GUÍA DE USUARIO

Bitdefender CONSUMER SOLUTIONS

Mobile Security for iOS

Bitdefender Mobile Security for iOS

Guía de usuario

Fecha de publicación 02/10/2023

Aviso Legal

Bitdefender

Tabla de contenidos

ACERCA DE ESTA GUÍA

Propósito y público al que se dirige

Esta guía va dirigida a todos los usuarios de Android que hayan elegido Bitdefender Mobile Security for iOS como solución de seguridad para sus dispositivos móviles. La información presentada en esta guía está indicada no sólo para quienes posean conocimientos técnicos, sino para todos aquellos que puedan trabajar con dispositivos móviles Apple.

Averiguará cómo configurar y usar Bitdefender Mobile Security for iOS para protegerse contra amenazas y otras aplicaciones maliciosas. Aprenderá a sacarle el máximo partido a Bitdefender.

Le deseamos una lectura útil y agradable.

Cómo usar esta guía

Esta guía está organizada en diversos temas principales:

Iniciando (página 5)

Comience con Bitdefender Mobile Security for iOS y su interfaz de usuario.

Características y funcionalidades (página 9)

Aprenda a utilizar Bitdefender Mobile Security for iOS para protegerse contra amenazas y aplicaciones maliciosas conociendo sus características y funcionalidades.

Obteniendo ayuda (página 29)

Dónde buscar y dónde solicitar ayuda si surge algo inesperado.

Convenciones utilizadas en esta guía

Convenciones tipográficas

En esta guía se utilizan distintos estilos de texto con el fin de mejorar su lectura. En la siguiente tabla se indican su aspecto y significado.

Apariencia	Descripción
sample syntax	Las muestras de sintaxis se imprimen con monospaced caracteres.
https://www.bitdefender.com	La URL del enlace señala a alguna ubicación externa, en servidores http o ftp.
documentation@bitdefender.com	Las direcciones de email se incluyen en el texto como información de contacto.
Acerca de esta guía (página 1)	Este es un enlace interno, hacia algún punto dentro del documento.
filename	Los archivos y directorios se imprimen usando monospaced fuente.
opción	Todas las opciones de productos se imprimen usando **atrevido** caracteres.
palabra clave	Las palabras clave o frases importantes se resaltan usando **atrevido** caracteres.

Advertencias

Las advertencias son notas en el texto, marcadas gráficamente, que brindan información adicional respecto al párrafo actual.

Nota

La nota es una pequeña observación. Aunque puede omitirla, las notas pueden proporcionar información valiosa, como características específicas o enlaces hacia temas relacionados.

Importante

Este tipo de advertencia requiere su atención y no es recomendable omitirla. Normalmente proporciona información importante, aunque no extremadamente crítica.

Advertencia

Se trata de información crítica que debería tratar con extrema cautela. No ocurrirá nada malo si sigue las indicaciones. Debería leer y entender estas notas, porque describen algo extremadamente arriesgado.

Solicitud de comentarios

Le invitamos a ayudarnos a mejorar el manual. Hemos comprobado y verificado toda la información como mejor hemos sabido. Por favor, escríbanos para explicarnos cualquier tipo de defecto que encuentre en este manual o cómo podría mejorarse, y así ayudarnos a ofrecerle la mejor documentación posible.

Háganos saber enviando un correo electrónico a documentation@bitdefender.com. Escriba todos sus correos electrónicos

relacionados con la documentación en inglés para que podamos procesarlos de manera eficiente.

1. QUÉ ES BITDEFENDER MOBILE SECURITY FOR IOS

Las actividades online, como por ejemplo pagar facturas, hacer reservas hoteleras o adquirir bienes y servicios son cómodas y sencillas. No obstante, como muchas otras actividades que han evolucionado en Internet, conllevan altos riesgos y, si no se actúa de forma segura, los datos personales pueden ser verse comprometidos. ¿Y qué hay más importante que proteger los datos almacenados en sus cuentas online y en su smartphone?

Bitdefender Mobile Security for iOS le permite lo siguiente:

- Ofrece la protección más potente contra amenazas con el menor impacto en la batería
- Proteja sus datos personales: contraseñas, dirección, información financiera y social
- Compruebe fácilmente la seguridad de su teléfono para detectar y corregir las configuraciones erróneas que pueden dejarlo expuesto
- Evite la exposición accidental de sus datos y el uso indebido de todas las apps que tiene instaladas
- Analice su dispositivo para lograr unos ajustes de seguridad y privacidad óptimos
- Obtenga información de uso sobre sus actividades online y el historial de incidentes prevenidos
- Compruebe si sus cuentas online han sido víctimas de vulneraciones o filtraciones de datos
- Cifre el tráfico de Internet con la VPN incluida

Bitdefender Mobile Security for iOS se proporciona de forma gratuita y requiere activarlo con una cuenta de Bitdefender. No obstante, algunas características importantes de Bitdefender, como nuestro módulo 'Protección web', requieren el pago de una suscripción para que nuestros usuarios puedan utilizarlas.

2. INICIANDO

2.1. Requisitos del Dispositivo

Bitdefender Mobile Security for iOS funciona en cualquier dispositivo con iOS 12 o versión superior del sistema operativo y necesita disponer de conexión a Internet para activarse y detectar si se ha producido alguna filtración de datos en sus cuentas online.

2.2. Instalación de Bitdefender Mobile Security for iOS

- **Desde Bitdefender Central**
  - Para iOS
    1. Acceda a **Bitdefender Central**.
    2. Seleccione el panel **Mis dispositivos**.
    3. Toque **INSTALAR PROTECCIÓN** y, a continuación, toque **Proteger este dispositivo**.
    4. Seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, toque el botón correspondiente.
    5. Se le redirigirá a la aplicación de **App Store**. En la pantalla de la App Store, toque la opción de instalación.
  - Para Windows, macOS y Android
    1. Acceso Centro de Bitdefender.
    2. Selecciona el **Mis dispositivos** panel.
    3. Pulse **INSTALAR PROTECCIÓN** y, a continuación, pulse **Proteger otros dispositivos**.
    4. Seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, pulse el botón correspondiente.
    5. Pulse **ENVIAR ENLACE DE DESCARGA**.
    6. Introduzca una dirección de correo electrónico en el campo correspondiente y pulse **ENVIAR CORREO ELECTRÓNICO**. Tenga en cuenta que el enlace de descarga generado solo es

válido durante las próximas 24 horas. Si caducase, debería generar uno nuevo siguiendo los mismos pasos.

7. En el dispositivo en que desee instalar Bitdefender, compruebe la cuenta de correo electrónico que introdujo y luego pulse el botón de descarga correspondiente.

- **En la App Store**
  Busque Bitdefender Mobile Security for iOS para encontrar e instalar la app.

La primera vez que abra la aplicación, aparecerá una ventana de introducción que le informará sobre las características del producto. Toque Empezar para pasar a la siguiente ventana.

Antes de llevar a cabo los pasos para la validación, debe aceptar el Acuerdo de suscripción. Por favor, dedique un momento a leer el Acuerdo de suscripción, dado que contiene los términos y condiciones bajo los cuales puede usar Bitdefender Mobile Security for iOS.

Toque **Continuar** para pasar a la siguiente ventana.

2.3. Iniciar sesión en su cuenta de Bitdefender

Para usar Bitdefender Mobile Security for iOS debe vincular su dispositivo a una cuenta de Bitdefender, Facebook, Google, Apple o Microsoft iniciando sesión en la cuenta desde la app. La primera vez que abra la app se le pedirá que registre una cuenta.

Para vincular su dispositivo a una cuenta de Bitdefender:

1. Introduzca la dirección de correo electrónico de su cuenta de Bitdefender en el campo correspondiente y, a continuación, toque **SIGUIENTE**. Si no tiene una cuenta de Bitdefender y desea crear una, seleccione el enlace correspondiente y luego siga las instrucciones que aparecen en la pantalla hasta activar la cuenta.
   Para iniciar sesión con una cuenta de Facebook, Google, Apple o Microsoft, toque el servicio que desee usar en el área de **O iniciar sesión con**. Se le redirige a la página de inicio de sesión del servicio seleccionado. Siga las instrucciones para vincular su cuenta a Bitdefender Mobile Security for iOS.

> **Nota**
> Bitdefender no tiene acceso a información confidencial, como la contraseña de la cuenta que utiliza para conectarse, o la información personal de sus amigos y contactos.

2. Escriba su contraseña y, a continuación, toque **INICIAR SESIÓN**.

Desde aquí también puede acceder a la Política de privacidad de Bitdefender.

2.4. Panel de Control

Toque el icono Bitdefender Mobile Security for iOS en la carpeta de aplicaciones del dispositivo para abrir la interfaz de la aplicación.

La primera vez que accede a la app, se le pide permiso para que Bitdefender le envíe notificaciones. Toque **Permitir<** para estar informado cada vez que Bitdefender tenga que comunicarle algo relevante relacionado con su app. Para administrar las notificaciones de Bitdefender, acceda a Ajustes > Notificaciones > Seguridad móvil.

Para acceder a la sección que necesita, toque el icono correspondiente en la parte inferior de la pantalla.

Protección web

Permanezca a salvo mientras navega por la web y siempre que las aplicaciones menos seguras intenten acceder a dominios que no son de confianza. Para obtener más información, consulte Protección Web (página 11).

VPN

Conserve su privacidad sin importar a qué red se conecte cifrando sus comunicaciones por Internet. Para obtener más información, consulte VPN (página 13).

Privacidad de cuentas

Averigüe si se ha filtrado o no la información de sus cuentas de correo electrónico. Para más información, diríjase a Privacidad de la cuenta (página 16).

Para ver opciones adicionales, toque el icono ••• en su dispositivo mientras esté en la pantalla principal de la aplicación. Aparecerán las siguientes opciones:

- **Restaurar compras**: Desde aquí puede restaurar las suscripciones anteriores que haya adquirido a través de su cuenta de iTunes.
- **Ajustes**: Desde aquí tiene acceso a lo siguiente:
  - **Ajustes de VPN**
    - **Acuerdo**: Puede leer los términos bajo los cuales utiliza el servicio Bitdefender VPN. Si toca **Ya no estoy de acuerdo**, no podrá usar Bitdefender VPN hasta que toque **Estoy de acuerdo**.
    - **Advertencia de red Wi-Fi abierta**: Puede habilitar o no la notificación del producto que aparece cada vez que se conecta a una red Wi-Fi insegura.
      El propósito de esta notificación es ayudarle a mantener la privacidad y seguridad de sus datos mediante el uso de Bitdefender VPN.
  - **Ajustes de Protección web**
    - **Acuerdo**: Puede leer los términos bajo los cuales utiliza el servicio Protección web de Bitdefender. Si toca **Ya no estoy de acuerdo**, no podrá usar Bitdefender VPN hasta que toque **Estoy de acuerdo**.
    - **Notificación de habilitación de la Protección web**: Le notifica que la Protección web se puede habilitar tras finalizar una sesión de VPN.
  - **Informes del producto**.
- **Comentarios**: Desde aquí puede ejecutar el cliente de correo electrónico por defecto para enviarnos sus comentarios acerca de la app.
- **Información de la app**: Desde aquí tiene acceso a la información sobre la versión instalada y el Acuerdo de suscripción, la Política de privacidad y el cumplimiento de las licencias de código abierto.

3. CARACTERÍSTICAS Y FUNCIONALIDADES

3.1. Analizar

Bitdefender Mobile Security for iOS le permite analizar su dispositivo en busca de vulnerabilidades de seguridad y amenazas potenciales. Al ejecutar el análisis se comprobará lo siguiente:

- **Versión del sistema operativo:** Comprobación de la versión de iOS para obtener las últimas actualizaciones.
- **Código de acceso/Biometría:** Comprobación del nivel de seguridad de acceso a su dispositivo.
- **Protección web:** Comprobación del estado del módulo de Protección web.
- **Privacidad de cuentas:** Comprobación de la presencia de cuentas monitorizadas incluidas en el módulo de Privacidad de cuentas.
- **Análisis de Wi-Fi:** Comprobación del estado de seguridad de la red a la que se conecta actualmente.

El estado de protección se determina tras ejecutar un análisis manual.

Después de ejecutar el primer análisis, accederá a las recomendaciones de Autopilot de Bitdefender. Se trata de su asesor de seguridad personal, que le proporciona recomendaciones contextuales basadas en el uso y las necesidades de su dispositivo. De esta manera, aprovechará todas las ventajas que su app le ofrece.

> **Nota**
> Cuando acceda a la app por primera vez, se le pedirá que ejecute un análisis.

3.2. Alerta de estafas

La función Alerta de estafa disponible en Bitdefender Mobile Security para iOS protege proactivamente a los usuarios de Apple contra estafas de phishing. Scam Alert para iOS incluye dos capas de protección que monitorean las estafas enviadas a través de mensajes SMS/MMS e invitaciones de calendario:

- **Filtro de mensajes de texto (SMS, MMS)**
  Esta función identifica y filtra mensajes SMS y MMS no deseados.
  Un SMS/MMS (servicio de mensajes cortos/servicio de mensajería multimedia) malicioso se refiere a un tipo de mensaje enviado a dispositivos móviles con intenciones dañinas. Estos mensajes están diseñados para explotar vulnerabilidades, engañar a los destinatarios o causar daños al dispositivo, la información personal o la seguridad del objetivo.
- **Escáner de enlaces de invitación de calendario**
  Esta función detecta calendarios y eventos de spam que contienen enlaces peligrosos. El virus del calendario es un tipo de spam que afecta a la aplicación Calendario de tu iPhone, lo que puede resultar molesto y potencialmente peligroso:
  - Recibe invitaciones de calendario o notificaciones de eventos no deseadas cuando acepta accidentalmente una invitación de calendario falsa enviada a su dirección de correo electrónico por piratas informáticos o spammers.
  - Cuando haces clic en el enlace de la invitación, sin saberlo, te suscribes al calendario del remitente, lo que le permite enviarte más eventos de spam.
  - Los eventos de spam pueden contener enlaces o archivos adjuntos que podrían conducirle a páginas de phishing u otras amenazas cibernéticas si las abre.

3.2.1. Cómo configurar una alerta de estafa

Para habilitar la Alerta de estafa, debe otorgar acceso a la aplicación Bitdefender Mobile Security a las notificaciones del calendario y a los mensajes SMS:

Cómo habilitar el filtrado de SMS:

Para que Bitdefender comience a filtrar mensajes, debe activar manualmente la opción Filtrar remitentes desconocidos en la configuración de la aplicación Mensajes:

1. Abre el **Ajustes** aplicación en tu iPhone o iPad.
2. Desplácese hacia abajo y seleccione **Mensajes** en la lista.
3. Toque en el **Desconocido y spam** sección.

4. Palanca **Filtrar remitentes desconocidos** a la posición de encendido.
5. Seleccionar **Seguridad móvil** en la sección Filtrado de SMS y luego elija **Permitir**.

Bitdefender ahora podrá filtrar mensajes basura en su iPhone/iPad.

> **Nota**
> Debido a las restricciones de iOS, el filtrado de SMS de Bitdefender sólo se puede utilizar para mensajes SMS y MMS que provienen de personas que no tiene guardadas en sus contactos. Esto significa que no filtrará mensajes de personas que ya están en su lista de contactos ni mensajes de iMessage de nadie.

Cómo habilitar el escaneo de calendario:

1. Abre el **Seguridad móvil de Bitdefender** aplicación instalada en su iPhone o iPad.
2. Ve a la **Alerta de estafas** opción en la barra de navegación inferior y presione **Configurar ahora**.
3. Grifo **Continuar** y luego toque **Permitir**.
4. Elegir **DE ACUERDO** para conceder a Bitdefender acceso a su calendario. Se iniciará un análisis del calendario inmediatamente.

3.3. Protección Web

Protección web de Bitdefender le garantiza una navegación segura al alertarle sobre posibles páginas web maliciosas y siempre que las aplicaciones instaladas menos seguras intenten acceder a dominios que no son de confianza.

Cuando una URL apunta a un sitio web conocido de phishing o fraudulento o a contenidos maliciosos como spyware o virus, se bloquea la página web y se muestra una alerta. Lo mismo sucede cuando las aplicaciones instaladas intentan acceder a dominios maliciosos.

> **Importante**
> Si se halla en una región donde la ley restrinja el uso de servicios VPN, la funcionalidad de Protección web no estará disponible.

Para activar la Protección web:

1. Toque el icono en la parte inferior de la pantalla.

2. Toque en **Estoy de acuerdo**.
3. Habilite el conmutador de Protección web.

> **Nota**
> Cuando active la Protección web por primera vez, puede que se le pida que permita que Bitdefender establezca configuraciones VPN que monitoricen el tráfico de red. Toque **Permitir** para continuar. Si se ha configurado un método de autenticación (huella dactilar o código PIN) para proteger su smartphone, debe usarlo. Para poder detectar el acceso a dominios que no son de confianza, Protección web trabaja conjuntamente con los servicios de VPN.

> **Importante**
> Las características de Protección web y VPN no pueden funcionar simultáneamente. Siempre que una de ellas esté habilitada, la otra (si estuviera activa en ese momento) se inhabilitará.

3.3.1. Alertas de Bitdefender

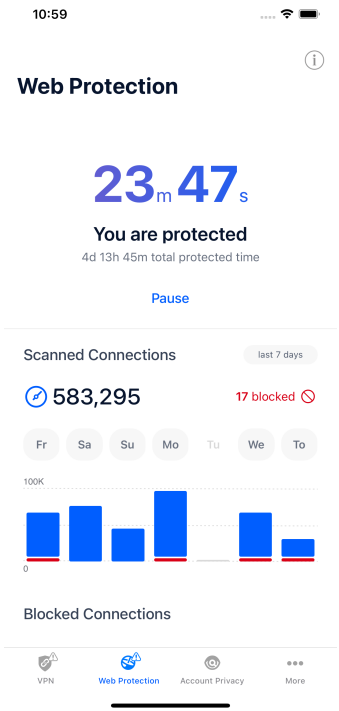
Cada vez que intenta visitar un sitio web clasificado como peligroso, este queda bloqueado. Para informarle de esa circunstancia, Bitdefender utiliza el Centro de notificaciones y su navegador. La página de advertencia contiene información como la URL del sitio web y la amenaza detectada. Tiene que decidir qué hacer a continuación.

Además, en el Centro de notificaciones se le informa siempre que una aplicación menos segura intenta acceder a dominios que no son de confianza. Toque la notificación que se muestra para pasar a la ventana donde puede decidir qué hacer a continuación.

Para ambos casos dispone de las opciones siguientes:

- Abandonar el sitio web tocando **LLÉVAME A UN SITIO SEGURO**.
- Acceder al sitio web, a pesar de la advertencia, tocando la notificación que se muestra y, luego, **Quiero acceder a la página**.

Confirme su elección.



3.4. VPN

Con Bitdefender VPN puede mantener la privacidad de sus datos personales cada vez que se conecta a redes inalámbricas inseguras de aeropuertos, centros comerciales, cafeterías u hoteles. De esta forma, se pueden evitar situaciones desafortunadas como el robo de datos personales o que piratas informáticos intenten acceder a la dirección IP de su dispositivo.

La VPN actúa como túnel entre su dispositivo y la red a la que se conecta para proteger su conexión, cifrar los datos mediante algoritmos de nivel militar y ocultar su dirección IP dondequiera que esté. Su tráfico se redirige a través de un servidor independiente, lo que hace que su dispositivo sea imposible de identificar por su proveedor de Internet entre la infinidad de dispositivos que utilizan nuestros servicios. Además, mientras está conectado a Internet a través de Bitdefender Mobile

Security for iOS, puede acceder a contenidos que normalmente están restringidos en determinadas zonas.

> **Nota**
> Algunos países practican la censura de Internet y, por lo tanto, el uso de las VPN en su territorio está prohibido por la ley. Para evitar responsabilidades legales, puede que aparezca un mensaje de advertencia cuando trate de utilizar la app Bitdefender VPN por primera vez. Al seguir haciendo uso de esa app, confirma que es consciente de las regulaciones nacionales aplicables y de los riesgos a los que podría exponerse.

Para activar Bitdefender VPN:

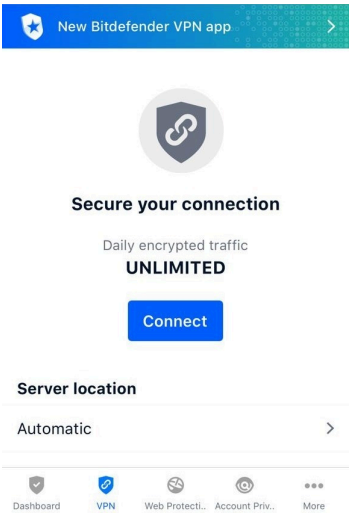
1. Toque en el icono de la parte inferior de la pantalla.
2. Toque **Conectar** siempre que desee permanecer protegido mientras se conecte a redes inalámbricas inseguras.
   Toque **Desconectar** cuando desee desactivar la conexión.

> **Nota**
> Cuando activa VPN por primera vez, se le pide que permita que Bitdefender establezca configuraciones VPN que monitoricen el tráfico de red. Toque **Permitir** para continuar. Si se ha configurado un método de autenticación (huella dactilar o código PIN) para proteger su smartphone, debe usarlo.

El icono VPN aparece en la barra de estado cuando VPN está activo.

Para prolongar la duración de la batería, le recomendamos que desactive VPN cuando no lo necesite.

Si posee una suscripción Premium y quiere conectarse a determinado servidor, toque en Automático en la interfaz de VPN y, a continuación, seleccione el lugar que desee. Para más información sobre las suscripciones a VPN, consulte Suscripciones (página 15).



3.4.1. Suscripciones

Bitdefender VPN ofrece de forma gratuita una cuota diaria de tráfico de 200 MB por dispositivo para proteger su conexión cada vez que lo necesite y le conecta automáticamente a la ubicación del servidor óptimo.

Para disfrutar de tráfico y acceso ilimitado a contenidos en todo el mundo y elegir la ubicación del servidor que desee, actualice a la versión premium.

Puede actualizar a la versión Bitdefender Premium VPN en cualquier momento tocando el botón **Activar Premium VPN** disponible en la ventana de VPN. Hay dos tipos de suscripciones para elegir: anual y mensual.

La suscripción Bitdefender Premium VPN es independiente de la suscripción gratuita a Bitdefender Mobile Security for iOS, lo que significa que podrá usarla en toda su extensión. En caso de que la suscripción Bitdefender Premium VPN caduque, se le revertirá automáticamente al plan gratuito.

Bitdefender VPN es un producto multiplataforma, disponible en los productos Bitdefender compatibles con Windows, macOS, Android y iOS. Una vez que actualice al plan Premium, podrá usar su suscripción en todos los productos, siempre que inicie sesión con la misma cuenta de Bitdefender.

Nota

Bitdefender VPN también funciona como aplicación independiente en todos los sistemas operativos compatibles: Windows, macOS, iOS y Android.

3.5. Privacidad de la cuenta

Privacidad de la cuenta de Bitdefender detecta si se ha producido alguna filtración de información en las cuentas que utiliza para realizar pagos y compras online, o para iniciar sesión en diferentes apps o sitios web. Una cuenta puede almacenar datos como contraseñas e información de tarjetas de crédito o de cuentas bancarias y, si no están adecuadamente protegidos, es posible que se produzcan robos de identidad o vulneraciones de la privacidad.

El estado de privacidad de la cuenta se indica justo después de la validación.

Para comprobar si se ha filtrado alguna de las cuentas, toque **Buscar filtraciones**.

Para empezar a poner a salvo su información personal:

1. Toque en el icono de la parte inferior de la pantalla.
2. Toque en **Añadir cuenta**.
3. Introduzca su dirección de correo electrónico en el campo correspondiente y, a continuación, toque **Siguiente**.
   Bitdefender tiene que validar esta cuenta antes de mostrar información privada. Por ello, se ha enviado un mensaje con un código de validación a la dirección de correo electrónico proporcionada.
4. Compruebe su bandeja de entrada y, a continuación, escriba el código que ha recibido en la zona **Privacidad de la cuenta** de su app. Si no encuentra el mensaje de validación en su bandeja de entrada, compruebe también la carpeta de correo no deseado.
   Se muestra el estado de privacidad de la cuenta validada.

En caso de detectarse filtraciones en cualquiera de sus cuentas, le recomendamos que cambie su contraseña lo antes posible. Para crear una contraseña realmente segura, siga estos consejos:

- Créela de por lo menos ocho caracteres de longitud.

- Utilice una combinación de mayúsculas y minúsculas.
- Incluya al menos un número o un símbolo, como por ejemplo #, @, % o !.

Una vez que haya protegido una cuenta que había sufrido una vulneración de la privacidad, puede confirmar los cambios marcando la filtración identificada como **Solucionada**. Para ello:

1. Toque en ··· junto a la vulneración que ha resuelto.
2. Toque **Marcar como resuelto**.

Cuando todas las filtraciones detectadas se hayan marcado como Solucionadas, la cuenta ya no aparecerá como objeto de filtraciones, al menos hasta que se vuelva a detectar una nueva filtración.

4. ACERCA DE BITDEFENDER CENTRAL

Bitdefender Central es la plataforma en la que tiene acceso a los servicios y características online del producto y desde donde puede realizar de forma remota tareas importantes en los dispositivos en los que está instalado Bitdefender. Puede iniciar sesión en su cuenta de Bitdefender desde cualquier equipo conectado a Internet accediendo a https://central.bitdefender.com o directamente desde la app Bitdefender Central en dispositivos iOS y Android.

Para instalar la app de Bitdefender Central en sus dispositivos:

- **En Android**: Busque Bitdefender Central en Google Play y luego descargue e instale la app. Siga los pasos necesarios para finalizar la instalación.
- **En iOS**: Busque Bitdefender Central en App Store y luego descargue e instale la app. Siga los pasos necesarios para finalizar la instalación.

Una vez que haya iniciado sesión, puede empezar por hacer lo siguiente:

- Descargar e instalar Bitdefender en los sistemas operativos Windows, iOS, macOS y Android. Los productos disponibles para descargar son:
  - Seguridad móvil de Bitdefender para iOS
  - Bitdefender Mobile Security for Android
  - Bitdefender Antivirus for Mac
  - La línea de productos de Windows de Bitdefender
- Administrar y renovar sus suscripciones de Bitdefender.
- Añadir nuevos dispositivos a su red y administrarlos desde cualquier lugar.

4.1. Acceso a Bitdefender Central

Existen dos formas de acceder a Bitdefender Central

- Desde su navegador Web:
  1. Abra un navegador Web en cualquier dispositivo con acceso a internet.
  2. Ir a: https://central.bitdefender.com .

3. Inicie sesión en su cuenta con su dirección de correo electrónico y contraseña.

❍ Desde su dispositivo Android o iOS:
Abra la app Bitdefender Central que ha instalado.

> **Nota**
> En este material, hemos incluido las opciones que puede encontrar en la interfaz web.

4.2. Autenticación en dos fases

El método de autenticación en dos fases aporta una capa adicional de seguridad a su cuenta de Bitdefender, ya que requiere un código de autenticación además de sus credenciales de inicio de sesión. De esta manera, evitará la toma de control de la cuenta y mantendrá alejados ciertos tipos de ataques informáticos, como los de registradores de pulsaciones de teclas, los de fuerza bruta o los de diccionario.

4.2.1. Activar la autenticación en dos fases

Al habilitar la autenticación en dos fases, su cuenta de Bitdefender estará mucho más segura. Su identidad se verificará cada vez que inicie sesión desde diferentes dispositivos, ya sea para instalar uno de los productos de Bitdefender, para verificar el estado de su suscripción o para ejecutar tareas en sus dispositivos de forma remota.

Para habilitar la autenticación en dos fases:

1. Acceso Centro de Bitdefender.
2. Toque el icono en la parte superior derecha de la pantalla.
3. Toque **Cuenta de Bitdefender** en el menú deslizante.
4. Seleccione la pestaña **Contraseña y seguridad**.
5. Toque **PUESTA EN MARCHA**.
Escoja uno de los siguientes métodos:

   ❍ **App de autenticación**: Use una app de autenticación para generar un código cada vez que desee iniciar sesión en su cuenta de Bitdefender.

Si desea utilizar una app de autenticación, pero no está seguro de cuál elegir, tiene a su disposición una lista con las que recomendamos.

a. Toque **USAR LA APP DE AUTENTICACIÓN** para comenzar.

b. Para iniciar sesión en un dispositivo con Android o iOS, use su dispositivo para leer el código QR.
Para iniciar sesión en un equipo de escritorio o portátil, puede añadir manualmente el código mostrado.
Toque **CONTINUAR**.

c. Inserte el código proporcionado por la app o el que se muestra en el paso anterior y, a continuación, toque **ACTIVAR**.

- **Correo electrónico**: Cada vez que inicie sesión en su cuenta de Bitdefender, se le enviará un código de verificación a su bandeja de entrada de correo electrónico. Consulte su cuenta de correo electrónico y escriba el código que se le proporciona.

  a. Toque **USAR CORREO ELECTRÓNICO** para comenzar.

  b. Lea su correo electrónico y escriba el código que se le proporciona.
  Tenga en cuenta que tiene cinco minutos para revisar su cuenta de correo electrónico y escribir el código generado. Si se agotase el tiempo, debería generar uno nuevo siguiendo los mismos pasos.

  c. Toque **ACTIVAR**.

  d. Se le proporcionan diez códigos de activación. Puede copiar, descargar o imprimir la lista y utilizarla en caso de que pierda su dirección de correo electrónico o no pueda iniciar sesión. Cada código puede utilizarse una sola vez.

  e. Toque **HECHO**.

En caso de que desee dejar de usar la autenticación en dos fases:

1. Toque **DESACTIVAR LA AUTENTICACIÓN EN DOS FASES**.
2. Consulte su app o su cuenta de correo electrónico y escriba el código que ha recibido.
   En caso de que haya optado por recibir el código de autenticación por correo electrónico, tiene cinco minutos para consultar su cuenta

de correo electrónico y escribir el código generado. Si se agotase el tiempo, debería generar uno nuevo siguiendo los mismos pasos.

3. Confirme su elección.

4.3. Añadir dispositivos de confianza

Para asegurarnos de que solo usted pueda acceder a su cuenta de Bitdefender, es posible que le solicitemos antes un código de seguridad. Si desea omitir este paso siempre que se conecte desde el mismo dispositivo, le recomendamos que lo añada como dispositivo de confianza.

Para añadir dispositivos de confianza:

1. Acceso Centro de Bitdefender.
2. Toque en el icono en la parte superior derecha de la pantalla.
3. Grifo **Cuenta de Bitdefender** en el menú deslizante.
4. Selecciona el **contraseña y seguridad** pestaña.
5. Toque **Dispositivos de confianza**.
6. Aparecerá la lista con los dispositivos en los que está instalado Bitdefender. Toque en el dispositivo deseado.

Puede añadir tantos dispositivos como desee, siempre y cuando tengan Bitdefender instalado y su suscripción sea válida.

4.4. Mis dispositivos

El área **Mis sispositivos** de su cuenta de Bitdefender le da la posibilidad de instalar, administrar y llevar a cabo acciones remotas en su producto de Bitdefender en cualquier dispositivo, siempre y cuando esté encendido y conectado a Internet. Las tarjetas de cada dispositivo muestran el nombre de este, su estado de protección y si existen riesgos para la seguridad que afecten a la protección de sus dispositivos.

4.4.1. Añadir un nuevo dispositivo

Si su suscripción cubre más de un dispositivo, puede añadir un nuevo dispositivo e instalarle Bitdefender Mobile Security for iOS de la siguiente manera:

1. Acceso Centro de Bitdefender.
2. Selecciona el **Mis dispositivos** panel y, a continuación, toque **INSTALAR PROTECCIÓN**.
3. Elija una de las dos opciones disponibles:
   - **Protege este dispositivo**
     Seleccione esta opción y luego seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, toque el botón correspondiente.
   - **Proteger otros dispositivos**
     Seleccione esta opción y luego seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, toque el botón correspondiente.
     Toque **ENVIAR ENLACE DE DESCARGA**. Introduzca una dirección de correo electrónico en el campo correspondiente y toque **ENVIAR CORREO**. Tenga en cuenta que el enlace de descarga generado solo es válido durante las próximas 24 horas. Si caducase, debería generar uno nuevo siguiendo los mismos pasos.
     En el dispositivo en el que desea instalar su producto Bitdefender, verifique la cuenta de correo electrónico que ingresó y luego toque el botón de descarga correspondiente.
4. Espere a que finalice la descarga y, acto seguido, ejecute el instalador.

4.4.2. Personalice su dispositivo

Para identificar fácilmente sus dispositivos, puede personalizar el nombre de los mismos:

1. Acceso Centro de Bitdefender.
2. Seleccione el panel **Mis dispositivos**.
3. Haga clic en la tarjeta del dispositivo deseado y, a continuación, en el icono ⋮ de la esquina superior derecha de la pantalla.
4. Seleccione **Ajustes**.
5. Escriba un nuevo nombre en el campo **Nombre del dispositivo** y, a continuación, toque **GUARDAR**.

Puede crear y asignar un propietario a cada uno de los dispositivos para gestionarlos mejor:

1. Acceso Centro de Bitdefender.
2. Selecciona el **Mis dispositivos** panel.
3. Toque la tarjeta del dispositivo deseado, y luego el ⋮ icono en la esquina superior derecha de la pantalla.
4. Seleccione **Perfil**.
5. Haga clic en **Añadir propietario** y, a continuación, rellene los campos correspondientes. Personalice el perfil incluyendo una foto, seleccionando una fecha de nacimiento y añadiendo una dirección de correo electrónico y un número de teléfono.
6. Haga clic en **AÑADIR** para guardar el perfil.
7. Seleccione el propietario deseado en la lista de **Propietarios de dispositivos** y, a continuación, toque **ASIGNAR**.

4.4.3. Acciones remotas

Para actualizar Bitdefender remotamente en un dispositivo:

1. Acceso Centro de Bitdefender.
2. Selecciona el **Mis dispositivos** panel.
3. Toque la tarjeta del dispositivo deseado, y luego el ⋮ icono en la esquina superior derecha de la pantalla.
4. Seleccione **Actualizar**.

Para tener acceso a más acciones remotas e información acerca de su producto Bitdefender en un dispositivo concreto, haga clic en la tarjeta de dicho dispositivo.

Una vez que haga clic en una tarjeta de dispositivo, tendrá a su disposición las siguientes pestañas:

- **Panel de control.** En esta ventana puede ver información sobre el dispositivo seleccionado, comprobar el estado de su protección, el de Bitdefender VPN y cuántas amenazas se han bloqueado en los últimos siete días. El estado de la protección puede ser verde, cuando no hay ningún problema que afecte a su producto; amarillo, si el dispositivo requiere su atención; o rojo, cuando el dispositivo está en riesgo. Cuando haya problemas que afecten a su dispositivo, toque la

flecha desplegable en el área de estado superior para obtener más información. Desde aquí, puede

- **Protección.** Desde esta ventana puede ejecutar de forma remota un análisis rápido o un análisis del sistema en sus dispositivos. Toque el botón **ANALIZAR** para poner en marcha el proceso. También puede comprobar cuándo se realizó el último análisis en el dispositivo, así como obtener un informe del último análisis con la información más importante disponible.
- **Optimizador.** Aquí puede mejorar el rendimiento de un dispositivo de forma remota mediante un rápido análisis, detección y limpieza de archivos inútiles. Toque el botón **INICIAR** y, a continuación, seleccione las áreas que desea optimizar. Toque nuevamente en el botón **INICIAR** para poner en marcha el proceso de optimización. Toque **Más detalles** para acceder a un informe pormenorizado acerca de los problemas solucionados.
- **Antirrobo.** Si no se acuerda de dónde ha puesto su dispositivo o si se lo han robado o lo ha perdido, con la función Antirrobo puede localizarlo y llevar a cabo acciones remotas. Toque **LOCALIZAR** para conocer la ubicación de su dispositivo. Se mostrará la última posición conocida, junto con la fecha y la hora.
- **Vulnerabilidad.** Para comprobar las vulnerabilidades de un dispositivo, como por ejemplo actualizaciones de Windows sin hacer, aplicaciones obsoletas o contraseñas débiles, toque el botón **ANALIZAR** en la pestaña de Vulnerabilidad. Las vulnerabilidades no se pueden solucionar de forma remota. En caso de encontrar cualquier vulnerabilidad, tendrá que ejecutar un nuevo análisis en el dispositivo y adoptar las medidas recomendadas. Toque **Más detalles** para acceder a un informe pormenorizado acerca de los problemas encontrados.

4.5. Actividad

En el área de Actividad, tiene acceso a información sobre los dispositivos que tienen Bitdefender instalado.

Una vez que accede a la ventana **Actividad**, tiene a su disposición las siguientes fichas:

- **Mis dispositivos.** Aquí puede ver el número de dispositivos conectados junto con el estado de su protección. Para solucionar

problemas de forma remota en los dispositivos detectados, toque **Solucionar problemas** y, a continuación, toque **ANALIZAR Y SOLUCIONAR LOS PROBLEMAS**.

Para ver más información sobre los problemas detectados, haga clic en **Ver problemas**.

La información sobre las amenazas detectadas no se puede recuperar de los dispositivos basados en iOS.

- **Amenazas bloqueadas.** Aquí puede ver un gráfico que muestra una estadística general con información sobre las amenazas bloqueadas durante las últimas 24 horas y siete días. La información mostrada se recupera dependiendo del comportamiento malicioso detectado en los archivos, aplicaciones y URL a los que se accede.
- **Principales usuarios con amenazas bloqueadas.** Aquí puede ver los usuarios que se han sido objeto de más amenazas.
- **Principales dispositivos con amenazas bloqueadas.** Aquí puede ver los dispositivos donde se han encontrado más amenazas.

4.6. Mis suscripciones

La plataforma Bitdefender Central le da la posibilidad de administrar fácilmente las suscripciones que tiene para todos sus dispositivos.

4.6.1. Compruebe las suscripciones disponibles

Para comprobar sus suscripciones disponibles:

1. Acceso Centro de Bitdefender.
2. Seleccione el panel **Mis suscripciones**.

Aquí tiene información sobre la disponibilidad de las suscripciones que posee y el número de dispositivos que utilizan cada una de ellas.

Puede añadir un nuevo dispositivo a una suscripción o renovarlo seleccionando una tarjeta de suscripción.

> **Nota**
> Puede tener una o más suscripciones en su cuenta siempre que sean para diferentes plataformas (Windows, macOS, iOS o Android).

4.6.2. Activar la suscripción

Una suscripción se puede activar durante el proceso de instalación mediante su cuenta de Bitdefender. Tras el proceso de activación, da comienzo la cuenta atrás de la validez de la suscripción.

Si ha comprado un código de activación a uno de nuestros resellers o lo ha recibido de regalo, puede añadir su disponibilidad a su suscripción de Bitdefender.

Para activar una suscripción mediante un código de activación, siga estos pasos:

1. Acceso Centro de Bitdefender.
2. Selecciona el **mis Suscripciónes** panel.
3. Haga clic en el botón **CÓDIGO DE ACTIVACIÓN** y, a continuación, escriba el código en el campo correspondiente.
4. Toque **ACTIVAR** para continuar.

La suscripción ya está activada.

4.6.3. Renovar suscripción

Si ha inhabilitado la renovación automática de su suscripción de Bitdefender, puede renovarla manualmente siguiendo los pasos que se exponen a continuación:

1. Acceso Centro de Bitdefender.
2. Selecciona el **mis Suscripciónes** panel.
3. Seleccione la tarjeta de suscripción deseada.
4. Toque **RENOVAR** para continuar.

Se abrirá una página web en su navegador de Internet, donde puede renovar su suscripción de Bitdefender.

4.7. Notificaciones

Para ayudarle a mantenerse informado de lo que sucede en los dispositivos asociados a su cuenta, tiene fácilmente accesible el icono . Haciendo clic en él dispondrá de una panorámica general con información acerca de la actividad de los productos de Bitdefender instalados en sus dispositivos.

5. PREGUNTAS MÁS FRECUENTES

¿Cómo me protege Bitdefender Mobile Security for iOS contra virus y amenazas digitales?

Bitdefender Mobile Security for iOS proporciona protección absoluta contra todas las amenazas digitales y está especialmente diseñado para mantener sus datos confidenciales a salvo de miradas indiscretas.

Obtiene una gran cantidad de características de seguridad y privacidad avanzadas para su iPhone y iPad, además de muchas otras, como VPN y Protección web.

Bitdefender Mobile Security for iOS reacciona instantáneamente ante virus y malware sin sacrificar el rendimiento de su sistema.

¿Qué tipo de dispositivos y sistemas operativos cubre Bitdefender Mobile Security for iOS?

Bitdefender Mobile Security for iOS protegerá sus smartphones y tablets con iOS contra todas las amenazas digitales.

¿Por qué necesito Bitdefender Mobile Security for iOS en el sistema operativo de Apple?

Algunos de sus datos más personales se almacenan en su iPhone o iPad y necesita saber que están seguros en todo momento. Bitdefender Mobile Security for iOS proporciona protección absoluta contra amenazas digitales y se encarga de su privacidad online y de su información confidencial sin interferir en sus actividades cotidianas.

¿Obtengo una VPN con mi suscripción a Bitdefender Mobile Security for iOS?

Bitdefender Mobile Security for iOS viene con una versión básica de Bitdefender VPN que incluye gratuitamente una generosa cantidad de tráfico (200 MB/día, un total de GB al mes).

6. OBTENIENDO AYUDA

6.1. Solicitando Ayuda

Bitdefender proporciona a sus clientes un nivel sin igual de soporte técnico rápido y preciso. Si tiene cualquier problema o alguna pregunta sobre su producto Bitdefender, dispone de varios recursos online para encontrar una solución o una respuesta. Además, puede ponerse en contacto con el equipo de Atención al Cliente de Bitdefender. Nuestros representantes de soporte técnico responderán a sus preguntas con diligencia y le proporcionarán la asistencia que necesite.

6.2. Recursos Online

Hay varios recursos online disponibles para ayudarle a resolver su problemas y preguntas relacionadas con Bitdefender.

- Centro de soporte de Bitdefender:
  https://www.bitdefender.es/consumer/support/
- La comunidad de expertos de Bitdefender:
  https://community.bitdefender.com/es
- Ciberpedia de Bitdefender:
  https://www.bitdefender.com/cyberpedia/

Puede además usar su motor de búsqueda favorito para encontrar más información sobre seguridad de equipo, los productos de Bitdefender y la compañía.

6.2.1. Centro de soporte de Bitdefender

El Centro de soporte Bitdefender es una librería de información online sobre el producto Bitdefender. Alberga, en un formato de fácil acceso, los informes sobre los resultados del soporte técnico en curso y las actividades de solución de errores a cargo de los equipos de soporte y desarrollo de Bitdefender, junto con artículos más generales sobre prevención de amenazas, la administración de las soluciones de Bitdefender con explicaciones detalladas, y muchos otros artículos.

El Centro de soporte de Bitdefender está abierto al público y puede consultarse gratuitamente. La amplia información que contiene es otro

medio de proporcionar a los clientes de Bitdefender los conocimientos técnicos y la información que necesitan. Todas las solicitudes válidas de información o informes de errores procedentes de los clientes acaban finalmente en el Centro de soporte de Bitdefender, como informes de resolución de errores, documentos técnicos o artículos informativos para complementar los archivos de ayuda del producto.

El Centro de soporte de Bitdefender está disponible en cualquier momento en la siguiente dirección: https://www.bitdefender.es/consumer/support/.

6.2.2. La comunidad de expertos de Bitdefender

La comunidad de expertos es un entorno en el que los usuarios, entusiastas y fanes de Bitdefender pueden participar, intercambiar ideas, apoyarse mutuamente y compartir sus conocimientos y soluciones. Además, es un lugar de creación de ideas y aporta valiosos comentarios a nuestros equipos de desarrollo. Los miembros de esta comunidad son usuarios experimentados de Bitdefender que se complacen en ayudar a otros en su tiempo libre. Con su inmensa contribución y su genuino esfuerzo de voluntariado, hemos creado una base de conocimientos en la que los usuarios pueden hallar respuestas y orientación, pero con un toque humano.

Aquí encontrará interesantes conversaciones con gente que usa Bitdefender en sus dispositivos. La comunidad establece una auténtica conexión entre sus miembros y hace oír su voz. Es un lugar donde se alienta la participación sabiendo que su opinión y aporte serán respetados y apreciados. Como valioso contribuyente, nos esforzamos por ofrecer un nivel sin igual de soporte técnico rápido y preciso y deseamos aproximarnos a nuestros usuarios. Con este propósito en mente hemos diseñado nuestra comunidad.

Puede encontrar la página web de nuestra comunidad de expertos aquí:

https://community.bitdefender.com/es

6.2.3. Ciberpedia de Bitdefender

Bitdefender Cyberpedia contiene toda la información que necesita conocer sobre las últimas amenazas digitales. Aquí es donde los expertos de Bitdefender dan a conocer consejos y trucos para protegerse contra piratas informáticos, vulneraciones de datos, robos de identidad e intentos de suplantación en las redes sociales.

En el siguiente enlace puede encontrar la página web de Bitdefender Cyberpedia:

https://www.bitdefender.com/cyberpedia/.

6.3. Información de contacto

La comunicación eficiente es la clave para un negocio exitoso. Desde 2001, BITDEFENDER ha establecido una reputación incuestionable al esforzarse constantemente por mejorar la comunicación para superar las expectativas de nuestros clientes y socios. Si tiene alguna pregunta, no dude en contactarnos directamente a través de nuestro Centro de soporte de Bitdefender (página 29).

https://www.bitdefender.es/consumer/support/

6.3.1. Distribuidores locales

Los distribuidores locales de Bitdefender están preparados para responder a cualquier pregunta relacionada con su área de actuación, tanto a nivel comercial como en otros áreas.

Para encontrar un distribuidor de Bitdefender en su país:

1. Ir a https://www.bitdefender.com/partners/localizador-de-socios.html.
2. Elija su país y ciudad mediante las opciones correspondientes.

GLOSARIO

Código de activación

Es una clave única que se puede comprar al por menor y se utiliza para activar un producto o servicio específico. Un código de activación permite la activación de una suscripción válida por un cierto período de tiempo y número de dispositivos y también se puede utilizar para extender una suscripción con la condición de generarse para el mismo producto o servicio.

ActiveX

ActiveX es un modelo para escribir programas para que otros programas y el sistema operativo puedan llamarlos. La tecnología ActiveX se usa con Microsoft Internet Explorer para crear páginas web interactivas que se ven y se comportan como programas de computadora, en lugar de páginas estáticas. Con ActiveX, los usuarios pueden hacer o responder preguntas, usar botones e interactuar de otras formas con la página web. Los controles ActiveX a menudo se escriben usando Visual Basic. Active X se destaca por una completa falta de controles de seguridad; los expertos en seguridad informática desaconsejan su uso a través de internet.

Amenaza Persistente Avanzada

La amenaza persistente avanzada (APT) explota las vulnerabilidades de los sistemas para robar información importante y entregarla a la fuente. Grandes grupos, como organizaciones, empresas o gobiernos, son el blanco de esta amenaza. El objetivo de una amenaza persistente avanzada es pasar desapercibida durante mucho tiempo y poder monitorear y recopilar información importante sin dañar las máquinas objetivo. El método utilizado para inyectar la amenaza en la red es a través de un archivo PDF o un documento de Office que parezca inofensivo para que cada usuario pueda ejecutar los archivos.

publicidad

El adware a menudo se combina con una aplicación host que se proporciona sin cargo siempre que el usuario acepte el adware. Debido a que las aplicaciones de adware generalmente se instalan después de que el usuario haya aceptado un acuerdo de licencia que establece el propósito de la aplicación, no se comete ningún delito. Sin embargo, los anuncios emergentes pueden convertirse en una molestia y, en algunos

casos, degradar el rendimiento del sistema. Además, la información que recopilan algunas de estas aplicaciones puede causar problemas de privacidad para los usuarios que no conocían completamente los términos del acuerdo de licencia.

Archivo

Disco, cinta o directorio conteniendo ficheros almacenados.

Un archivo que contiene uno o más archivos en un formato comprimido.

Puerta trasera

Un agujero en la seguridad de un sistema dejado deliberadamente por diseñadores o mantenedores. La motivación de tales agujeros no siempre es siniestra; algunos sistemas operativos, por ejemplo, vienen listos para usar con cuentas privilegiadas destinadas a los técnicos de servicio de campo o los programadores de mantenimiento del proveedor.

Sector de arranque

Un sector al comienzo de cada disco que identifica la arquitectura del disco (tamaño del sector, tamaño del clúster, etc.). Para los discos de inicio, el sector de arranque también contiene un programa que carga el sistema operativo.

virus de arranque

Una amenaza que infecta el sector de arranque de un disco fijo o disquete. Un intento de arrancar desde un disquete infectado con un virus del sector de arranque hará que la amenaza se active en la memoria. Cada vez que inicie su sistema a partir de ese momento, tendrá la amenaza activa en la memoria.

red de bots

El término “botnet” se compone de las palabras “robot” y “red”. Los botnets son dispositivos conectados a Internet infectados con amenazas y se pueden usar para enviar correos electrónicos no deseados, robar datos, controlar de forma remota dispositivos vulnerables o propagar spyware, ransomware y otros tipos de amenazas. Su objetivo es infectar el mayor número posible de dispositivos conectados, como PC, servidores, dispositivos móviles o IoT pertenecientes a grandes empresas o industrias.

Navegador

Abreviatura de navegador web, una aplicación de software utilizada para localizar y mostrar páginas web. Los navegadores populares incluyen Microsoft Internet Explorer, Mozilla Firefox y Google Chrome. Estos son navegadores gráficos, lo que significa que pueden mostrar gráficos además de texto. Además, la mayoría de los navegadores modernos pueden presentar información multimedia, incluidos sonido y video, aunque requieren complementos para algunos formatos.

Ataque de fuerza bruta

Ataque de adivinación de contraseñas utilizado para ingresar en un sistema informático ingresando posibles combinaciones de contraseñas, en su mayoría comenzando con la contraseña más fácil de adivinar.

Línea de comando

En una interfaz de línea de comandos, el usuario escribe los comandos en el espacio provisto directamente en la pantalla usando el lenguaje de comandos.

Galletas

Dentro de la industria de Internet, las cookies se describen como pequeños archivos que contienen información sobre computadoras individuales que los anunciantes pueden analizar y usar para rastrear sus intereses y gustos en línea. En este ámbito, la tecnología de cookies aún se está desarrollando y la intención es orientar los anuncios directamente a lo que ha dicho que son sus intereses. Es un arma de doble filo para muchas personas porque, por un lado, es eficiente y pertinente, ya que solo ve anuncios sobre lo que le interesa. Por otro lado, implica realmente "rastrear" y "seguir" a dónde va y lo que haces clic. Comprensiblemente, existe un debate sobre la privacidad y muchas personas se sienten ofendidas por la noción de que se les considera un "número SKU" (ya sabe, el código de barras en la parte posterior de los paquetes que se escanea en la línea de pago del supermercado) . Si bien este punto de vista puede ser extremo, en algunos casos es exacto.

Ciberacoso

Cuando compañeros o extraños están cometiendo actos abusivos contra los niños con el propósito de lastimarlos físicamente. Para dañar emocionalmente, los agresores envían mensajes crueles o fotos poco favorecedoras, lo que hace que sus víctimas se aíslen de los demás o se sientan frustradas.

Ataque de diccionario

Los ataques de adivinación de contraseñas solían entrar en un sistema informático ingresando una combinación de palabras comunes para generar posibles contraseñas. El mismo método se utiliza para adivinar las claves de descifrado de mensajes o documentos cifrados. Los ataques de diccionario tienen éxito porque muchas personas se inclinan por elegir contraseñas cortas y de una sola palabra que sean fáciles de adivinar.

Disco duro

Es una máquina que lee y escribe datos en un disco. Una unidad de disco duro lee y escribe discos duros. Una unidad de disquete accede a disquetes. Las unidades de disco pueden ser internas (alojadas dentro de una computadora) o externas (alojadas en una caja separada que se conecta a la computadora).

Descargar

Para copiar datos (generalmente un archivo completo) desde una fuente principal a un dispositivo periférico. El término se usa a menudo para describir el proceso de copiar un archivo de un servicio en línea a la propia computadora. Descargar también puede referirse a copiar un archivo desde un servidor de archivos de red a una computadora en la red.

Correo electrónico

Correo electrónico. Un servicio que envía mensajes en computadoras a través de redes locales o globales.

Eventos

Una acción u ocurrencia detectada por un programa. Los eventos pueden ser acciones del usuario, como hacer clic con el botón del mouse o presionar una tecla, o eventos del sistema, como quedarse sin memoria.

hazañas

Una forma de aprovechar diferentes errores o vulnerabilidades que están presentes en una computadora (software o hardware). Por lo tanto, los piratas informáticos pueden obtener el control de las computadoras o las redes.

Falso positivo

Ocurre cuando un escáner identifica un archivo como infectado cuando en realidad no lo está.

Extensión de nombre de archivo

La parte de un nombre de archivo, después del punto final, que indica el tipo de datos almacenados en el archivo. Muchos sistemas operativos utilizan extensiones de nombre de archivo, por ejemplo, Unix, VMS y MS-DOS. Por lo general, tienen de una a tres letras (algunos sistemas operativos tristes y antiguos no admiten más de tres). Los ejemplos incluyen "c" para código fuente C, "ps" para PostScript, "txt" para texto arbitrario.

Heurístico

Un método basado en reglas para identificar nuevas amenazas. Este método de escaneo no se basa en una base de datos de información de amenazas específica. La ventaja del análisis heurístico es que no se deja engañar por una nueva variante de una amenaza existente. Sin embargo, ocasionalmente puede reportar código sospechoso en programas normales, generando el llamado "falso positivo".

Tarro de miel

Un sistema informático de señuelo configurado para atraer a los piratas informáticos para que estudien la forma en que actúan e identifiquen los métodos heréticos que utilizan para recopilar información del sistema. Las empresas y corporaciones están más interesadas en implementar y utilizar trampas trampa para mejorar su estado general de seguridad.

IP

Protocolo de Internet: un protocolo enrutable en el conjunto de protocolos TCP/IP que es responsable del direccionamiento IP, el enrutamiento y la fragmentación y reensamblaje de paquetes IP.

Subprograma de Java

Un programa Java que está diseñado para ejecutarse solo en una página web. Para usar un subprograma en una página web, debe especificar el nombre del subprograma y el tamaño (largo y ancho, en píxeles) que puede utilizar el subprograma. Cuando se accede a la página web, el navegador descarga el applet de un servidor y lo ejecuta en la máquina del usuario (el cliente). Los applets se diferencian de las aplicaciones en que se rigen por un estricto protocolo de seguridad.

Por ejemplo, aunque los subprogramas se ejecutan en el cliente, no pueden leer ni escribir datos en la máquina del cliente. Además, los subprogramas están más restringidos para que solo puedan leer y escribir datos del mismo dominio desde el que se sirven.

registrador de teclas

Un keylogger es una aplicación que registra todo lo que escribes. Los keyloggers no son de naturaleza maliciosa. Se pueden usar para fines legítimos, como monitorear la actividad de los empleados o los niños. Sin embargo, los ciberdelincuentes los utilizan cada vez más con fines maliciosos (por ejemplo, para recopilar datos privados, como credenciales de inicio de sesión y números de seguridad social).

Virus de macros

Un tipo de amenaza informática que se codifica como una macro incrustada en un documento. Muchas aplicaciones, como Microsoft Word y Excel, admiten potentes lenguajes de macros. Estas aplicaciones le permiten incrustar una macro en un documento y hacer que la macro se ejecute cada vez que se abre el documento.

cliente de correo

Un cliente de correo electrónico es una aplicación que le permite enviar y recibir correo electrónico.

Memoria

Áreas de almacenamiento interno en la computadora. El término memoria identifica el almacenamiento de datos que viene en forma de chips, y la palabra almacenamiento se usa para la memoria que existe en cintas o discos. Cada computadora viene con una cierta cantidad de memoria física, generalmente denominada memoria principal o RAM.

no heurístico

Este método de escaneo se basa en una base de datos de información de amenazas específicas. La ventaja del análisis no heurístico es que no se deja engañar por lo que podría parecer una amenaza y no genera falsas alarmas.

Depredadores en línea

Individuos que buscan atraer a menores o adolescentes a conversaciones con el propósito de involucrarlos en actividades sexuales ilegales. Las redes sociales son el lugar ideal donde los niños vulnerables pueden ser perseguidos y seducidos fácilmente para que cometan actividades sexuales, en línea o cara a cara.

Programas empaquetados

Un archivo en un formato de compresión. Muchos sistemas operativos y aplicaciones contienen comandos que le permiten empaquetar un archivo para que ocupe menos memoria. Por ejemplo, suponga que tiene un archivo de texto que contiene diez caracteres de espacio consecutivos. Normalmente, esto requeriría diez bytes de almacenamiento.

Sin embargo, un programa que empaqueta archivos reemplazaría los caracteres de espacio por un carácter de serie de espacio especial seguido por la cantidad de espacios que se reemplazan. En este caso, los diez espacios requerirían solo dos bytes. Esta es solo una técnica de empaque, hay muchas más.

Camino

Las direcciones exactas a un archivo en una computadora. Estas direcciones generalmente se describen mediante el sistema de archivo jerárquico de arriba hacia abajo.

La ruta entre dos puntos, como el canal de comunicación entre dos computadoras.

Suplantación de identidad

El acto de enviar un correo electrónico a un usuario que afirma falsamente ser una empresa legítima establecida en un intento de estafar al usuario para que entregue información privada que se utilizará para el robo de identidad. El correo electrónico dirige al usuario a visitar un sitio web donde se le pide que actualice la información personal, como contraseñas y números de tarjetas de crédito, seguridad social y cuentas bancarias, que ya tiene la organización legítima. El sitio web, sin embargo, es falso y está configurado solo para robar la información del usuario.

Fotón

Photon es una innovadora tecnología no intrusiva de Bitdefender, diseñada para minimizar el impacto en el rendimiento de su solución de seguridad. Al monitorear la actividad de su PC en segundo plano, crea patrones de uso que ayudan a optimizar los procesos de arranque y escaneo.

Virus polimórfico

Una amenaza que cambia de forma con cada archivo que infecta. Como no tienen un patrón binario constante, estas amenazas son difíciles de identificar.

Puerto

Interfaz en un ordenador a la que se puede conectar un dispositivo. Los ordenadores personales tienen distintos tipos de puertos. Hay varios puertos internos para conectar las unidades de disco, las pantallas, los teclados. Asimismo, los ordenadores personales tienen puertos externos para conectar módems, impresoras, ratones y otros dispositivos periféricos.

En las redes de tipo TCP/IP y UDP representa el endpoint de una conexión lógica. El número de puerto indica el tipo del dicho puerto. Por ejemplo, el puerto 80 se usa para el tráfico http.

Ransomware

El ransomware es un programa malicioso que trata de obtener dinero de los usuarios mediante el bloqueo de sus sistemas vulnerables. Cryptolocker, CryptoWall y TeslaWall son solo algunas de las variantes que secuestran los sistemas personales de los usuarios.

La infección puede propagarse al acceder a spam, descargar archivos adjuntos, o instalar aplicaciones, evitando que el usuario se percate de lo que está sucediendo en su sistema. Los usuarios habituales y empresas son el objetivo de los hackers de ransomware.

Archivo de informe

Es un fichero que lista las acciones realizadas. BitDefender genera un archivo de informe (log) que contiene una lista de las rutas analizadas, las carpetas, el número de archivos y archivos comprimidos analizados, el número de archivos infectados y sospechosos que se han detectado.

Rootkit

Un rootkit es un conjunto de herramientas de software que ofrecen acceso al sistema a nivel de administrador. El término empezó a usarse con los sistemas operativos UNIX y se refería a las herramientas que proporcionaban permisos de administrador a los intrusos, permitiéndoles ocultar su presencia para no ser vistos por los administradores de sistema.

El papel principal de los rootkits es ocultar procesos, archivos, conexiones y logs. También pueden interceptar datos de terminales, conexiones de red o periféricos, si éstos incorporan el software apropiado.

Rootkits no son de naturaleza mala. Por ejemplo, los sistemas y algunas aplicaciones esconden ficheros críticos usando rootkits. No obstante, se usan habitualmente para ocultar amenazas o para encubrir la presencia

de un intruso en el sistema. Cuando se combinan con amenazas, los rootkits representan un gran peligro para la integridad y la seguridad de un sistema. Pueden monitorizar el tráfico, crear puertas traseras en el sistema, alterar ficheros y logs y evitar su detección.

Script

Es otro término para macro o fichero batch y se constituye de una lista de comandos que se pueden ejecutar sin la intervención del usuario.

Spam

Correo basura o posts basura en grupos de noticias. Se conoce generalmente como correo no deseado.

Spyware

Se trata de cualquier software que, en secreto, recopile información del usuario a través de su conexión a Internet sin su consentimiento, generalmente con fines comerciales. Las aplicaciones Spyware son, generalmente, componentes ocultos de programas freeware o shareware que pueden descargarse por Internet; sin embargo, debe observarse que la gran mayoría de aplicaciones shareware y freeware no contienen spyware. Una vez instalado, el spyware monitoriza la actividad del usuario en Internet y, en segundo plano, envía esa información a una tercera persona. El spyware también puede recoger información sobre direcciones de correo, e incluso contraseñas y números de tarjetas de crédito.

La similitud del spyware con una amenaza de tipo troyano radica en el hecho de que los usuarios instalan involuntariamente el producto al instalar otra cosa. Una forma habitual de infectarse con spyware es descargando, a través de programas de intercambio de ficheros, un determinado archivo que intercambia el nombre de los productos compartidos.

A parte de las cuestiones de ética y privacidad, el spyware roba al usuario recursos de memoria y ancho de banda mientras envía la información al creador del spyware a través de la conexión de Internet del usuario. Puesto que el spyware utiliza memoria y recursos del sistema, las aplicaciones que se ejecutan en segundo plano pueden provocar errores del sistema o inestabilidad general del mismo.

Elementos de inicio

Todos los ficheros de esta carpeta se abren al iniciar el ordenador. Por ejemplo, una pantalla de inicio, un archivo de sonido para que se reproduzca cuando se inicie el equipo, un calendario de recordatorios o apps pueden ser elementos de inicio. Normalmente, se elige un alias del fichero para ubicar en esta carpeta y no directamente el fichero.

Suscripción

Acuerdo de compra que otorga al usuario el derecho a utilizar un producto o servicio determinado en un número concreto de dispositivos y durante cierto periodo de tiempo. Una suscripción caducada puede renovarse automáticamente utilizando la información proporcionada por el usuario en su primera compra.

Bandeja del sistema

Elemento introducido con el sistema Windows 95,la bandeja de sistema está ubicada en la barra de tareas de Windows (normalmente al lado del reloj) y contiene iconos en miniatura para acceder fácilmente a las funciones del sistema, como el fax, la impresora, el módem, el volumen etc. Al hacer doble clic o clic derecho en el icono correspondiente, verá y abrirá los detalles y los mandos de los programas.

TCP/IP

Transmission Control Protocol/Internet Protocol - Es una gama de protocolos de red, extremadamente utilizados en Internet para proporcionar comunicaciones en las redes interconectadas, que incluyen ordenadores con distintas arquitecturas de hardware y varios sistemas operativos. TCP/IP ofrece estándares para el modo de comunicación entre ordenadores y convenciones para las redes interconectadas.

Amenaza

Es un programa o una parte de un código cargado en su ordenador sin avisarle y en contra de su voluntad. La mayoría de las amenazas también pueden autorreplicarse. Todas las amenazas informáticas están creadas por el hombre. Una amenaza sencilla que pueda copiarse una y otra vez es relativamente fácil de producir. Incluso una amenaza tan simple es peligrosa porque consumirá rápidamente toda la memoria disponible y hará que el sistema se detenga. Un tipo de amenaza aún más peligrosa es la capaz de transmitirse a través de las redes y eludir los sistemas de seguridad.

Actualización de información sobre amenazas

El patrón binario de una amenaza, utilizado por la solución de seguridad para detectarla y eliminarla.

Troyano

Es un programa destructivo disfrazado como aplicación benigna. A diferencia de los programas de software malicioso y gusanos, los troyanos no se autorreplican, pero pueden ser igualmente destructivos. Uno de los tipos de troyanos más graves es una amenaza que pretende desinfectar su equipo, pero en cambio introduce amenazas en él.

El término tiene origen en la famosa obra "La Ilíada" de Homero, en la cual Grecia entrega un gigantesco caballo de madera a sus enemigos, los Troyanos, como supuesta oferta de paz. Pero una vez los Troyanos arrastraron el caballo hasta el interior de las murallas de la ciudad, los soldados Griegos salieron de un hueco del vientre del caballo y abrieron las puertas de las murallas, permitiendo la entrada de sus compatriotas y la conquista de Troya.

Actualizar

Una nueva versión de un producto de software o hardware, diseñada para reemplazar una versión anterior del mismo producto. Además, durante la instalación se verifica si en su ordenador existe una versión anterior; si no se encuentra ninguna, no se instalará la actualización.

Bitdefender posee una característica de actualización que le permite comprobar manualmente las actualizaciones o actualizar automáticamente el producto.

Red privada virtual (VPN)

Es una tecnología que permite una conexión directa temporal y cifrada a una determinada red a través de una red menos segura. De esta forma, el envío y recepción de datos está cifrado y es seguro, lo que dificulta su intercepción por parte de los fisgones. Una muestra de seguridad es la autenticación, que solo se puede lograr utilizando un nombre de usuario y contraseña.

Gusano

Un programa que se autopropaga a través de una red, reproduciéndose a medida que avanza. No puede adjuntarse a otros programas.