GUÍA DE USUARIO

Bitdefender CONSUMER SOLUTIONS

Digital Identity Protection

Bitdefender Digital Identity Protection

Guía de usuario

Fecha de publicación 06/09/2023

Aviso Legal

Bitdefender

Tabla de contenidos

ACERCA DE ESTA GUÍA

Propósito y público al que se dirige

Esta guía va dirigida a los usuarios de Bitdefender Digital Identity Protection que han elegido Bitdefender Digital Identity Protection como su herramienta de software para mantenerse a salvo de la creciente ola de vulneraciones de datos online. La información presentada en ella no solo es adecuada para quienes posean conocimientos sobre informática, sino que está al alcance de cualquiera.

Descubrirá cómo empezar a tomar el control de su privacidad online haciendo que Bitdefender Digital Identity Protection busque en la web vulneraciones de sus datos de carácter personal, controle si sus cuentas se han visto expuestas y le facilite la adopción de medidas mucho antes de que se produzca un desastre. Descubrirá cómo 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:

Primeros pasos (página 6)

Comience con Bitdefender Digital Identity Protection y su interfaz de usuario.

Violaciones de datos (página 11)

Aprenda a cuidar adecuadamente su identidad digital. Empiece por comprender qué son las vulneraciones de datos y cómo revisarlas para adoptar las medidas oportunas de cara a proteger su privacidad online.

Obteniendo ayuda (página 17)

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 DIGITAL IDENTITY PROTECTION

Actualmente, entre las principales preocupaciones de los usuarios de Internet se cuentan la privacidad y la seguridad online. No es de extrañar. Dado que cada vez con mayor frecuencia se producen importantes vulneraciones de datos, es primordial asegurarse de que nuestra información de carácter personal esté a salvo.

Pero ¿qué se entiende por información de carácter personal? Tradicionalmente, se ha considerado como tal la información confidencial como el nombre completo, el número de la Seguridad Social o del permiso de conducir, la dirección postal o los datos de las tarjetas de crédito. A veces también se incluía en esta categoría información menos confidencial, como el código postal, la dirección IP o los nombres de usuario. Con el paso del tiempo, su huella digital, es decir, los datos que deja tras de sí al navegar por Internet, podría incluir algunos de ellos.

Bitdefender Digital Identity Protection es su camino hacia la libertad online, que le permite recuperar el control de su vida digital. Además, solo le pregunta su nombre, la dirección de correo electrónico que emplee más habitualmente y su número de teléfono. En base a estos datos, busca en la Internet pública y en la oscura información personal que le pertenezca y haya podido verse expuesta públicamente.

Bitdefender Digital Identity Protection ofrece lo siguiente:

- **Servicios de monitorización y detección:** Monitoriza más de cien datos de carácter personal, como el número de la Seguridad Social, las tarjetas de crédito o su domicilio, y muestra todos los datos encontrados en relación con su presencia online.

  > **Nota**
  > Bitdefender no almacena ni procesa información de carácter personal. Únicamente se conservan las referencias a posibles vulneraciones, sin incluir datos confidenciales.

- **Alertas en tiempo real:** Recibe notificaciones sobre vulneraciones y datos expuestos en la Internet oscura, información de carácter personal presente en la Internet pública y personas que puedan estar suplantando su identidad en las redes sociales.

- **Soluciones:** Nuestro servicio sugiere medidas claras para resolver los problemas y le recuerda si algún problema no se ha acabado de resolver. Asimismo, puede proporcionar instrucciones sobre cómo eliminar los anuncios personalizados, exportar sus datos o desactivar el rastreo.

2. PRIMEROS PASOS

2.1. Active Digital Identity Protection

Active la suscripción a Bitdefender Digital Identity Protection después de realizar y abonar su pedido.

1. Abra el correo electrónico de confirmación que recibió poco después de realizar su pedido y haga clic en **PUESTA EN MARCHA**.
2. Se le redirigirá a https://central.bitdefender.com.
   Inicie sesión con su cuenta de Bitdefender Central. Si aún no dispone de ella, puede crear una aquí.
3. Tras iniciar sesión, la suscripción se añadirá automáticamente a su cuenta de Central y se pondrá en marcha el proceso de incorporación.

Como alternativa:

- acceda al panel **Mis suscripciones** desde Central, a la izquierda de la ventana, y haga clic en **+ Activar con código**.
- escriba la clave de diez dígitos que hallará en su correo electrónico de confirmación y pulse **ACTIVAR**.
- si se le solicita, seleccione cómo quiere usar el código y, luego, haga clic en **ACTIVAR**.

2.2. Configurar Digital Identity Protection

1. Acceda a https://central.bitdefender.com/ e inicie sesión en su cuenta.
   Si aún carece de ella, haga clic en **CREAR CUENTA** y, a continuación, escriba su nombre completo, una dirección de correo electrónico y una contraseña.
2. Seleccione el panel de Digital Identity Protection.
   Aparece una pantalla de bienvenida.
3. Haga clic en **EMPEZAR**.
4. Ahora, se le informará de qué datos debe proporcionar. Sus datos siempre estarán cifrados y a salvo.
   Haga clic en **SIGUIENTE**.

5. Escriba su nombre y apellidos en los campos correspondientes y, a continuación, haga clic en **SIGUIENTE**.
6. Escriba su dirección de correo electrónico y, a continuación, haga clic en **SIGUIENTE**.
   Asegúrese de introducir una dirección de correo electrónico válida a la que tenga acceso.
7. Se le enviará un código de seguridad a la dirección que proporcione.
   Abra el correo electrónico, copie el código y péguelo en el campo correspondiente.
   A continuación, haga clic en **COMPROBAR**.
8. Seleccione su país, introduzca su número de teléfono y, luego, haga clic en **SIGUIENTE**.
9. Poco después debería recibir un código de seguridad.
   Introduzca el código y, a continuación, seleccione **COMPROBAR**.
10 Una vez realizada la comprobación inicial, haga clic en **FINALIZAR**.
.

> **Nota**
> En caso de que durante esta primera comprobación se descubra alguna vulneración, datos de carácter personal o posibles intentos de suplantación de su identidad, se le informará de ello.

Bitdefender Digital Identity Protection ya está configurado.

2.3. Revisar su huella digital, vulneraciones de datos y posibles suplantaciones

Tras finalizar la configuración, Bitdefender Digital Identity Protection lleva a cabo una comprobación online para descubrir posibles suplantaciones, vulneraciones de datos e información de carácter personal en la Internet pública. Le recomendamos que revise toda la información incluida en las pestañas **HUELLA DIGITAL**, **VULNERACIONES DE DATOS** y **COMPROBACIÓN DE SUPLANTACIÓN**.

- Revisión de su huella digital (página 10)
- Revisión de las vulneraciones de datos (página 11)
- Revisión de posibles suplantaciones (página 12)

2.4. Mejore su comprobación

Usamos los datos que nos proporciona para monitorizar la Internet pública y la oscura con el fin de detectar cualquier actividad que pueda afectar a su privacidad o a su reputación personal.

Si desea añadir otra dirección de correo electrónico o número de teléfono, haga clic en ⊕ y, a continuación, haga clic en **AÑADIR DIRECCIÓN DE CORREO ELECTRÓNICO** o **AÑADIR NÚMERO DE TELÉFONO** y siga las instrucciones.

3. PANEL DE CONTROL

El panel añade información incluida en las pestañas **HUELLA DIGITAL**, **VULNERACIONES DE DATOS** y **COMPROBACIÓN DE SUPLANTACIÓN**.

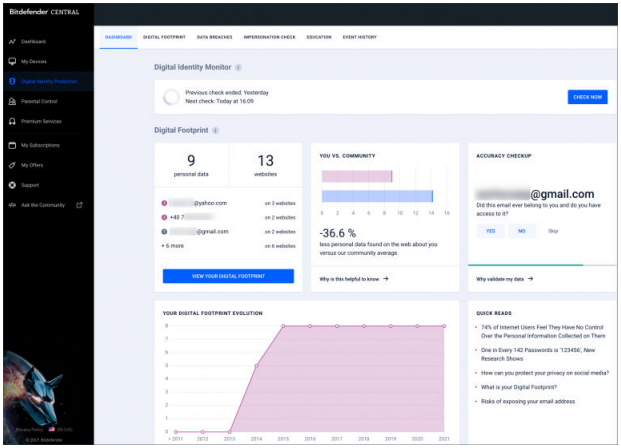
Incluye lo siguiente:

- Sus datos expuestos y sus fuentes web
- La media de datos expuestos en toda la comunidad
- La evolución de su huella digital
- Contenido relacionado con la privacidad
- Vulneraciones de datos
- La media de vulneraciones de datos en la comunidad

3.1. Monitor de identidad digital

Utilizando solo información precisa, el sistema de Bitdefender busca nuevos datos de carácter personal expuestos en la Internet pública y la oscura y analiza las principales plataformas de redes sociales en busca de señales de un intento de suplantación.

Haga clic en **COMPROBAR AHORA** para realizar un análisis online.



4. HUELLA DIGITAL

Aquí aparecen su información de carácter personal y sus fuentes. Depende de usted evaluar si el hecho de tener información pública en la web supone una amenaza.

Nuestro monitor basado en inteligencia artificial depende en gran medida de los datos correctos para detectar nuevas amenazas. Por favor, indíquenos si la información es exacta o no.

Una vez que confirme que un dato es suyo, lo añadimos a nuestro sistema de monitorización y mejoramos las posibilidades de descubrir otros en el futuro.

4.1. Revisión de su huella digital

Para revisar su huella digital:

1. Acceda a la pestaña **HUELLA DIGITAL**.
2. La información que aún no se haya verificado aparecerá con el texto **Verificar** a la derecha. Haga clic en **Verificar** y, a continuación, seleccione Sí o No, según el caso.

> **Nota**
> Los datos confirmados se añaden a nuestro algoritmo de monitorización, lo que mejora los resultados que ofrecen nuestros servicios. La información que se descarte dejará de mostrarse. No obstante, seguirá estando disponible en la web.

5. VIOLACIONES DE DATOS

Las vulneraciones se producen cuando los piratas informáticos logran eludir las medidas de seguridad de una empresa y obtienen su información de carácter personal para venderla en la Internet oscura. Por lo general, los delincuentes informáticos buscan datos de inicio de sesión, información de carácter personal, historiales médicos y datos financieros.

Cualquier organización o servicio puede sufrir una vulneración de datos, pero los que tienen una gran base de clientes son objetivos más atractivos. Dichas vulneraciones suelen incluir nombres, direcciones de correo electrónico, nombres de usuario, contraseñas, direcciones postales, números de teléfono, números de la Seguridad Social (SSN) y datos de tarjetas de crédito (número, fecha de vencimiento y CVV).

5.1. Revisión de las vulneraciones de datos

Para revisar sus vulneraciones de datos:

1. Acceda a la pestaña **VULNERACIONES DE DATOS**.
2. Debajo de algunos elementos, hallará una lista de las medidas necesarias para proteger su cuenta. Tras aplicar alguna de estas medidas, haga clic en la casilla que hay junto a ella para confirmar que lo ha hecho.
   Si no está seguro de cómo llevar a cabo una tarea, siempre puede hacer clic en el enlace que incluye su descripción para acceder a una página donde podrá ver todos los pasos necesarios.
   No todas las vulneraciones pueden abordarse así. Para algunas, como la denominada **Collection #1**, no se le proporcionarán pasos. En vez de eso, se le redirigirá a artículos disponibles en Internet donde podrá encontrar más ayuda.

> **Nota**
> Bitdefender no almacena ni procesa información de identificación personal. Solo se conservan las referencias a posibles violaciones de datos, sin incluir datos sensibles.

6. COMPROBACIÓN DE SUPLANTACIÓN

Los delincuentes especializados en “pretextar” manejan el arte de la suplantación de identidad de diversas maneras y desempeñan el papel de alguien de confianza para engañar a sus víctimas y obtener información confidencial. Por “pretextar” se entiende presentarse como otra persona para manipular a un tercero con el fin de que le proporcione datos confidenciales, como contraseñas, números de tarjetas de crédito o cualquier otra información confidencial.

Bitdefender Digital Identity Protection monitoriza 25 plataformas de redes sociales y le notifica de inmediato si encuentra un perfil que pueda ser un intento de suplantación.

6.1. Revisión de posibles suplantaciones

En la pestaña **COMPROBACIÓN DE SUPLANTACIÓN** se mostrarán todos los posibles intentos. Por cada detección, puede optar entre las siguientes posibilidades:

- Es un intento de suplantación
- Es su propio perfil
- Es un perfil diferente

Dependiendo de su elección, Bitdefender Digital Identity Protection le recomendará pasos concretos para solucionar el problema. Cada vez que complete un paso, puede marcarlo como **Hecho**.

7. EDUCACIÓN

La pestaña Educación actúa como una base de conocimientos donde el usuario puede encontrar más información para proteger su identidad digital.

Los artículos que incluye pueden clasificarse en varias categorías:

- vulneraciones
- Exposiciones
- Comprobación de suplantación de identidad

Para acceder a la versión completa de un artículo, haga clic en su enlace **Más información**.

8. HISTORIAL DE EVENTOS

La sección Historial de eventos es la forma de comunicarnos constantemente con nuestros usuarios. Constituye una lista de eventos ordenados cronológicamente relativos a la protección de su identidad digital.

Aparte de por las amenazas recientemente detectadas (si las hubiera), puede regresar a esta página para obtener valiosos consejos sobre cómo actuar correctamente online para aumentar sus posibilidades de evitar los problemas de privacidad.

En la sección Historial de eventos puede encontrar la siguiente información:

- Acciones realizadas
- Actualizaciones del servicio
- Violaciones de datos

9. PREGUNTAS FRECUENTES

¿Por qué es tan importante la privacidad online actualmente?

La privacidad online significa proteger sus datos personales y económicos contra los delincuentes informáticos. Esa información de carácter personal posee un gran valor en Internet y, en cuanto se filtran esos datos, su dinero deja de estar a salvo. Necesitará un servicio fiable para la continua protección y monitorización de la identidad con el fin de asegurarse de que sus datos confidenciales se siguen manteniendo en privado.

¿Cuál es mi huella digital?

Su huella digital es toda su actividad online. Sus inicios de sesión en las redes sociales, sus transacciones bancarias, todo lo que compra online puede verse expuesto a una vulneración de datos. Ha de conocer en todo momento cómo se almacenan y gestionan sus datos personales y económicos y adoptar las medidas necesarias para protegerlos.

¿Qué son las vulneraciones de datos y cómo afectan a mis cuentas personales?

Las vulneraciones de datos son incidentes de seguridad que filtran datos privados a entornos poco fiables. Delincuentes informáticos de todo el mundo pueden aprovecharse de ellos para obtener acceso a su identidad online. Las vulneraciones de datos pueden afectar a su puntuación crediticia, su seguro de salud, sus fondos o incluso su plan de pensiones.

¿Cómo puede contribuir Bitdefender Digital Identity Protection a mi privacidad online?

Bitdefender Digital Identity Protection monitoriza continuamente su información personal y le envía alertas en tiempo real en caso de detectar una vulneración. Así podrá cambiar sus contraseñas y proteger sus cuentas para evitar pérdidas económicas o que suplanten su identidad en las redes sociales.

¿Dónde busca los datos Bitdefender Digital Identity Protection?

Bitdefender Digital Identity Protection busca los datos en la Internet pública (redes sociales, publicaciones, blogs, foros, corredores de datos, publicaciones, bases de datos sin conexión), pero también en la Internet oscura, donde los delincuentes informáticos comercian con la información recopilada en las vulneraciones de datos.

¿En qué se diferencia Bitdefender Digital Identity Protection de otros servicios (gratuitos)?

Bitdefender Digital Identity Protection tiene una capacidad sin igual para monitorizar la Internet oscura en busca de volúmenes considerables de datos de mayor calidad. La información de la Internet oscura se selecciona y se eliminan duplicidades para poder reducir las alertas de falsos positivos.

¿Cómo puedo usar el servicio? ¿Tengo que descargar algo?

Como Bitdefender Digital Identity Protection es un servicio online, no hace falta que descargue nada. Obtendrá acceso a un panel en la web desde el cual podrá monitorizar todas sus cuentas personales en tiempo real.

¿Cómo puedo recibir alertas sobre futuras vulneraciones de datos?

Para recibir alertas sobre futuras vulneraciones de datos, basta con que se registre en su panel web para recibir alertas por correo electrónico. A partir de ese momento, empezará a recibir alertas sobre la privacidad e informes de seguridad de Bitdefender Digital Identity Protection.

10. OBTENIENDO AYUDA

10.1. 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.

10.2. 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.

10.2.1. 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/.

10.2.2. 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

10.2.3. 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/.

10.3. 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 17).

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

10.3.1. 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.