IBM MaaS360 Mobile Threat Management

Impida el ingreso de "malware" móvil en los dispositivos iOS y Android

Principales ventajas

- Soporta con seguridad tanto los dispositivos BYOD como los de propiedad corporativa
- Gestione proactivamente las amenazas móviles en tiempo casi real
- Reduzca el riesgo de filtraciones de datos sensibles de información corporativa y personal
- Aplique acciones automatizadas para anular los riesgos de seguridad móvil

"Malware" móvil – la próxima gran amenaza de seguridad

Las organizaciones están siendo transformadas a una velocidad sin precedentes mediante la movilidad. La tendencia Traiga Su Propio Dispositivo (BYOD, por sus siglas en inglés) continúa expandiéndose en las empresas. Las aplicaciones móviles están creando nuevos y eficientes flujos de trabajo para los empleados. Paralelamente, está creciendo el acceso sin problemas a datos de trabajo, correo electrónico y contenidos, reforzando los incrementos de productividad de estas tendencias.

Como resultado de la popularidad y la velocidad con las que los dispositivos móviles se han convertido en un pilar de la empresa, los "hackers" y ladrones están apuntando a los dispositivos móviles con "malware", creando la siguiente gran amenaza de seguridad. Los datos corporativos son especialmente vulnerables a las aplicaciones delictivas y a los sitios web maliciosos.

- En 2014 se descargaron 138.000 millones de aplicaciones.[1]
- El "malware" móvil está creciendo. Los códigos maliciosos están infectando más de 11,6 millones de dispositivos móviles a cada instante.[2]
- Recientes ataques de WireLurker y Masque amenazan a los dispositivos iOS.[3,4]
- El daño a la marca de una compañía se ve agravado por las pérdidas financieras, por lo que el costo de una sola violación se estima en más de $11 millones.[5]

Los líderes de TI y Seguridad necesitan una solución de seguridad moderna y robusta para detectar, analizar y remediar proactivamente el "malware" móvil.

Detenga las amenazas móviles en su empresa

IBM® MaaS360® Mobile Threat Management entrega un sistema de avanzada para protección contra "malware" en dispositivos iOS y Android. Usted podrá detectar riesgos y gestionar las amenazas antes de que comprometan los datos de su empresa.

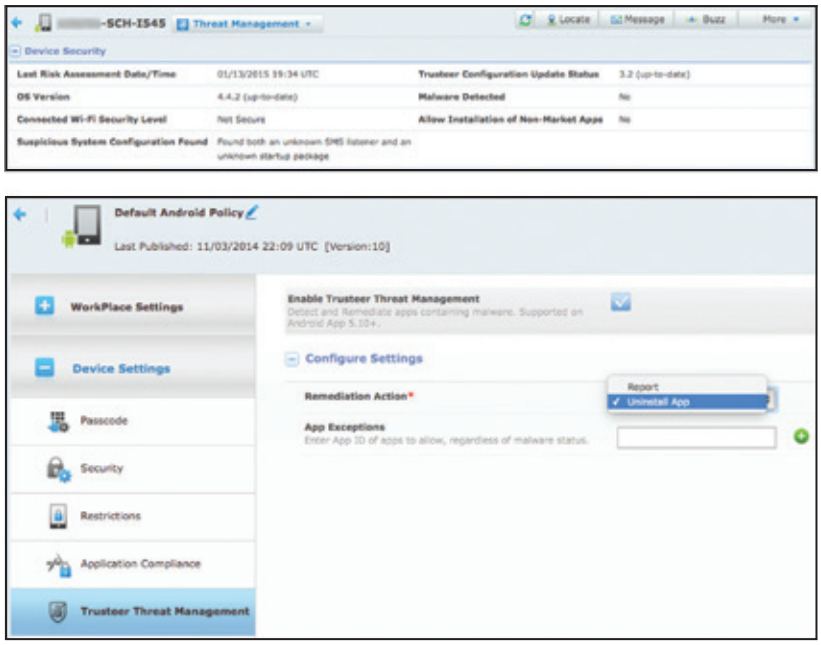

Figura 1: Ejemplos de datos informados sobre un dispositivo protegido y los ajustes de políticas en MaaS360 Mobile Threat Management

Mediante la integración con IBM Trusteer®, usado por cientos de millones de usuarios para proteger a las organizaciones contra el fraude y las violaciones de datos, MaaS360 proporciona una nueva capa de seguridad a la Administración de Movilidad Empresarial (EMM, por sus siglas en inglés).

No permita que el "malware" desbarate la transformación móvil de su organización. Equilibre las iniciativas de productividad de su empresa con la seguridad que entrega MaaS360.

Detección y remediación de "malware" móvil

- Detecte y analice las aplicaciones para iOS y Android que tengan firmas de "malware" y comportamiento malicioso desde una base de datos permanentemente actualizada
- Agregue excepciones de aplicaciones para personalizar el uso de aplicaciones aceptables
- Establezca controles de política granular para tomar las medidas adecuadas
- Use un motor de reglas de cumplimiento en tiempo casi real para automatizar la remediación
- Alerte al usuario y las partes responsables cuando se detecte "malware"
- Visualice los dispositivos comprometidos y los eventos de detección en los tableros My Alert Center (Mi centro de alertas) y My Activity Feed (Mi fuente de actividad), respectivamente
- Desinstale aplicaciones con "malware" automáticamente (para dispositivos Android selectos tales como Samsung SAFE™)
- Bloquee el acceso, de manera selectiva o limpie totalmente los dispositivos
- Restrinja el uso de soluciones de contenedores en MaaS360
- Recopile y visualice atributos de amenazas de dispositivos, incluyendo:
  - "Malware" detectado
  - Configuraciones de sistemas sospechosas halladas, tales como un oyente SMS desconocido o un paquete de inicio
  - Conexión a un "hot spot" de Wi-Fi inseguro
  - Autorización para instalar aplicaciones que no son de mercado
  - Versión de sistema operativo
- Revise el historial de auditoría de eventos de detección de "malware"

Detección suplementaria de "jailbreak" (liberación) y "root" (modificación)

- Detecte dispositivos móviles comprometidos o vulnerables
- Protéjase contra dispositivos iOS liberados y Android modificados que puedan brindar a los atacantes privilegios adicionales en los sistemas operativos
- Descubra a los "hiders" (escondedores) y técnicas de "hiding" (ocultamiento) que tratan de enmascarar la detección de dispositivos liberados y modificados
- Use lógica de detección con actualización aérea sin actualizaciones de aplicaciones para tener una mejor respuesta ante "hackers" rápidos
- Establezca políticas de seguridad y reglas de cumplimiento para automatizar la remediación
- Bloquee el acceso, de manera selectiva o limpie totalmente los dispositivos

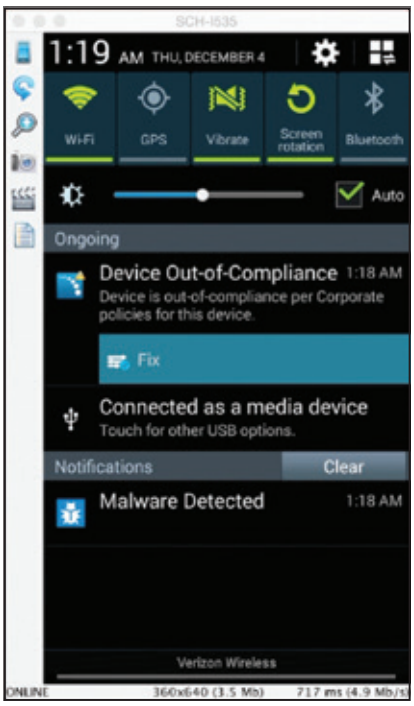

Figura 2: Ejemplo de una notificación de "malware" en un dispositivo

IBM Security Trusteer, Motor de riesgo móvil

- Proporciona capas de protección e inteligencia contra el ciberdelito para prevención adaptiva de "malware"
- Detecta rápidamente y se adapta a los últimos comportamientos de ataque, por lo que el "malware" tiene virtualmente cero oportunidad de cometer el fraude
- Realiza una evaluación de riesgo móvil en tiempo casi real, basándose en factores del dispositivo y riesgos de la aplicación
- Se actualiza continuamente para proveer las últimas verificaciones de "malware", "jailbreak" y "root"

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

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Creado en los Estados Unidos de América
Enero de 2016

Por favor, recicle

1 Informe anual de Arxan: "*El estado de seguridad de aplicaciones móviles revela un incremento en ataques de hackers para las 100 primeras aplicaciones móviles*", noviembre 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 Kindsight Security Labs Malware Report (Informe de "malware" de Kindsight Security Labs) – Cuarto trimestre de 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: Una nueva era en "malware" de OS X y iOS, publicación en blog de 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 y Zhang, Yulong; Ataque de Masque: Todas sus aplicaciones iOS nos pertenecen, 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 Estudio 2013 sobre el costo del ciber-delito: Estados Unidos, auspiciado por HP Enterprise Security, Ponemon Institute, octubre de 2014, http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf

WGD03057-COES-01