(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 775 874**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/55 (2013.01)
G06F 21/56 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **30.09.2016 PCT/CN2016/101263**

(87) Fecha y número de publicación internacional: **29.06.2017 WO17107616**

(96) Fecha de presentación y número de la solicitud europea: **30.09.2016 E 16877427 (1)**

(97) Fecha y número de publicación de la concesión europea: **05.02.2020 EP 3288231**

(54) Título: **Método, aparato y sistema para detectar condiciones de seguridad de un terminal**

(30) Prioridad:

24.12.2015 CN 201510988051

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.07.2020

(73) Titular/es:

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

(72) Inventor/es:

GAN, YONGCUN

(74) Agente/Representante:

SÁNCHEZ SILVA, Jesús Eladio

DESCRIPCIÓN

Método, aparato y sistema para detectar condiciones de seguridad de un terminal

Campo técnico

Esta solicitud se refiere al campo de los ordenadores y, en particular, al campo de la protección de la seguridad informática.

Antecedentes

A medida que surge una amenaza de próxima generación representada por una APT (Advanced Persistent Threat, amenaza persistente avanzada), un enfoque de protección de seguridad convencional enfrenta desafíos. Una vez atacado por la APT, se filtra un secreto comercial central de una empresa, lo que resulta en pérdidas incalculables para la empresa, o más severamente, las industrias relacionadas con las economías nacionales y el sustento de las personas, tales como la industria financiera, la industria energética y la industria del transporte, están paralizados. Su efecto es tan severo como el de una guerra.

En 2010, Google (Google Incorporation) fue atacado por una amenaza de próxima generación de Aurora. Como resultado, se filtró una gran cantidad de correos electrónicos de Gmail (un servicio de correo electrónico de red gratuito de Google), lo que afectó gravemente a la marca Google. En 2010, las instalaciones nucleares de Irán fueron atacadas por Stuxnet (Stuxnet), causando un daño severo a una centrífuga, que es un componente central, de las instalaciones nucleares. Una consecuencia de este ataque es tan grave como un bombardeo de precisión. En 2011, RSA fue atacado por una amenaza de próxima generación para SecureID. En consecuencia, se filtró una gran cantidad de datos de SecureID y la seguridad de los clientes que usaban SecureID se vio gravemente afectada. Las dudas sobre la seguridad de RSA afectaron gravemente la imagen pública de RSA. En marzo de 2013, la industria bancaria de la República de Corea fue atacada por una APT orientada. En consecuencia, muchos sistemas de aplicaciones principales bancarias se averiaron, afectando gravemente la imagen de los bancos en la mente de los clientes. Cómo hacer frente a la amenaza de la próxima generación representada por la APT en el futuro y cómo hacer frente a una posible guerra de red en el futuro son problemas importantes que enfrentan las personas.

En una red de usuarios existente, el programa informático antivirus generalmente se instala en un dispositivo terminal y se implementa un entorno de prueba frente a una puerta de enlace o un servidor de correo electrónico. El programa informático antivirus instalado en el dispositivo terminal detecta el programa informático malicioso principalmente mediante el uso de una biblioteca de características más reciente proporcionada por un proveedor de programas informáticos, y el entorno limitado se implementa frente a la puerta de enlace o el servidor de correo electrónico, principalmente para detectar una APT de Internet.

Un entorno de prueba existente es capaz de detectar la APT desde Internet. En la técnica anterior, puede controlarse que la APT ataque una red interna, pero no se puede detectar si un terminal de usuario está infectado con la APT y los terminales de usuario infectados con la APT. Por ejemplo, un entorno de prueba detecta que una red interna a la que pertenece el entorno de prueba es atacada por una APT, y el ataque APT se envía a los terminales de usuario mediante un correo electrónico. Algunos terminales de usuario están infectados con la APT porque han abierto el correo electrónico, incluido un archivo adjunto de APT, y algunos terminales de usuario no están infectados con la APT porque no han abierto el correo electrónico. Para otro ejemplo, un entorno de prueba detecta que una red interna a la que pertenece el entorno de prueba es atacada por una APT, y el ataque APT se implementa mediante el uso de una vulnerabilidad de una versión particular del programa informático de la aplicación. Algunos terminales de usuario usan esta versión del programa informático de la aplicación y, por lo tanto, son atacados por la APT. Algunos terminales de usuario usan una versión posterior, que no tiene la vulnerabilidad correspondiente, del programa informático de la aplicación y, por lo tanto, la APT no ataca a los terminales de usuario.

Sin embargo, si una APT ataca una red puede detectarse mediante el uso de una solución técnica existente, no se puede determinar si un terminal de usuario está infectado con la APT y los terminales de usuario específicos infectados con la APT. Por lo tanto, no se puede utilizar ninguna operación dirigida.

El documento WO 2015/127475 A1 describe un sistema configurado para detectar programa malicioso. El sistema incluye un paquete de verificación de infección configurado para realizar detonación de comportamiento, identificar un objeto de programa malicioso basado en aprendizaje automático; y seleccionar uno o más artefactos persistentes del programa malicioso en el sistema de destino en función de uno o más algoritmos aplicados a los rastros de comportamiento del objeto de programa malicioso.

Resumen

En esta descripción se describe un método, un aparato y un sistema para detectar el estado de seguridad de un terminal, para detectar si un terminal específico está infectado con una APT.

De acuerdo con un primer aspecto, una modalidad de esta solicitud proporciona un aparato para detectar un estado de seguridad del terminal. El aparato está ubicado en una unión entre una red privada y una red pública, y un terminal está ubicado en la red privada. El aparato incluye un módulo de generación de resultados de comportamiento dinámico, un módulo de análisis de comportamiento dinámico y un indicador de generador de compromiso.

El módulo de generación de resultados de comportamiento dinámico se configura para: recibir un archivo de la red pública y ejecutar el archivo en el aparato, para generar un resultado de comportamiento dinámico. El resultado del comportamiento dinámico incluye una secuencia de comportamiento que se genera de acuerdo con un orden cronológico de ocurrencia de comportamientos. Los comportamientos en la secuencia de comportamiento pertenecen a diferentes tipos de comportamiento, y los tipos de comportamiento incluyen crear un archivo, modificar un registro, configurar un nombre de dominio, resolver una dirección, conectarse a una red, cargar un proceso y agregar un usuario. El módulo de análisis de comportamiento dinámico se configura para determinar, de acuerdo con el resultado del comportamiento dinámico generado por el módulo de generación de resultados de comportamiento dinámico, si el archivo incluye una amenaza persistente avanzada. El indicador de generador de compromiso se configura para: si el módulo de análisis de comportamiento dinámico determina que el archivo incluye la amenaza persistente avanzada, obtener una característica de comportamiento estable en el resultado del comportamiento dinámico, generar un indicador de compromiso correspondiente de acuerdo con la característica de comportamiento estable, y enviar el indicador de compromiso al terminal. La característica de comportamiento estable es un comportamiento que siempre existe en una secuencia de comportamiento que se genera cada vez que se ejecuta el archivo.

El indicador de generador de compromiso se configura para implementar las siguientes etapas para obtener una característica de comportamiento estable en el resultado del comportamiento dinámico: ejecutar el archivo en el aparato dos veces, obtener por separado una secuencia de comportamiento que se obtiene después de cada vez que se ejecuta, para obtener una primera secuencia de comportamiento y una segunda secuencia de comportamiento; determinar comportamientos idénticos que existen en la primera secuencia de comportamiento y la segunda secuencia de comportamiento, en donde los comportamientos idénticos son comportamientos que son iguales en términos de tipos de comportamiento y contenido de comportamiento; y obtener un conjunto formado por comportamientos idénticos en la primera secuencia de comportamiento y la segunda secuencia de comportamiento, y usar el conjunto como la característica de comportamiento estable.

De acuerdo con un segundo aspecto, una modalidad de esta solicitud proporciona un sistema para detectar un estado de seguridad del terminal. El sistema incluye el aparato para detectar un estado de seguridad del terminal de acuerdo con el primer aspecto, y un dispositivo de terminal configurado para: recibir un indicador de compromiso del dispositivo de protección de seguridad; analizar el indicador de compromiso, para obtener una característica de comportamiento que corresponde a una amenaza persistente avanzada, APT, y que se incluye en el indicador de compromiso; buscar un sistema operativo y un sistema de archivos del dispositivo terminal, para determinar si un comportamiento descrito por una característica de comportamiento correspondiente a la APT ha ocurrido en el dispositivo terminal; y si el comportamiento descrito por la característica de comportamiento correspondiente a la APT ha ocurrido en el dispositivo terminal, determine que el dispositivo terminal se ha infectado con la APT.

De acuerdo con un tercer aspecto, una modalidad de esta solicitud proporciona un método para detectar un estado de seguridad del terminal. El método lo ejecuta un dispositivo de protección de seguridad, el dispositivo de protección de seguridad está ubicado en una unión entre una red privada y una red pública, y un terminal está ubicado en la red privada.

Primero, el dispositivo de protección de seguridad recibe un archivo de la red pública y ejecuta el archivo en el dispositivo de protección de seguridad para generar un resultado de comportamiento dinámico. El resultado del comportamiento dinámico incluye una secuencia de comportamiento que se genera de acuerdo con un orden cronológico de ocurrencia de comportamientos. Los comportamientos en la secuencia de comportamiento pertenecen a diferentes tipos de comportamiento, y los tipos de comportamiento incluyen crear un archivo, modificar un registro, configurar un nombre de dominio, resolver una dirección, conectarse a una red, cargar un proceso y agregar un usuario. El dispositivo de protección de seguridad determina, de acuerdo con el resultado del comportamiento dinámico generado, si el archivo incluye una amenaza persistente avanzada; si el archivo incluye la amenaza persistente avanzada, obtiene una característica de comportamiento estable en el resultado del comportamiento dinámico; genera un indicador correspondiente de compromiso de acuerdo con la característica de comportamiento estable; y envía el indicador de compromiso al terminal. La característica de comportamiento estable es un comportamiento que siempre existe en una secuencia de comportamiento que se genera cada vez que se ejecuta el archivo.

La obtención de una característica de comportamiento estable en el resultado del comportamiento dinámico comprende:

ejecutar el archivo en el dispositivo de protección de seguridad dos veces, para obtener por separado una secuencia de comportamiento que se obtiene después de cada vez que se ejecuta, para obtener una primera secuencia de comportamiento y una segunda secuencia de comportamiento;

determinar comportamientos idénticos que existen en la primera secuencia de comportamiento y la segunda secuencia de comportamiento, en donde los comportamientos idénticos son comportamientos que son iguales en términos de tipos de comportamiento y contenido de comportamiento; y obtener un conjunto formado por comportamientos idénticos en la

primera secuencia de comportamiento y la segunda secuencia de comportamiento, y usar el conjunto como la característica de comportamiento estable.

Breve descripción de los dibujos

Para describir más claramente las soluciones técnicas en las modalidades de la presente solicitud o la técnica anterior, a continuación, se describen brevemente los dibujos adjuntos necesarios para describir las modalidades o la técnica anterior.

La Figura 1 es un diagrama esquemático de una arquitectura de red para detectar que un terminal está infectado con una APT de acuerdo con una modalidad de esta solicitud;

La Figura 2 es un diagrama de bloques de un aparato para detectar un estado de seguridad del terminal de acuerdo con una modalidad de esta solicitud;

La Figura 3 es un diagrama esquemático de un resultado de comportamiento dinámico;

La Figura 4 es un diagrama esquemático de un dispositivo terminal de acuerdo con una modalidad de esta solicitud;

La Figura 5 es un diagrama esquemático gráfico de una salida IOC resumida por un editor de acuerdo con una modalidad de esta solicitud;

La Figura 6 es un diagrama esquemático de un sistema para detectar un estado de seguridad del terminal de acuerdo con una modalidad de esta solicitud;

La Figura 7 es un diagrama de flujo de un método para detectar un estado de seguridad del terminal de acuerdo con una modalidad de esta solicitud;

La Figura 8 es un diagrama de flujo de un método para detectar un estado de seguridad del terminal de acuerdo con otra modalidad de esta solicitud;

La Figura 9 es un diagrama esquemático de un IOC de tipo archivo de acuerdo con una modalidad de esta solicitud;

La Figura 10 es un diagrama esquemático de un IOC de tipo registro de acuerdo con una modalidad de esta solicitud; y

La Figura 11 es un diagrama esquemático de un IOC resumido de acuerdo con una modalidad de esta solicitud.

Descripción de las modalidades

Las soluciones técnicas en las modalidades de esta solicitud se describen clara y completamente a continuación con referencia a los dibujos adjuntos.

La Figura 1 es un diagrama esquemático de una arquitectura de red de un sistema para detectar un estado de seguridad del terminal de acuerdo con una modalidad de esta solicitud. Un dispositivo terminal 110 obtiene datos mediante el uso de Internet, por ejemplo, recibe un correo electrónico. Un cortafuegos 120 dispuesto en una puerta de enlace restaura el tráfico a un archivo. Por ejemplo, el cortafuegos restaura el tráfico a un archivo mediante el uso de un método proxy HTTP (Hypertext Transfer Protocol, Protocolo de transferencia de hipertexto). Los tipos de archivo incluyen un archivo exe (executable program, programa ejecutable), un archivo DLL (Dynamic Link Library, biblioteca de enlaces dinámicos, también denominado expansión de programa de la aplicación), un archivo sys (System, sistema), un archivo com, un archivo doc (un archivo de Word), un archivo xls (hoja de cálculo de Microsoft Excel), un archivo PDF (Portable Document Format, Formato de documento portátil) y similares. El cortafuegos 120 envía un archivo restaurado a un entorno de prueba 130 para su detección. El entorno de prueba 130 se dispone en la puerta de enlace y detecta si el archivo del cortafuegos 120 es un archivo malicioso que incluye una APT (Advanced Persistent Threat, amenaza persistente avanzada). Si se detecta que el archivo incluye el APT, el entorno de prueba 130 genera un IOC (Indicador de compromiso, indicador de compromiso) correspondiente al APT. El entorno de prueba 130 sincroniza el IOC con cada dispositivo terminal. Cada dispositivo terminal analiza el IOC, para obtener una característica de comportamiento que corresponde a una APT y que está incluida en el IOC, y busca un sistema operativo y un sistema de archivos de un terminal correspondiente de acuerdo con la característica, para determinar si el terminal de usuario está infectado con la APT. El entorno de prueba es un mecanismo de seguridad que proporciona un entorno de aislamiento para un programa en ejecución. El entorno de prueba generalmente controla estrictamente un recurso al que puede acceder un programa que se ejecuta en el entorno de prueba. Por ejemplo, el entorno de pruebas puede proporcionar espacio en disco y memoria que puede reciclarse después de usarse. En el entorno de pruebas, el acceso a la red, el acceso a un sistema operativo real y los permisos de lectura y escritura en un dispositivo de entrada están prohibidos o estrictamente restringidos. Un cambio realizado en el entorno de prueba no causa ninguna pérdida en el sistema operativo real. Por lo tanto, dicha tecnología generalmente se aplica ampliamente a las pruebas de un archivo ejecutable que contiene un virus u otro código malicioso.

El terminal de usuario en esta solicitud puede incluir un dispositivo terminal tal como un teléfono móvil, una tableta, un ordenador portátil, una UMPC (Ultra-mobile Personal Computer, computadora personal ultramóvil), un miniordenador portátil o una PDA (Personal Digital Assistant, asistente personal digital).

La Figura 2 es un diagrama de bloques de un aparato para detectar un estado de seguridad del terminal de acuerdo con una modalidad de esta solicitud. El aparato 200 para detectar un estado de seguridad del terminal, es decir, un aparato de protección de seguridad, está ubicado en una unión entre una red privada y una red pública, y un terminal está ubicado en la red privada. El aparato 200 incluye: un módulo de generación de resultados de comportamiento dinámico 210, un módulo de análisis de comportamiento dinámico 230, una biblioteca de características de comportamiento dinámico 220 y un generador de IOC 240.

En un ejemplo, el aparato 200 para detectar el estado de seguridad de un terminal es un entorno de prueba. Además, el entorno de prueba se dispone en una puerta de enlace.

El módulo de generación de resultados de comportamiento dinámico 210 se configura para: recibir un archivo de la red pública y ejecutar el archivo en el aparato 200 para detectar un estado de seguridad del terminal, para generar un resultado de comportamiento dinámico (refiriéndose a la Figura 3). El resultado del comportamiento dinámico incluye una secuencia de comportamiento que se genera de acuerdo con un orden cronológico de ocurrencia de comportamientos. Los comportamientos en la secuencia de comportamiento pertenecen a diferentes tipos de comportamiento, y los tipos de comportamiento incluyen crear un archivo, modificar un registro, configurar un nombre de dominio, resolver una dirección, conectarse a una red, cargar un proceso y agregar un usuario.

El módulo de análisis de comportamiento dinámico 230 se configura para determinar, de acuerdo con el resultado de comportamiento dinámico generado por el módulo de generación de resultados de comportamiento dinámico 210, si el archivo incluye una APT.

El generador de IOC 240 se configura para: si el módulo de análisis de comportamiento dinámico determina que el archivo incluye la APT, obtener una característica de comportamiento estable en el resultado del comportamiento dinámico, generar un IOC correspondiente de acuerdo con la característica de comportamiento estable y enviar el IOC al terminal. La característica de comportamiento estable es un comportamiento que siempre existe en una secuencia de comportamiento que se genera cada vez que se ejecuta el archivo.

En un ejemplo, un archivo de la red pública es, por ejemplo, un archivo exe, un archivo DLL, un archivo sys, un archivo com, un archivo doc, un archivo xls o un archivo PDF.

En un ejemplo, el resultado del comportamiento dinámico incluye una serie de operaciones de comportamiento. Cada operación de comportamiento incluye una secuencia de comportamiento basada en el tiempo.

En un ejemplo, el módulo de generación de resultados de comportamiento dinámico 210 incluye un módulo de motor de detección heurística y un módulo de entorno de ejecución virtual (que no se muestran en la Figura 2) en un entorno de prueba existente. El módulo del motor de detección heurística incluye un submódulo del motor de detección heurística web, un submódulo del motor de detección heurística PDF y un submódulo del motor de detección heurística PE (que no se muestran en la Figura 2). El módulo del motor de detección heurística y el módulo del entorno de ejecución virtual en el entorno limitado se configuran para generar un resultado de comportamiento dinámico correspondiente.

Como se muestra en la Figura 3, la Figura 3 es un diagrama esquemático de un resultado de comportamiento dinámico. El resultado del comportamiento dinámico en la Figura 3 incluye una secuencia de comportamiento que se genera de acuerdo con un orden cronológico de ocurrencia de comportamientos. Los comportamientos en la secuencia de comportamiento pertenecen a diferentes tipos de comportamiento. En la Figura 3, los tipos de comportamiento incluyen crear un archivo, cargar un proceso, modificar un registro y conectarse a una red.

En la Figura 2, la biblioteca de características de comportamiento dinámico 220 incluye múltiples características de comportamiento dinámico relacionadas con una APT. Por ejemplo, la biblioteca de características de comportamiento dinámico 220 incluye una biblioteca de características de comportamiento falso positivo y una biblioteca de características de comportamiento de amenaza (que no se muestran en la Figura 2). La biblioteca de características de comportamiento falso positivo incluye múltiples características de comportamiento falso positivo. La biblioteca de características de comportamiento de amenaza incluye múltiples características de comportamiento de amenaza.

En un ejemplo, el módulo de análisis de comportamiento dinámico 230 coincide con el resultado del comportamiento dinámico del módulo de generación de resultados de comportamiento dinámico 210 con cada característica de comportamiento dinámico en la biblioteca 220 de características de comportamiento dinámico, para determinar si el resultado de comportamiento dinámico incluye la APT.

En un ejemplo, el módulo de análisis de comportamiento dinámico 230 coincide con el resultado del comportamiento dinámico primero con cada característica de comportamiento falso positivo en la biblioteca de características de comportamiento falso positivo de la biblioteca de características de comportamiento dinámico 220, y luego con cada

característica de comportamiento de amenazas en la biblioteca de características de comportamiento de amenazas, para determinar si el resultado del comportamiento dinámico incluye la APT.

En un ejemplo, después de determinar que el resultado del comportamiento dinámico incluye la APT, el módulo 230 de análisis del comportamiento dinámico envía el resultado del comportamiento dinámico a un generador de IOC 240. Después de determinar que el resultado del comportamiento dinámico no incluye la APT, el módulo de análisis del comportamiento dinámico 230 envía el archivo (es decir, un archivo normal o un archivo no infectado) recibido por el aparato 200 a un dispositivo terminal. Es decir, el resultado del comportamiento dinámico recibido por el generador de IOC 240 incluye la APT.

La APT tiene un alto encubrimiento, y un método de ataque de la APT es ocultar la APT. La APT invade crónicamente un terminal de usuario para un objetivo particular de una manera planificada mediante el uso de una serie de operaciones de comportamiento.

En un ejemplo, el generador de IOC 240 incluye un primer cargador 241, múltiples generadores de IOC y un módulo de resumen de IOC 243. Los múltiples generadores de IOC incluyen múltiples tipos de generadores de IOC, por ejemplo, incluyen un generador de archivos (File generator), un generador de registros (Registry generator), un generador de nombres de dominio (DNS generator), un generador de protocolo de resolución de direcciones (ARP generator), un generador de red (Network generator), un generador de proceso (Process generator) y un generador de usuario (User generator). Un tipo del generador IOC está relacionado con un tipo de comportamiento en la característica de comportamiento estable de la APT. Por ejemplo, si una característica de comportamiento en un resultado de comportamiento dinámico que incluye una APT está creando un archivo, el tipo del generador IOC incluye el generador de archivos.

El primer cargador (loader) 241 en el generador de IOC 240 carga un programa correspondiente del resultado del comportamiento dinámico en la memoria, y asigna operaciones de comportamiento en el resultado del comportamiento dinámico a diferentes generadores. El resultado del comportamiento dinámico incluye una serie de operaciones de comportamiento. Cada operación de comportamiento incluye una secuencia de comportamiento basada en el tiempo.

En un ejemplo, el primer cargador 241 analiza las operaciones de comportamiento en el resultado de comportamiento dinámico uno por uno de acuerdo con un orden cronológico, para obtener las características de comportamiento correspondientes, y envía una operación de comportamiento correspondiente en el resultado de comportamiento dinámico a un generador correspondiente de acuerdo con una característica de comportamiento determinada. Por ejemplo, el primer cargador 241 verifica una operación de comportamiento y obtiene que una característica de comportamiento de la operación de comportamiento es FCreate, es decir, crear un archivo; entonces el primer cargador 241 envía la operación de comportamiento al generador de archivos.

En un ejemplo, el primer cargador 241 incluye una tabla de comparación. La tabla de comparación muestra una correspondencia entre cada característica de comportamiento y cada generador de múltiples tipos de generadores. El primer cargador 241 obtiene una característica de comportamiento de cada operación de comportamiento en el resultado de comportamiento dinámico recibido, determina, buscando en la tabla de comparación, un generador correspondiente a cada operación de comportamiento, y asigna la operación de comportamiento al generador correspondiente.

Por ejemplo, si el primer cargador 241 verifica que una característica de comportamiento de una operación de comportamiento en el resultado de comportamiento dinámico recibido (es decir, ya se determina que el resultado de comportamiento dinámico incluye una APT) incluye la creación de un archivo, el primer cargador 241 determina, al buscar en la tabla de comparación, que un generador correspondiente a la operación de comportamiento es un generador de archivos, y el primer cargador 241 asigna la operación de comportamiento al generador de archivos.

Cada generador de IOC en el generador de IOC 240 analiza una operación de comportamiento correspondiente en el resultado de comportamiento dinámico del primer cargador 241, para obtener la característica de comportamiento estable en el resultado de comportamiento dinámico, es decir, extraer un rastro dejado por la APT, y genera un IOC correspondiente de acuerdo con la característica de comportamiento estable. La característica de comportamiento estable es un comportamiento que siempre existe en una secuencia de comportamiento que se genera cada vez que se ejecuta el archivo, incluida la APT.

En un ejemplo, que el generador de IOC 240 obtiene una característica de comportamiento estable en el resultado del comportamiento dinámico incluye: ejecutar el archivo en el aparato 200 al menos dos veces, para obtener por separado una secuencia de comportamiento que se genera cada vez después de la ejecución, para obtener al menos dos secuencias de comportamiento; determinar comportamientos idénticos que existen en al menos dos secuencias de comportamiento, donde los comportamientos idénticos son comportamientos que son iguales en términos de tipos de comportamiento y contenido de comportamiento; y obtener un conjunto formado por comportamientos idénticos en al menos dos secuencias de comportamiento, y usar el conjunto como la característica de comportamiento estable.

Obviamente, en un proceso de obtención de la característica de comportamiento estable, una mayor cantidad de veces de ejecución del archivo indica una mayor precisión de la característica de comportamiento estable finalmente obtenida,

y una mayor precisión de identificación, de acuerdo con el IOC generado de acuerdo con la característica de comportamiento estable, si el dispositivo terminal está infectado con la APT.

Un IOC (indicator of compromise, indicador de compromiso) describe un rastro dejado por una APT capturada, y el rastro se describe en un formulario de documento xml. El contenido incluye un atributo de un archivo de virus, una característica modificada de un registro, memoria virtual y similares. Por ejemplo, un rastro que describe un IOC y que deja una APT es: buscar una ruta C:\WINDOWS\apocalyps32.exe para un archivo, y una longitud del archivo es 108544 bytes. El módulo de resumen de IOC 243 resume múltiples IOC de múltiples generadores de IOC (por ejemplo, un generador de archivos y un generador de registro) en un IOC, y envía el IOC resumido al dispositivo terminal. El IOC resumido se representa mediante el uso de un documento XML (Lenguaje de marcado extensible).

La Figura 4 es un diagrama esquemático de un dispositivo terminal de acuerdo con una modalidad de esta solicitud. El dispositivo terminal 400 incluye un intérprete IOC 410, un módulo receptor 430 y un módulo determinante 440.

El módulo receptor 430 se configura para recibir un IOC desde un dispositivo de protección de seguridad.

El intérprete 410 de IOC se configura para analizar el IOC recibido por el módulo receptor 430, para obtener una característica de comportamiento que corresponde a un APT y que está incluida en el IOC.

El módulo de determinación 440 se configura para buscar un sistema operativo y un sistema de archivos del dispositivo terminal 400, para determinar si se ha producido un comportamiento descrito por la característica de comportamiento correspondiente a la APT en el dispositivo terminal 400; y si el comportamiento descrito por la característica de comportamiento correspondiente a la APT ha ocurrido en el dispositivo terminal 400, determine que el dispositivo terminal 400 se ha infectado con la APT.

En un ejemplo, el dispositivo terminal 400 incluye además un editor 420. El editor 420 se configura para describir y mostrar un IOC recibido, tal como un IOC resumido, en forma gráfica, haciendo referencia a la Figura 5. La Figura 5 un diagrama esquemático de una forma de representación gráfica de un IOC resumido. El editor 420 es un módulo opcional.

En un ejemplo, el intérprete IOC 410 está en un módulo TSM (Terminal Security Management, programa informático de gestión de seguridad de terminal) del dispositivo terminal 400.

Un experto en la técnica puede entender que la estructura del dispositivo terminal que se muestra en la Figura 4 no constituye ninguna limitación para el dispositivo terminal, y puede incluir más o menos componentes que los mostrados en la figura, o algunos componentes pueden combinarse, o puede usarse un diseño de componente diferente.

En un ejemplo, el intérprete 410 del IOC incluye un segundo cargador 411 y múltiples tipos de intérpretes.

En la Figura 4, el segundo cargador 411 en el intérprete 410 de IOC recibe un IOC del módulo receptor 430, por ejemplo, recibe un IOC resumido, carga un programa correspondiente del IOC resumido en la memoria y asigna IOC en el IOC resumido a diferentes intérpretes.

En un ejemplo, el segundo cargador 411 analiza los IOC en el IOC resumido uno por uno, para obtener tipos de IOC, y asigna los IOC en el IOC resumido de acuerdo con los tipos determinados de IOC. Por ejemplo, en un IOC, si un tipo de documento de contexto incluido en el IOC es FileItem, indica que el IOC es un IOC de tipo archivo.

En un ejemplo, el segundo cargador 411 incluye una tabla de comparación. La tabla de comparación muestra una correspondencia entre cada tipo de IOC y cada intérprete de múltiples tipos de intérpretes. El segundo cargador 411 obtiene el tipo de IOC del IOC recibido por el segundo cargador 411, determina, buscando en la tabla de comparación, un intérprete correspondiente a cada IOC, y asigna cada IOC en el IOC resumido a un intérprete correspondiente.

Debe observarse que el intérprete de IOC 410 puede incluir alternativamente un asignador (no mostrado en la Figura 4). En este caso, el asignador asigna cada IOC en el IOC resumido a un intérprete correspondiente, y el segundo cargador 411 se configura solo para cargar el programa correspondiente del IOC resumido en la memoria.

El intérprete 410 del IOC incluye algunos o todos los siguientes tipos múltiples de intérpretes: un intérprete de archivos (File interpreter), un intérprete de registro (Registry interpreter), un intérprete de nombre de dominio (DNS interpreter), un intérprete de protocolo de resolución de direcciones (ARP interpreter), un intérprete de red (Network interpreter), un intérprete de proceso (Process interpreter) y un intérprete de usuario (User interpreter). Un tipo de intérprete está relacionado con un tipo de IOC.

Cada intérprete en el intérprete 410 del IOC recibe un IOC correspondiente del segundo cargador 411, y analiza el IOC, para obtener una característica de comportamiento que corresponde a la APT y que se incluye en el IOC, es decir, para obtener un rastro dejado por la APT. El módulo de determinación 440 busca el sistema operativo y el sistema de archivos del dispositivo terminal 400 de acuerdo con la característica, para determinar si se ha producido un comportamiento descrito por la característica de comportamiento correspondiente a la APT en el dispositivo terminal 400; y si el

comportamiento descrito por la característica de comportamiento correspondiente a la APT ha ocurrido en el dispositivo terminal 400, determina que el dispositivo terminal 400 se ha infectado con la APT. Por ejemplo, el intérprete de archivos obtiene, al analizar, que una primera característica que corresponde a una APT y que está en un IOC es: una ruta C:\WINDOWS\apocalyps32.exe; y una segunda característica que corresponde a la APT y que está en el IOC es: un archivo cuya longitud es 108544 bytes. El módulo de determinación 440 busca el sistema operativo y el sistema de archivos del dispositivo terminal 440, y consulta una ruta C:\WINDOWS\apocalyps32.exe, para determinar si hay un archivo cuya longitud es 108544 bytes, para determinar si el dispositivo terminal 400 está infectado con el APT.

HIGO. 6 muestra un sistema para detectar un estado de seguridad del terminal de acuerdo con una modalidad de esta solicitud. El sistema incluye el aparato 200 para detectar un estado de seguridad del terminal y el dispositivo terminal 400, el aparato 200 para detectar un estado de seguridad del terminal está ubicado en una unión entre una red privada y una red pública, y el dispositivo terminal 400 está ubicado en la red privada.

El aparato 200 para detectar un estado de seguridad del terminal recibe un archivo de la red pública y ejecuta el archivo para generar un resultado de comportamiento dinámico; determina, de acuerdo con el resultado del comportamiento dinámico, si el archivo incluye una APT; y si el resultado del comportamiento dinámico incluye la APT, obtiene una característica de comportamiento estable en el resultado del comportamiento dinámico y genera un IOC correspondiente de acuerdo con la característica de comportamiento estable. El resultado del comportamiento dinámico incluye una secuencia de comportamiento que se genera de acuerdo con un orden cronológico de ocurrencia de comportamientos. Los comportamientos en la secuencia de comportamiento pertenecen a diferentes tipos de comportamiento, y los tipos de comportamiento incluyen crear un archivo, modificar un registro, configurar un nombre de dominio, resolver una dirección, conectarse a una red, cargar un proceso y agregar un usuario. La característica de comportamiento estable es un comportamiento que siempre existe en una secuencia de comportamiento que se genera cada vez que se ejecuta el archivo.

El dispositivo terminal 400 recibe un IOC del aparato 200 para detectar un estado de seguridad del terminal, analiza el IOC, para obtener una característica de comportamiento que corresponde a una APT y que está incluida en el IOC, y busca un sistema operativo y un sistema de archivos del dispositivo terminal 400 de acuerdo con la característica de comportamiento, para determinar si el comportamiento descrito por la característica de comportamiento correspondiente a la APT ha ocurrido en el dispositivo terminal 400; y si el comportamiento descrito por la característica de comportamiento correspondiente a la APT ha ocurrido en el dispositivo terminal 400, determina que el dispositivo terminal 400 se ha infectado con la APT.

Debe observarse que, para los módulos incluidos en el aparato 200 para detectar un estado de seguridad del terminal y el dispositivo terminal 400 y las funciones de los módulos, consulte la Figura 2, la Figura 4, y descripciones relacionadas. Los detalles no se describen nuevamente en la presente descripción.

La Figura 7 es un diagrama de flujo de un método para detectar un estado de seguridad del terminal de acuerdo con una modalidad de esta solicitud. El método para detectar el estado de seguridad de un terminal lo ejecuta un dispositivo de protección de seguridad. El dispositivo de protección de seguridad está ubicado en una unión entre una red privada y una red pública, y un terminal está ubicado en la red privada.

En un ejemplo, el método para detectar el estado de seguridad de un terminal lo realiza un entorno de prueba, y el entorno de prueba se dispone en una puerta de enlace.

En la etapa 710, el dispositivo de protección de seguridad recibe un archivo de la red pública y ejecuta el archivo en el dispositivo de protección de seguridad, para generar un resultado de comportamiento dinámico, en referencia a la Figura 3. El resultado del comportamiento dinámico incluye una secuencia de comportamiento que se genera de acuerdo con un orden cronológico de ocurrencia de comportamientos. Los comportamientos en la secuencia de comportamiento pertenecen a diferentes tipos de comportamiento, y los tipos de comportamiento incluyen crear un archivo, modificar un registro, configurar un nombre de dominio, resolver una dirección, conectarse a una red, cargar un proceso y agregar un usuario.

En un ejemplo, el resultado del comportamiento dinámico incluye una serie de operaciones de comportamiento. Cada operación de comportamiento incluye una característica de comportamiento basada en el tiempo.

En un ejemplo, un archivo de Internet es, por ejemplo, un archivo exe, un archivo DLL, un archivo sys, un archivo com, un archivo doc, un archivo xls o un archivo PDF.

En la etapa 720, el dispositivo de protección de seguridad determina, de acuerdo con el resultado del comportamiento dinámico generado, si el archivo incluye una APT.

En un ejemplo, el resultado del comportamiento dinámico se corresponde con cada característica de comportamiento dinámico en una biblioteca de características de comportamiento dinámico, para determinar si el resultado del comportamiento dinámico incluye la APT.

En la etapa 730, si el resultado del comportamiento dinámico incluye la APT, el dispositivo de protección de seguridad analiza las operaciones de comportamiento en el resultado del comportamiento dinámico uno por uno, para obtener una característica de comportamiento estable en cada operación de comportamiento, es decir, extraer un rastro dejado por la APT, y genera un IOC correspondiente de acuerdo con la característica de comportamiento estable. La característica de comportamiento estable es un comportamiento que siempre existe en una secuencia de comportamiento que se genera cada vez que se ejecuta el archivo.

En un ejemplo, la obtención de una característica de comportamiento estable en el resultado del comportamiento dinámico incluye: ejecutar el archivo en el dispositivo de protección de seguridad al menos dos veces, para obtener por separado una secuencia de comportamiento que se genera después de cada vez que se ejecuta, para obtener al menos dos secuencias de comportamiento; determinar comportamientos idénticos que existen en al menos dos secuencias de comportamiento, donde los comportamientos idénticos son comportamientos que son iguales en términos de tipos de comportamiento y contenido de comportamiento; y obtener un conjunto formado por comportamientos idénticos en al menos dos secuencias de comportamiento, y usar el conjunto como una característica de comportamiento estable.

En el paso 740, el dispositivo de protección de seguridad resume múltiples IOC generados de acuerdo con el resultado del comportamiento dinámico en un IOC. El IOC resumido se representa mediante el uso de un documento XML (Lenguaje de marcado extensible).

La etapa 740 es una etapa opcional. Cuando se obtiene una IOC de acuerdo con el resultado del comportamiento dinámico, no es necesario resumir el IOC, es decir, no es necesario realizar la etapa 740.

En la etapa 750, el dispositivo de protección de seguridad envía el IOC resumido al dispositivo terminal.

La Figura 8 es un diagrama de flujo de un método para detectar un estado de seguridad del terminal de acuerdo con otra modalidad de esta solicitud.

En la etapa 810, el dispositivo terminal recibe un IOC, tal como un IOC resumido, de un dispositivo de protección de seguridad, donde el IOC resumido incluye múltiples IOC.

En la etapa 820, el dispositivo terminal analiza el IOC para obtener una característica de comportamiento que corresponde a una APT y que está incluida en el IOC.

En un ejemplo, el IOC es un IOC resumido. Los IOC en el IOC resumido se analizan uno por uno, para obtener una característica de comportamiento que corresponde a un APT y que se incluye en cada IOC.

En la etapa 830, el dispositivo terminal busca un sistema operativo y un sistema de archivos del dispositivo terminal de acuerdo con la característica de comportamiento obtenida, para determinar si un comportamiento descrito por la característica de comportamiento correspondiente a la APT ha ocurrido en el dispositivo terminal; y si el comportamiento descrito por la característica de comportamiento correspondiente a la APT ha ocurrido en el dispositivo terminal, determina que el dispositivo terminal se ha infectado con la APT.

Por ejemplo, una primera característica que corresponde a una APT y que está en un IOC es: una ruta C:\WINDOWS\apocalyps32.exe. Una segunda característica correspondiente a la APT es: un archivo cuya longitud es 108544 bytes. Por lo tanto, el terminal de usuario busca la ruta C:\WINDOWS\apocalyps32.exe en el sistema operativo y el sistema de archivos del terminal de usuario, y comprueba si hay un archivo cuya longitud es 108544 bytes en la ruta. Si hay un archivo cuya longitud es 108544 bytes en la ruta, se determina que el terminal se ha infectado con la APT.

En un ejemplo, cuando el dispositivo terminal encuentra que un IOC en el IOC resumido incluye la APT, se determina que el dispositivo terminal está infectado con el APT.

Un resultado de comportamiento dinámico infectado con una APT típica en la Figura 3 se use como ejemplo para describir en detalle cómo un generador de IOC convierte resultado del comportamiento dinámico infectado con la APT en un IOC, y cómo el dispositivo terminal determina, de acuerdo con el IOC recibido, si el dispositivo terminal está infectado con la APT.

Un primer cargador 241 en un generador 240 de IOC analiza las operaciones de comportamiento en un resultado de comportamiento dinámico recibido, uno por uno, y primero verifica una primera operación de comportamiento en el resultado de comportamiento dinámico, es decir, verifica una operación de comportamiento "Una muestra libera un archivo PE "en la Figura 3. El primer cargador 241 aprende, de acuerdo con una "acción" de campo en la primera operación de comportamiento, que la característica de comportamiento es FCreate, es decir, crear un archivo. El primer cargador 241 asigna la primera operación de comportamiento, es decir, la operación de comportamiento "Una muestra libera un archivo PE" a un generador de archivos.

El generador de archivos analiza la primera operación de comportamiento y descubre que la operación de comportamiento es FCreate, es decir, crear un archivo, en una ruta C:\windows\apocalyps32.exe; y FWritePE, es decir, escribir un archivo

ejecutable. Una longitud es 43008 bytes, es decir, la longitud del archivo es 43008 bytes; un desplazamiento es 65536 bytes y, por lo tanto, la longitud total del archivo es 43008 + 65536 = 108544. Por lo tanto, el generador de archivos analiza la operación de comportamiento, para obtener que una característica de comportamiento correspondiente esté creando un archivo ejecutable apocalyps32.exe en un directorio C:\windows\, y una longitud del archivo ejecutable es 108544 bytes. Este tipo de característica de comportamiento es estable y no varía con diferentes terminales. Se deja un rastro que tiene la característica de comportamiento siempre que el dispositivo terminal esté infectado con una APT correspondiente. La característica de comportamiento estable es un comportamiento que siempre existe en una secuencia de comportamiento que se genera cada vez que se ejecuta el archivo, incluida la APT. El generador de archivos genera un IOC de tipo archivo de acuerdo con la característica de comportamiento estable. Para el IOC de tipo de archivo, consulte la Figura 9. Por lo tanto, la primera operación de comportamiento en el resultado del comportamiento dinámico se convierte en un IOC.

La Figura 9 es un diagrama esquemático de un IOC de tipo archivo. En la Figura 9, el IOC de tipo de archivo representa que un rastro dejado por una APT es un archivo cuya longitud es 108544 bytes en la ruta C:\windows\apocalyps32.exe.

(2) El primer cargador 241 verifica una segunda operación de comportamiento en el resultado de comportamiento dinámico, es decir, verifica una operación de comportamiento "Ejecutar la muestra". El primer cargador 241 aprende, de acuerdo con el campo "acción", que la operación de comportamiento es CreateProcess, es decir, crear un proceso, en una ruta C:\windows\apocalyps32.exe: 1252. El primer cargador 241 asigna la operación de comportamiento a un generador de procesos.

El generador de procesos analiza la segunda operación de comportamiento, para saber que la operación de comportamiento es CreateProcess, es decir, cargar un proceso, en la ruta C:\windows\apocalyps32.exe: 1252, donde el valor de un pid es 1448; y luego FOpen, es decir, abrir un archivo, donde el valor de un pid (un identificador de proceso) es 1488. El pid es una característica inestable, y un valor del pid varía con diferentes dispositivos terminales. Por lo tanto, la operación de comportamiento "Ejecutar la muestra" es una operación de comportamiento inestable y no se genera IOC.

(3) El primer cargador 241 verifica una tercera operación de comportamiento en el resultado de comportamiento dinámico, es decir, verifica una operación de comportamiento "Crear una amenaza e inyectar la amenaza en un proceso IEXPLORE.EXE para ocultar la amenaza". El primer cargador 241 aprende, de acuerdo con el campo "acción", que la operación de comportamiento es Open-Process explorer.exe, es decir, abrir un navegador. El primer cargador 241 asigna la operación de comportamiento a un generador de procesos.

El generador de procesos analiza la tercera operación de comportamiento, para saber que la operación de comportamiento es primero OpenProcess explorer.exe, es decir, abrir un navegador, donde el valor de un pid (un identificador de proceso) es 1244; y luego, WriteOtherProcMem, es decir, escribir una amenaza de IE, donde el valor de un pid es 1488. El pid es una característica inestable, y un valor del pid varía con diferentes dispositivos terminales. Por lo tanto, la operación de comportamiento es una operación de comportamiento inestable y no se genera IOC.

(4) El primer cargador 241 verifica una cuarta operación de comportamiento en el resultado de comportamiento dinámico, es decir, verifica una operación de comportamiento "Modificar un registro para agregar un elemento de inicio automático". El primer cargador 241 aprende, de acuerdo con el campo "acción", que la operación de comportamiento es RegCreateKey, es decir, crear un elemento de registro, en una ruta HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. El primer cargador 241 envía la operación de comportamiento a un generador de registro. El generador de registro analiza la cuarta operación de comportamiento, para saber que la operación de comportamiento es RegCreateKey, es decir, crear un elemento de registro, en HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. Un valor clave del elemento de registro se establece en C:\WINDOWS\apocalyps32.exe. Por lo tanto, el generador de registro analiza la operación de comportamiento, para obtener que una característica de comportamiento correspondiente esté agregando un elemento de inicio automático C:\WINDOWS\apocalyps32.exe en una ruta HKLM\SOFTWARE\Microsoft\Windows\Current Version\Run\apocalyps32.

Este tipo de característica de comportamiento es estable y no varía con diferentes dispositivos terminales. Se deja un rastro de la característica de comportamiento siempre que el dispositivo terminal esté infectado con una APT correspondiente. La característica de comportamiento estable es un comportamiento que siempre existe en una secuencia de comportamiento que se genera cada vez que se ejecuta un archivo que incluye la APT. El generador de registro convierte la operación de comportamiento en un IOC de tipo registro, haciendo referencia a la Figura 10.

La Figura 10 es un diagrama esquemático de un IOC de tipo registro. En la Figura 10, un rastro dejado por una APT es: buscar una ruta de registro HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\apocalyps32 para determinar si la ruta existe. Si la ruta existe, un valor correspondiente a la ruta es C:\windows\apocalyps32.exe.

(5) El primer cargador 241 verifica una quinta operación de comportamiento en el resultado de comportamiento dinámico, es decir, verifica una operación de comportamiento "Conectarse a una red externa". El primer cargador 241 aprende, de acuerdo con el campo "acción", que la operación de comportamiento es conectarse, es decir, conectarse a una red externa. El primer cargador 241 asigna la operación de comportamiento a un generador de conexión de red.

El generador de conexión de red analiza la quinta operación de comportamiento, para saber que la operación de comportamiento se está conectando a la red externa, y una dirección IP es 5.5.66.101:1453. 1453 en la dirección IP es una característica inestable, y sus valores varían con los diferentes dispositivos terminales. Por lo tanto, la operación de comportamiento "Conectarse a una red externa" es una operación de comportamiento inestable y no se genera IOC.

Se puede aprender, de acuerdo con el análisis anterior, que un proceso de ejecución APT en la Figura 3 es: primero lanzar un archivo ejecutable; posteriormente, ejecutar el archivo ejecutable; luego, ocultar el proceso de ejecución APT en un navegador IE, de modo que el proceso de ejecución APT no se pueda encontrar en el administrador de tareas; agregar un elemento de registro de inicio automático, para que la APT exista en un sistema cada vez que se reinicie el sistema; y finalmente, robar información o dañar el sistema conectándose a una red externa.

(6) El módulo de resumen de IOC 243 recibe el IOC de tipo de archivo (como se muestra en la Figura 9) del generador de archivos, recibe el IOC de tipo registro (como se muestra en la Figura 10) del generador de registros, resume el IOC de tipo archivo y el IOC de tipo registro, para obtener un IOC resumido, y muestra el IOC resumido en un formulario de documento XML, haciendo referencia a la Figura 11.

La Figura 11 es un diagrama esquemático de un IOC resumido. El IOC resumido se representa en un formulario de archivo XML. El archivo XML incluye información tal como una breve descripción sobre el IOC, un autor y una fecha de creación, e incluye una descripción sobre el rastro de la APT: un archivo ejecutable cuya longitud es 108544 bytes en la ruta C:\windows\apocalyps32.exe; o agregar un elemento de inicio automático C:\WINDOWS\apocalyps32.exe en la ruta HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\apocalyps32.

(7) Un módulo receptor 430 en el dispositivo terminal recibe el IOC resumido (incluyendo el IOC de tipo archivo y el IOC de tipo registro) desde el aparato 200 para detectar un estado de seguridad del terminal (es decir, el dispositivo de protección de seguridad), donde para un IOC resumido específico, consulte la Figura 11, y envía el IOC resumido a un segundo cargador 411.

(8) El segundo cargador 411 analiza los IOC en el IOC resumido uno por uno, y primero verifica un primer IOC, es decir, el IOC de tipo archivo, en el IOC resumido. El segundo cargador 411 aprende, de acuerdo con un campo "Documento de contexto", que una característica de comportamiento es FileItem, es decir, un elemento de archivo. El segundo cargador 411 asigna el primer IOC, es decir, el IOC de tipo de archivo, a un intérprete de archivos.

(9) El intérprete de archivos analiza el IOC de tipo archivo, para obtener dos características de comportamiento de la APT que se incluyen en el IOC: Una característica de comportamiento es determinar si existe C:\WINDOWS\apocalyps32.exe; y la otra característica de comportamiento es determinar si una longitud del archivo es de 108544 bytes. Las dos características de comportamiento están en una relación "y (inglés: and)", en referencia a la Figura 9.

(10) Un módulo de determinación 440 busca un sistema operativo y un sistema de archivos de un dispositivo terminal 400, para determinar si ha ocurrido un comportamiento descrito por una característica de comportamiento correspondiente a la APT en el dispositivo terminal 400; y si el comportamiento descrito por la característica de comportamiento correspondiente a la APT ha ocurrido en el dispositivo terminal 400, determina que el dispositivo terminal 400 se ha infectado con la APT. Es decir, si se encuentra un archivo cuya longitud es 108544 bytes en la ruta C:\WINDOWS\apocalyps32.exe, el módulo de determinación 440 determina que el dispositivo terminal 400 se ha infectado con la APT.

(11) El segundo cargador 411 verifica un segundo IOC, es decir, el IOC de tipo de registro, en el IOC resumido. El segundo cargador 411 aprende, de acuerdo con el campo "Documento de contexto", que la característica es RegistryItem, es decir, un elemento de registro. El segundo cargador 411 asigna el segundo IOC, es decir, el IOC del elemento de registro, a un intérprete de registro.

El intérprete de registro analiza el elemento de registro IOC, para obtener dos características de comportamiento de la APT que se incluyen en el IOC: Una característica de comportamiento es determinar si existe una ruta de registro "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\apocalyps32"; y la otra característica de comportamiento es determinar si el contenido del elemento del registro es "C:\WINDOWS\apocalyps32.exe". Las dos características de comportamiento están en una relación "y (inglés: and)", en referencia a la Figura 10.

(12) El módulo de determinación 440 busca el sistema operativo y el sistema de archivos del dispositivo terminal 400, para determinar si el comportamiento descrito por la característica de comportamiento correspondiente a la APT ha ocurrido en el dispositivo terminal 400; y si el comportamiento descrito por la característica de comportamiento correspondiente a la APT ha ocurrido en el dispositivo terminal 400, determina que el dispositivo terminal 400 se ha infectado con la APT. Es decir, el módulo de determinación 440 busca en la ruta HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\apocalyps32 para determinar si se incluye el contenido C:\WINDOWS\apocalyps32.exe. Si se incluye el contenido, indica que el dispositivo terminal 400 está infectado con la APT.

Las etapas del método o algoritmo que se describen en el contenido descrito en esta solicitud pueden implementarse de manera de soporte físico, o pueden implementarse de manera de una instrucción de programa informático ejecutada por un procesador. La instrucción de programa informático puede incluir un módulo de programa informático correspondiente. El módulo de programa informático puede ubicarse en una memoria RAM, una memoria flash, una memoria ROM, una memoria EPROM, una memoria EEPROM, un registro, un disco duro, un disco duro extraíble, un CDROM o un medio de almacenamiento de cualquier otra forma conocido en la técnica. Por ejemplo, un medio de almacenamiento está acoplado a un procesador, de modo que el procesador puede leer información del medio de almacenamiento o escribir información en el medio de almacenamiento. Ciertamente, el medio de almacenamiento puede ser un componente del procesador. El procesador y el medio de almacenamiento pueden estar ubicados en un ASIC. Además, el ASIC puede estar ubicado en el equipo del usuario. Ciertamente, el procesador y el medio de almacenamiento pueden existir en el equipo del usuario como componentes discretos.

Una persona experta en la técnica debe ser consciente de que en uno o más de los ejemplos anteriores, las funciones descritas en esta solicitud pueden implementarse mediante soporte físico, programa informático, microprograma o cualquier combinación de los mismos. Cuando la presente solicitud se implementa mediante programa informático, las funciones anteriores pueden almacenarse en un medio legible por ordenador o transmitirse como una o más instrucciones o código en el medio legible por ordenador. El medio legible por ordenador incluye un medio de almacenamiento informático y un medio de comunicaciones, donde el medio de comunicaciones incluye cualquier medio que permita la transmisión de un programa informático de un lugar a otro. El medio de almacenamiento puede ser cualquier medio disponible accesible para un ordenador dedicado o de propósito general.

Los objetivos, las soluciones técnicas y los efectos beneficiosos de esta solicitud se describen con más detalle en las modalidades específicas anteriores. Debe entenderse que las descripciones anteriores son meramente modalidades específicas de esta solicitud, pero la invención está definida por el alcance de las siguientes reivindicaciones.

REIVINDICACIONES

1. Un aparato (200) para detectar un estado de seguridad del terminal, en donde el aparato (200) está ubicado en una unión entre una red privada y una red pública, un terminal está ubicado en la red privada y el aparato comprende:
un módulo de generación de resultados de comportamiento dinámico (210), configurado para: recibir un archivo de la red pública y ejecutar el archivo en el aparato para generar un resultado de comportamiento dinámico, en donde el resultado de comportamiento dinámico comprende una secuencia de comportamiento que se genera de acuerdo con un orden cronológico de ocurrencia de comportamientos, los comportamientos en la secuencia de comportamiento pertenecen a diferentes tipos de comportamiento, y los tipos de comportamiento comprenden crear un archivo, modificar un registro, configurar un nombre de dominio, resolver una dirección, conectarse a una red, cargar un proceso y agregar un usuario;
un módulo de análisis de comportamiento dinámico (230), configurado para determinar, de acuerdo con el resultado de comportamiento dinámico generado por el módulo de generación de resultados de comportamiento dinámico (210), si el archivo comprende una amenaza persistente avanzada; y
un indicador de generador de compromiso (250), configurado para: si el módulo de análisis de comportamiento dinámico (230) determina que el archivo comprende la amenaza persistente avanzada, obtenga una característica de comportamiento estable en el resultado del comportamiento dinámico, genere un indicador de compromiso correspondiente de acuerdo con la característica de comportamiento estable, y envía el indicador de compromiso al terminal, en donde la característica de comportamiento estable es un comportamiento que siempre existe en una secuencia de comportamiento que se genera cada vez que se ejecuta el archivo; en donde el indicador de generador de compromiso (250) se configura para implementar las siguientes etapas para obtener una característica de comportamiento estable en el resultado del comportamiento dinámico:
ejecutar el archivo en el aparato dos veces, para obtener por separado una secuencia de comportamiento que se obtiene después de cada vez que se ejecuta, para obtener una primera secuencia de comportamiento y una segunda secuencia de comportamiento;
determinar comportamientos idénticos que existen en la primera secuencia de comportamiento y la segunda secuencia de comportamiento, en donde los comportamientos idénticos son comportamientos que son iguales en términos de tipos de comportamiento y contenido de comportamiento; y
obtener un conjunto formado por comportamientos idénticos en la primera secuencia de comportamiento y la segunda secuencia de comportamiento, y usar el conjunto como la característica de comportamiento estable.

2. El aparato de acuerdo con la reivindicación 1, en donde el aparato comprende además una biblioteca de características de comportamiento dinámico (220), en donde la biblioteca de características de comportamiento dinámico (220) comprende múltiples características de comportamiento falso positivo y múltiples características de comportamiento de amenaza; y
el módulo de análisis de comportamiento dinámico (230) se configura para: recibir el resultado del comportamiento dinámico y hacer coincidir el resultado del comportamiento dinámico con las múltiples características de comportamiento falso positivo y las múltiples características de comportamiento de amenaza en la biblioteca de características de comportamiento dinámico (220), para determinar si el archivo comprende la amenaza persistente avanzada.

3. El aparato de acuerdo con la reivindicación 1 o 2, en el que el indicador de compromiso generador (250) comprende múltiples tipos de generadores, y un tipo de generador está relacionado con un tipo de comportamiento en la característica de comportamiento estable.

4. El aparato de acuerdo con una cualquiera de las reivindicaciones 1 a 3, en donde el indicador de generador de compromiso (250) comprende uno o más de un generador de archivos, un generador de registro, un generador de nombres de dominio, un generador de Protocolo de Resolución de Direcciones, un generador de conexión de red, un generador de proceso o un generador de usuario.

5. Un sistema para detectar un estado de seguridad de terminal, en donde un dispositivo de protección de seguridad (200) se encuentra en una unión entre una red privada y una red pública, un dispositivo de terminal (400) se encuentra en la red privada y el sistema comprende:
el dispositivo de protección de seguridad (200), configurado para: recibir un archivo de la red pública y ejecutar el archivo para generar un resultado de comportamiento dinámico; determinar, de acuerdo con el resultado del comportamiento dinámico, si el archivo comprende una amenaza persistente avanzada; si el resultado del comportamiento dinámico comprende la amenaza persistente avanzada, obtener una característica de comportamiento estable en el resultado del comportamiento dinámico y generar un indicador correspondiente de compromiso de acuerdo con la característica de comportamiento estable, en donde el resultado del comportamiento dinámico comprende una secuencia de comportamiento que se genera de acuerdo con un orden cronológico de ocurrencia de comportamientos, los comportamientos en la secuencia de comportamiento pertenecen a diferentes tipos de comportamiento, los tipos de comportamiento comprenden crear un archivo, modificar un registro, configurar un nombre de dominio, resolver una dirección, conectarse a una red, cargar un

proceso y agregar un usuario, y la característica de comportamiento estable es un comportamiento que siempre existe en una secuencia de comportamiento que se genera cada vez que se ejecuta el archivo;
en donde el dispositivo de protección de seguridad (200) se configura además para: ejecutar el archivo en el dispositivo de protección de seguridad (200) dos veces, para obtener por separado una secuencia de comportamiento que se obtiene después de cada vez que se ejecuta, para obtener una primera secuencia de comportamiento y una segunda secuencia de comportamiento; determinar comportamientos idénticos que existen en la primera secuencia de comportamiento y la segunda secuencia de comportamiento, en donde los comportamientos idénticos son comportamientos que son iguales en términos de tipos de comportamiento y contenido de comportamiento; y obtener un conjunto formado por comportamientos idénticos en la primera secuencia de comportamiento y la segunda secuencia de comportamiento, y usar el conjunto como la característica de comportamiento estable; y
el dispositivo terminal (400), configurado para: recibir un indicador de compromiso del dispositivo de protección de seguridad; analizar el indicador de compromiso, para obtener una característica de comportamiento que corresponde a una amenaza persistente avanzada, APT, y que se incluye en el indicador de compromiso; buscar un sistema operativo y un sistema de archivos del dispositivo terminal, para determinar si un comportamiento descrito por una característica de comportamiento correspondiente al APT ha ocurrido en el dispositivo terminal; y si el comportamiento descrito por la característica de comportamiento correspondiente a la APT ha ocurrido en el dispositivo terminal, determinar que el dispositivo terminal ha sido infectado con la APT.

6. Un método para detectar el estado de seguridad de un terminal, en donde el método lo realiza un dispositivo de protección de seguridad, el dispositivo de protección de seguridad se encuentra en una unión entre una red privada y una red pública, un terminal se encuentra en la red privada; y el método comprende:
recibir (710), por el dispositivo de protección de seguridad, un archivo de la red pública y ejecutar el archivo en el dispositivo de protección de seguridad, para generar un resultado de comportamiento dinámico, en donde el resultado de comportamiento dinámico comprende una secuencia de comportamiento que se genera de acuerdo con un el orden cronológico de ocurrencia de comportamientos, los comportamientos en la secuencia de comportamiento pertenecen a diferentes tipos de comportamiento, y los tipos de comportamiento comprenden crear un archivo, modificar un registro, configurar un nombre de dominio, resolver una dirección, conectarse a una red, cargar un proceso y agregar un usuario; y
determinar (720), mediante el dispositivo de protección de seguridad de acuerdo con el resultado del comportamiento dinámico generado, si el archivo comprende una amenaza persistente avanzada; si el archivo comprende la amenaza persistente avanzada, obtener (730) una característica de comportamiento estable en el resultado del comportamiento dinámico; generar (740) un indicador correspondiente de compromiso de acuerdo con la característica de comportamiento estable; y enviar (750) el indicador de compromiso al terminal, en donde la característica de comportamiento estable es un comportamiento que siempre existe en una secuencia de comportamiento que se genera cada vez que se ejecuta el archivo;
en donde la obtención de una característica de comportamiento estable en el resultado del comportamiento dinámico comprende:
ejecutar el archivo en el dispositivo de protección de seguridad dos veces, para obtener por separado una secuencia de comportamiento que se obtiene después de cada vez que se ejecuta, para obtener una primera secuencia de comportamiento y una segunda secuencia de comportamiento;
determinar comportamientos idénticos que existen en la primera secuencia de comportamiento y la segunda secuencia de comportamiento, en donde los comportamientos idénticos son comportamientos que son iguales en términos de tipos de comportamiento y contenido de comportamiento; y
obtener un conjunto formado por los comportamientos idénticos en la primera secuencia de comportamiento y la segunda secuencia de comportamiento, y usar el conjunto como la característica de comportamiento estable.

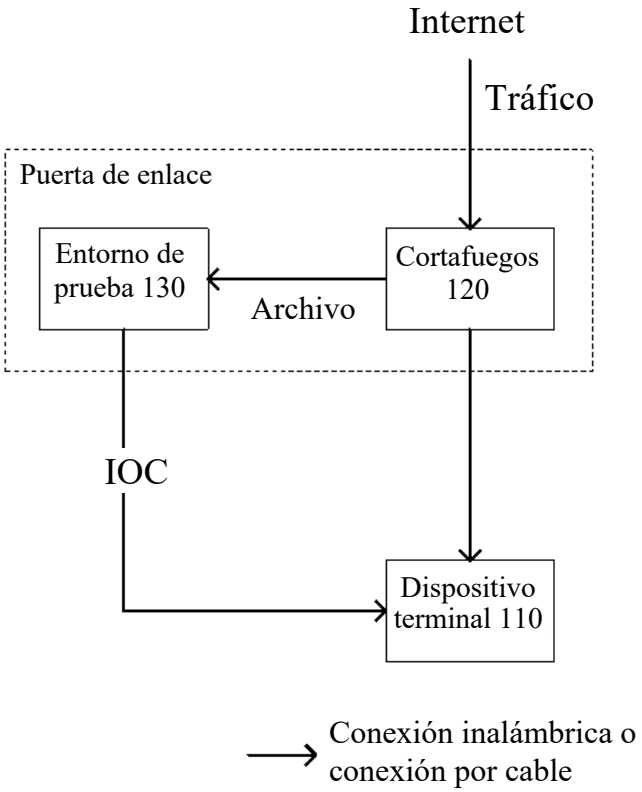
Internet
Tráfico
Puerta de enlace
Entorno de prueba 130
Archivo
Cortafuegos 120
IOC
Dispositivo terminal 110
Conexión inalámbrica o conexión por cable

Figura 1

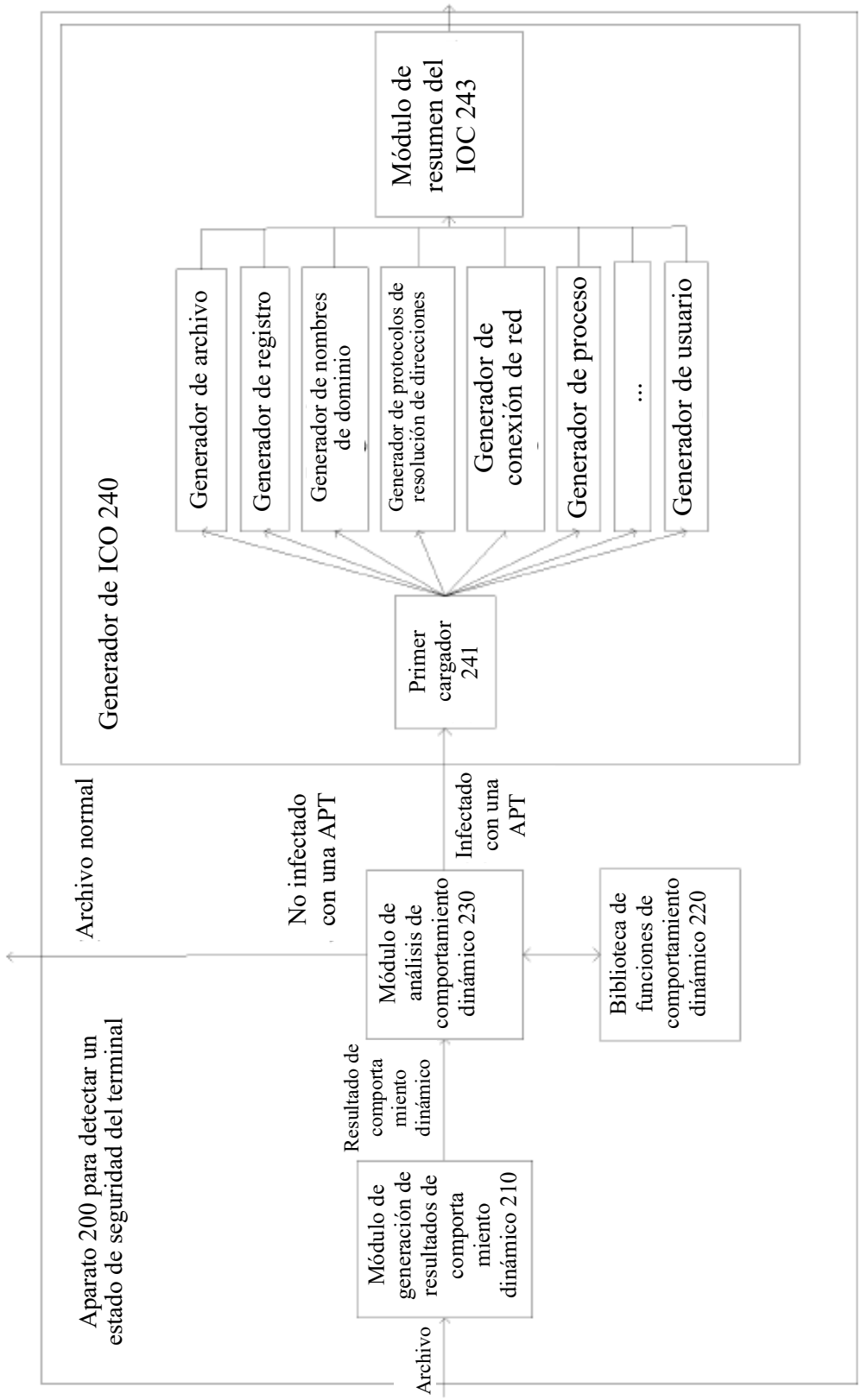
Aparato 200 para detectar un estado de seguridad del terminal
Archivo
Módulo de generación de resultados de comporta miento dinámico 210
Resultado de comporta miento dinámico
Módulo de análisis de comportamiento dinámico 230
Biblioteca de funciones de comportamiento dinámico 220
Archivo normal
No infectado con una APT
Infectado con una APT
Generador de ICO 240
Primer cargador 241
Generador de archivo
Generador de registro
Generador de nombres de dominio
Generador de protocolos de resolución de direcciones
Generador de conexión de red
Generador de proceso
...
Generador de usuario
Módulo de resumen del IOC 243

Figura 2

Un resultado de comportamiento dinámico que incluye una amenaza ATP típica

```
/* Una muestra libera un archivo PE: C:\WINDOWS\apocalyps32.exe*/
<record id="314"><pname>1077.exe</pname><pid>1448</pid><action
arg1="C:\WINDOWS\apocalyps32.exe" arg2="32">FCreate</action></record>
<record id="316"><pname>1077.exe</pname><pid>1448</pid><action
arg1="C:\windows\apocalyps32.exe" arg2="Offset: 0 Length:
65536">FWritePE</action></record>
<record id="317"><pname>1077.exe</pname><pid>1448</pid><action
arg1="C:\WINDOWS\apocalyps32.exe" arg2="Offset: 65536 Length: 43008"
arg3="SUCCESS">FAST_FWRITE</action></record>
/* Ejecutar la muestra: C:\WINDOWS\apocalyps32.exe*/
<record id="370"><pname>1077.exe</pname><pid>1448</pid><action
arg1="C:\WINDOWS\apocalyps32.exe:1252">CreateProcess</action></record>
<record id="371"><pname>1077.exe</pname><pid>1448</pid><action
arg1="C:\WINDOWS\apocalyps32.exe.Manifest">FOpen</action></record>
<record id="372"><pname>1077.exe</pname><pid>1448</pid><action
arg1="None">KillSelf</action></record>
/* Crear una amenaza, e inyectar la amenaza en el proceso IEXPLORE.EXE para ocultar la
amenaza*/
<record id="1780"><pname>IEXPLORE.EXE</pname><pid>1244</pid><action
arg1="explorer.exe">OpenProcesss</action></record>
<record id="1781"><pname>IEXPLORE.EXE</pname><pid>1244</pid><action
arg1="explorer.exe:2016">WriteOtherProcMem</action></record>
<record id="1782"><pname>IEXPLORE.EXE</pname><pid>1244</pid><action
arg1="explorer.exe:2016">WriteOtherProcMem</action></record>
<record id="1783"><pname>IEXPLORE.EXE</pname><pid>1244</pid><action
arg1="explorer.exe:2016">WriteOtherProcMem</action></record>
<record id="1784"><pname>IEXPLORE.EXE</pname><pid>1244</pid><action
arg1="explorer.exe:2016">WriteOtherProcMem</action></record>
<record id="1785"><pname>IEXPLORE.EXE</pname><pid>1244</pid><action
arg1="explorer.exe:2016">WriteOtherProcMem</action></record>
<record id="1786"><pname>IEXPLORE.EXE</pname><pid>1244</pid><action
arg1="explorer.exe:2016">WriteOtherProcMem</action></record>
<record id="1787"><pname>IEXPLORE.EXE</pname><pid>1244</pid><action
arg1="explorer.exe:2016">CreateRemoteThread</action></record>
/* Modificar un registro para adicionar un elemento de inicio*/
<record id="1788"><pname>IEXPLORE.EXE</pname><pid>1244</pid><action
arg1="HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
arg2="Open">RegCreateKey</action></record>
<record id="1789"><pname>IEXPLORE.EXE</pname><pid>1244</pid><action
arg1="HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\apocalyps32"
arg2="C:\WINDOWS\apocalyps32.exe">RegSetValue</action></record>
/* Conectarse a una red externa: 5.5.66.101:1453*/
<record id="1850"><pname>iexplore.exe</pname><pid>1244</pid><action
arg1="340" arg2="5.5.66.101:1453">Connect</action></record>
```

Figura 3

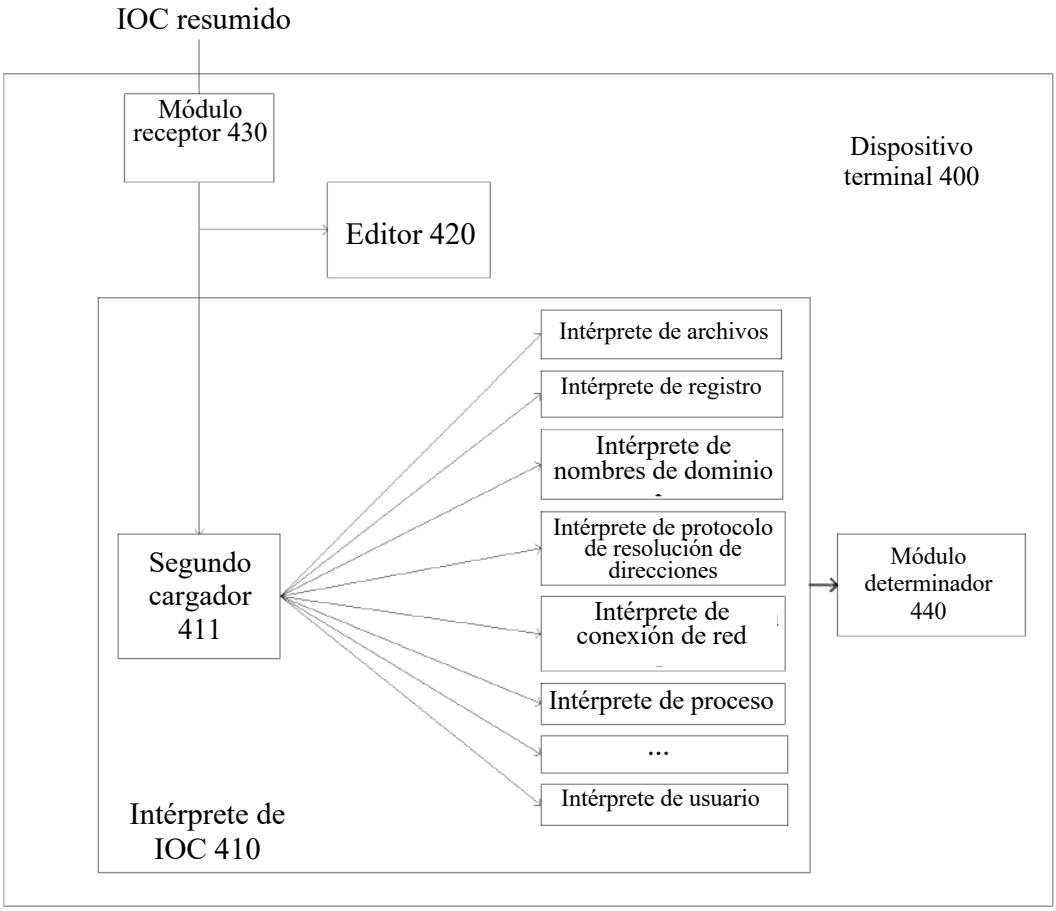
IOC resumido
Módulo receptor 430
Dispositivo terminal 400
Editor 420
Intérprete de archivos
Intérprete de registro
Intérprete de nombres de dominio
Intérprete de protocolo de resolución de direcciones
Intérprete de conexión de red
Intérprete de proceso
...
Intérprete de usuario
Segundo cargador 411
Módulo determinador 440
Intérprete de IOC 410

Figura 4

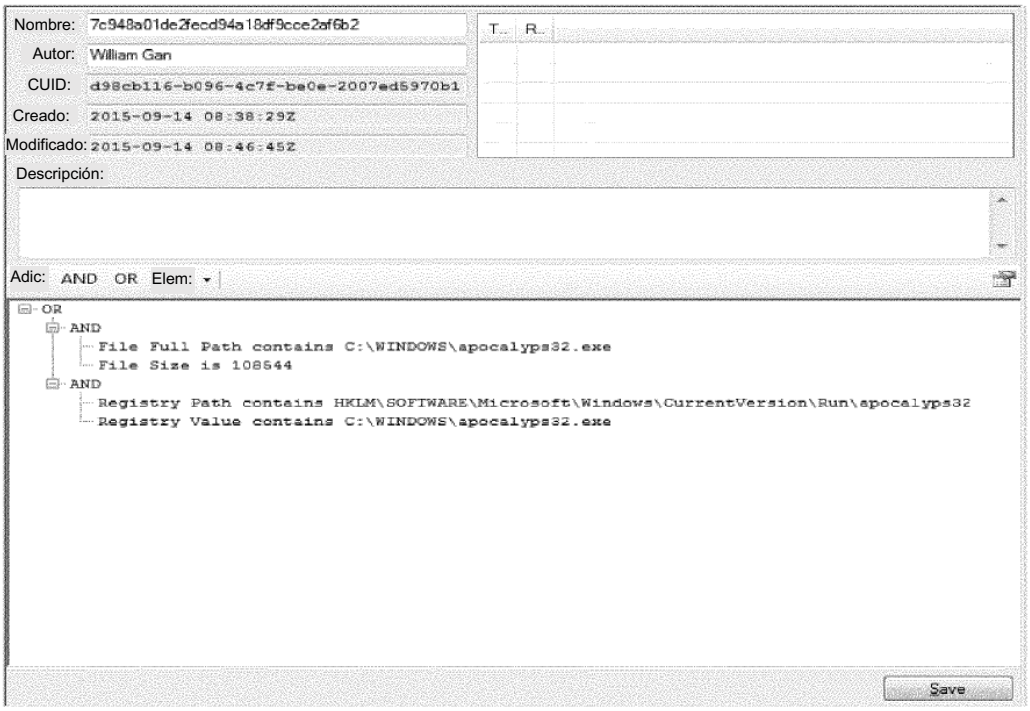

Figura 5

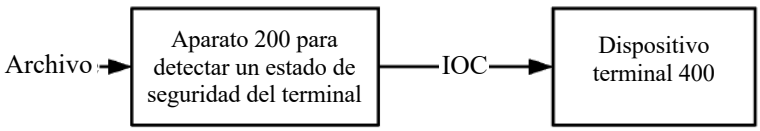

Figura 6

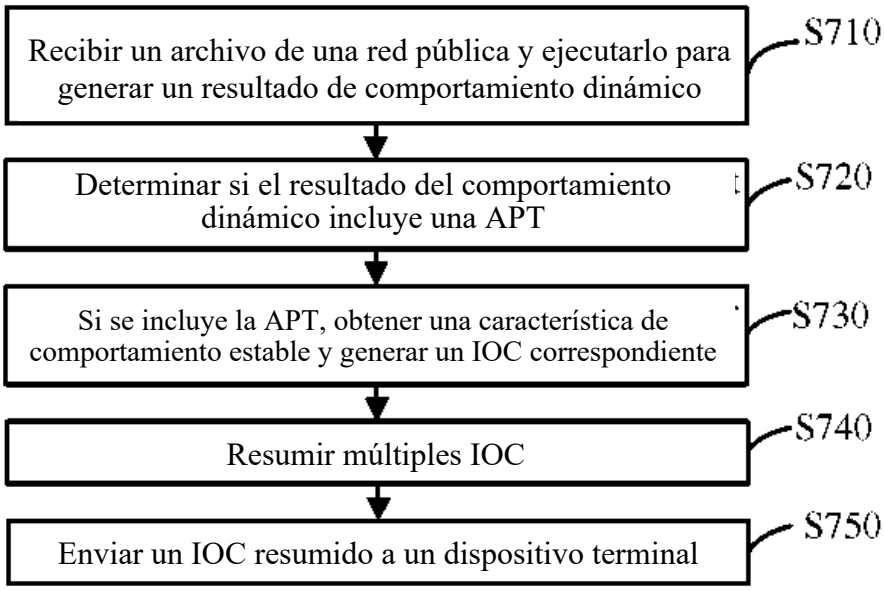

Figura 7

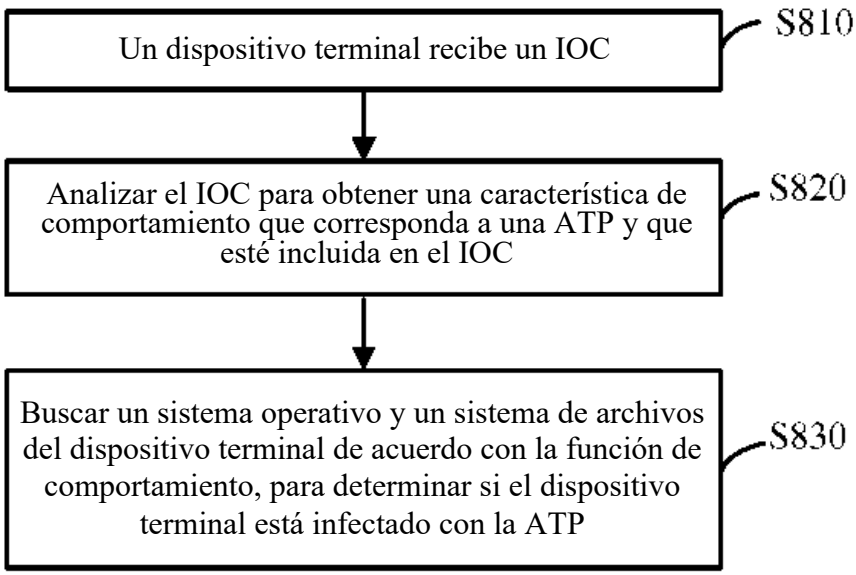

Figura 8

IOC de tipo archivo

```
<Indicator operator="AND" id="4c032204-5441-4c32-accc-d8777bd3cf53">
      <IndicatorItem id="0df0bdb5-8c53-47e2-9242-96830aeb1508"
condition="contains">
        <Context document="FileItem" search="FileItem/FullPath" type="mir" />
        <Content type="string">C:\WINDOWS\apocalyps32.exe</Content>
      </IndicatorItem>
      <IndicatorItem id="bd99c707-a7bf-4968-bed0-cc50d472b794" condition="is">
        <Context document="FileItem" search="FileItem/SizeInBytes" type="mir" />
        <Content type="int">108544</Content>
      </IndicatorItem>
    </Indicator>
```

Figura 9

IOC de tipo registro

```
<Indicator operator="AND" id="98f5e9ce-b591-43f0-95d3-36a4d3331ea5">
      <IndicatorItem id="43f047d6-1a9f-4a67-a524-a57d1e0231d3" condition="contains">
        <Context document="RegistryItem" search="RegistryItem/Path" type="mir" />
        <Content
type="string">HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\apocalyps32
</Content>
      </IndicatorItem>
      <IndicatorItem id="48e07653-2008-4cac-8abe-defb250a47da" condition="contains">
        <Context document="RegistryItem" search="RegistryItem/Value" type="mir" />
        <Content type="string">C:\WINDOWS\apocalyps32.exe</Content>
      </IndicatorItem>
    </Indicator>
```

Figura 10

IOC resumido

```
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://
www.w3.org/2001/XMLSchema" id="d98cb116-b096-4c7f-be0e-2007ed5970b1" last-
modified="2015-09-14T08:46:45" xmlns="http://schemas.mandiant.com/2010/ioc">
  <short_description>7c948a01de2fecd94a18df9cce2af6b2</short_description>
  <authored_by>William Gan</authored_by>
  <authored_date>2015-09-14T08:38:29</authored_date>
  <links />
<definition>
<Indicator operator="OR" id="b9199f67-2b9b-4377-ad90-b1f3e316d487">
    <Indicator operator="AND" id="4c032204-5441-4c32-accc-d8777bd3cf53">
      <IndicatorItem id="0df0bdb5-8c53-47e2-9242-96830aeb1508"
condition="contains">
        <Context document="FileItem" search="FileItem/FullPath" type="mir" />
        <Content type="string">C:\WINDOWS\apocalyps32.exe</Content>
      </IndicatorItem>       <IndicatorItem id="bd99c707-a7bf-4968-bed0-cc50d472b794"
condition="is">
        <Context document="FileItem" search="FileItem/SizeInBytes" type="mir" />
        <Content type="int">108544</Content>       </IndicatorItem>     </Indicator>
    <Indicator operator="AND" id="98f5e9ce-b591-43f0-95d3-36a4d3331ea5">
      <IndicatorItem id="43f047d6-1a9f-4a67-a524-a57d1e0231d3" condition="contains">
        <Context document="RegistryItem" search="RegistryItem/Path" type="mir" />
        <Content type="string">HKLM\SOFTWARE\Microsoft\Windows\
CurrentVersion\Run\apocalyps32</Content>
      </IndicatorItem>       <IndicatorItem id="48e07653-2008-4cac-8abe-defb250a47da"
condition="contains">         <Context document="RegistryItem" search="RegistryItem/
Value" type="mir" />
        <Content type="string">C:\WINDOWS\apocalyps32.exe</Content>
      </IndicatorItem>     </Indicator>
</Indicator>  </definition> </ioc>
```

Figura 11