AXAN BY BOTECH

AXAN, innovación tecnológica para la seguridad de los dispositivos Android, Windows y Linux

- **Accesos no autorizados, destrucción de datos, código malicioso, sabotajes informáticos, comportamientos anómalos de los sistemas..., son sólo algunos de los incidentes frente a los que protege AXAN**
- **Solo 3 horas para conocer en profundidad el estado de tu dispositivo y sus vulnerabilidades**

Introducción

La tecnología se ha convertido es algo imprescindible en nuestro día a día y es que ya nadie puede pasar un día entero sin conectarse a la red ya sea a través de su dispositivo móvil, su ordenador o su tablet. Esta hiperconectividad, y esta dependencia de la Red, ha convertido a todos estos dispositivos en un objetivo prioritario para los ciberdelincuentes que los han convertido en su vía de entrada para acceder a información tanto profesional como personal.

La tecnología avanza sin descanso en 2 sentidos: hacia la innovación para mejorar en el desarrollo de nuestra sociedad, y, por otro lado, hacia la sofisticación de la ciberdelincuencia, como consecuencia de la proliferación de dispositivos conectados a la red en los últimos años. Por este motivo, 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 AXAN.

Pero ¿qué es AXAN?

Se trata de un análisis en profundidad a través del cual se puede saber si un dispositivo ha estado expuesto a un ataque o vulnerabilidad y que permite tomar las medidas oportunas para evitar incidentes futuros. AXAN se convierte en un servicio imprescindible para las organizaciones. Un servicio que combina tecnología puntera con un equipo de expertos internacionales en análisis forense, para ofrecer información sobre la procedencia de los incidentes, algo que permite tomar las medidas de precaución necesarias para evitar futuros ataques que puedan afectar a la organización, tanto a nivel económico como reputacional.

AXAN, innovación tecnológica para la seguridad de los dispositivos Android, Windows y Linux

Este estudio en profundidad, que dura aproximadamente 3 horas, unifica la tecnología más vanguardista con el equipo de expertos de BOTECH. Una unión que permite conocer si un terminal ha estado expuesto a un ataque o vulnerabilidad y tomar las medidas oportunas para evitar incidentes futuros. Una tecnología puntera que nos da la oportunidad de conocer el tipo de malware, cómo ha entrado y el origen de ese ataque para estudiarlo en profundidad y evitar incidentes a los que seguro que nos enfrentaremos ya que solo **en 2019 el malware se incrementó casi un 14%.**

¿Cuándo se debe hacer este análisis en profundidad?

- 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.

- Cuando creamos que las cuentas corporativas de la compañía pueden estar comprometidas y ser

Realizar un análisis forense remoto permite proteger al equipo frente:

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

Además, en caso de un procedimiento judicial ante el ataque, el informe realizado en el forense remoto puede ser utilizado como evidencia.

¿Cómo se realiza un forense remoto con AXAN? ¿Puedo disponer mientras se ejecuta de mi terminal?

. 1) Identifica el incidente y recopila evidencias del dispositivo afectado.

2) Es necesario garantizar la cuarentena del equipo hasta que el forense complete el análisis. Es importante no utilizarlo, para conservar las huellas que ha podido dejar el incidente, analizarlo y extraer información que será de gran utilidad para prevenir futuros ataques.

3) Busca y analiza evidencias. Se instala un software proporcionado siempre por el analista que permite obtener todas las evidencias ocultas en el equipo. Cuando la aplicación está instalada, el usuario debe abrirla manualmente y conectar el cargador al dispositivo.

Una vez realizado esto, se realiza una conexión con el servidor forense sin que el usuario tenga que intervenir más. De hecho, es conveniente que el usuario no realice ninguna acción mientras se lleva a cabo el análisis forense que suele durar poco más de 3 horas. No obstante, el dispositivo se encuentra totalmente operativo mientras se realiza el mismo.

. 4) Se elabora un informe forense.

5) Una vez finalizado el proceso basta con desinstalar la aplicación del dispositivo.

Exactamente ¿qué analiza AXAN?

Esta tecnología no sólo ve y analiza los dispositivos Android, Linux y Windows, sino todas las conexiones relacionadas con los mismos y las clasifica en diferentes secciones, otorgando finalmente un score, o puntuación de riesgo, que se clasifica en tres categorías:

High Risk / Medium Risk / Low Risk No Risk

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 peligrosos

- 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
- Obtiene las dns configuradas actualmente en el dispositivo para determinar:
- Obtiene la IP publica que está siendo usada por el dispositivo para determinar la geolocalización.

Si mi dispositivo ya dispone de antivirus ¿por qué me interesaría AXAN?

Además de los malwares más comunes, detectados por los antivirus, esta tecnología rastrea los más sofisticados que suelen pasar inadvertidos ante los sistemas de protección más habituales. Realiza un exhaustivo análisis del terminal y toda esa información, analizada por el equipo de expertos de BOTECH, permite enviar al correo electrónico del usuario un detallado informe que recoge lo que se ha detectado.

CONTACT US

www.botechfpi.com

info@botechfpi.com