IBM MaaS360 Mobile Threat Management

Despídase del malware móvil en los dispositivos iOS y Android

Principales ventajas

- Soporte de BYOD (Traiga su propio dispositivo) y de dispositivos de empresa de forma segura
- Gestione de forma proactiva las amenazas móviles casi en tiempo real
- Reduzca el riesgo de filtración de datos confidenciales que contengan información personales y corporativos
- Tome medidas automatizadas para corregir los riesgos de seguridad móvil

Malware móvil: la próxima gran amenaza para la seguridad

Las organizaciones se están transformando a un ritmo sin precedentes con movilidad. La tendencia BYOD (Traiga su propio dispositivo) se sigue extendiendo en las empresas. Las apps móviles están creando nuevos y eficientes flujos de trabajo para los empleados. El acceso ininterrumpido a datos de trabajo, correos electrónicos y otros contenidos está creciendo en paralelo y aumentando las mejoras de productividad de estas tendencias.

Gracias a la popularidad y a lo rápido que los dispositivos móviles se han convertido en un pilar de las empresas, los hackers y los ladrones están atacando los dispositivos móviles con malware, lo que supone la próxima gran amenaza para la seguridad. Los datos corporativos son especialmente vulnerables a las aplicaciones deshonestas y a los sitios web maliciosos.

- En 2014 se descargaron más de 138 000 millones de aplicaciones.[1]
- El malware móvil está creciendo. Los códigos maliciosos infectan más de 11,6 millones de dispositivos móviles en cualquier momento dado.[2]
- Los recientes ataques de WireLurker y Masque amenazan a los dispositivos iOS.[3,4]
- El daño a la imagen de una empresa se puede agravar por la pérdida financiera. El coste de una sola brecha está estimado en más de 11 millones de dólares.[5]

Los líderes de TI y seguridad necesitan una solución de seguridad moderna y sólida para detectar, analizar y solucionar de manera proactiva el malware móvil.

Detenga las amenazas móviles en su empresa

IBM® MaaS360® Mobile Threat Management ofrece un sistema de última generación para la protección contra el malware en dispositivos iOS y Android. Puede detectar riesgos y gestionar amenazas antes de que pongan en peligro sus datos de empresa.

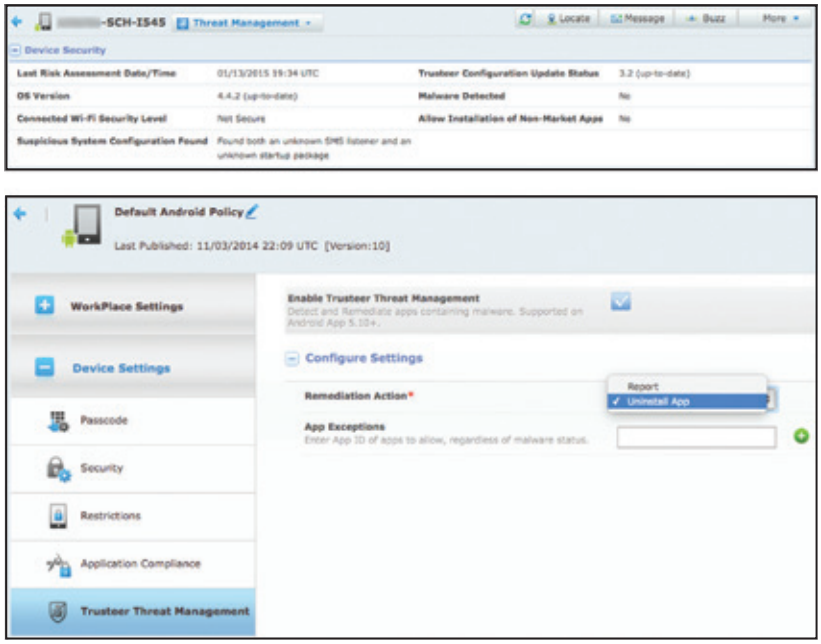

Figura 1: Ejemplos de datos facilitados sobre un dispositivo protegido y la configuración de políticas en MaaS360 Mobile Threat Management

Gracias a la integración con IBM Trusteer®, usado por cientos de millones de usuarios para proteger organizaciones contra el fraude y la filtración de datos, MaaS360 ofrece una nueva capa de seguridad a la gestión de la movilidad empresarial (EMM).

No permita que el malware arruine la transformación móvil de su organización. Equilibre las iniciativas de productividad de su empresa con la seguridad que le proporciona MaaS360.

Detección y corrección de malware móvil

- Detecte y analice apps de iOS y Android con firmas de malware y comportamiento malicioso desde una base de datos actualizada continuamente
- Añada excepciones de apps para personalizar un uso de apps aceptable
- Establezca controles de política granulares para realizar las acciones necesarias
- Utilice un motor de reglas de cumplimiento casi en tiempo real para automatizar las reparaciones
- Avise al usuario y a las partes responsables cuando se detecte malware
- Vea los dispositivos comprometidos en el panel My Alert Center y los eventos de detección en el panel My Activity Feed
- Desinstale aplicaciones con malware automáticamente (para seleccionar dispositivos Android como el Samsung SAFE™)
- Bloquee el acceso de manera selectiva o limpie totalmente los dispositivos
- Restrinja el uso de las soluciones de contenedor de MaaS360
- Recopile y vea atributos de amenazas del dispositivo como:
  - Malware detectado
  - Configuraciones del sistema sospechosas encontradas, como un receptor de SMS o un paquete de arranque desconocido
  - Conexión a un punto de acceso Wi-Fi no seguro
  - Instalación de apps no comercializadas permitida
  - Versión del sistema operativo
- Revise el historial de auditoría de los eventos de detección de malware

Detección adicional de dispositivos rooteados y liberados

- Detecte dispositivos móviles en peligro o vulnerables
- Protéjase contra dispositivos iOS liberados y dispositivos Android rooteados que pueden proporcionar a los atacantes privilegios adicionales sobre los sistemas operativos
- Descubra ocultadores y técnicas de ocultación activas que intentan enmascarar la detección de dispositivos liberados y rooteados
- Use la lógica de detección actualizada con OTA sin actualizaciones de apps para responder mejor a los rápidos hackers
- Establezca políticas de seguridad y reglas de cumplimiento para automatizar las reparaciones
- Bloquee el acceso de manera selectiva o limpie totalmente los dispositivos

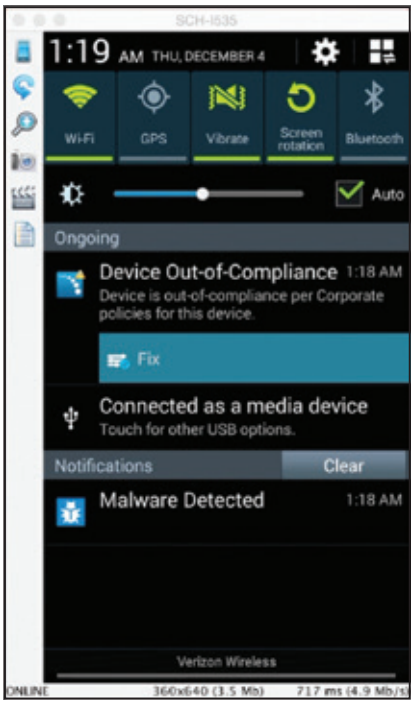

Figura 2: Ejemplo de una notificación de malware en un dispositivo

IBM Security Trusteer Mobile Risk Engine

- Ofrece capas de protección e inteligencia de ciberdelincuencia para una protección adaptada contra el malware
- Detecta y se adapta rápidamente a los comportamientos de ataques más avanzados para que el malware tenga virtualmente cero oportunidades de cometer fraude
- Realiza una evaluación del riesgo móvil casi en tiempo real basada en los factores de riesgo de dispositivos y apps
- Se actualiza continuamente para ofrecer las comprobaciones más avanzadas de malware y de dispositivos rooteados y liberados

Para obtener más información sobre las soluciones de prevención del fraude de IBM Security, póngase en contacto con su representante o Business Partner de IBM, o bien visite el siguiente sitio web: **ibm.com**/security.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Creado en EE. UU.
Enero de 2016

Por favor, recicle

1 Informe anual de Arxan: "*State of Mobile App Security Reveals an Increase in App Hacks for Top 100 Mobile Apps*", Noviembre de 2014, Arxan Technologies, Inc., https://www.arxan.com/2014/11/17/arxans-annual-report-state-of-mobile-app-security-reveals-an-increase-in-app-hacks-for-top-100-mobile-apps/

2 Informe sobre malware de Kindsight Security – 4.º trimestre 2013, Alcatel-Lucent, http://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2014/9861-kindsight-security-labs-malware-report-q4-2013.pdf

3 Xiao, Claud, WireLurker: A New Era in OS X and iOS Malware, entrada de blog en Palo Alto Networks; 5 de noviembre de 2014, http://researchcenter.paloaltonetworks.com/2014/11/wirelurker-new-era-os-x-ios-malware/

4 Zue, Hui, Wei, Tao and Zhang, Yulong; Masque Attack: All Your iOS Apps Belong to Us, 10 de noviembre de 2014, https://www.fireeye.com/blog/threat-research/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html

5 2013 Cost of Cyber Crime Study: United States, Patrocinado por HP Enterprise Security, Ponemon Institute, Octubre de 2014, http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf