(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 609 253**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.08.2014 E 14180871 (7)**

(97) Fecha y número de publicación de la concesión europea: **12.10.2016 EP 2846512**

(54) Título: **Procedimiento y sistema de defensa duradera frente a software malicioso de botnet**

(30) Prioridad:

04.09.2013 EP 13182958

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.04.2017

(73) Titular/es:

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

(72) Inventor/es:

KRAFT, ANDREAS;
SCHMALL, MARKUS;
MANECKE, ALEXANDER;
SCHROER, MARKUS y
SINNING, THORSTEN

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Procedimiento y sistema de defensa duradera frente a software malicioso de botnet

Campo de la invención

La presente invención concierne al ámbito de las telecomunicaciones, en particular a un procedimiento y un dispositivo para información inmediata de usuarios, que están infectados con software malicioso, en particular software de clientes para botnets.

Los botnets constan de ordenadores de cualquier clase en internet, que se han infectado por programas maliciosos. Estos ordenadores pueden generar entonces tráfico de datos controlado de manera remota de forma autónoma por un ordenador de control externo, con la intención de provocar daños en los servidores y otros ordenadores por medio de tráfico de datos (tráfico) excesivo o inducir la manipulación de medidas de seguridad en un servidor.

Estado de la técnica

Por la solicitud de patente EP 2 403 187 A1 se conocen un procedimiento y un sistema para reconocer ordenadores centrales de una botnet que comprenden un procedimiento, un dispositivo y un sistema para la detección de botnets y una red con funciones para reconocer ordenadores infectados por botnets. Otros antecedentes tecnológicos se explican en los documentos US2010/162399 A1 y US 2010/036947 A1. El documento US 2010/162399 A1 divulga un procedimiento y un dispositivo para proteger una red frente a malware y actividad de botnet. El documento US 2010/036947 A1 divulga un procedimiento y un dispositivo para la reducción de tráfico no deseado entre redes paritarias.

El redireccionamiento de datos puede realizarse a sitios web que muestran sólo una copia de la página original y graban el tráfico de datos abusivo. Asimismo, son conocidos ordenadores que simulan los objetivos de ataque potenciales por parte de ordenadores botnet, designándose estos también señuelos (honeypots). Véase también https://en.wikipedia.org/wiki/Honeypot (computing). Las redes de señuelos sirven para descubrir un uso fraudulento por botnets, y para cuantificar y reconocer las informaciones de origen de ordenadores infectados.

La invención está definida en la reivindicación independiente 1. Las formas de realización preferidas de la invención se definen en las reivindicaciones subordinadas. En particular, la presente invención se refiere a procedimientos para la configuración de un enrutador (aparato de datos), que está conectado con una intranet y una internet. El enrutador intercambia con un servidor en internet informaciones sobre una identidad de terminales de datos o aparatos de datos, que están conectados con el enrutador (aparato de datos) por medio de la intranet. El servidor compara la identidad del terminal de datos/aparato de datos con identidades de un primer grupo de identidades de los terminales de datos/aparatos de datos, en donde el enrutador influye en el tráfico de datos del terminal de datos cuando la identidad del terminal de datos/aparato de datos corresponde al primer grupo de identidades, en donde la influencia sobre el tráfico de datos del terminal de datos es un redireccionamiento del tráfico de datos.

La intranet puede ser una LAN cableada, una red inalámbrica como una WLAN, Zigbees, ANT+, una red Bluetooth o cualquier red parcial como una red parcial de internet, en particular también una WAN. Una internet es una red de ordenadores en general muy alejados o integrados globalmente en la red como una WAN. No obstante, una internet en el sentido de la invención podría ser también una red local o corporativa.

Además, la invención prevé que el primer grupo de identidades de terminales de datos conciernen a tales terminales de datos que se han manipulado por un software malicioso.

Además, la invención prevé preferentemente que la identidad de un terminal de datos/aparato de datos cuya dirección IP es particularmente una dirección IP WAN pública.

La invención prevé preferiblemente que la influencia sobre el tráfico de datos del terminal de datos sea el redireccionamiento del tráfico de datos a una página web predeterminada.

La invención prevé preferiblemente que la influencia sobre el tráfico de datos del terminal de datos sea el redireccionamiento del tráfico de datos a una página web predeterminada archivado localmente en el enrutador.

Además, la invención está configurada de modo que esté previsto un sistema que realiza el procedimiento según la invención.

La ventaja de la presente invención consiste en cotejar regularmente las informaciones, que se presentan en redes de señuelos, con una configuración de enrutador para mantener así tan pequeños como sea posible los daños de un ordenador o red local (doméstica) infectado por uno o varios botnets y hacerlos presentes para el usuario del ordenador infectado o red local, sin intervenir en el contenido del tráfico de datos del ordenador infectado.

El presente procedimiento y sistema según la invención se describe por medio del croquis adjunto, mostrándose en este caso:

La figura 1, una estructura a modo de ejemplo de una infraestructura para realizar el procedimiento según la invención que consta de un enrutador que está en interacción con una LAN y la internet.

La figura 2a, la estructura esquemática de una arquitectura de enrutador.

La figura 2b, la estructura esquemática de una arquitectura de enrutador incluyendo una unidad de control doméstica para la comunicación audiovisual y multimedia, en caso de la presencia de un incidente.

La figura 3, una página web de avisos que se presenta al usuario de un ordenador infectado en lugar de una página web objetivo.

Descripción detallada de la invención

La figura 1 muestra un PC 2 (PC de usuario; terminal de datos), que se ha infectado por un virus botnet. El ordenador 2 está conectado con un enrutador 1 (enrutador domestico; aparato de datos) por medio de una LAN. El virus botnet en el ordenador 2 envía paquetes de datos por medio del enrutador 1 a la internet, en particular para localizar en el entorno ordenadores y servidores fáciles de manipular. Un ataque/barrido de este tipo puede registrarse en un señuelo 9 del operador de red telefónica y conducirse al sistema de alerta temprana 7 (EWS). El EWS facilita una lista negra de las direcciones IP identificadas como maliciosas de un intervalo de tiempo libremente seleccionable como, por ejemplo, los últimos 30 minutos. Además, un sistema de alerta temprana (EWS; servidor 7) puede constar también de servidores que agregan datos de diferentes señuelos 9.

El virus botnet ataca particularmente al servidor web 8 (cualquier servidor web) que el usuario quisiera activar y provoca un tráfico elevado y daños económicos a los servidores web atacados. Además, el operador de red telefónica está obligado a mantener tan pequeño como sea posible el ataque de software malicioso desde su red.

Según la invención el requisito del impedimento de solicitudes de botnets se resuelve como sigue.

Al software de funcionamiento del enrutador se añade una aplicación que pregunta, en intervalos regulares, al sistema de señuelo 9 o al sistema de alerta temprana 7 si un ordenador genera una solicitud de botnet en la internet o la red de área local (LAN) que está conectada al enrutador 1. Esto se hace a través del cotejo de la dirección IP pública.

Si esta solicitud se responde positivamente de parte del sistema de señuelo 9 (aquí, por ejemplo, el sistema de alerta temprana 7), el enrutador 1 filtra el tráfico del ordenador infectado 2 en la LAN conectada extrayéndolo de la corriente de datos. En una solicitud de un usuario del ordenador infectado 2 se intercala entonces una página web local con un aviso de advertencia en lugar de una página web objetivo solicitada. Además, la solicitud de un usuario del ordenador infectado 2 se redirecciona opcionalmente a una página web externa, en particular a un jardín vallado (Walled Garden). Se le indica al usuario que un ordenador 2 está infectado por un virus botnet y se libera la página web objetivo originalmente solicitada únicamente después de leer y confirmar el aviso de advertencia y, opcionalmente, la resolución de una pregunta de seguridad para asegurarse de que es un usuario y no un programa de software el que hace la solicitud. Es posible también que se inicien en este caso programas automáticos que eliminan el software malicioso del ordenador botnet.

Alternativa o adicionalmente, puede conducirse también un mensaje desde el enrutador 1 al servidor de alerta temprana o a un servidor 7 determinado por éste, el cual retransmite un aviso predeterminado a un centro de mensajes cortos 6 (SMSC) de un operador de red telefónica. El SMSC 6 envía entonces a un número de teléfono móvil predeterminado asociado al usuario un mensaje corto al teléfono 5 con una indicación de una infección de un ordenador botnet utilizado por un software malicioso.

Además, puede enviarse también un mensaje por medio de otro servicio de comunicaciones cortas o también por correo electrónico, mensajero o correo postal.

Los componentes de una arquitectura esquemática a modo de ejemplo de un enrutador 1 están representados en la figura 2a. La arquitectura presenta sustancialmente dos componentes: el entorno de realización OSGi Framework y el sistema operativo de enrutador OpenWRT. En el OSGI Framework está incorporada una aplicación, Botnet Servlet.

El servlet interactúa con el servidor HTTP y el DMT Admin que de nuevo controla los componentes correspondientes para el control del tráfico de red.

Esta aplicación sirve para el establecimiento de llamada, la pregunta de la red de señuelo 9 y también para la notificación del usuario de un ordenador infectado 2 por medio de una página web especial en conexión con el servidor HTTP, que está representado en la figura 3. Además, la aplicación Botnet Servlet inicia también el SceneManager & Interpreter, que envía una notificación, por medio del servicio de comunicaciones cortas, al SMSC 6 por SMS al aparato de telefonía móvil del usuario.

Además, existe también un DataPlugin Botnet, que interactúa con la parte del sistema operativo OpenWRT para configurar el cortafuegos del enrutador 1, de modo que se redireccione el tráfico de datos sospechoso de un ordenador infectado 2 a través del cortafuegos.

En la figura 2b está representada una ampliación de la figura 2a, en la que el enrutador 1 está conectado con un control doméstico. Aquí, el SceneManager & Interpreter (que son, en este caso, componentes para el procesamiento regular en el control doméstico) se encuentra en interacción con un Hue®Driver y un EQ3®/Zwave® Driver. El SceneManager&Interpreter puede intervenir, en caso del reconocimiento de un ordenador como ordenador botnet, en el control doméstico en una red domótica (HAN) y, por tanto, enviar señales a través de la electrónica doméstica, como, por ejemplo conectar o desconectar una luz de señal de color.

Otras realizaciones pueden tener sentido para el experto al considerar la descripción de la presente invención. Por ejemplo, el ordenador puede identificarse automáticamente en la intranet y analizarse por medio de un software de exploración de virus e instalarse de nuevo.

Además, el enrutador puede emitir también un anuncio en una página web del proveedor de servicio de internet, en el que se procesan informaciones sobre el estado de seguridad del ordenador habilitado en la red.

REIVINDICACIONES

1. Procedimiento de configuración de un aparato de datos (1), que está conectado con una intranet (LAN) y una internet, y que intercambia informaciones sobre una identidad del aparato de datos (1) con un servidor (7) en internet,

en el que la identidad del aparato de datos (1) se compara con identidades de un primer grupo de identidades de aparatos de datos (1),

en el que el aparato de datos (1) influye en el tráfico de datos de un terminal de datos (2) conectado al aparato de datos (1) cuando la identidad del aparato de datos (1) pertenece al primer grupo de identidades, y

en el que la influencia sobre el tráfico de datos del terminal de datos (2) es un redireccionamiento del tráfico de datos,

en el que el primer grupo de identidades de aparatos de datos (1) concierne a aquellos aparatos de datos (1) que están conectados con un terminal de datos (2) que se ha manipulado con software malicioso.

2. Procedimiento según la reivindicación 1, en el que el aparato de datos (1) es un enrutador (1).

3. Procedimiento según la reivindicación 1 o 2, en el que la comparación de la identidad del aparato de datos (1) se realiza en el servidor (7).

4. Procedimiento según una de las reivindicaciones anteriores, en el que la identidad de un aparato de datos (1) es su dirección IP.

5. Procedimiento según la reivindicación 4, en el que la comparación de la dirección IP del aparato de datos (1) con un primer grupo de direcciones se realiza en el servidor en forma de un sistema de alerta temprana (7) que facilita una lista negra de las direcciones IP identificadas como maliciosas de un intervalo temporal libremente seleccionable.

6. Procedimiento según una de las reivindicaciones anteriores, en el que la influencia sobre el tráfico de datos desde el terminal de datos (2) es un redireccionamiento del tráfico de datos a una página web predeterminada.

7. Procedimiento según una de las reivindicaciones anteriores, en el que la influencia sobre el tráfico de datos desde el terminal de datos (2) es el redireccionamiento del tráfico de datos a una página web predeterminado archivada localmente en el aparato de datos (1).

8. Sistema con un servidor (7) y con un aparato de datos (1) que está conectado con una intranet (LAN) y una internet, y que intercambia informaciones sobre una identidad del aparato de datos (1) con el servidor (7) en internet, para realizar el procedimiento según una de las reivindicaciones anteriores en el aparato de datos (1), en el que el servidor está adaptado para realizar la comparación.

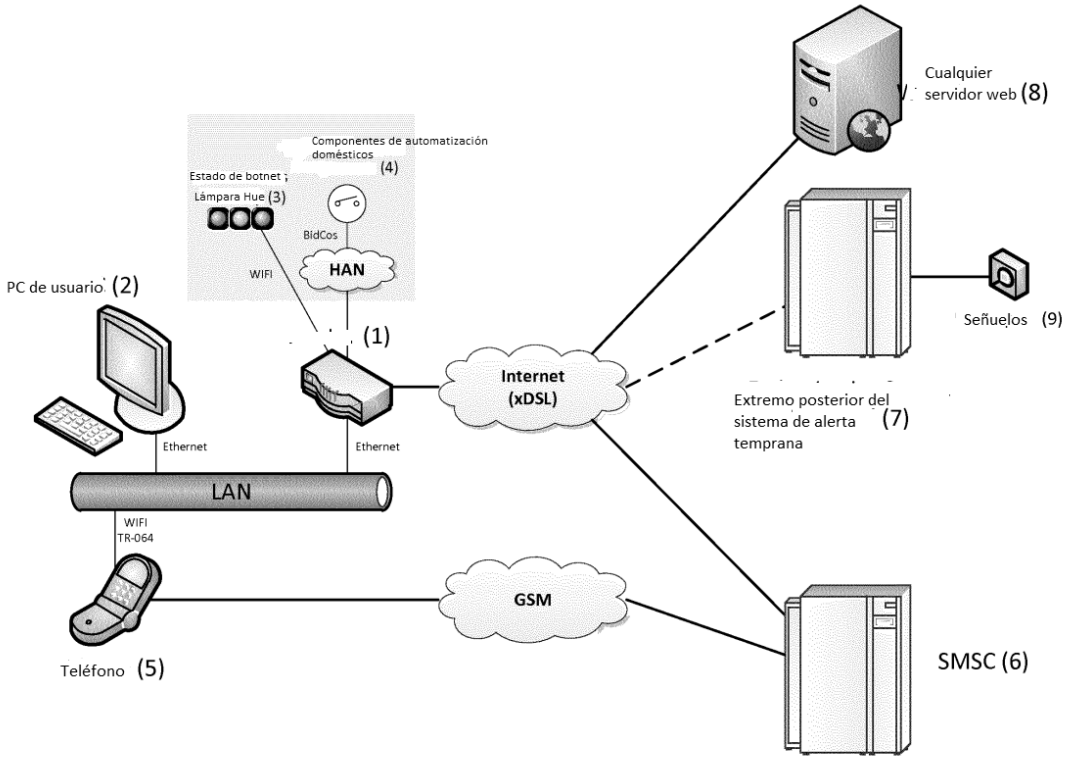
Componentes de automatización domésticos
(4)
Estado de botnet
Lámpara Hue (3)
BidCos
WIFI
HAN
PC de usuario (2)
(1)
Internet (xDSL)
Cualquier servidor web (8)
Señuelos (9)
Extremo posterior del sistema de alerta temprana (7)
Ethernet
Ethernet
LAN
WIFI TR-064
GSM
Teléfono (5)
SMSC (6)

Fig. 1

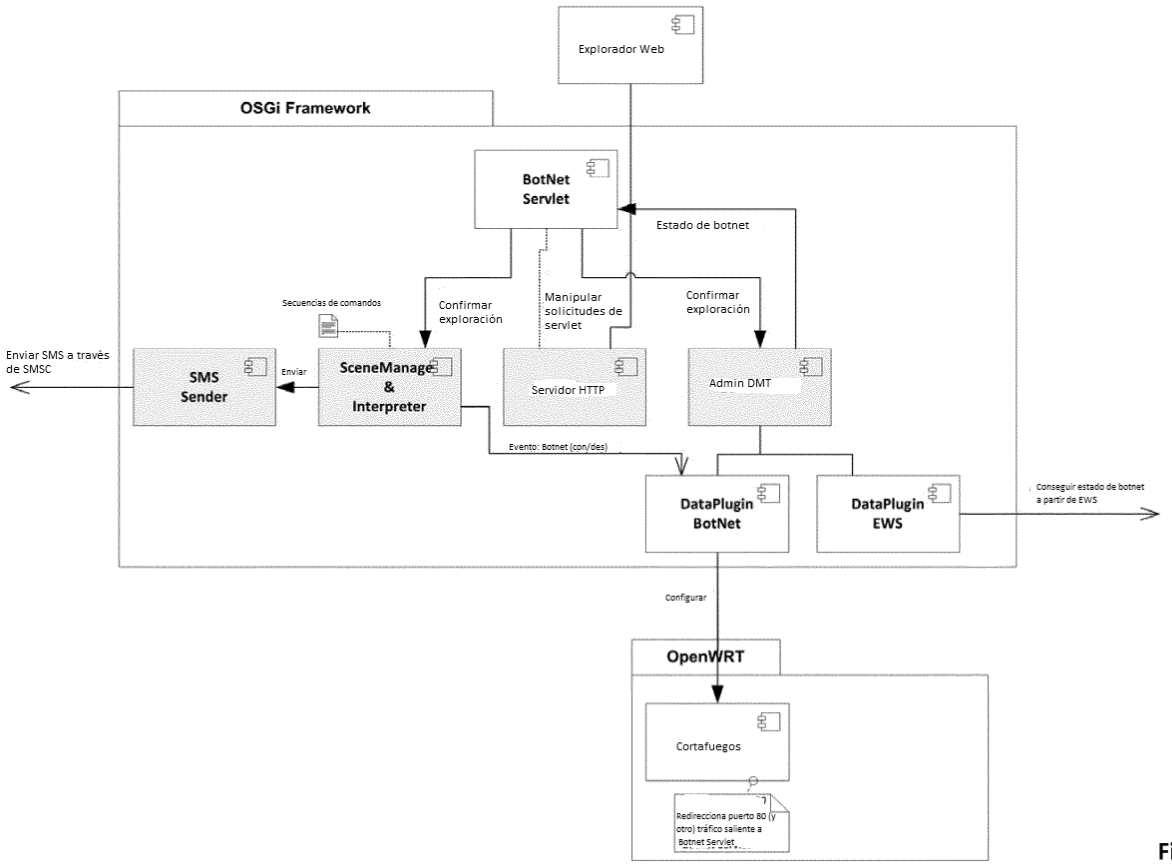
Explorador Web
OSGi Framework
BotNet Servlet
Estado de botnet
Secuencias de comandos
Confirmar exploración
Manipular solicitudes de servlet
Confirmar exploración
Enviar SMS a través de SMSC
SMS Sender
Enviar
SceneManager & Interpreter
Servidor HTTP
Admin DMT
Evento: Botnet (con/des)
DataPlugin BotNet
DataPlugin EWS
Conseguir estado de botnet a partir de EWS
Configurar
OpenWRT
Cortafuegos
Redirecciona puerto 80 (y otro) tráfico saliente a Botnet Servlet

Fig.2a

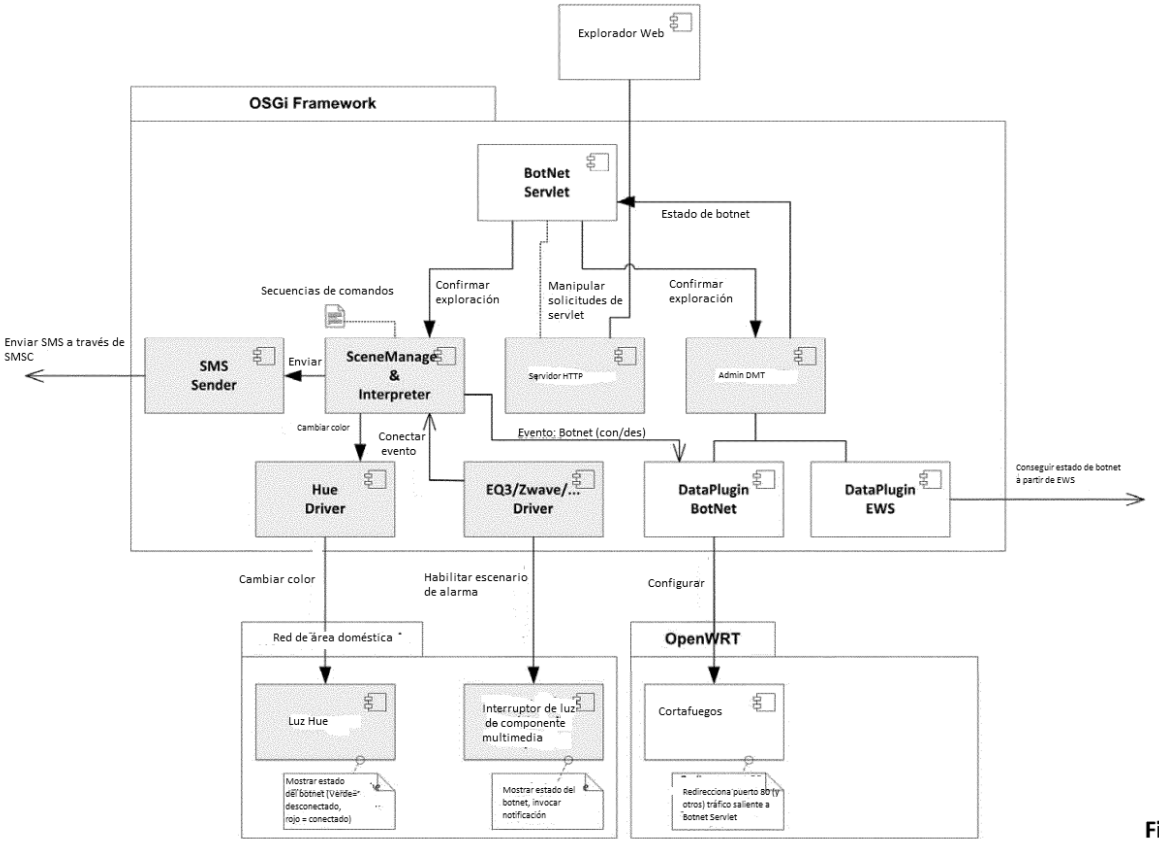
Explorador Web
OSGi Framework
BotNet Servlet
Estado de botnet
Secuencias de comandos
Confirmar exploración
Manipular solicitudes de servlet
Confirmar exploración
Enviar SMS a través de SMSC
SMS Sender
Enviar
SceneManager & Interpreter
Servidor HTTP
Admin DMT
Cambiar color
Conectar evento
Evento: Botnet (con/des)
Hue Driver
EQ3/Zwave/... Driver
DataPlugin BotNet
DataPlugin EWS
Conseguir estado de botnet a partir de EWS
Cambiar color
Habilitar escenario de alarma
Configurar
Red de área doméstica
OpenWRT
Luz Hue
Interruptor de luz de componente multimedia
Cortafuegos
Mostrar estado del botnet (Verde= desconectado, rojo = conectado)
Mostrar estado del botnet, invocar notificación
Redirecciona puerto 80 (y otros) tráfico saliente a Botnet Servlet

Fig. 2b

PÁGINA WEB
BOTNET

Fig.3