo de determinación de amenazas y el módulo para la detección de la característica del robot informático. El módulo de gestión de entorno de prueba se configura para realizar operaciones tales como crear, deshabilitar y monitorear un entorno de prueba.

Después de que el dispositivo de puerta de enlace 201 obtiene un archivo a detectar, el módulo de gestión de entorno de prueba crea un entorno de prueba 1 y un entorno de prueba 2. El dispositivo de puerta de enlace 201 ingresa el archivo a detectar en el entorno de prueba 1 y en el entorno de prueba 2 por separado. Después de recibir el archivo a detectar por separado, el entorno de prueba 1 y el entorno de prueba 2 del dispositivo de puerta de enlace 201 realizan la detección de comportamiento estático y la detección de comportamiento dinámico en el archivo a detectar e ingresa los resultados de la detección en el módulo de determinación de amenazas. Específicamente, el entorno de prueba 1 ingresa un archivo de comportamiento estático 1 y un archivo de comportamiento dinámico 1 del archivo a detectar en el módulo de determinación de amenazas y, el entorno de prueba 2 ingresa un archivo de comportamiento estático 2 y un archivo de comportamiento dinámico 2 del archivo a detectar en el módulo de determinación de amenazas.

Como se muestra en la Tabla 1, la Tabla 1 es un diagrama esquemático de una modalidad de una estructura de un archivo de comportamiento estático.

Tabla 1

Número de serie	Elemento	Datos de muestra
1	ID de tarea	
2	Nombre del archivo	
3	Tamaño del archivo	
4	Firma digital	
5	Información de la versión	
6	Información de la envoltura	
7	Si desinstalar un programa	
8	Resultado de analizar un formato Win32 PE incorrecto	
9	Recuento de éxitos en comparación de coincidencias de secuencias API maliciosas	
9	Firma de unicidad del archivo	
10	Firma AV del flujo de archivos	

Como se muestra en la Tabla 2, la Tabla 2 es un diagrama esquemático de una modalidad de una estructura de un archivo de comportamiento dinámico.

Tabla 2

Número de serie	Elemento de nivel 1	Elemento de nivel 2	Datos de muestra
1	ID de tarea		
2	Nombre del archivo		
3	Secuencia de comportamiento dinámico		
4	Objeto operativo de comportamiento dinámico		
5	Datos de paquetes de red	Paquete de sesión 1	
		Paquete de sesión 2	
		...	
		Paquete de sesión n	

El módulo de determinación de amenazas determina si el archivo a detectar es un archivo malicioso en base a los archivos de comportamiento estático 1 y 2 y los archivos de comportamiento dinámico 1 y 2. Específicamente, el módulo de determinación de amenazas realiza una puntuación basada en el peso en un elemento de excepción en los cuatro archivos y, determina, en base a un resultado de puntuación, si el archivo a detectar es un archivo malicioso. La manera cómo se realiza específicamente la puntuación basada en el peso es la técnica anterior y, los detalles no se describen en la presente descripción.

El módulo de determinación de amenazas envía un resultado de determinación al módulo de gestión y control, de modo que el módulo de gestión y control notifique al módulo de gestión de entorno de prueba el resultado de determinación. Si el resultado de determinación indica que el archivo a detectar no es un archivo malicioso, el módulo de gestión de entorno de prueba deshabilita el entorno de prueba 1 y el entorno de prueba 2. Si el resultado de determinación indica que el archivo a detectar es un archivo malicioso, el módulo de determinación de amenazas envía los archivos de comportamiento dinámico 1 y 2 recibidos del archivo malicioso al módulo de gestión y control, de modo que el módulo de gestión y control reenvíe los dos archivos al módulo para la detección de la característica del robot informático.

Después de recibir los archivos de comportamiento dinámico 1 y 2 del archivo malicioso, el módulo para la detección de la característica del robot informático obtiene todos los paquetes de sesión en el archivo de comportamiento dinámico 1 y todos los paquetes de sesión en el archivo de comportamiento dinámico 2. El módulo para la detección de la característica del robot informático obtiene una lista blanca de protocolos. La lista blanca de protocolos almacena al menos un protocolo de capa de transporte. El módulo para la detección de la característica del robot informático marca todos los paquetes de sesión, en los archivos de comportamiento dinámico 1 y 2, que utilizan un protocolo de capa de transporte que se encuentra en la lista blanca de protocolos, numera los paquetes de sesión no marcados en el archivo de comportamiento dinámico 1 secuencialmente y, numera los paquetes de sesión no marcados en el archivo de comportamiento dinámico 2 secuencialmente. Los paquetes de sesión, en los archivos de comportamiento dinámico 1 y 2, que tienen una misma dirección IP de destino y un mismo puerto de destino tienen el mismo número. Durante la detección de la característica del robot informático, se analizan dos paquetes de sesión cualesquiera con el mismo número en los archivos de comportamiento dinámico 1 y 2, para obtener una característica clave en cada paquete de sesión. La característica clave incluye un campo de carga útil, un campo de solicitud y, un campo de

agente. Específicamente, a continuación se utiliza un paquete de sesión numerado 1 en el archivo de comportamiento dinámico 1 y un paquete de sesión numerado 1 en el archivo de comportamiento dinámico 2 como un ejemplo para la descripción.

El contenido en el paquete de sesión numerado 1 en el archivo de comportamiento dinámico 1 es el siguiente:

GET /ip.txt HTTP1.1
User-Agent:Huai_Huai
Host:2.2.2.3
Cache-Control:no-cache
HTTP/1.1 200 OK
Content-Type: text/plain
Content-Range:bytes 0-18/19
Content-Length: 19
Server:HFS 2.1d
Accept-Ranges:bytes
Content-Disposition:filename="ip.txt"
Last-Modified:Sat,12 May 2007
02:16:42 GMT
kvo2.2.2.60: 8000kid

El contenido en el paquete de sesión numerado 1 en el archivo de comportamiento dinámico 2 es el siguiente:

GET /ip.txt HTTP1.1
User-Agent:Huai_Huai
Host:2.2.2.3
Cache-Control:no-cache
HTTP/1.1 200 OK
Content-Type: text/plain
Content-Range:bytes 0-18/19
Content-Length: 19
Server:HFS 2.1d
Accept-Ranges:bytes
Content-Disposition:filename="ip.txt"
Last-Modified:Sat,12 May 2007
02:17:15 GMT
kvo2.2.2.18:8000kid

Para los dos paquetes de sesión, se utilizan los siguientes diferentes esquemas para detectar una característica del robot informático en los paquetes de sesión.

Esquema 1:

La identificación del protocolo se realiza en los dos paquetes de sesión para obtener los siguientes campos de carga útil mediante el análisis:
el paquete de sesión numerado 1 en el archivo de comportamiento dinámico 1: Packet1.HTTP. payload = kvo2.2.2.60:8000kid; y
el paquete de sesión numerado 1 en el archivo de comportamiento dinámico 2: Packet2.HTTP. payload = kvo2.2.2.18: 8000kid.

Los campos de carga útil se preprocesan de acuerdo con una regla de operación de preprocesamiento. La regla de operación de preprocesamiento ordena que se eliminen tales cadenas de caracteres como la IP del entorno de prueba: puerto "2.2.2.60:8000" en los campos. Específicamente, una cadena de caracteres "2.2.2.60:8000" se elimina cuando se obtiene posteriormente una característica común de los dos paquetes.

Para los campos de carga útil en los dos paquetes de sesión, los dos campos se comparan para verificar si los dos campos contienen la misma cadena de caracteres. Puede obtenerse que kvo y kid son tales cadenas de caracteres, que una ubicación de kvo en el campo de carga útil es una posición de dirección 0 en un orden normal y, una ubicación de kid en el campo de carga útil es una posición de dirección 1 en un orden inverso. Por lo tanto, la característica del robot informático incluye kvo y kid en el campo de carga útil y, las ubicaciones de las dos cadenas de caracteres en el campo de carga útil.

Esquema 2:

La identificación del protocolo se realiza en los dos paquetes de sesión para obtener los siguientes campos de solicitud mediante el análisis:

el paquete de sesión numerado 1 en el archivo de comportamiento dinámico 1: Packet1.HTTP.requst = GET /ip.txt HTTP/1.1; y
el paquete de sesión numerado 1 en el archivo de comportamiento dinámico 2: Packet2.HTTP.requst = GET /ip.txt HTTP/1.1.

Los campos de solicitud se preprocesan de acuerdo con una regla de operación de preprocesamiento. La regla de operación de preprocesamiento ordena que se eliminen las palabras clave HTTP "GET" y "HTTP/1.1" en los campos. Específicamente, dos cadenas de caracteres "GET" y "HTTP/1.1" se eliminan cuando se obtiene posteriormente una característica común de los dos paquetes.

Para los campos de solicitud en los dos paquetes de sesión, los dos campos se comparan para verificar si existe una misma cadena de caracteres en los dos campos. Puede obtenerse que /ip.txt es una cadena de caracteres y, una ubicación de la cadena de caracteres en el campo de solicitud es una posición de dirección 0 en un orden normal. Por lo tanto, la característica del robot informático incluye la cadena de caracteres /ip.txt en el campo de solicitud y, la ubicación de la cadena de caracteres en el campo de solicitud.

Esquema 3:

La identificación del protocolo se realiza en los dos paquetes de sesión para obtener los siguientes campos de agente mediante el análisis:
el paquete de sesión numerado 1 en el archivo de comportamiento dinámico 1: Packet1.HTTP.Agent = Huai_Huai; y
el paquete de sesión numerado 1 en el archivo de comportamiento dinámico 2: Packet2.HTTP.Agent = Huai_Huai.

Para los campos de agente en los dos paquetes de sesión, los dos campos se comparan para verificar si existe una misma cadena de caracteres en los dos campos. Puede obtenerse que Huai_Huai es una cadena de caracteres. Esta cadena de caracteres es diferente del contenido preestablecido en el campo de agente. Por lo tanto, se determina que la característica del robot informático incluye la cadena de caracteres Huai_Huai en el campo de agente.

Después de detectar una característica del robot informático en dos paquetes de sesión cualesquiera con un mismo número en los archivos de comportamiento dinámico 1 y 2, el módulo para la detección de la característica del robot informático describe la característica del robot informático para formar una entrada de regla y, envía la entrada de regla al módulo de gestión y control.

El módulo de gestión y control envía la entrada de regla al dispositivo de ciberseguridad 202. El dispositivo de ciberseguridad 202 recopila entradas de reglas de los dispositivos de puerta de enlace y, proporciona una función de descarga de datos de la característica del robot informático, de modo que otro dispositivo pueda descargar y almacenar datos de la característica del robot informático desde el dispositivo de ciberseguridad 202 y, los dispositivos de puerta de enlace puedan identificar, en base a los datos de la característica del robot informático, si un archivo es un archivo malicioso.

Lo anterior describe el método para la detección de la característica del robot informático en las modalidades y, a continuación se describe un aparato para la detección de la característica del robot informático en las modalidades.

Con referencia a la Figura 4, la Figura 4 es un diagrama estructural esquemático de una modalidad del aparato para la detección de la característica del robot informático en las modalidades. En esta modalidad, el aparato para la detección de la característica del robot informático 400 incluye:
un módulo de obtención 401, configurado para obtener un primer archivo de comportamiento dinámico y un segundo archivo de comportamiento dinámico, donde el primer archivo de comportamiento dinámico es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada en un archivo malicioso en un primer entorno de prueba y, el segundo archivo de comportamiento dinámico es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada en el archivo malicioso en un segundo entorno de prueba; y
un módulo de determinación 402, configurado para determinar una característica del robot informático del archivo malicioso en base a una característica común del primer archivo de comportamiento dinámico y del segundo archivo de comportamiento dinámico.

En algunas posibles implementaciones de esta modalidad, el primer archivo de comportamiento dinámico incluye un primer paquete de sesión, el segundo archivo de comportamiento dinámico incluye un segundo paquete de sesión, una dirección IP de destino de protocolo de Internet del primer paquete de sesión es la misma que una dirección IP de destino del segundo paquete de sesión y, un puerto de destino del primer paquete de sesión es el mismo que un puerto de destino del segundo paquete de sesión; y

el módulo de determinación 402 se configura específicamente para determinar la característica del robot informático del archivo malicioso en base a una característica común del primer paquete de sesión y del segundo paquete de sesión.

En las implementaciones anteriores, opcionalmente, el módulo de determinación 402 se configura específicamente para:
obtener una regla de operación de preprocesamiento, donde la regla de operación de preprocesamiento ordena que se elimine un carácter especificado en un paquete;
obtener el primer contenido restante del primer paquete de sesión y el segundo contenido restante del segundo paquete de sesión de acuerdo con la regla de operación de preprocesamiento, donde el primer contenido restante es el contenido del paquete en el primer paquete de sesión excepto el carácter especificado y, el segundo contenido restante es el contenido del paquete en el segundo paquete de sesión excepto el carácter especificado; y
determinar la característica del robot informático del archivo malicioso en base a una característica común del primer contenido restante y del segundo contenido restante.

En las implementaciones anteriores, opcionalmente, el módulo de determinación 402 se configura específicamente para:
obtener un primer campo preconfigurado; y
determinar si el contenido en el primer campo preconfigurado en el primer paquete de sesión y el contenido en el primer campo preconfigurado en el segundo paquete de sesión contienen una misma cadena de caracteres; y si el contenido en el primer campo preconfigurado en el primer paquete de sesión y el contenido en el primer campo preconfigurado en el segundo paquete de sesión contienen una misma cadena de caracteres, determinar que la característica del robot informático del archivo malicioso incluye la cadena de caracteres y una ubicación de la cadena de caracteres en el primer campo preconfigurado.

En las implementaciones anteriores, opcionalmente, el módulo de determinación 402 se configura específicamente para:
obtener un segundo campo preconfigurado y un contenido preestablecido en el segundo campo preconfigurado; y
cuando el segundo campo preconfigurado existe en la característica común del primer paquete de sesión y del segundo paquete de sesión y, el contenido en el segundo campo preconfigurado en la característica común es diferente del contenido preestablecido, determinar que la característica del robot informático incluye el contenido en el segundo campo preconfigurado en la característica común.

En algunas posibles implementaciones de esta modalidad, el módulo de obtención 401 se configura específicamente para:
obtener un archivo de comportamiento estático y un archivo de comportamiento dinámico que se generan mediante el primer entorno de prueba y, un archivo de comportamiento estático y un archivo de comportamiento dinámico que se generan mediante el segundo entorno de prueba, donde el archivo de comportamiento estático generado mediante el primer entorno de prueba es un archivo de comportamiento que resulta de la detección de comportamiento estático realizada en un archivo a detectar en el primer entorno de prueba, el archivo de comportamiento estático generado mediante el segundo entorno de prueba es un archivo de comportamiento que resulta de la detección de comportamiento estático realizada en el archivo a detectar en el segundo entorno de prueba, el archivo de comportamiento dinámico generado mediante el primer entorno de prueba es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada en el archivo a detectar en el primer entorno de prueba y, el archivo de comportamiento dinámico generado mediante el segundo entorno de prueba es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada en el archivo a detectar en el segundo entorno de prueba;
determinar si el archivo a detectar es un archivo malicioso en base al archivo de comportamiento estático y al archivo de comportamiento dinámico que se generan mediante el primer entorno de prueba y, al archivo de comportamiento estático y al archivo de comportamiento dinámico que se generan mediante el segundo entorno de prueba; y
al determinar que el archivo a detectar es un archivo malicioso, determinar que el archivo de comportamiento dinámico generado mediante el primer entorno de prueba es el primer archivo de comportamiento dinámico y, que el archivo de comportamiento dinámico generado mediante el segundo entorno de prueba es el segundo archivo de comportamiento dinámico.

En algunas posibles implementaciones de esta modalidad, el módulo de obtención 401 se configura específicamente para:
obtener el archivo malicioso;
ingresar el archivo malicioso en el primer entorno de prueba y en el segundo entorno de prueba por separado para la detección de comportamiento dinámico; y obtener un archivo de comportamiento dinámico generado mediante el primer entorno de prueba y un archivo de comportamiento dinámico generado mediante el segundo entorno de prueba.

El aparato para la detección de la característica del robot informático mostrado en la Figura 4 puede implementarse mediante software o hardware integrado en un dispositivo informático. Para las funciones adicionales que el aparato puede implementar, consulte las descripciones del dispositivo de puerta de enlace en la modalidad del método y, los detalles no se describen de nuevo en la presente descripción.

En esta modalidad, el aparato para la detección de la característica del robot informático realiza la detección de comportamiento dinámico en el archivo malicioso en los entornos de prueba, recopila, mediante la utilización de los entornos de prueba, todos los comportamientos de red del archivo malicioso durante un proceso en ejecución, genera

los archivos de comportamiento dinámico que registran los comportamientos de red y, extrae la característica del robot informático de los archivos de comportamiento dinámico. De esta forma, puede extraerse una firma de comunicación del robot informático. Esto ayuda a implementar la detección de un archivo malicioso en base a la firma característica de comunicación y, evita los falsos positivos y los falsos negativos informados debido a la interferencia de varias variantes de un archivo de robot informático. Además, debido a que la detección de comportamiento dinámico se realiza en el mismo archivo malicioso en al menos dos entornos de prueba, durante la extracción de la característica del robot informático, extraer la característica del robot informático de la característica común de los archivos de comportamiento dinámico respectivamente generados mediante al menos dos entornos de prueba puede evitar que la característica del robot informático extraída incluya cadenas de caracteres rellenadas aleatoriamente mediante diferentes entornos de prueba en los archivos de comportamiento dinámico y una cadena de caracteres utilizada para describir información sobre un entorno de prueba (por ejemplo, una dirección IP y una dirección de puerto del entorno de prueba), mejorando, de esta manera, la precisión de la característica del robot informático.

Lo anterior describe el aparato para la detección de la característica del robot informático en las modalidades desde una perspectiva de entidades funcionales unificadas. A continuación se describe el aparato para la detección de la característica del robot informático en las modalidades desde una perspectiva de procesamiento de hardware.

Con referencia a la Figura 5, la Figura 5 es un diagrama estructural esquemático de una modalidad de un dispositivo de puerta de enlace en las modalidades. En esta modalidad, el dispositivo de puerta de enlace 500 incluye:
uno o varios procesadores 502, una memoria 501 y, un bus de comunicaciones 503, donde los procesadores 502 y la memoria 501 se conectan mediante la utilización del bus de comunicaciones 503,
uno o varios programas se almacenan en la memoria 501, el único o demás programas incluyen una instrucción y, cuando la instrucción se ejecuta mediante el dispositivo de puerta de enlace, el dispositivo de puerta de enlace realiza las siguientes operaciones:
obtener un primer archivo de comportamiento dinámico y un segundo archivo de comportamiento dinámico, donde el primer archivo de comportamiento dinámico es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada en un archivo malicioso en un primer entorno de prueba y, el segundo archivo de comportamiento dinámico es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada en el archivo malicioso en un segundo entorno de prueba; y
determinar una característica del robot informático del archivo malicioso en base a una característica común del primer archivo de comportamiento dinámico y del segundo archivo de comportamiento dinámico.

Opcionalmente, el primer archivo de comportamiento dinámico incluye un primer paquete de sesión, el segundo archivo de comportamiento dinámico incluye un segundo paquete de sesión, una dirección IP de destino de protocolo de Internet del primer paquete de sesión es la misma que la dirección IP de destino del segundo paquete de sesión y, un puerto de destino del primer paquete de sesión es el mismo que un puerto de destino del segundo paquete de sesión; y

la determinación de la característica del robot informático del archivo malicioso en base a una característica común del primer archivo de comportamiento dinámico y del segundo archivo de comportamiento dinámico incluye:

determinar la característica del robot informático del archivo malicioso en base a una característica común del primer paquete de sesión y del segundo paquete de sesión.

Opcionalmente, la determinación de la característica del robot informático del archivo malicioso en base a una característica común del primer paquete de sesión y del segundo paquete de sesión incluye:
obtener una regla de operación de preprocesamiento, donde la regla de operación de preprocesamiento ordena que se elimine un carácter especificado en un paquete;
obtener el primer contenido restante del primer paquete de sesión y el segundo contenido restante del segundo paquete de sesión de acuerdo con la regla de operación de preprocesamiento, donde el primer contenido restante es el contenido del paquete en el primer paquete de sesión excepto el carácter especificado y, el segundo contenido restante es el contenido del paquete en el segundo paquete de sesión excepto el carácter especificado; y
determinar la característica del robot informático del archivo malicioso en base a una característica común del primer contenido restante y del segundo contenido restante.

Opcionalmente, la determinación de la característica del robot informático del archivo malicioso en base a una característica común del primer paquete de sesión y del segundo paquete de sesión incluye:
obtener un primer campo preconfigurado; y
determinar si el contenido en el primer campo preconfigurado en el primer paquete de sesión y el contenido en el primer campo preconfigurado en el segundo paquete de sesión contienen la misma cadena de caracteres; y si el contenido en el primer campo preconfigurado en el primer paquete de sesión y el contenido en el primer campo preconfigurado en el segundo paquete de sesión contienen una misma cadena de caracteres, determinar que la característica del robot informático del archivo malicioso incluye la cadena de caracteres y una ubicación de la cadena de caracteres en el primer campo preconfigurado.

Opcionalmente, la determinación de la característica del robot informático del archivo malicioso en base a una característica común del primer paquete de sesión y del segundo paquete de sesión incluye:
obtener un segundo campo preconfigurado y un contenido preestablecido en el segundo campo preconfigurado; y
cuando el segundo campo preconfigurado existe en la característica común del primer paquete de sesión y del segundo paquete de sesión y, el contenido en el segundo campo preconfigurado en la característica común es diferente del contenido preestablecido, determinar que la característica del robot informático incluye el contenido en el segundo campo preconfigurado en la característica común.

Opcionalmente, la obtención de un primer archivo de comportamiento dinámico y de un segundo archivo de comportamiento dinámico incluye:
obtener un archivo de comportamiento estático y un archivo de comportamiento dinámico que se generan mediante el primer entorno de prueba y, un archivo de comportamiento estático y un archivo de comportamiento dinámico que se generan mediante el segundo entorno de prueba, donde el archivo de comportamiento estático generado mediante el primer entorno de prueba es un archivo de comportamiento que resulta de la detección de comportamiento estático realizada en un archivo a detectar en el primer entorno de prueba, el archivo de comportamiento estático generado mediante el segundo entorno de prueba es un archivo de comportamiento que resulta de la detección de comportamiento estático realizada en el archivo a detectar en el segundo entorno de prueba, el archivo de comportamiento dinámico generado mediante el primer entorno de prueba es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada en el archivo a detectar en el primer entorno de prueba y, el archivo de comportamiento dinámico generado mediante el segundo entorno de prueba es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada en el archivo a detectar en el segundo entorno de prueba;
determinar si el archivo a detectar es un archivo malicioso en base al archivo de comportamiento estático y al archivo de comportamiento dinámico que se generan mediante el primer entorno de prueba y, al archivo de comportamiento estático y al archivo de comportamiento dinámico que se generan mediante el segundo entorno de prueba; y
al determinar que el archivo a detectar es un archivo malicioso, determinar que el archivo de comportamiento dinámico generado mediante el primer entorno de prueba es el primer archivo de comportamiento dinámico y, que el archivo de comportamiento dinámico generado mediante el segundo entorno de prueba es el segundo archivo de comportamiento dinámico.

Opcionalmente, la obtención de un primer archivo de comportamiento dinámico y de un segundo archivo de comportamiento dinámico incluye:
obtener el archivo malicioso;
ingresar el archivo malicioso en el primer entorno de prueba y en el segundo entorno de prueba por separado para la detección de comportamiento dinámico; y
obtener un archivo de comportamiento dinámico generado mediante el primer entorno de prueba y, un archivo de comportamiento dinámico generado mediante el segundo entorno de prueba.

Un experto en la técnica puede entender claramente que, para el propósito de una descripción conveniente y breve, para un proceso de trabajo detallado del dispositivo de puerta de enlace 500, consulte la descripción relacionada con el dispositivo de puerta de enlace en la modalidad del método anterior y, los detalles no se describen de nuevo en la presente descripción.

En las diversas modalidades proporcionadas en esta solicitud, debe entenderse que el sistema, aparato y método descritos pueden implementarse de otras maneras. Por ejemplo, las modalidades del aparato descritas son simplemente ejemplos. Por ejemplo, la división de unidades es simplemente una división de función lógica y puede ser otra división en la implementación real.

Las soluciones técnicas de las modalidades 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 informático se almacena en un medio de almacenamiento e incluye varias instrucciones para ordenar a un dispositivo informático (que puede ser un ordenador personal, un servidor, un dispositivo de red o similar) que realice la totalidad o parte de las etapas del método descrito en las modalidades de la presente invención. El medio de almacenamiento anterior incluye cualquier medio que pueda almacenar código de programa, tal como una unidad flash USB, un disco duro extraíble, una memoria de sólo lectura (ROM, Memoria de Sólo Lectura), una memoria de acceso aleatorio (RAM, Memoria de Acceso Aleatorio), un disco magnético o un disco óptico.

Las modalidades anteriores se destinan simplemente a describir las soluciones técnicas de las modalidades, en lugar de limitar las modalidades. Con referencia a las modalidades anteriores, un experto en la técnica puede realizar modificaciones a las soluciones técnicas descritas en las modalidades o realizar sustituciones equivalentes a algunas características técnicas de las mismas. Sin embargo, estas modificaciones o sustituciones no hacen que sus soluciones técnicas correspondientes se aparten del ámbito de las soluciones técnicas de las modalidades.

REIVINDICACIONES

1. Un método para la detección de la característica del robot informático, que comprende:
obtener (101)
un primer archivo de comportamiento dinámico y un segundo archivo de comportamiento dinámico, en donde el primer archivo de comportamiento dinámico es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada en un archivo malicioso en un primer entorno de prueba y, el segundo archivo de comportamiento dinámico es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada en el archivo malicioso en el segundo entorno de prueba; y
determinar (102) una característica del robot informático del archivo malicioso en base a una característica común del primer archivo de comportamiento dinámico y del segundo archivo de comportamiento dinámico,
en donde el primer archivo de comportamiento dinámico comprende un primer paquete de sesión, el segundo archivo de comportamiento dinámico comprende un segundo paquete de sesión, una dirección de Protocolo de Internet, IP, de destino del primer paquete de sesión es la misma que la dirección IP de destino del segundo paquete de sesión y, un puerto de destino del primer paquete de sesión es el mismo que un puerto de destino del segundo paquete de sesión; y
la determinación de la característica del robot informático del archivo malicioso en base a una característica común del primer archivo de comportamiento dinámico y del segundo archivo de comportamiento dinámico comprende:
determinar la característica del robot informático del archivo malicioso en base a una característica común del primer paquete de sesión y del segundo paquete de sesión.

2. El método para la detección de la característica del robot informático de acuerdo con la reivindicación 1, en donde la determinación de la característica del robot informático del archivo malicioso en base a una característica común del primer paquete de sesión y del segundo paquete de sesión comprende:
obtener una regla de operación de preprocesamiento, en donde la regla de operación de preprocesamiento ordena que se elimine un carácter especificado en un paquete;
obtener el primer contenido restante del primer paquete de sesión y el segundo contenido restante del segundo paquete de sesión de acuerdo con la regla de operación de preprocesamiento, en donde el primer contenido restante es el contenido del paquete en el primer paquete de sesión excepto el carácter especificado y, el segundo contenido restante es el contenido del paquete en el segundo paquete de sesión excepto el carácter especificado; y
determinar la característica del robot informático del archivo malicioso en base a una característica común del primer contenido restante y del segundo contenido restante.

3. El método para la detección de la característica del robot informático de acuerdo con la reivindicación 1, en donde la determinación de la característica del robot informático del archivo malicioso en base a una característica común del primer paquete de sesión y del segundo paquete de sesión comprende:
obtener un primer campo preconfigurado; y
determinar si el contenido en el primer campo preconfigurado en el primer paquete de sesión y el contenido en el primer campo preconfigurado en el segundo paquete de sesión contienen la misma cadena de caracteres; y si el contenido en el primer campo preconfigurado en el primer paquete de sesión y el contenido en el primer campo preconfigurado en el segundo paquete de sesión contienen una misma cadena de caracteres, determinar que la característica del robot informático del archivo malicioso comprende la cadena de caracteres y una ubicación de la cadena de caracteres en el primer campo preconfigurado.

4. El método para la detección de la característica del robot informático de acuerdo con la reivindicación 1, en donde la determinación de la característica del robot informático del archivo malicioso en base a una característica común del primer paquete de sesión y del segundo paquete de sesión comprende:
obtener un segundo campo preconfigurado y un contenido preestablecido en el segundo campo preconfigurado; y
cuando el segundo campo preconfigurado existe en la característica común del primer paquete de sesión y del segundo paquete de sesión y, el contenido en el segundo campo preconfigurado en la característica común es diferente del contenido preestablecido, determinar que la característica del robot informático comprende el contenido en el segundo campo preconfigurado en la característica común.

5. El método para la detección de la característica del robot informático de acuerdo con cualquiera de las reivindicaciones 1 a la 4, en donde la obtención de un primer archivo de comportamiento dinámico y de un segundo archivo de comportamiento dinámico comprende:
obtener un archivo de comportamiento estático y un archivo de comportamiento dinámico que se generan mediante el primer entorno de prueba y, un archivo de comportamiento estático y un archivo de comportamiento dinámico que se generan mediante el segundo entorno de prueba, en donde el archivo de comportamiento estático generado mediante el primer entorno de prueba es un archivo de comportamiento que resulta de la detección de comportamiento estático realizada en un archivo a detectar en el primer entorno de prueba, el archivo de comportamiento estático generado mediante el segundo entorno de prueba es un archivo de comportamiento que resulta de la detección de comportamiento estático realizada en el archivo a detectar en

el segundo entorno de prueba, el archivo de comportamiento dinámico generado mediante el primer entorno de prueba es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada en el archivo a detectar en el primer entorno de prueba y, el archivo de comportamiento dinámico generado mediante el segundo entorno de prueba es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada en el archivo a detectar en el segundo entorno de prueba;
determinar si el archivo a detectar es un archivo malicioso en base al archivo de comportamiento estático y al archivo de comportamiento dinámico que se generan mediante el primer entorno de prueba y, al archivo de comportamiento estático y al archivo de comportamiento dinámico que se generan mediante el segundo entorno de prueba; y
al determinar que el archivo a detectar es un archivo malicioso, determinar que el archivo de comportamiento dinámico generado mediante el primer entorno de prueba es el primer archivo de comportamiento dinámico y, que el archivo de comportamiento dinámico generado mediante el segundo entorno de prueba es el segundo archivo de comportamiento dinámico.

6. El método para la detección de la característica del robot informático de acuerdo con cualquiera de las reivindicaciones 1 a la 4, en donde la obtención de un primer archivo de comportamiento dinámico y de un segundo archivo de comportamiento dinámico comprende:
obtener el archivo malicioso;
ingresar el archivo malicioso en el primer entorno de prueba y en el segundo entorno de prueba por separado para la detección de comportamiento dinámico; y
obtener un archivo de comportamiento dinámico generado mediante el primer entorno de prueba y, un archivo de comportamiento dinámico generado mediante el segundo entorno de prueba.

7. Un aparato para la detección de la característica del robot informático (400), que comprende:
un módulo de obtención (401), configurado para obtener un primer archivo de comportamiento dinámico y un segundo archivo de comportamiento dinámico, en donde el primer archivo de comportamiento dinámico es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada en un archivo malicioso en un primer entorno de prueba y, el segundo archivo de comportamiento dinámico es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada en el archivo malicioso en un segundo entorno de prueba; y
un módulo de determinación (402), configurado para determinar una característica del robot informático del archivo malicioso en base a una característica común del primer archivo de comportamiento dinámico y del segundo archivo de comportamiento dinámico,
en donde el primer archivo de comportamiento dinámico comprende un primer paquete de sesión, el segundo archivo de comportamiento dinámico comprende un segundo paquete de sesión, una dirección de Protocolo de Internet, IP, de destino del primer paquete de sesión es la misma que la dirección IP de destino del segundo paquete de sesión y, un puerto de destino del primer paquete de sesión es el mismo que un puerto de destino del segundo paquete de sesión; y
el módulo de determinación (402) se configura específicamente para determinar la característica del robot informático del archivo malicioso en base a una característica común del primer paquete de sesión y del segundo paquete de sesión.

8. El aparato para la detección de la característica del robot informático (400) de acuerdo con la reivindicación 7, en donde el módulo de determinación (402) se configura específicamente para:
obtener una regla de operación de preprocesamiento, en donde la regla de operación de preprocesamiento ordena que se elimine un carácter especificado en un paquete;
obtener el primer contenido restante del primer paquete de sesión y el segundo contenido restante del segundo paquete de sesión de acuerdo con la regla de operación de preprocesamiento, en donde el primer contenido restante es el contenido del paquete en el primer paquete de sesión excepto el carácter especificado y, el segundo contenido restante es el contenido del paquete en el segundo paquete de sesión excepto el carácter especificado; y
determinar la característica del robot informático del archivo malicioso en base a una característica común del primer contenido restante y del segundo contenido restante.

9. El aparato para la detección de la característica del robot informático (400) de acuerdo con la reivindicación 7, en donde el módulo de determinación (402) se configura específicamente para:
obtener un primer campo preconfigurado; y
determinar si el contenido en el primer campo preconfigurado en el primer paquete de sesión y el contenido en el primer campo preconfigurado en el segundo paquete de sesión contienen una misma cadena de caracteres; y si el contenido en el primer campo preconfigurado en el primer paquete de sesión y el contenido en el primer campo preconfigurado en el segundo paquete de sesión contienen una misma cadena de caracteres, determinar que la característica del robot informático del archivo malicioso comprende la cadena de caracteres y una ubicación de la cadena de caracteres en el primer campo preconfigurado.

10. El aparato para la detección de la característica del robot informático (400) de acuerdo con la reivindicación 7, en donde el módulo de determinación (402) se configura específicamente para:

obtener un segundo campo preconfigurado y un contenido preestablecido en el segundo campo preconfigurado; y
cuando el segundo campo preconfigurado existe en la característica común del primer paquete de sesión y del segundo paquete de sesión y, el contenido en el segundo campo preconfigurado en la característica común es diferente del contenido preestablecido, determinar que la característica del robot informático comprende el contenido en el segundo campo preconfigurado en la característica común.

11. El aparato para la detección de la característica del robot informático (400) de acuerdo con cualquiera de las reivindicaciones 7 a la 10, en donde el módulo de obtención (401) se configura específicamente para:
obtener un archivo de comportamiento estático y un archivo de comportamiento dinámico que se generan mediante el primer entorno de prueba y, un archivo de comportamiento estático y un archivo de comportamiento dinámico que se generan mediante el segundo entorno de prueba, en donde el archivo de comportamiento estático generado mediante el primer entorno de prueba es un archivo de comportamiento que resulta de la detección de comportamiento estático realizada en un archivo a detectar en el primer entorno de prueba, el archivo de comportamiento estático generado mediante el segundo entorno de prueba es un archivo de comportamiento que resulta de la detección de comportamiento estático realizada en el archivo a detectar en el segundo entorno de prueba, el archivo de comportamiento dinámico generado mediante el primer entorno de prueba es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada en el archivo a detectar en el primer entorno de prueba y, el archivo de comportamiento dinámico generado mediante el segundo entorno de prueba es un archivo de comportamiento que resulta de la detección de comportamiento dinámico realizada en el archivo a detectar en el segundo entorno de prueba;
determinar si el archivo a detectar es un archivo malicioso en base al archivo de comportamiento estático y al archivo de comportamiento dinámico que se generan mediante el primer entorno de prueba y, al archivo de comportamiento estático y al archivo de comportamiento dinámico que se generan mediante el segundo entorno de prueba; y
al determinar que el archivo a detectar es un archivo malicioso, determinar que el archivo de comportamiento dinámico generado mediante el primer entorno de prueba es el primer archivo de comportamiento dinámico y, que el archivo de comportamiento dinámico generado mediante el segundo entorno de prueba es el segundo archivo de comportamiento dinámico.

12. El aparato para la detección de la característica del robot informático (400) de acuerdo con cualquiera de las reivindicaciones 7 a la 11, en donde el módulo de obtención (401) se configura específicamente para:
obtener el archivo malicioso;
ingresar el archivo malicioso en el primer entorno de prueba y en el segundo entorno de prueba por separado para la detección de comportamiento dinámico; y
obtener un archivo de comportamiento dinámico generado mediante el primer entorno de prueba y, un archivo de comportamiento dinámico generado mediante el segundo entorno de prueba.

13. Un producto de programa informático comprende instrucciones de código de programa para realizar un método de acuerdo con cualquiera de las reivindicaciones 1 a la 6 cuando las instrucciones de código de ordenador se ejecutan en un ordenador.

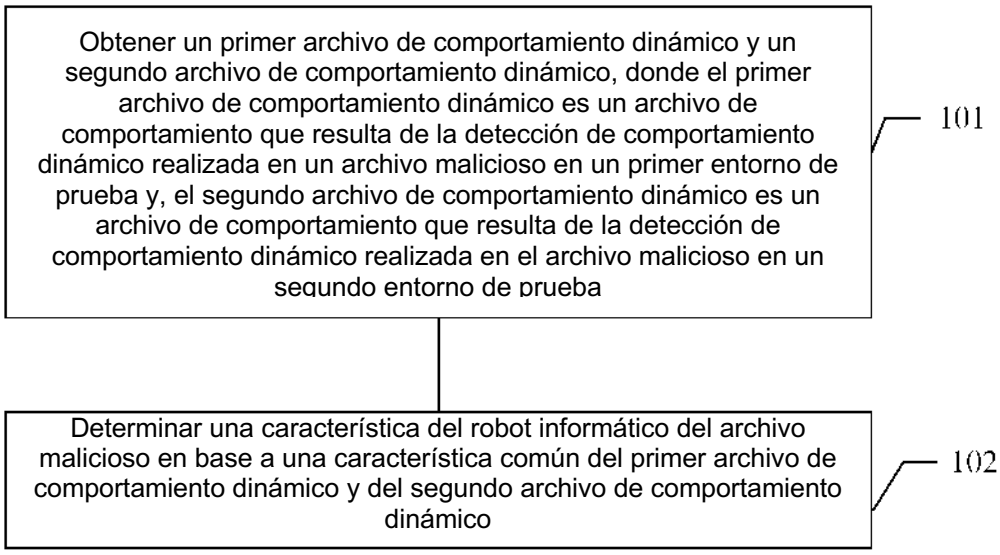

Figura 1

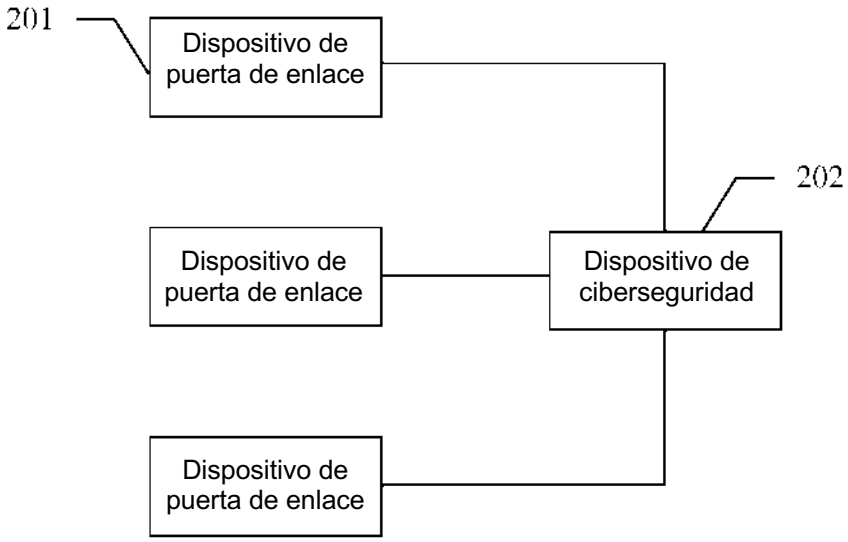

Figura 2

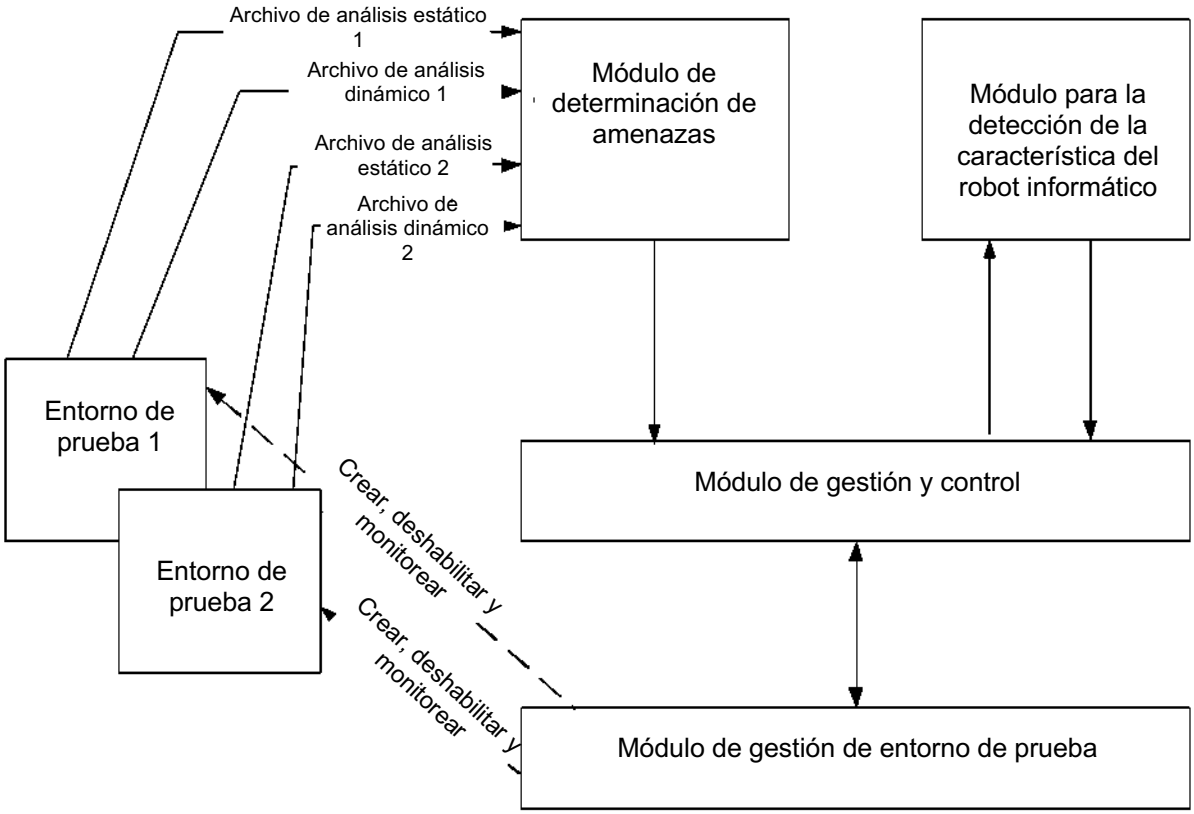

Figura 3

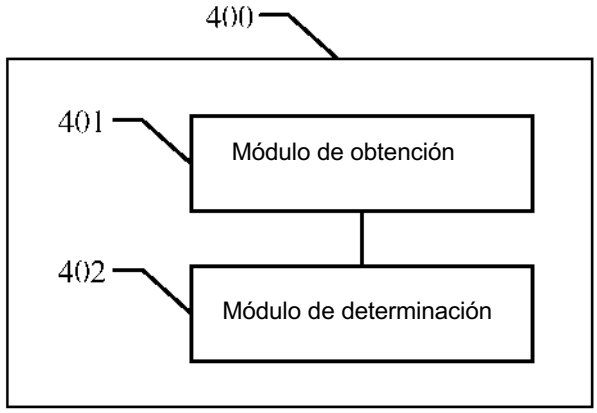

Figura 4

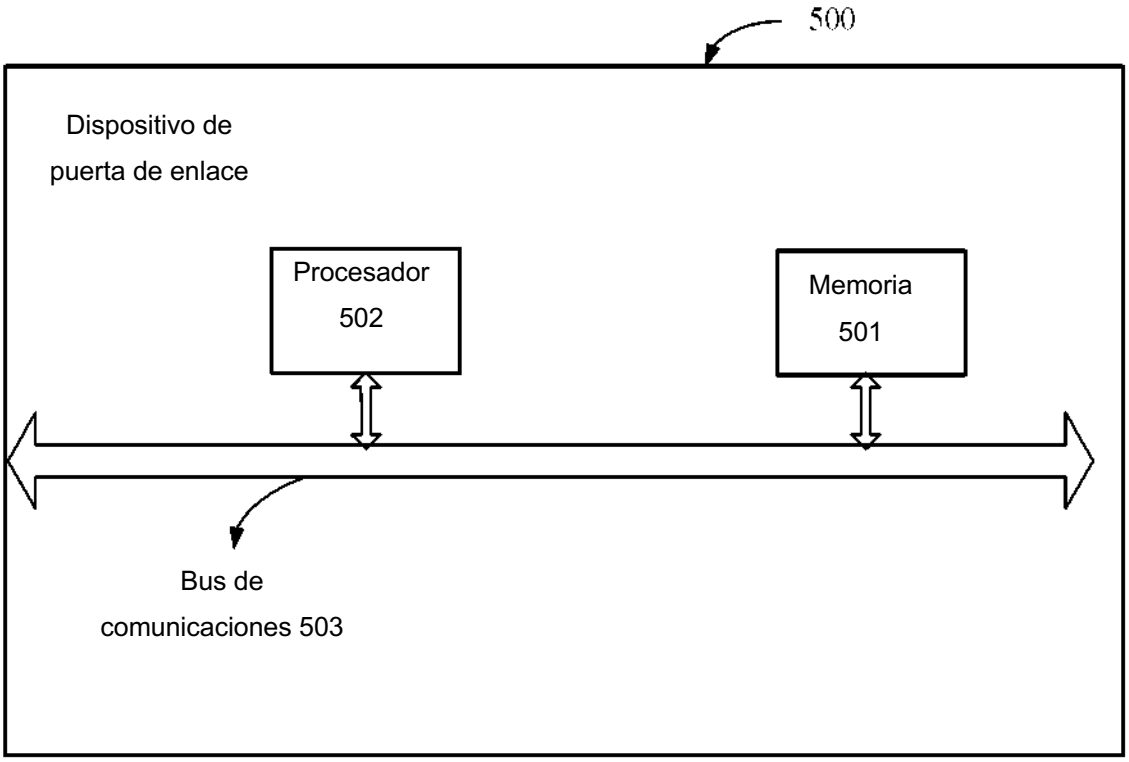
500
Dispositivo de
puerta de enlace
Procesador
502
Memoria
501
Bus de
comunicaciones 503

Figura 5