CONAN mobile

Servicio ANTIBOTNET

Manual de usuario

ANDROID

¿Es mi terminal seguro?

Aprenda a utilizar esta aplicación que analiza la configuración de seguridad de dispositivos móviles con sistema operativo Android

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

INDICE

1 INTRODUCCIÓN

CONAN mobile es una aplicación para dispositivos Android cuya misión es analizar la configuración de seguridad del dispositivo, la peligrosidad de las aplicaciones instaladas o las que sean instaladas posteriormente, analizar los permisos que usan las aplicaciones instaladas y mostrar eventos relevantes para la seguridad del dispositivo móvil (envío de SMS Premium, realización de llamadas a números de tarificación especial, conexión a redes wifi inseguras, conexión a direcciones IP potencialmente peligrosas, identificar si desde nuestra conexión a internet se ha detectado algún incidente de seguridad relacionado con botnets u otras amenazas). Además, el usuario podrá consultar las direcciones IP y servicios a los cuales se conectan las aplicaciones instaladas en el terminal y, en el caso de que alguna sea considerada como potencialmente maliciosa será notificada al usuario.

También el usuario podrá consultar los consejos de la Oficina de Seguridad del Internauta acerca de seguridad en dispositivos a través de la propia aplicación.

CONAN mobile se puede instalar en dispositivos con versión 4.3 de Android o superior, además, para poder usar todas las funcionalidades de la aplicación es necesario que el dispositivo tenga acceso a Internet.

Este manual tiene como objetivo explicar el funcionamiento de la aplicación CONAN mobile para dispositivos Android, describiendo tanto su instalación como las funcionalidades que pone a disposición de los usuarios para conseguir aumentar la seguridad de sus móviles y tabletas Android.

Para más información, puede escribir a conan-mobile@osi.es

2 INSTALACIÓN

La aplicación CONAN mobile se distribuye de forma gratuita a través de Google Play, por lo que el proceso de instalación es equivalente al de cualquier otra aplicación para Android:

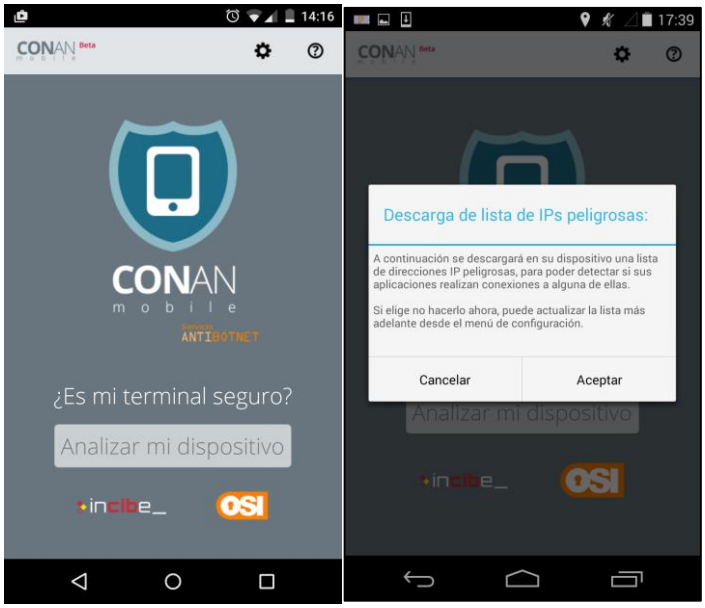
- Localizar la aplicación en Google Play.
- Seleccionar la opción “Instalar”.
- Aceptar los permisos solicitados para la instalación.
- Esperar a que la aplicación se descargue y se instale.

Una vez instalado CONAN mobile en el dispositivo, ejecute la aplicación pulsando en su correspondiente icono:

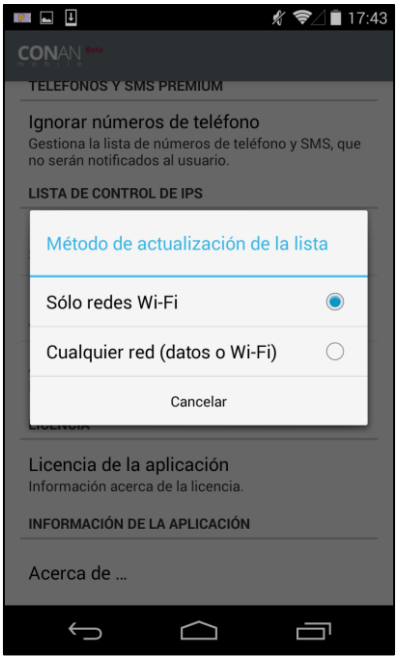
Al iniciar la aplicación cliente, se lanza una pantalla inicial en la que se muestra al usuario una presentación de la aplicación y el acuerdo de licencia de uso que el usuario deberá aceptar para comenzar a usarla.

3 LISTADO DE IPS PELIGROSAS

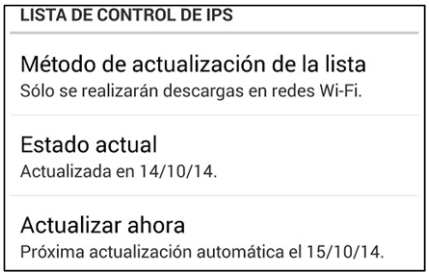
CONAN mobile solicitará al usuario la descarga del listado de direcciones IPs peligrosas al iniciar la aplicación, la cual será utilizada en la detección de conexiones potencialmente peligrosas realizadas por las aplicaciones del dispositivo. Por defecto, CONAN mobile está configurado para descargar este listado cuando el dispositivo se encuentre conectado a una red wifi, en cuyo caso la lista se descargará en segundo plano. Si el dispositivo no está conectado a una red wifi, solicitará la descarga por cualquier red disponible en el dispositivo.



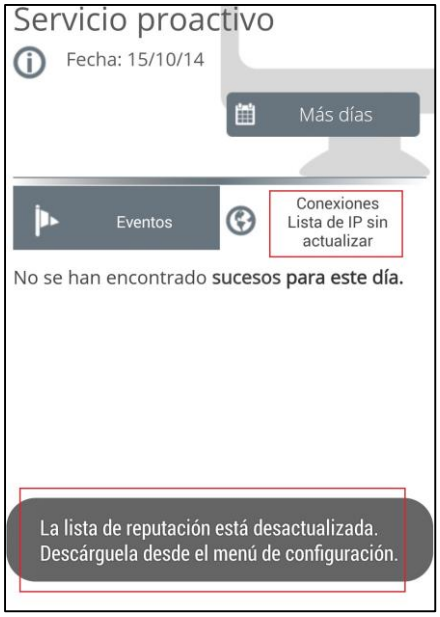
El usuario puede cambiar esta configuración desde el panel de configuración de CONAN mobile, determinando si la descarga se realizara solo desde conexión wifi o usando cualquier red de datos disponible (tanto wifi como otra red de datos). El listado se actualizará cada 24 horas.



Por otro lado, el usuario puede solicitar la descarga de la lista en cualquier momento bajo demanda, desde el panel de configuración en la sección “Lista de control de IPs” y pulsando en “Actualizar ahora”.



En el caso de que la lista no esté actualizada, CONAN mobile notificará al usuario de esta situación.



CONAN mobile no notificará al usuario de las conexiones potencialmente peligrosas si el listado no se encuentra actualizado. El tiempo de vida máximo de cada listado es de 48 horas. Esto es debido a que las listas de reputación son muy dinámicas y cambian continuamente y una lista desactualizada podría producir falsos positivos.

4 ANÁLISIS DE SEGURIDAD

Para determinar si un dispositivo es seguro, CONAN mobile debe realizar un análisis del mismo verificando los parámetros de configuración y las aplicaciones instaladas. Para ejecutar este análisis el usuario debe presionar el botón “Analizar mi dispositivo” que aparece en la pantalla inicial.

Durante el proceso de análisis, se mostrará una pantalla de progreso como se puede ver en la siguiente ilustración.

Durante este tiempo, CONAN mobile analiza la información del dispositivo para determinar su estado de seguridad. La duración del análisis puede variar en función del número de aplicaciones instaladas, del dispositivo y de la conexión a Internet disponible.

Para poder verificar las aplicaciones instaladas en el dispositivo, CONAN mobile necesita disponer de una conexión a Internet para realizar consultas a la base de conocimiento de INCIBE, por lo que es necesario que el dispositivo disponga de una conexión activa a Internet durante la realización del análisis.

Una vez finalizado el análisis, se muestra la información sobre el estado de seguridad del dispositivo. Esta información está dividida en varias pantallas a las que se puede acceder deslizándose lateralmente. Las diferentes pantallas se explican en las siguientes secciones.

Se recomienda realizar un análisis del dispositivo de manera periódica.

5 PANTALLA PRINCIPAL

Ofrece una visión general del estado de seguridad del dispositivo. En la misma se muestra el resultado del análisis del **Estado global de la seguridad**, enlaces directos a las diferentes pantallas de resultados de los análisis realizados y un botón que permite al usuario repetir el análisis.

El resultado global de configuración sirve para ofrecer al usuario un resumen del estado de la seguridad del dispositivo en función de los distintos análisis realizados, por lo que se calcula en base a los mismos, pudiendo tomar los siguientes valores:

- **EN RIESGO:** Se detecta algún problema de seguridad, ya sea en la configuración del dispositivo o en las aplicaciones instaladas en él. Visitando las diferentes secciones el usuario puede ver los problemas que han sido detectados.
- **PENDIENTE:** Se ha producido un error de conexión con el servidor de CONAN mobile y no se ha podido realizar un análisis de las aplicaciones.
- **CORRECTO:** El dispositivo es seguro, no se han detectado problemas de seguridad.

El resultado del análisis está dividido en cuatro secciones:

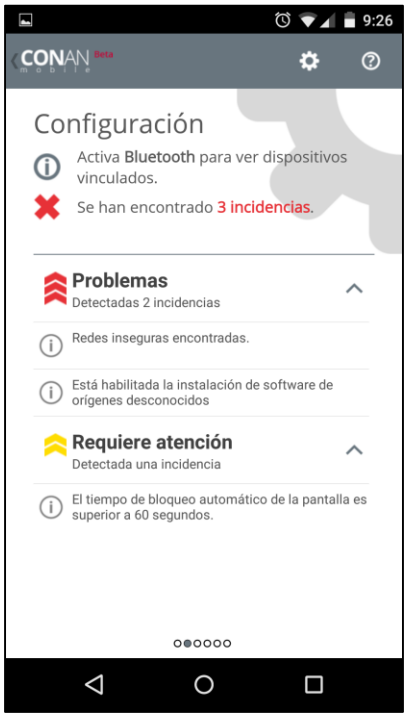
- **Configuración**, describe los problemas de configuración encontrados en el dispositivo.
- **Aplicaciones**, muestra incidencias detectadas en las aplicaciones instaladas.
- **Permisos**, acceso a los permisos declarados por las aplicaciones por orden de peligrosidad.

- **Servicio Proactivo**, eventos de seguridad detectados y eventos sobre las conexiones realizadas por las aplicaciones del dispositivo, así como información extendida de las mismas.
- **Consejos OSI,** recomendaciones de la Oficina de Seguridad del Internauta acerca de la seguridad en dispositivos móviles.

6 CONFIGURACIÓN

Presenta los resultados obtenidos en el análisis realizado sobre varios elementos de configuración que ofrece el sistema operativo Android y que, según como estén establecidos, pueden suponer un riesgo de seguridad.

En función de las incidencias detectadas, CONAN mobile establece un estado general de seguridad de la configuración del dispositivo, indicando si se han detectado problemas o si la configuración es segura.



Las comprobaciones realizadas por CONAN mobile se clasifican según el nivel de peligrosidad (Problemas y Requiere atención):

- **Dispositivo Rooteado**: en un dispositivo rooteado se tiene la capacidad de ejecutar procesos con los permisos del administrador del sistema (root), lo cual permitiría a aplicaciones maliciosas acceder a información sensible y/o realizar modificaciones que puedan afectar al dispositivo o a su contenido.
- **Modo debug ADB**: El dispositivo tiene habilitado el modo de depuración a través del interfaz ADB, lo que permitiría a un atacante obtener información del dispositivo conectándolo por USB a un ordenador.

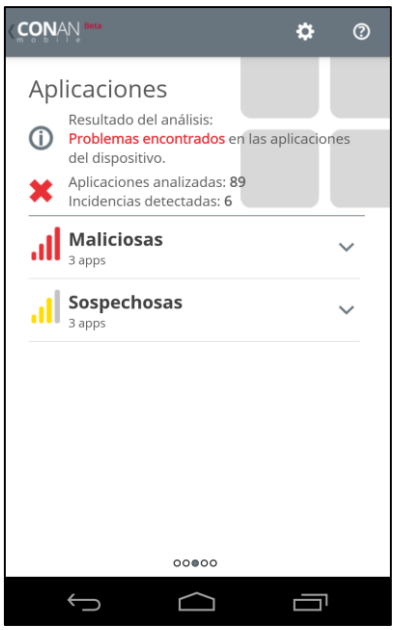
- **Orígenes desconocidos**: El dispositivo permite la instalación de aplicaciones desde otras fuentes diferentes a Google Play. Si bien esto no es un problema de seguridad por sí solo, permite instalar aplicaciones de orígenes dudosos.
- **Administrador de dispositivos:** En caso de extravío o robo del terminal, el administrador de dispositivos permite la geolocalización, el borrado de los datos y el bloqueo del terminal de manera remonta
- **Verificar aplicaciones:** Cuando se instala una nueva aplicación, esta puede ser verificada mediante los procedimientos de Google. Es recomendable que está opción este habilitada a fin de evitar la instalación de software malicioso.
- **Password en claro**: El dispositivo muestra las contraseñas al ser introducidas sin ninguna ocultación.
- **Bloqueo de pantalla**: El dispositivo no dispone de un mecanismo de seguridad de tipo bloqueo de la pantalla.
- **Bloquear automáticamente (deshabilitado o habilitado con un tiempo superior a 1 minuto):** Es recomendable que está opción este habilitada a fin de evitar un acceso no deseado al terminal.
- **Bloquear al encender:** Este bloqueo se produce en el dispositivo cuando se apaga de forma manual o automatizada, solicitando el método de acceso configurado en el terminal.
- **Configuración de GPS:** Permite que determinadas aplicaciones conozcan la ubicación del dispositivo.
- **Configuración de NFC:** Se recomienda deshabilitar el NFC cuando no se esté usando.
- **Configuración Zona wifi:** Detecta si tiene habilitada la conexión de datos para otros terminales mediante wifi.
- **Compartir por Bluetooth:** Detecta si tiene habilitada la conexión de datos para otros terminales mediante BlueTooth.
- **Configuración de Bluetooth**: En caso de que el bluetooth esté activado, se advertirá al usuario.
- **Redes Wi-Fi inseguras**: Muestra las redes wifi que el dispositivo tiene configuradas que son inseguras, bien porque no utilizan mecanismos de cifrado o bien porque el mecanismo utilizado es inseguro, como por ejemplo si se usa el protocolo de seguridad WEP. Además, se comunica al usuario de si su dispositivo tiene configuradas varias redes con el mismo SSID, dado que este hecho podría hacer que el usuario se conectara a un punto de acceso no legítimo con los riesgos de seguridad que esto supone. Las redes inseguras se muestran en formato de lista, indicando en cada una de ellas cuál es el problema y qué pasos pueden realizarse para corregirlo.
- **Dispositivos Bluetooth vinculados**: Se muestra al usuario los datos de emparejamiento con dispositivos por Bluetooth. A modo de información extendida, se informa al usuario de qué tipo de dispositivo se trata (según informe del sistema Android).

7 APLICACIONES

En esta pantalla se presentan los resultados obtenidos durante el análisis de la peligrosidad de las aplicaciones instaladas en el dispositivo. Para este análisis, CONAN mobile verifica las aplicaciones instaladas contra las fuentes de información de INCIBE para realizar una valoración de cada aplicación. Las aplicaciones que presentan algún tipo de incidencia o particularidad son agrupadas en función de este caso.

En caso de que no se pueda establecer la comunicación con el servidor, se advertirá al usuario y no se mostrará información sobre las aplicaciones.

Además, se nos presenta en pantalla el número de aplicaciones analizadas y el número de incidencias detectadas (la suma de aplicaciones maliciosas y sospechosas).

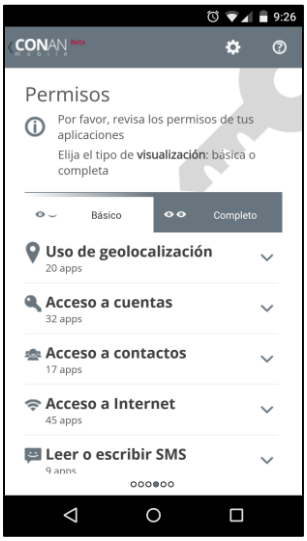


Las categorías posibles para las aplicaciones son:

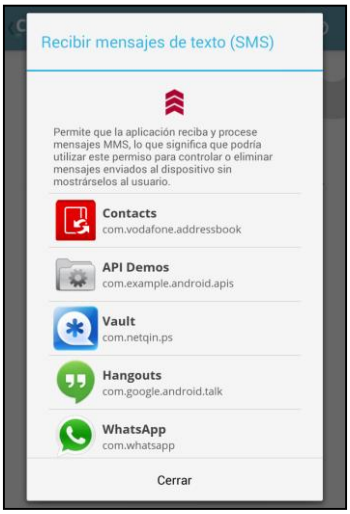
- **Maliciosas**: hay dos causas para considerar una aplicación peligrosa:
  - Se detectan cambios en el certificado de la aplicación instalada en el dispositivo con respecto a la disponible el Google Play. Además, en este caso se revisan los permisos declarados por la aplicación instalada y la disponible en Google Play, advirtiendo al usuario en caso de que haya diferencias.
  - Varios antivirus detectan la aplicación como maliciosa (dicho proceso se lleva a cabo haciendo uso del servicio VirusTotal).
- **Sospechosas**: son aplicaciones dudosas porque aunque algún antivirus la detecta como peligrosa, el número de antivirus no es lo suficientemente alto como para tener la certeza de que se trata de una aplicación maliciosa.

8 PERMISOS

Se presenta una clasificación de los permisos que declaran las aplicaciones en función de los permisos más relevantes (básico) y en función de la peligrosidad de los mismos desde el punto de vista del riesgo para la seguridad (completo). A pesar de que Google ya establece un nivel de peligrosidad asociado a cada permiso, el cliente utiliza una clasificación de los permisos establecida por INCIBE, agrupando los mismos en permisos de riesgo **Alto**, **Medio**, **Bajo** y **Otros**.



Al pulsar en la categoría de permisos, CONAN mobile despliega un listado con los permisos que los forman. Además al pulsar en cada uno de los permisos se mostrara una breve descripción de la misma junto con un listado de las aplicaciones instaladas en el dispositivo que lo poseen.

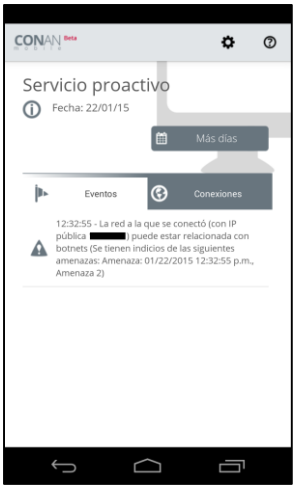


9 SERVICIO PROACTIVO

En esta pantalla se muestra al usuario la información recogida de forma autónoma por CONAN mobile, aun cuando no se está utilizando la aplicación. Esta información permite detectar comportamientos anómalos y potencialmente maliciosos, los cuales quedan registrados para su posterior consulta.

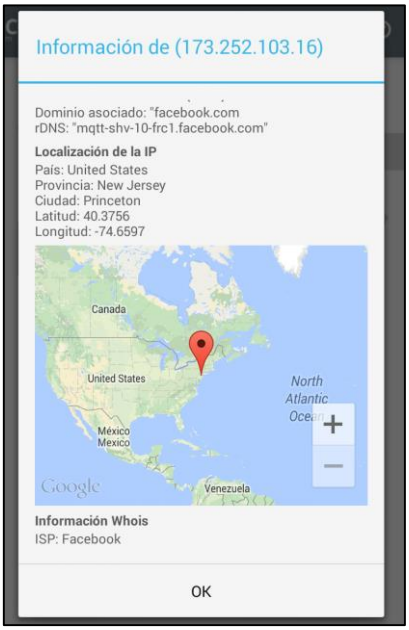
Esta pantalla cuenta con dos secciones, de acuerdo al tipo de registros:

- Pestaña de eventos: se registran diferentes eventos relacionados con la seguridad:
    - **Cambios en el fichero /etc/hosts:** Se registra cuando se modifica, elimina o crea el fichero /etc/hosts, que contiene información de las direcciones IP relacionadas con máquinas "conocidas" por el dispositivo. Modificaciones no autorizadas de este fichero pueden alterar la navegación desde el dispositivo y facilitar la suplantación por parte de un atacante.
    - **Cambios en la conectividad:** Se registra cuando el usuario se conecta a una red wifi insegura.
    - **Detección de conexiones potencialmente maliciosas**: Se registra cuando una aplicación instalada en el dispositivo realiza una conexión potencialmente maliciosa en base a la lista de reputación descargada en el dispositivo.
    - **Llamadas y envío de mensajes a números de tarificación especial**: Se registra cuando se realiza una llamada o se envía un mensaje a un número *premium* .
    - **Cambios en aplicaciones:** Se registra cuando se instala una aplicación maliciosa o sospechosa en el dispositivo (es necesario disponer del servicio de comprobación en tiempo real de las aplicaciones instaladas).
    - **Servicio AntiBotnet**: Identifica si desde la conexión a internet (solo disponible para España) se ha detectado algún incidente de seguridad relacionado con botnets u otras amenazas.

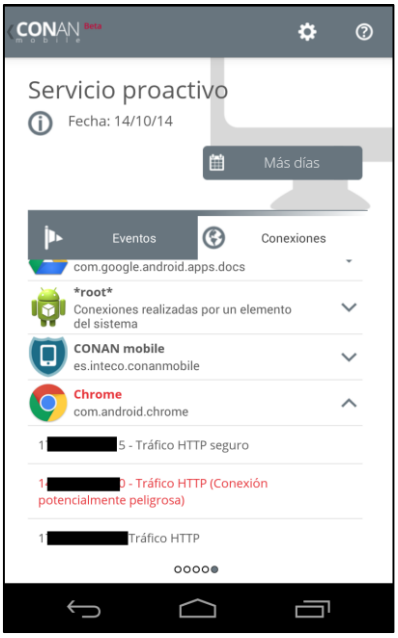


- Pestaña de conexiones: Para cada aplicación instalada se muestran las conexiones de red que realiza. De esta forma, el usuario podrá comprobar la IP y servicio al que cada aplicación establece una conexión o varias. Además, el usuario podrá acceder a información extendida de cada conexión:

    - Geolocalización.
    - Propietario de la IP.
    - ISP.
    - Nombre de dominio asociado.



Cada una de las conexiones establecidas será chequeada con la lista de reputación de IPs suministrada por INCIBE, a fin de determinar si alguna aplicación realiza conexiones a direcciones IP catalogadas como potencialmente maliciosas. En este caso, se notificará al usuario tanto en la pestaña de eventos como en forma de notificación, indicando qué aplicación realizó la conexión. En la pestaña de conexiones, la aplicación también aparecerá marcada en rojo, así como la conexión concreta que es considerada como potencialmente maliciosa.



Además de mostrar eventos y conexiones del día actual, ofrece un calendario para poder mostrar información de las detecciones registradas en días pasados.

Por defecto, el servicio proactivo en el que se basa esta pantalla para el registro de eventos y conexiones está habilitado por defecto, aunque puede deshabilitarse a través del menú de configuración.

10 SERVICIO DE MENSAJERÍA

CONAN mobile dispone de un servicio de mensajería que permite a INCIBE el envío de notificaciones o alertas de interés para los usuarios. Este servicio se encuentra activado por defecto, aunque el usuario puede desactivarlo en cualquier momento desmarcando la opción para recibir mensajes de este tipo desde la pestaña de configuración.

Los mensajes son considerados urgentes o de alta relevancia para el usuario, por lo que se mostrarán como una notificación. Al acceder a la notificación se abrirá una ventana de CONAN mobile donde se mostrará el contenido completo del mensaje enviado.

11 NOTIFICACIONES AL USUARIO

CONAN mobile envía notificaciones al usuario cuando se producen eventos de seguridad que requieran de su atención. Estas alertas son mostradas en el área de notificación del dispositivo. Estas son las notificaciones generadas:

- **Mensajes enviados por INCIBE**: Mensajes enviados por INCIBE haciendo uso del sistema de mensajería GSM.
- **Eventos de seguridad**: cuando se registra un evento de seguridad en la pantalla del servicio proactivo, se envía una notificación al usuario:

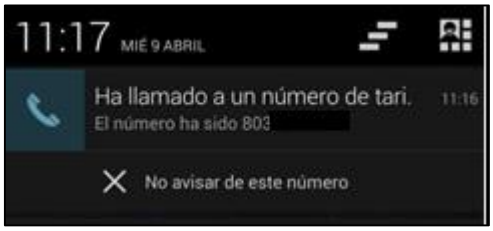
    - **Modificación en fichero host**: Se notifica al usuario en el caso de que este fichero sufra algún tipo de modificación

    - **Conexión potencialmente peligrosa**: Se notifica al usuario de que una aplicación instalada en el dispositivo ha realizado una conexión potencialmente peligrosa a una de las direcciones contenidas dentro de la lista de reputación de IPs.

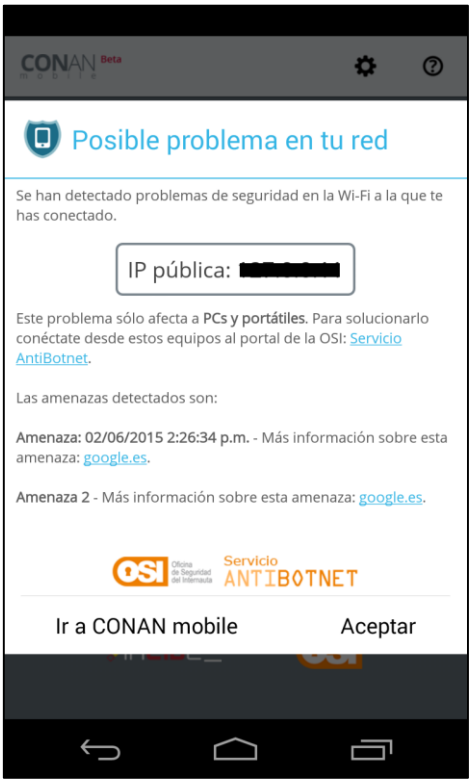
    - **Instalación de aplicación maliciosa o sospechosa**: en caso de que CONAN mobile esté configurado para hacer análisis al vuelo de aplicaciones instaladas y que una de estas aplicaciones se detecte como maliciosa o sospechosa, se genera una notificación para advertir al usuario.

    - **Conexión a red inalámbrica insegura**: Se notifica al usuario en caso de que el dispositivo se conecte a una red wifi con seguridad WEP o abierta.

    - **Evento de tarificación especial**: cuando se detecta una llamada o sms a un número de tarificación especial se envía una notificación al usuario.



- **Servicio Antibotnet**: Identifica si desde la actual conexión a Internet se han detectado amenazas de seguridad relacionadas con redes de ordenadores comprometidos o botnets, u otras amenazas.



12 CONSEJOS OSI

CONAN mobile permite acceder a artículos publicados en la Oficina de Seguridad del Internauta que hacen referencia a consejos de seguridad en dispositivos móviles. Se puede acceder a un artículo simplemente pulsando en él y accediendo mediante el navegador predeterminado.

13 SERVICIO ANTIBOTNET

El Servicio AntiBotnet (solo disponible para España) es un servicio gratuito que nos da la posibilidad de conocer si desde su actual conexión wifi (WEP o WPA) a Internet se han identificado amenazas de seguridad relacionadas con redes de ordenadores comprometidos o botnets, u otras amenazas. Para ello se utiliza la dirección IP pública que está utilizando para navegar por Internet (IP pública del router) y se comprueba en la base de datos del servicio AntiBotnet.

El Servicio no identifica dispositivos de usuario infectados de la red a la que se está conectado, sólo contrasta la dirección IP pública en la base de datos, siempre en el marco de la legalidad vigente.

En caso de que el Servicio arroje un resultado positivo, se ofrece información relacionada con la amenaza que puede estar afectando a alguno de los dispositivos (PC´s o portátiles de su red), para ayudar a identificarlo (como puede ser el sistema operativo al que afecta); y enlaces a herramientas de limpieza, para ayudar en la desinfección.

Este servicio es un mecanismo de detección puntual y no sustituye en ningún caso a los sistemas antivirus o anti-malware.

INCIBE utiliza tu dirección IP pública, siempre con tu consentimiento explícito al aceptar las condiciones de uso y privacidad del servicio, para contrastarla contra nuestra base de datos en tiempo real y poder ofrecerte el resultado del servicio. La dirección IP se guarda solamente con fines estadísticos y nunca asociada a un usuario en concreto.

El Servicio Antibotnet en CONAN mobile se activará cuando se conecta a una red wifi (WEP, WPA o WPA2), no pudiéndose hacer uso del mismo en conexiones 3G o 4G.

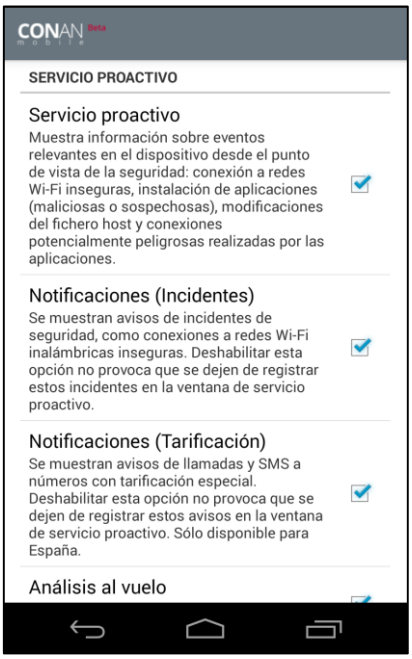
Dispones de toda la información acerca de este servicio en https://www.osi.es/servicio-antibotnet/informacion

14 CONFIGURACIÓN

Desde todas las pantallas de CONAN mobile se puede acceder a una ventana de configuración de la aplicación, desde el siguiente icono:

Se muestran las siguientes opciones:

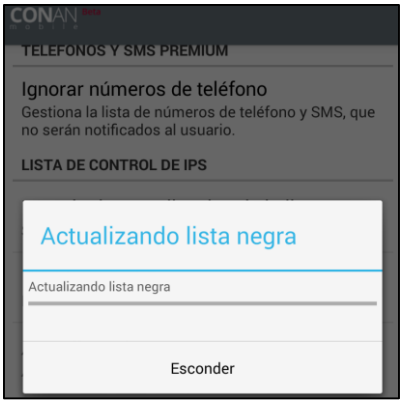
- **Servicio proactivo**: se corresponde con el servicio utilizado para recopilar la información presentada en la pantalla con el mismo nombre. En caso de encontrase desactivado, CONAN mobile no recopilará, guardara o advertirá al usuario en caso de que se produzcan conexiones o eventos potencialmente maliciosos.
    - **Notificaciones (Incidentes):** permite activar o desactivar la generación de notificaciones para los eventos de seguridad detectados por el servicio proactivo.
    - **Notificaciones (Tarificación):** permite activar o desactivar la generación de notificaciones para los eventos relacionados con las llamadas y SMS a servicios de tarificación especial.
    - **Análisis al vuelo:** permite a CONAN mobile realizar una análisis en tiempo real cada vez que se instale una aplicación con el fin de determinar si esta es o no maliciosa o sospechosa.



- **Google Cloud Messaging:**
  - **Notificaciones (INCIBE):** permite activar o desactivar la recepción de mensajes o alertas generados por INCIBE.
- **Teléfonos y SMS premium:**
  - **Ignorar número de teléfono**: permite la gestión de una lista de números de teléfono con aquellos números que el usuario desea que no sean tenidos en cuenta en el análisis y notificación de llamadas y SMS a números de tarificación especial. Funcionalidad sólo disponible para España.

- **Lista de control de Ips:**
  - **Método de actualización de la lista:** Determina si la lista se actualizará solo mediante wifi o usando cualquier conexión de red disponible (wifi o 3G/4G). Esta última opción implicaría consumo de datos al hacer uso de la conexión 3G o 4G del cliente.

  - **Estado Actual:** Indica si la lista está actualizada y la fecha de la última actualización.
  - **Actualizar Ahora:** Permite actualizar la lista, a solicitud del usuario. Además, muestra la fecha de la siguiente actualización.



- **Servicio AntiBotnet**: Comprueba la dirección IP pública contra el Servicio AntiBotnet cada vez que el dispositivo se conecte a una red inalámbrica segura, con el fin de identificar si la conexión a Internet está relacionada con algún incidente de seguridad relacionado con botnets u otras amenazas. Se podrá habilitar o deshabilitar el servicio.
- **Licencia:** Muestra la licencia de la aplicación.
- **Información de la aplicación:** Muestra información relativa a la aplicación.