(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 771 951**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/701 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **03.02.2015 E 15153573 (9)**

(97) Fecha y número de publicación de la concesión europea: **15.01.2020 EP 2903238**

(54) Título: **Un señuelo basado en encaminador para detectar amenazas persistentes avanzadas**

(30) Prioridad:

03.02.2014 IL 23080014

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.07.2020

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
Friedrich-Ebert-Allee 140
53113 Bonn, DE

(72) Inventor/es:

ELOVICI, YUVAL;
SHABTAI, ASAF y
PEYLO, CHRISTOPH

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Un señuelo basado en encaminador para detectar amenazas persistentes avanzadas

Campo de la invención

La presente invención se refiere al campo de detección de ciberataques. Más particularmente, la invención se refiere a un señuelo basado en encaminador para detectar amenazas persistentes avanzadas.

Antecedentes de la invención

A medida que los ciberataques se están volviendo cada vez más sofisticados, uno de los principales objetivos de un atacante es los dispositivos de red. Como parte del ataque, un atacante puede intentar modificar la configuración de dispositivos de red (por ejemplo, encaminadores, conmutadores, etc.), para acceder, modificar o redirigir tráfico de interés o interferir con diversos servicios soportados por el dispositivo (por ejemplo, Denegación de Servicio). Detectar un ataque de este tipo es una tarea compleja, ya que en muchos casos no crea ninguna anormalidad observable, o ya que el atacante lanza un ataque altamente sofisticado (ganando de este modo el control total) que le permite ocultar pruebas.

Muchos encaminadores y conmutadores de internet que forman la infraestructura básica de la red, y se ignoran en gran medida como vulnerabilidades de seguridad. Esto incluye no únicamente instalar "implantes" encubiertos en ordenadores de sobremesa ajenos, sino también en encaminadores y cortafuegos. Piratear encaminadores es una forma ideal para que una agencia de inteligencia o militar mantenga una restricción sobre el tráfico de red porque los sistemas no se actualizan con nuevo software muy a menudo o se parchean de la forma en que lo hacen los sistemas Windows y Linux.

Los encaminadores de red apenas se actualizan ya que el equipo de interconexión en red es demasiado crítico, ya que normalmente no tiene redundancia para hacerse correctamente. También, los encaminadores no tienen software de seguridad que pueda ayudar a detectar una brecha.

Vulnerabilidades de encaminador ubicuas son difíciles de encontrar ya que existen demasiadas configuraciones diferentes para encaminadores, y un ataque que funciona contra una configuración de encaminador podría no funcionar para otra. Pero una vulnerabilidad que afecta al sistema operativo principal es mucho más valiosa ya que es menos probable que dependa de la configuración. Una vez que el fabricante de software conoce una vulnerabilidad y se parchea, pierde mucho de su valor. Pero debido a que muchos usuarios y administradores no parchean sus sistemas, algunas vulnerabilidades pueden usarse de forma efectiva durante años, incluso después de que un parche esté disponible. El gusano Conficker, por ejemplo, continuó infectando millones de ordenadores mucho después de que Microsoft lanzase un parche que debería haber detenido la expansión del gusano.

Para estudiar las actividades de los atacantes de red y para supervisar cómo son capaces de acceder a un servidor, muchos administradores de red emplean un señuelo que tiene un nivel de seguridad reducido para atraer potenciales atacantes a la red. Un señuelo de la técnica anterior es un servidor virtual que emula un servidor real, proporcionándose con datos reales, aplicaciones y otros tipos de funcionalidad que convencen a usuarios de red que es un servidor auténtico incluso aunque el señuelo esté realmente aislado de la red. Después de que un atacante intenta comprometer el señuelo, puede recopilarse información relacionada con el ataque, tal como la dirección IP del atacante. También, el administrador puede determinar la técnica de ataque, para aprender las vulnerabilidades de la red que conducen a la brecha de seguridad. Adicionalmente, puede capturarse al atacante mientras intenta acceder a la red a través del señuelo.

Un sistema de señuelo de este tipo se describe, por ejemplo, en el documento US 2012/023572, en el que un señuelo simula una red completa, atrayendo, por lo tanto, a intrusos y habilitando la recopilación de información para ayudar a rastrear e identificar la fuente de intrusión.

Un sistema para evitar auditar y tender tráfico no autorizado en sistemas de red se describe en el documento US 2006/024701, en el que un señuelo ubicado dentro un encaminador de red rastrea intentos de ataque.

Debido a la prevalencia de señuelos y otros módulos de protección y seguridad tales como cortafuegos, los atacantes tienen acceso muy limitado a servidores. En consecuencia, los atacantes han intentado recientemente acceder a una red a través de un encaminador u otros dispositivos de red. Reconfigurando un encaminador, un atacante puede redirigir tráfico de interés a una ubicación específica y, de este modo, acceder a información sensible. Ya que un encaminador tiene hardware y software especializados para dirigir paquetes de datos desde una red de datos a otra a pesar del alto volumen de datos que pasa a través, un señuelo basado en encaminador tendría que ser capaz de operar lo suficientemente rápido y de acuerdo con un proceso de reconfiguración esperado para hacer que un atacante atraído al señuelo crea que ha accedido a un encaminador real.

"Honeypot router for routing protocols protection" de Ghourabi A. et al., publicado en Risks and Security of Internet and

Systems (CRiSIS), 2009 Cuarta Conferencia Internacional el 19-22 de octubre de 2009, páginas 127-130, divulga un señuelo de encaminador para detectar ataques de configuración de encaminamiento.

"Data analyzer based on data mining for honeypot router" de Ghourabi A. et al., publicado en Computer Systems and Applications (AICCSA), 2010 Conferencia Internacional de IEEE/ACS, 16-19 de mayo de 2010, páginas 1-6, describe una herramienta de análisis de datos basándose en agrupación de minería de datos para un encaminador de señuelo.

Es un objeto de la presente invención proporcionar un señuelo basado en encaminador que puede detectar de forma precisa y fiable un intento de reconfigurar un encaminador.

Es un objeto adicional de la presente invención proporcionar un señuelo basado en encaminador para emular de forma suficiente a un encaminador para convencer a un atacante que se ha accedido a un encaminador de red real.

Otros objetos y ventajas de la invención serán evidentes a medida que la descripción avanza.

Sumario de la invención

La presente invención proporciona un sistema de señuelo basado en encaminador, que comprende un encaminador de red, un componente de intermediario para interceptar todo el tráfico de datos previsto para, o devuelto desde, dicho encaminador, y un señuelo en comunicación de datos con dicho componente de intermediario, en donde un procesador asociado con dicho componente de intermediario es operable para analizar los datos que se transmiten a dicho encaminador y para reenviar los mismos a dicho señuelo si se descubren que no son legítimos.

El componente de intermediario puede ser transparente a atacantes y disponerse más cerca de bordes de red que el encaminador, y puede adaptarse para decidir si no interferir con los canales de comunicación normales entre un dispositivo cliente y el encaminador, de acuerdo con reglas predeterminadas almacenadas en el procesador.

La presente invención se dirige también a un sistema de señuelo basado en encaminador, que comprende un encaminador de red, y un señuelo de dispositivo de red de comportamiento en comunicación de datos con dicho encaminador que es operable para obtener datos de configuración de encaminador actualizados, para obtener comportamiento de encaminador supervisado y para obtener datos indicativos de una comparación entre comportamiento de encaminador esperado en respuesta a dichos datos de configuración de encaminador actualizados obtenidos y dicho comportamiento de encaminador supervisado.

El comportamiento esperado de un encaminador con una configuración dada puede obtenerse, basándose en una ontología de dispositivo de red predefinida que representa comportamiento o actividades o capacidades posibles de un componente de red.

El señuelo de dispositivo de red de comportamiento operativo puede interactuar con el encaminador por los siguientes canales:

un canal de interfaz de configuración para recibir la configuración de encaminador instantánea;
un canal de muestreo de datos para muestrear datos de control dirigidos al encaminador;
un canal de supervisión para extraer datos relacionados con el comportamiento del encaminador en respuesta a los datos entrantes muestreados;
un canal de derivación a través del cual todos los datos de control normalmente dirigidos al encaminador se derivan al señuelo de dispositivo de red de comportamiento, si se determina que el comportamiento del encaminador es incompatible con el comportamiento de encaminador esperado para la configuración de encaminador instantánea.

El sistema de señuelo basado en encaminador puede comprender adicionalmente:

un sistema de gestión de activos de red para transmitir cambios de configuración del encaminador al señuelo de dispositivo de red de comportamiento usando credenciales legítimas de un Directorio Activo;
un componente de supervisión confiable para:

supervisar el comportamiento del encaminador; y
comparar el comportamiento del encaminador con el comportamiento de encaminador esperado para la configuración de encaminador instantánea, en respuesta a datos entrantes muestreados.

Puede usarse un servidor externo para comparar el comportamiento de encaminador supervisado con el comportamiento de encaminador esperado, de tal forma que el señuelo de dispositivo de red de comportamiento recibe datos de control a través del canal de derivación después de que se ha detectado una anomalía.

El sistema de señuelo basado en encaminador puede comprender adicionalmente un canal de inyección, a través del cual el señuelo de dispositivo de red de comportamiento transmite datos virtuales simulados de este modo al encaminador, en el que cada artículo de datos es identificable, y se compara una reacción de encaminador esperada

en respuesta al artículo de datos simulado y en respuesta a la configuración de encaminador instantánea con la reacción de encaminador supervisada, para determinar una ocurrencia de un evento de anomalía.

Breve descripción de los dibujos

En los dibujos:

- La Figura 1 es una ilustración esquemática de un proceso metodológico para llevar a cabo un ataque;
- La Figura 2 es un diagrama de bloques de un señuelo de encaminador de red típico;
- La Figura 3 es una ilustración esquemática de un sistema de señuelo basado en encaminador, de acuerdo con una realización de la presente invención;
- La Figura 4 es una ilustración esquemática de ontología de dispositivo de red predefinida para obtener comportamiento esperado de un encaminador;
- La Figura 5 es un método para detectar anomalías de encaminador; y
- Las Figuras 6-8 son tres ilustraciones esquemáticas de un sistema de señuelo basado en encaminador, de acuerdo con tres realizaciones de la invención, respectivamente.

Descripción detallada de las realizaciones preferidas

La presente invención es un sistema y método para atraer atacantes a un señuelo asociado con un dispositivo de red tal como un encaminador.

Amenazas Persistentes Avanzadas (APT) para mantener acceso a largo plazo a información sensible objetivo de una organización normalmente siguen un proceso metodológico para llevar a cabo un ataque en un encaminador de red. Como se muestra en la Figura 1, este proceso incluye las siguientes etapas principales: Reconocimiento, Exploración, Ganar Acceso, Atacar y Mantener Acceso y Borrar rastro.

Detectar una APT en la Fase 1 de Reconocimiento es casi imposible ya que la actividad se realiza normalmente de forma externa a la organización. En algún punto, la actividad de reconocimiento continúa a un punto de entrada a la organización durante las siguientes fases. Durante la Fase 2 de Exploración, el atacante/APT explora la infraestructura de organización para detectar encaminadores en servicio, descubrir puertos abiertos y revelar servicios en ejecución y vulnerabilidades potenciales. Detección en la Fase 2 de Exploración es muy desafiante ya que no está claro dónde supervisar y detectar la actividad exploración. Durante la Fase 3 de Ganar Acceso, el atacante/APT puede interactuar con los componentes de IT de la organización (por ejemplo, Directorio Activo, servidores, encaminadores, etc.) para extraer nombres de usuario y contraseñas que permitirá que la APT acceda a diversos recursos sin la necesidad de superar mecanismos de seguridad y, por lo tanto, permaneciendo indetectable. Detectar la actividad de APT en esta fase tiene un gran potencial. Durante la Fase 4 de Mantener Acceso, la APT realizará el ataque real y en la última fase, Fase 5 de Borrar rastro, el atacante intenta borrar su rastro para evitar detección e investigación forense.

Las APT pueden intentar modificar o reconfigurar encaminadores como parte del ataque, para detectar o redirigir tráfico de datos de interés. Detectar un ataque de este tipo es muy complejo ya que en muchos casos no crea ninguna anormalidad observable, o el atacante lanza un ataque altamente sofisticado ganando control total del dispositivo de red para permitir que se oculte la evidencia del ataque. Una operación de reconfiguración ilustrativa que es bastante beneficiosa para atacantes y que debería detectarse preferentemente mediante un señuelo es la redirección de direcciones IP relacionadas con bancos desde un canal seguro a un canal no seguro, permitiendo que se accedan o supervisen datos confidenciales.

Un atacante tiene dos métodos principales para reconfigurar encaminadores:

(1) El atacante reconfigura el encaminador a través de un sistema de gestión de activos de red o directamente por medio de la interfaz de configuración regular del dispositivo usando credenciales legítimas adquiridas en fases anteriores del ataque (por ejemplo, comprometiendo servidores de Directorio Activo o atacando a ordenadores administradores para revelar credenciales);
(2) Suponiendo que se conoce una vulnerabilidad existente en el dispositivo (a través de exploración o por medio de un componente preinstalado), el atacante puede acceder encubierto y reconfigurar el encaminador explotando la vulnerabilidad.

Ya que las APT son muy sofisticadas e incorporan métodos avanzados para evadir mecanismos de seguridad actuales, señuelos de la técnica anterior desplegados en servidores no serán capaces de detectar adecuadamente un intento para comprometer un encaminador de red. El sistema de la presente invención es capaz ventajosamente de detectar una APT que intenta modificar la configuración de un encaminador de red durante la Fase de Mantener Acceso por medio de dos tipos alternativos de implementaciones de Señuelo de Encaminador de Red (NRH): un señuelo basado en intermediario y un señuelo basado en comportamiento.

Pueden desplegarse una pluralidad de señuelos que funcionan como trampas para detectar un intento no autorizado de reconfigurar un encaminador, que puede ser parte de un ataque de APT. Cada señuelo se configura para funcionar

como un dispositivo de red real, aunque es capaz de exponer muchos servicios con vulnerabilidades conocidas a un atacante, proporcionan alta sensibilidad e interacción, y es fácil de detectar. Los señuelos emplean módulos de supervisión y un motor de detecciones inteligente que procesará datos en un registro recopilado y correlacionará eventos para detectar intentos de ataque de APT.

En la Figura 2 se ilustra un diagrama de bloques de un NRH típico. El NRH 10 comprende una pluralidad de puertos de E/S 12 que son prácticamente conectables a una correspondiente línea de datos 7, y un módulo de rendimiento 14 para generar tráfico virtual a través de la pluralidad de puertos de E/S 12 de modo que se hará pensar a los atacantes potenciales, después de recibir datos de rendimiento, que el NRH 10 es un encaminador real. Los datos de rendimiento se generan también prácticamente por el módulo de rendimiento 14, y refleja diversos parámetros asociados con el tráfico virtual, tal como tasa de datos, nivel de seguridad y otra información estadística para cada transferencia de datos virtual.

El NRH 10 también comprende un módulo de configuración 15 para establecer la prioridad de cada transferencia de datos virtual y un módulo de encaminamiento 16 para proporcionar una asignación de canal para que los datos se transfieran prácticamente a través de uno o más de los puertos de E/S 12. Un conjunto por defecto de reglas y una política de seguridad se almacenan también en el módulo de configuración 15. Un módulo de sincronización 19 que comprende un controlador que se ejecuta en un sistema operativo sincroniza la operación del NRH 10, para proporcionar una emulación en tiempo real y respuesta de un encaminador real y para generar una interfaz ficticia para un atacante que accede y comunica con el NRH 10.

El módulo de sincronización 19 puede también realizar las funciones de procesamiento de paquetes virtual, con lo que cada paquete entrante, si los datos entrantes son en forma de paquetes, parece estar asignado a diferentes direcciones objetivo, priorizado y posiblemente transmitido para minimizar retardos entre la transmisión de dos paquetes para mantener una calidad de servicio predefinida o para gestionar congestión de datos.

El módulo de sincronización 19 se adapta, por consiguiente, para responder a consultas enviadas por atacantes atraídos de este modo que desean reconfigurar un encaminador enlazado al mismo, para iniciar una operación de acceso malicioso de información sensible de seguridad. Ejemplos no limitantes de consultas a las que responde el módulo de sincronización 19, preferentemente dentro de un tiempo de respuesta similar al de un encaminador real, incluyen consultas relacionadas con caudal, volumen de tráfico y una lista de direcciones a las que se han reenviado datos. Las respuestas generadas están preferentemente dentro del intervalo de rendimiento esperado de un encaminador real.

Durante interacción con un atacante, tal como cuando se responde a una consulta iniciada por un atacante, el NRH 10 se adapta para parecer un encaminador genuino de forma que la metodología normal y no reservada efectuada por el atacante durante una operación de acceso malicioso puede supervisarse y analizarse. El módulo de sincronización 19 puede operar en uno de tres niveles de emulación: (1) emulación baja, (2) emulación media y (3) emulación alta. Selección de un nivel de emulación particular puede proporcionar protección más amplia para el encaminador asociado con el NRH, o puede mejorar en entendimiento del comportamiento de un atacante/APT, incluyendo los tipos de información que el atacante está buscando. Sin embargo, cada nivel de emulación se asocia con una complejidad de implementación diferente. Si así se desea, puede emplearse más de un NRH, de tal forma que cada señuelo tiene un nivel de emulación diferente.

En el nivel de emulación baja, se despliega un encaminador real en una ubicación de red que es atractiva para un atacante, por ejemplo en términos del volumen de tráfico de datos, nivel de seguridad de los datos que se transmiten y vulnerabilidad a ataque. El señuelo al que se reenvían los datos del atacante, por una parte, es capaz de atraer un número máximo de atacantes, pero, por otra parte, pueden identificarse fácilmente. Un señuelo de este tipo generalmente se instala con firmware vulnerable conocido y tiene configuraciones de puerto o de nombre de usuario por defecto. Los atacantes cesarán generalmente para transmitir datos a una ubicación de red particular después de determinar que se está interceptando por un señuelo. En consecuencia, un señuelo de nivel de emulación baja generalmente no se puede supervisar.

Un señuelo de nivel de emulación media es capaz de atraer atacantes de forma similar a un señuelo de emulación de nivel bajo, pero parece aparentemente real generando de forma inteligente tráfico virtual a través de sus puertos de E/S. Después de un atacante intenta comprometer el señuelo, información relacionada con ataque puede supervisarse y analizarse. Como una herramienta adicional para recibir información relacionada con ataque, dentro del tráfico virtual puede implantarse un testigo de señuelo, o una entidad que contiene datos digitales para indicar un evento de robo digital tal como una entrada de datos ficticios, por ejemplo, una dirección de correo electrónico ficticia, proporcionado con un marcador.

En el nivel de emulación alta, el NRH opera en conjunto con un encaminador real que es parte de la red de producción o infraestructura de una organización. El NRH de emulación alta es capaz de responder a la mayoría de las consultas del atacante empleando un módulo de rendimiento sofisticado para generar datos de rendimiento realísticos y un módulo de sincronización de nivel alto para coordinar los datos de rendimiento para responder realistamente al atacante. En el caso de que el NRH sea incapaz de responder a una consulta particular, o responderá de forma no

realista a la misma, el módulo de sincronización se conectará al controlador del encaminador real y recibirá una respuesta precisa a la consulta. Cuando una consulta incluye uno o más términos predeterminados que son indicativos de una consulta que se sabe que se puede contestar únicamente por un encaminador real, el descubrimiento de tales términos desencadenará una operación de interfaz mediante la que el módulo de sincronización se conectará al controlador del encaminador real. El módulo de sincronización transmitirá, a continuación, la respuesta al atacante, mientras el atacante permanece aislado del encaminador real incluso aunque la respuesta aparentemente se origina desde el encaminador real.

Consideraciones de red significativas implican decidir sobre una ubicación apropiada para desplegar un NRH, cuántos de los mismos deberían desplegarse y cuál debería ser el equilibrio correcto entre los tres tipos de emulación. Puede desarrollarse una metodología de soporte de decisión para garantizar que cada NRH se desplegará en una ubicación adecuada. Un sistema puede basarse en un simulador de red e implementar las siguientes fases: recuperación de topología de red, recuperación de matriz de tráfico típico, un algoritmo para calcular el despliegue óptimo, y una herramienta de simulación para simular ataques. El despliegue óptimo puede calcularse usando algoritmos avanzados que se desarrollarán específicamente para esta tarea.

Señuelo de dispositivo de red basado en intermediario

En el sistema 20 ilustrado en la Figura 3, el señuelo 25 está en comunicación de datos con un componente de intermediario 22 para interceptar todo el tráfico de datos previsto para, o devuelto desde, el encaminador 23. El intermediario 22, que se dispone más cerca de los bordes de red que el encaminador 23, es transparente para atacantes. Los atacantes continuarán, por lo tanto, sus intentos de acceder maliciosamente al encaminador 23 incluso aunque los datos transmitidos se han interceptado, ya que la presencia del intermediario 22 es desconocida para ellos. Un procesador asociado con el intermediario 22 analiza el tráfico de datos que se transmiten al encaminador 23. Si el tráfico se clasifica como legítimo, se reenviará al encaminador 23; de lo contrario, se reenviará al señuelo 25.

Reglas predeterminadas almacenadas en el procesador ayudan al intermediario 22 para decidir si no interferir con los canales de comunicación normales entre un dispositivo cliente 21 y encaminador 23, junto con los cuales pueden transmitirse datos de acuerdo con el Protocolo de Intérprete de Comandos Seguro (SSH), para detectar diversos patrones operacionales de atacantes, o si los datos son claramente indicativos de ser maliciosos, por ejemplo, cuando existe un intento de acceder al dispositivo de red 23 con credenciales por defecto, en cuyo caso los datos se transfieren al señuelo 25 para aislarse del encaminador 23.

Otras indicaciones de un intento de una operación de acceso a encaminador maliciosa incluyen un evento de introducción de contraseñas secuencial con lo que la contraseña de cada uno de un gran número de intentos de introducción de contraseña difiere de una entrada previa por únicamente uno o dos caracteres, un intento de reconfiguración para reencaminar tráfico de datos desde una canal seguro a un canal no seguro que podría conducir a daño irreversible de proporciones calamitosas cuando el canal seguro se asocia con la dirección IP de un banco de renombre mundial, y la supervisión de tráfico de datos que permite que un atacante vea o intercepte información sensible.

Señuelo de dispositivo de red basado en comportamiento

Un Señuelo de Dispositivo de Red de Comportamiento (BNDH) se adapta para detectar una vulnerabilidad existente o puerta trasera oculta en el firmware/software de un encaminador, o de cualquier otro dispositivo de red. Una puerta trasera es un componente de software instalado que habilita los procedimientos de autenticación normal a derivar, permitiendo a los atacantes acceder de forma furtiva posteriormente y reconfigurar al encaminador. Supervisando el comportamiento de un encaminador y comparando su comportamiento observado con un comportamiento esperado, un BNDH es capaz de detectar la reconfiguración o manipulación de un encaminador a través de un canal oculto o puerta trasera.

El estado de configuración de un encaminador se puede supervisar de forma continua de dos formas:

(1) rastreando cambios de configuración mediante un sistema de gestión de activos de red usando credenciales legítimas; y
(2) supervisando tráfico de red y detectando comandos de cambio de configuración.

Para cada estado de configuración el sistema obtendrá el comportamiento esperado del encaminador dada su configuración actual. Derivación del comportamiento esperado se basará en una ontología de dispositivo de red predefinida que representa el comportamiento/actividades/capacidades posibles de un componente de red (véase un ejemplo en la Figura 4). Esta ontología subyacente será la base para implementar un señuelo nuevo específico. Capa de supervisión y emulación de tráfico se implementarán usando la ontología.

Por lo tanto, un sistema que comprende un BNDH operará en el proceso de tres etapas mostrado en la Figura 5. Una precondición está obteniendo una configuración de encaminador en la etapa 37. La configuración de encaminador puede notificarse a través de un cortafuegos unidireccional que asegura comunicación segura y confiable, tras lo cual

el BNDH es capaz de interceptar cambios de configuración, por ejemplo, a través de un sistema de gestión de activos de red. En la etapa 38, el comportamiento de encaminador se supervisa externamente al dispositivo a nivel de red usando tecnologías de supervisión confiables. Finalmente, el comportamiento de encaminador observado se compara con el comportamiento de encaminador esperado en la etapa 39, para identificar anormalidades que no son compatibles con la configuración de encaminador conocida.

La Figura 6 ilustra esquemáticamente un sistema 40 que emplea el encaminador 43 y BNDH 45. En esta realización, el BNDH 45 interactúa con el encaminador 43 mediante cuatro canales separados: (1) canal de interfaz de configuración 41 para recibir la configuración de encaminador instantánea, (2) canal de muestreo de datos 46 a través del cual el BNDH 45 muestrea datos entrantes, preferentemente datos de control dirigidos al encaminador 43, (3) canal de supervisión 47 para extraer datos relacionados con el comportamiento del encaminador en respuesta a los datos entrantes muestreados, y (4) canal de derivación 48 a través del cual todos los datos de control normalmente dirigidos un encaminador 43 se derivan al BNDH 45 si se determina que el comportamiento del encaminador es incompatible con el comportamiento de encaminador esperado para la configuración de encaminador instantánea.

Se apreciará que estos canales no son canales físicos, sino canales lógicos, y pueden implementarse como capas relacionadas con señuelo.

En la Figura 7, el sistema 50 comprende un sistema de gestión de activos de red (NAMS) 52 para transmitir cambios de configuración de encaminador 43 al BNDH 45 mediante el canal 51 usando credenciales legítimas de un Directorio Activo, y un componente de supervisión confiable 57 para supervisar el comportamiento del encaminador a través del canal 59. El BNDH 45 compara el comportamiento del encaminador con el comportamiento de encaminador esperado para la configuración de encaminador instantánea en respuesta a los datos entrantes muestreados recibidos en el canal 56, y recibirá todos los datos de control normalmente dirigidos un encaminador 43 a través del canal 58 después de determinar que el comportamiento del encaminador es incompatible con el comportamiento de encaminador esperado para la configuración de encaminador instantánea.

En otra realización, un servidor externo puede comparar el comportamiento de encaminador supervisado con el comportamiento de encaminador esperado, mientras el BNDH recibirá datos de control a través del canal de derivación después de que se ha detectado una anomalía, indicando que el encaminador se manipuló a través de un canal de comunicación no conocido/encubierto, por ejemplo, por un atacante que explotó una vulnerabilidad en el software/firmware del encaminador.

A veces, supervisar un encaminador real es difícil debido a la cantidad de tráfico de datos y ruido dentro del tráfico. Por lo tanto, para proporcionar supervisión de comportamiento preciso, el encaminador puede probarse activamente recibiendo desafíos predefinidos a través de la red supervisada. Por lo tanto, en lugar de supervisar todo el tráfico de datos que pasan a través del encaminador, o incluso a través de un señuelo, por ejemplo de un nivel de emulación medio o alto, el sondeo activo permite centrarse únicamente en tráfico de datos de bajo volumen ya que el volumen de tráfico sondeado es muy bajo, en comparación con tráfico de producción. El sistema 60 mostrado en la Figura 8, por consiguiente, depende de tráfico de datos que se autogeneró para propósitos de sondeo, para aprender algunas propiedades del encaminador.

La principal ventaja de sondear en relación con la supervisión pasiva, es decir supervisión de todo el tráfico de datos reales, es que el tráfico autogenerado se caracteriza por una variabilidad muy baja que es crucial para detectar de forma fiable cualquier modificación en la configuración.

Como se muestra en la Figura 8, el sistema 60 comprende un canal de inyección 64 a través del cual el BNDH 45 transmite datos virtuales simulados de este modo al encaminador 43. Cada artículo de datos es identificable, y se compara una reacción de encaminador esperada en respuesta al artículo de datos simulado y en respuesta a la configuración de encaminador instantánea con la reacción de encaminador supervisada para determinar una ocurrencia de un evento de anomalía.

Ejemplos de tipos de sondeo/desafío incluyen: paquetes de ICMP, peticiones de DNS, paquetes de VoIP, solicitación de descubrimiento de vecino, correo electrónico y datos de capa de aplicación.

Mientras algunas realizaciones de la invención se han descrito por medio de ilustración, será evidente que la invención puede efectuarse con muchas modificaciones, variaciones y adaptaciones, y con el uso de numerosos equivalentes o soluciones alternativas que están dentro del alcance de expertos en la materia, sin exceder el alcance de las reivindicaciones.

REIVINDICACIONES

1. Un sistema de señuelo basado en encaminador, que comprende:

a) un encaminador de red (22);
b) un señuelo de dispositivo de red de comportamiento (43) en comunicación de datos con dicho encaminador que es operable para obtener datos de configuración de encaminador actualizados, para obtener comportamiento de encaminador supervisado y para obtener datos indicativos de una comparación entre comportamiento de encaminador esperado en respuesta a dichos datos de configuración de encaminador actualizados obtenidos y dicho comportamiento de encaminador supervisado,

caracterizado por que, dicho sistema de señuelo basado en encaminador (22) comprende además:

c) un canal de inyección (64) a través del cual se configura dicho señuelo de dispositivo de red de comportamiento (43) para transmitir datos virtuales, simulados de este modo, a dicho encaminador (22); y
d) medios para sondear activamente dicho encaminador usando dichos datos virtuales para ser tráfico de datos autogenerado y de volumen bajo específico, de tal forma que cada artículo de datos simulado en dichos datos virtuales es identificable, y que una reacción de encaminador esperada en respuesta al artículo de datos simulado y en respuesta a dicha configuración de encaminador actualizada se compara con el comportamiento de encaminador supervisado para determinar una ocurrencia de un evento de anomalía.

2. Un sistema de señuelo basado en encaminador, de acuerdo con la reivindicación 1, en el que el comportamiento esperado de un encaminador con una configuración dada se obtiene, basándose en una ontología de dispositivo de red predefinida que representa comportamiento o actividades o capacidades posibles de un componente de red.

3. Un sistema de señuelo basado en encaminador, de acuerdo con la reivindicación 1, en el que el señuelo de dispositivo de red de comportamiento operativo interactúa con el encaminador por los siguientes canales:

un canal de interfaz de configuración (41) para recibir la configuración de encaminador instantánea;
un canal de muestreo de datos (46) para muestrear datos de control dirigidos a dicho encaminador;
un canal de supervisión (47) para extraer datos relacionados con el comportamiento del encaminador en respuesta a los datos entrantes muestreados;
un canal de derivación (48) a través del cual todos los datos de control normalmente dirigidos a dicho encaminador se derivan a dicho señuelo de dispositivo de red de comportamiento, si se determina que el comportamiento del encaminador es incompatible con el comportamiento de encaminador esperado para la configuración de encaminador instantánea.

4. Un sistema de señuelo basado en encaminador, de acuerdo con la reivindicación 3, en el que el canal de interfaz de configuración (41), canal de muestreo de datos (46), canal de supervisión (47) y canal de derivación (48) son canales lógicos.

5. Un sistema de señuelo basado en encaminador, de acuerdo con la reivindicación 1, comprendiendo adicionalmente:

un sistema de gestión de activos de red (52) para transmitir cambios de configuración del encaminador al señuelo de dispositivo de red de comportamiento usando credenciales legítimas de un Directorio Activo;
un componente de supervisión confiable (57) para:

supervisar el comportamiento del encaminador;
comparar el comportamiento del encaminador con el comportamiento de encaminador esperado para la configuración de encaminador instantánea, en respuesta a datos entrantes muestreados.

6. Un sistema de señuelo basado en encaminador, de acuerdo con la reivindicación 1, en el que se usa un servidor externo para comparar el comportamiento de encaminador supervisado con el comportamiento de encaminador esperado, de tal forma que el señuelo de dispositivo de red de comportamiento recibe datos de control a través del canal de derivación después de que se ha detectado una anomalía.

7. Un sistema de señuelo basado en encaminador, de acuerdo con la reivindicación 1, en el que el medio para sondear activamente dicho encaminador usando dichos datos virtuales es un módulo de rendimiento (14) del señuelo de dispositivo de red de comportamiento (43) que también se adapta para generar los datos virtuales.

8. Un sistema de señuelo basado en encaminador, de acuerdo con la reivindicación 1, en el que el medio para sondear activamente dicho encaminador usando dichos datos virtuales comprende medios para sondear mediante desafíos predefinidos relacionados con el tráfico de datos autogenerado y de volumen bajo específico.

9. Un sistema de señuelo basado en encaminador, de acuerdo con la reivindicación 8, en el que se seleccionan tipos de datos de desafío o sondeo que constituyen el tráfico de datos autogenerado y de volumen bajo específico a partir

del grupo que consiste en paquetes de ICMP, peticiones de DNS, paquetes de VoIP, solicitación de descubrimiento de vecino, datos de capa de aplicación y correo electrónico.

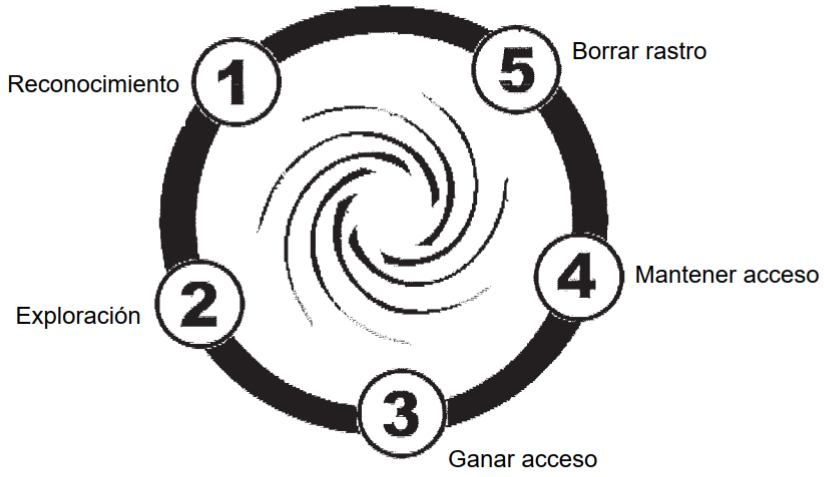
Reconocimiento
1
5
Borrar rastro
Exploración
2
4
Mantener acceso
3
Ganar acceso

Fig. 1

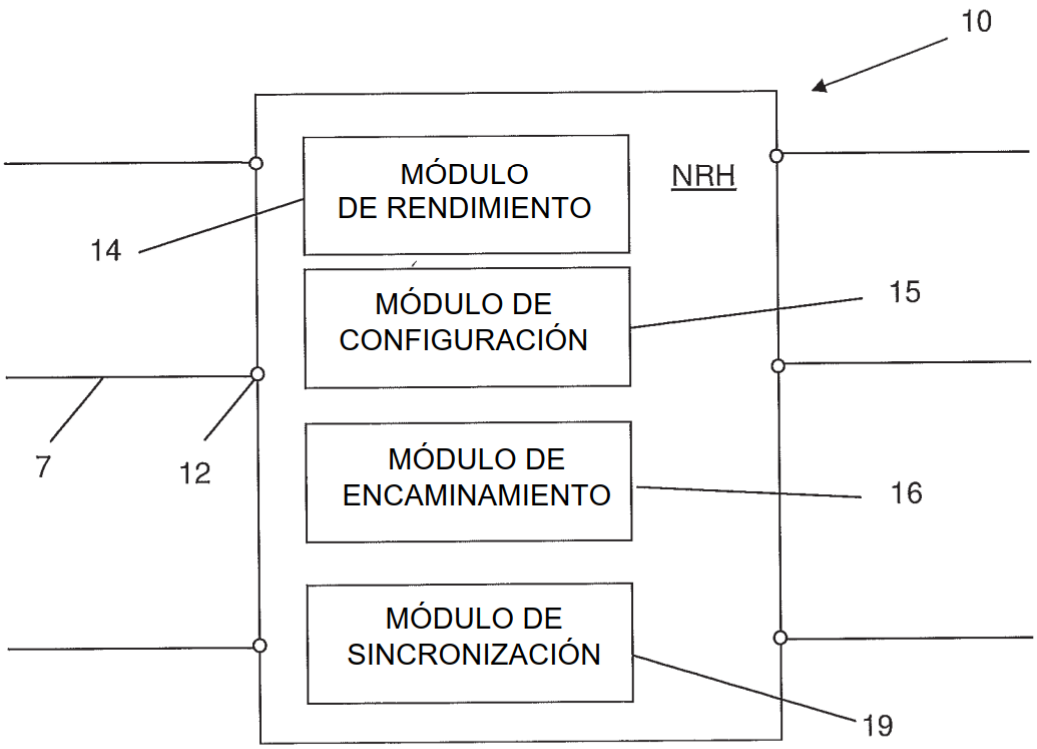
10
MÓDULO DE RENDIMIENTO
NRH
14
MÓDULO DE CONFIGURACIÓN
15
7
12
MÓDULO DE ENCAMINAMIENTO
16
MÓDULO DE SINCRONIZACIÓN
19

Fig. 2

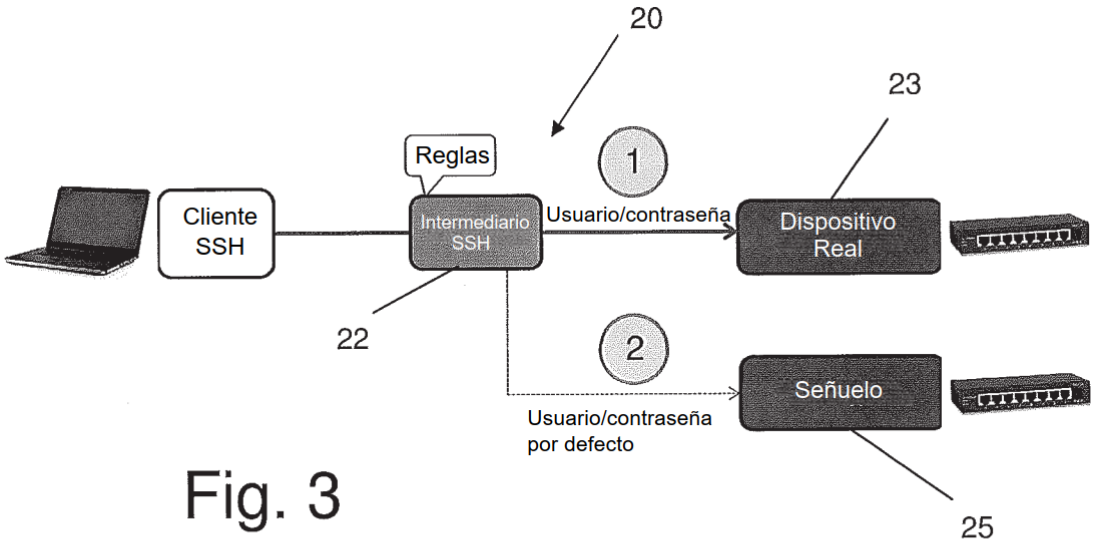
20
23
Reglas
1
Cliente SSH
Intermediario SSH
Usuario/contraseña
Dispositivo Real
22
2
Señuelo
Usuario/contraseña por defecto
25

Fig. 3

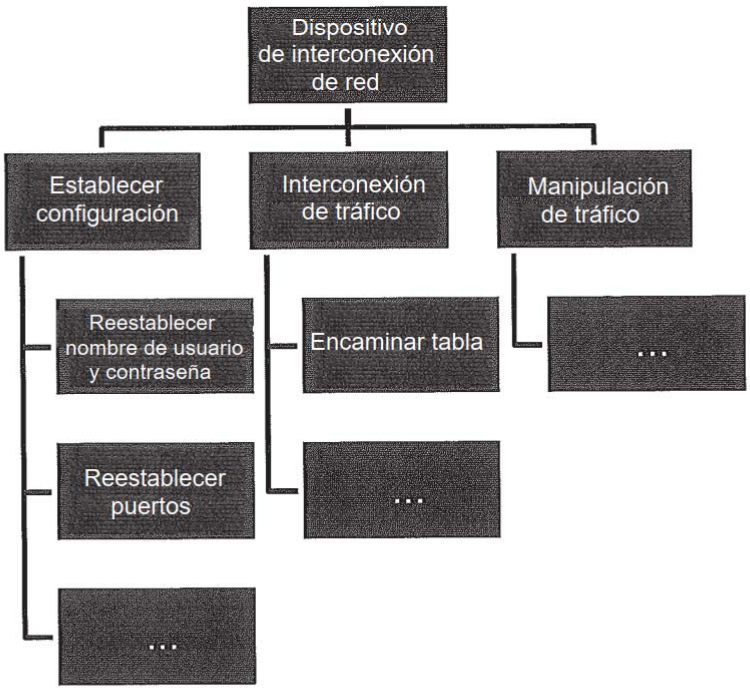
Dispositivo de interconexión de red
Establecer configuración
Interconexión de tráfico
Manipulación de tráfico
Reestablecer nombre de usuario y contraseña
Encaminar tabla
...
Reestablecer puertos
...
...

Fig. 4

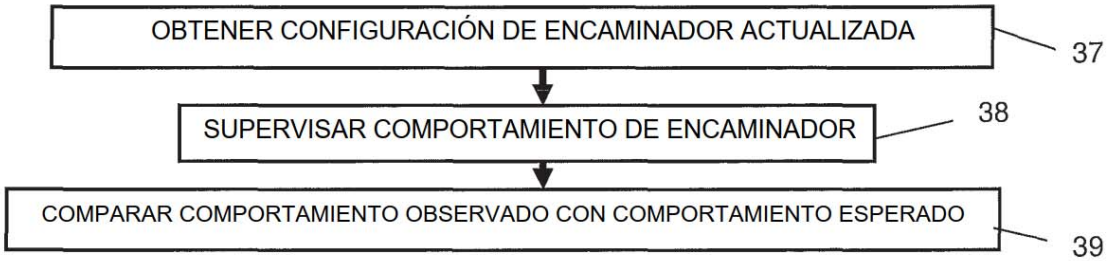

Fig. 5

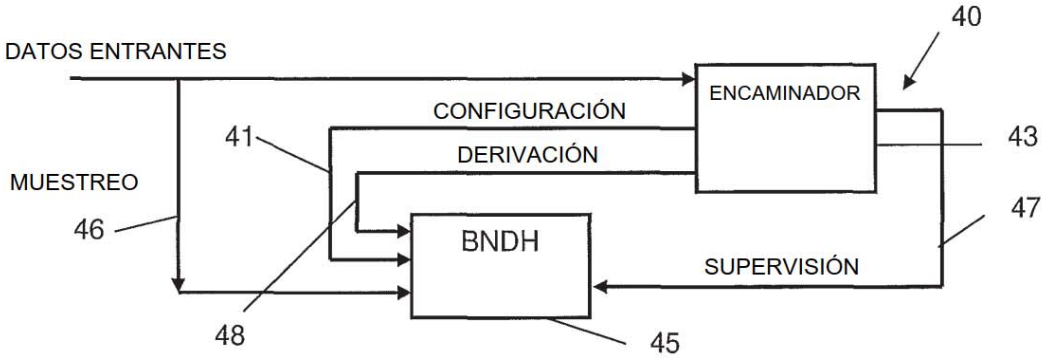

Fig. 6

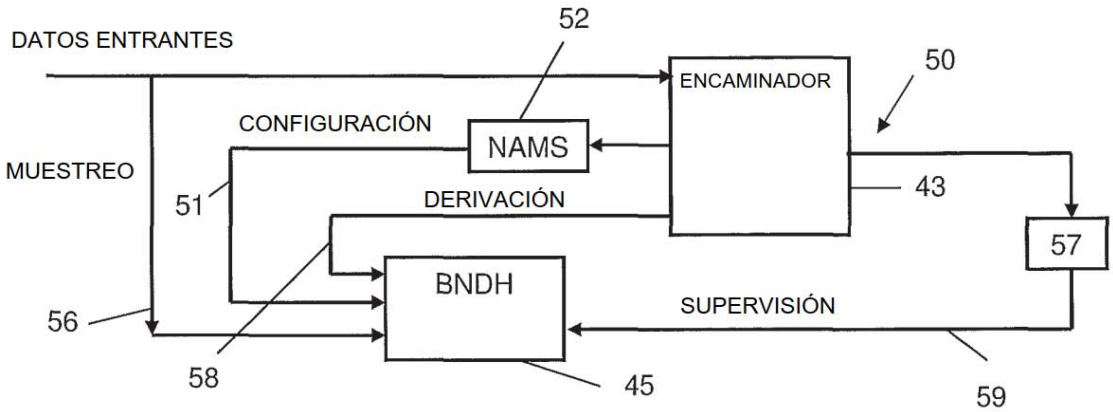

Fig. 7

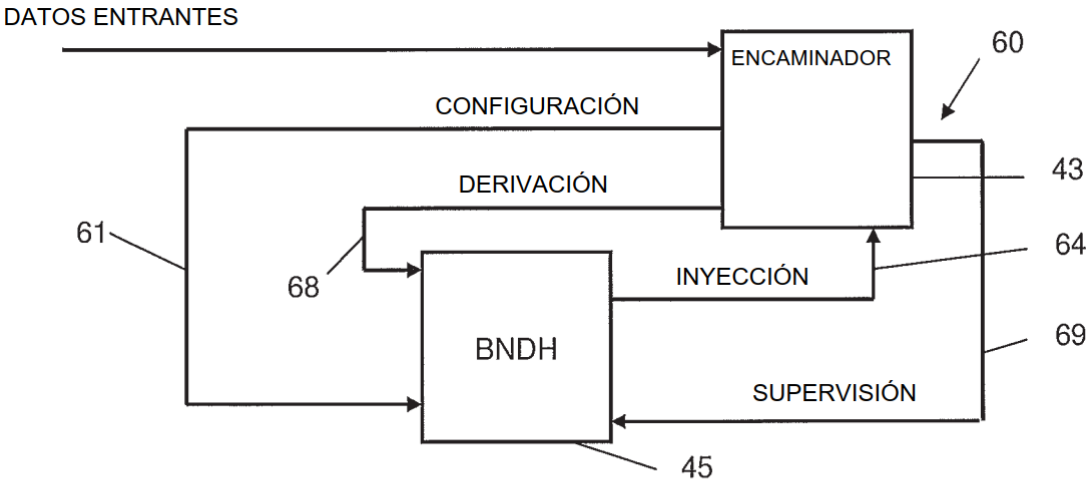
DATOS ENTRANTES
ENCAMINADOR
60
CONFIGURACIÓN
43
DERIVACIÓN
61
64
68
INYECCIÓN
BNDH
69
SUPERVISIÓN
45

Fig. 8