Los teléfonos Android vía de entrada de ciberataques

1. Código malicioso, ataques contra el derecho a la intimidad, filtración de documentos confidenciales, destrucción de datos..., son sólo algunos de los incidentes frente a los que te protege BOTECH Android Forensics Analytics

2. En tan solo 5 minutos conocerás el estado de tu dispositivo y sus vulnerabilidades con esta aplicación gratuita disponible en Play Store

Introducción

Es innegable que los teléfonos móviles son un elemento imprescindible en nuestro día a día y es que ya nadie puede pasar un día entero sin consultar su dispositivo. Android se ha convertido en el sistema operativo líder a nivel mundial y con él operan el 72% de los terminales. En la actualidad 9 de cada 10 dispositivos tienen el sistema operativo de Google. 1.300 fabricantes, 24.000 modelos, más de 2.000 millones de dispositivos en todo el mundo, ha convertido a Android en un objetivo prioritario para los ciberdelincuentes para acceder a información tanto profesional como personal.

Cada vez es más habitual que aplicaciones tan comunes como las linternas, las meteorológicas y los juegos online sean las vías de entrada de diferentes tipos de malware en los terminales. Los ciberdelincuentes saben que cada día, crece el número de personas que sustituyen su ordenador por su teléfono móvil o tablet y cualquier vía de acceso es buena. En BOTECH hemos convertido la innovación constante en una obligación para estar a la vanguardia de la seguridad en lo que a temas de fraude se refiere.

En este panorama, de amenazas sofisticadas y en constante crecimiento, es donde toma especial relevancia nuestra app Android Forensics Analytics.

info@botechfpi.com

Pero ¿qué es Android Forensics Analytics de BOTECH?

La aplicación Android Forensics Analytics, disponible gratuitamente en Play Store, realiza un rápido análisis del dispositivo Android y permite saber si ha estado expuesto a un ataque o vulnerabilidad. BOTECH Android Forensics Analytics se convierte en un servicio imprescindible para las organizaciones ofreciendo información sobre la procedencia de los incidentes para tomar las medidas de precaución necesarias y evitar futuros ataques que puedan afectar a la organización, tanto a nivel económico como reputacional.

¿Cuándo se debe utilizar la app Android Forensics Analytics?

- Regularmente, ya que las revisiones regulares de los dispositivos de la compañía evitarán incidentes y por tanto pérdidas económicas y de imagen.
- Siempre que detectemos que las aplicaciones y utilidades del sistema operativo están teniendo un comportamiento anómalo.

Una aplicación cuya información te permite tomar medidas y protegerte frente a:

- **Incidentes de código malicioso**
- **Incidentes por uso inapropiado**
- **Comportamientos anómalos de los sistemas**
- **Futuros ataques**
- **Ataques contra el derecho a la intimidad**
- **Fraude informático**
- **Incidentes de acceso no autorizado**
- **Filtración de documentos confidenciales**
- **Ataques contra la propiedad intelectual**
- **Destrucción de datos**
- **Sabotajes informáticos**

info@botechfpi.com

Exactamente ¿qué se analiza en mi dispositivo? ¿Cómo se me comunica el resultado?

BOTECH Android Forensics Analytics no sólo ve y analiza lo que tiene el dispositivo, sino todas las conexiones relacionadas con el mismo y las clasifica en diferentes secciones.

Tras el análisis, la aplicación envía vía email un informe en el que se otorga un score, o puntuación de riesgo, sobre el estado del terminal para mostrar la seguridad del mismo: High Risk, Medium Risk, Low Risk y No Risk.

Secciones de análisis

Device Information – Enviroment

Cambios hechos por el usuario a nivel de permisos y opciones en el sistema operativo.

Conexiones Wifi no seguras

Obtiene la lista de conexiones WIFI y determina las que usan un tipo de cifrado débil.

Leaks de las cuentas configuradas en el dispositivo

Obtiene todos los emails de las cuentas configuradas en el dispositivo y determina si las cuentas están comprometidas en leaks públicos y privados.

User Certificates

Obtiene la lista de procesos que están corriendo actualmente en el terminal.
Comprueba los certificados de seguridad presentes en el dispositivo y alerta si alguno es posiblemente malicioso.

Localización de aplicaciones instaladas infectadas

Revisa todas las aplicaciones del dispositivo, su versión y si pueden ser posiblemente dañinas.

Localización de archivos descargados infectados

Archivos descargados por el usuario potencialmente peligrosos

Apps con permisos peligroso

Obtiene las apps que hacen de administradores del dispositivo y alerta sobre las no comunes.
Detección de keyloggers.

Malicious connections

Obtiene la lista de conexiones del dispositivo de las apps.
Detección de proxys peligrosos.

CONTACT US

www.botechfpi.com

info@botechfpi.com