IBM Security
Folleto acerca del Liderazgo Intelectual

La Movilidad es el Nuevo Entretenimiento de los Ladrones

Cómo protegerse del malware móvil

IBM

La movilidad avanza y las amenazas le siguen los pasos

Introducción

La movilidad está transformando a las empresas a una velocidad sin precedentes con la continua proliferación de dispositivos inteligentes, el vertiginoso desarrollo de aplicaciones móviles y el mayor acceso a archivos de trabajo. Las organizaciones permiten a sus empleados ser más productivos en casi cualquier momento y lugar, gracias a la implementación de políticas para "Traiga su Propio Dispositivo" (Bring Your Own Device – BYOD) y al otorgamiento de permisos para utilizar aplicaciones personales para actividades laborales.

Sin embargo, las organizaciones no han seguido el ritmo de esta increíble expansión y no han implementado la seguridad a nivel empresarial necesaria para proteger su información confidencial. Los piratas informáticos y los ladrones están aprovechando esta oportunidad para ingresar a las redes y obtener datos corporativos confidenciales a partir de los puntos móviles. Los líderes de las áreas de TI y seguridad necesitan una solución de seguridad moderna y sólida para detectar, analizar y resolver de manera proactiva estas amenazas móviles.

Se calcula que unos 16 millones de dispositivos móviles están infectados con malware en un momento dado.

La Expansión Móvil en la Empresa

Las cifras asociadas con el crecimiento de la movilidad son impactantes. Se predijo que en 2014 la cantidad de teléfonos celulares (7,3 miles de millones) excedería el número de personas en el planeta (7 mil millones).[1]

Según Arxan Technologies, 138 mil millones de aplicaciones móviles se descargaron en 2014, y se espera que esta cifra sea casi el doble de 268 mil millones para 2017.[2]

Los primeros catalizadores de esta tendencia móvil fueron los consumidores, quienes adoptaron aplicaciones y dispositivos inteligentes para uso personal. Sin embargo, sin lugar a dudas las empresas se beneficiaron de estas tendencias crecientes. La tendencia BYOD en los lugares de trabajo continúa creciendo, lo que ayuda a las organizaciones a movilizar toda su fuerza de trabajo y ahorrar en costos de contratación y soporte. De hecho, Gartner predice que la mitad de los empleados exigirá BYOD para 2017.[3]

Las aplicaciones móviles están creando flujos de trabajo nuevos y eficientes para los empleados. A su vez, el acceso constante al contenido, los e-mails y los datos del trabajo están creciendo, lo que mejora los niveles de productividad. Las organizaciones están comenzando a pensar en la movilidad en primer lugar para cada uno de sus procesos, lo que ayuda a impulsar aún más el crecimiento de la movilidad en la empresa.

Cuando las Aplicaciones Móviles Atacan

Sin embargo, los piratas informáticos y los ladrones amenazan con arruinar estos importantes avances para la transformación empresarial. Las infecciones en los dispositivos móviles continúan ganando velocidad, con un aumento del 25 % en 2014, comparado con el 20 % de 2013. Se estima que 16 millones de dispositivos móviles están infectados por malware en un momento dado.[4]

El malware móvil es software malintencionado creado específicamente para atacar dispositivos móviles, a expensas de vulnerabilidades de determinados sistemas operativos.

Las consecuencias de una violación de datos pueden ser muy costosas, ya que los daños producidos a la marca de una empresa se pueden combinar con una posible pérdida financiera. El Ponemon Institute calcula que el costo de una única violación fue de USD 3,5 millones en 2014, un aumento del 15 % en relación al año anterior.[5]

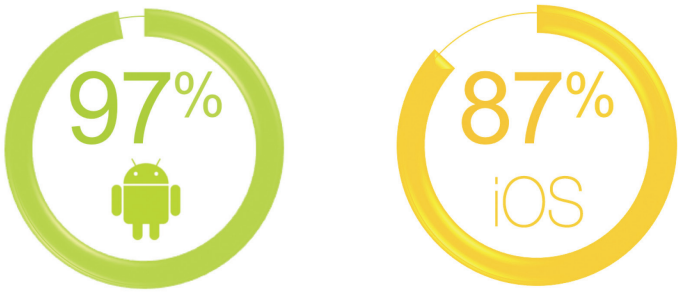

Figura 1: principales aplicaciones pagas para Android e iOS que fueron pirateadas.

Generalmente, los dispositivos en peligro debido a aplicaciones móviles malintencionadas son la principal fuente de riesgo para casi todas las empresas. Cuando los usuarios se conectan a redes inseguras o instalan aplicaciones riesgosas de fuentes no confiables, los dispositivos móviles se vuelven vulnerables al malware, según Arxan Technologies. El 97 % y el 87 % de las principales aplicaciones para Android e iOS pagas, respectivamente, fueron pirateadas y publicadas en tiendas de aplicaciones de terceros.[6]

Según se descubrió en otro estudio de Ponemon Institute[7], inclusive las aplicaciones de organizaciones confiables que se encuentran disponibles en tiendas de aplicaciones tradicionales pueden representar enormes riesgos. El 82 % de los encuestados dijo que las aplicaciones móviles utilizadas en los lugares de trabajo habían aumentado de manera muy significativa (50 %) o de manera significativa (32 %) los riesgos de seguridad. Si bien la mayoría de los empleados son "usuarios activos de aplicaciones" (66 %), más de la mitad (55 %) afirmó que su organización no cuenta con una política que defina el uso aceptable de aplicaciones móviles en el lugar de trabajo.

Solamente el 30 % de los encuestados dijo que sus organizaciones habían implementado una tienda de aplicaciones empresariales, aunque una amplia mayoría (67 %) de los encuestados admitió que si bien tenían una tienda de aplicaciones, los empleados podían usar aplicaciones móviles no verificadas de otras fuentes. Además, el 55 % de las organizaciones dice que se permite a los empleados descargar y utilizar aplicaciones de trabajo de la tienda de aplicaciones empresariales en sus dispositivos personales.

La Situación Actual del Malware Móvil

¿Qué es el malware móvil?

El malware móvil es software malintencionado creado específicamente para atacar dispositivos móviles, a expensas de vulnerabilidades de determinados sistemas operativos.Tres tipos comunes de programas malintencionados son:

- Spyware: espías y ladrones de datos de dispositivos toman determinados tipos de datos y se los entregan a los piratas informáticos para obtener beneficios.
- Troyano: malware que afecta las funciones de las aplicaciones o los dispositivos, realiza transacciones automáticas o inicia comunicaciones sin que el usuario lo perciba.
- Jailbreak o malware raíz: le otorga a los piratas informáticos determinados privilegios administrativos en el dispositivo y acceso a los archivos.

Para comprender mejor la amenaza y por qué se concentra en el punto terminal móvil, analicemos los procesos intelectuales de los ciberdelincuentes. Los dispositivos móviles son uno de los caminos más fáciles para acceder a datos confidenciales. Si bien los sistemas de back-end empresariales están bien protegidos por firewalls, sistemas de prevención de intrusiones y gateways para antivirus, generalmente ni los dispositivos corporativos ni los personales emplean el mismo nivel de protección. Los dispositivos personales (BYOD) son especialmente vulnerables, ya que se encuentran fuera del perímetro y normalmente fuera del control de la organización.

Si los piratas informáticos logran atacar el punto terminal, pueden utilizar el malware para implementar ingeniería social y obtener información de identificación personal (PII) y credenciales. Pueden apropiarse de la cuenta del usuario y beneficiarse de las sesiones autenticadas para reunir datos privados y realizar transacciones ilícitas.

La Preocupación en torno a Android

Android dominó el mercado de los dispositivos móviles con una participación en el mercado del 81,2 % y más de mil millones de dispositivos despachados en 2014, según IDC.[8] Si bien en la actualidad es el líder en el mercado de consumidores, el nivel de adopción en las empresas fue, como mucho, bajo.

La apertura y el diseño base de la plataforma y el ecosistema de la aplicación son el motivo por el cual Android es el sistema operativo más vulnerable a las infecciones de malware de la industria móvil actual.

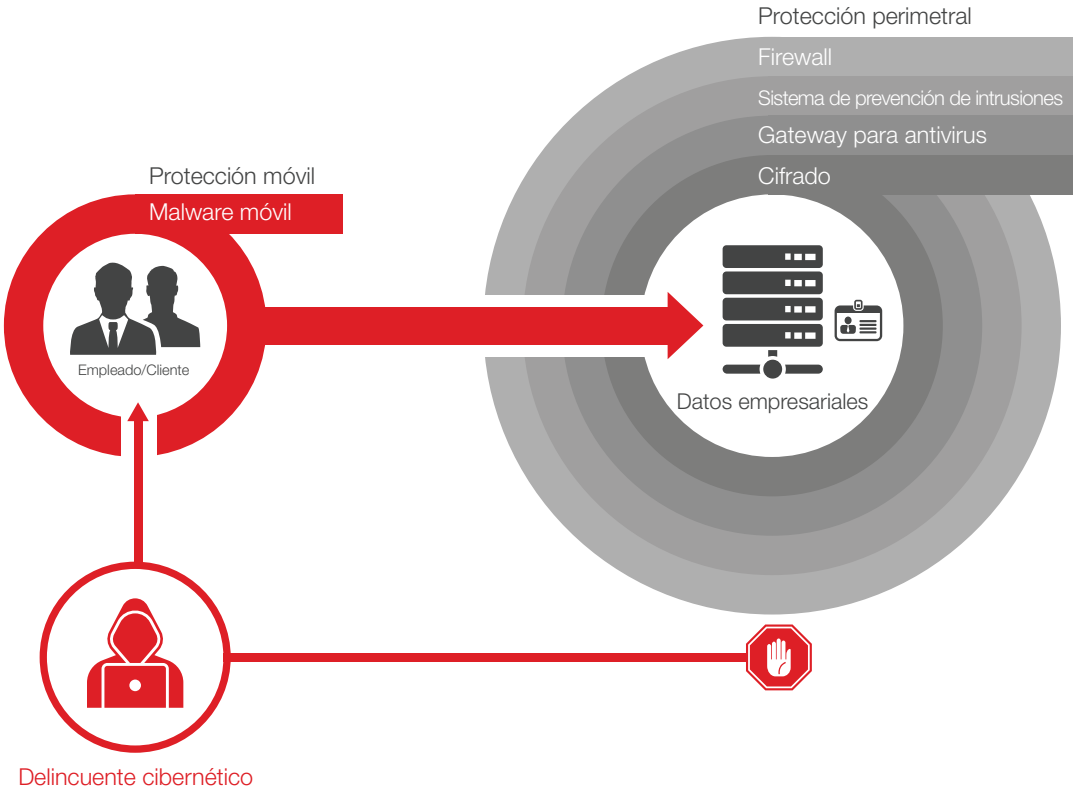

Figura 2: los delincuentes atacan el enlace más débil para acceder a datos confidenciales.

La apertura y el diseño base de la plataforma y el ecosistema de la aplicación son el motivo por el cual Android es el sistema operativo más vulnerable a las infecciones de malware de la industria móvil actual.Las características que tornan a Android el blanco más fácil para los piratas informáticos y los ladrones son las siguientes:

- Las aplicaciones para Android se pueden descargar e instalar a partir de sitios web y tiendas de aplicaciones de terceros.
- Google Play Store no analiza ni aprueba detenidamente cada aplicación, como sí lo hace Apple antes de que una aplicación para iOS se publique en iTunes.
- No existen controles de los certificados digitales para firmar las aplicaciones para Android. Generalmente, estas aplicaciones están autofirmadas y no es posible rastrearlas hasta su desarrollador. Eso facilita piratear una aplicación para Android, introducirle malware y volver a firmarla.

Los ciberdelincuentes están continuamente probando maneras nuevas y creativas de atacar las vulnerabilidades de las plataformas de los sistemas operativos móviles, que son diferentes a los de las PC.

Google implementó prácticas de seguridad para erradicar las aplicaciones malintencionadas en Google Play Store. Examina las aplicaciones a medida que se cargan en la tienda, ejecuta cada aplicación para detectar y eliminar malware, spyware y troyanos. Cuando Google descubre rastros de malware, sus sistemas logran volver a Google Play y eliminar los archivos sospechosos de la tienda. Google también deshabilita las cuentas y aplicaciones de los desarrolladores si violan las políticas de contenido y los términos de la compañía.

Sin embargo, como se mencionó anteriormente, el 97 % de las principales aplicaciones pagas para Android fueron pirateadas y se pueden encontrar en sitios web y tiendas de aplicaciones de terceros. Por ese motivo, si su empleado (o los hijos de él) descarga e instala la aplicación de juegos premium más actualizada de manera gratuita en un dispositivo con Android personal o corporativo de una de estas fuentes no oficiales, es posible que el dispositivo se infecte con malware. Su organización puede implementar políticas y capacitaciones para los usuarios que ayuden a prevenir estas prácticas, pero los dispositivos con Android pueden ser vulnerables sin una capa de protección automática.

Un ejemplo de malware que afecta a Android es SVPENG, un troyano destinado a bancos que se descubrió intentando atacar instituciones financieras europeas y rusas. SVPENG representa un avance importante en el malware móvil. El blanco de este ataque son los usuarios de aplicaciones bancarias móviles, que son engañados para que brinden sus credenciales con una técnica de malware de PC común llamada ataque encubierto.

En este ataque, el malware del dispositivo infectado espera a que el usuario abra la aplicación móvil del banco. Una vez que el malware identifica que se está iniciando una sesión en la aplicación móvil del banco, muestra una pantalla por encima de la aplicación (por ese motivo se llama “encubierto”) que imita la apariencia de la aplicación del banco, pero en realidad es una página falsa. Esto obliga al usuario a interactuar sin saberlo con una página generada por un malware, pensando que es la página verdadera del banco, y brinda sus credenciales.

Ataques encubiertos similares podrían atacar los datos corporativos confidenciales. Un empleado podría, inconscientemente, ingresar las credenciales del trabajo, lo que le brindaría a los ladrones los datos que necesitan para autenticarse en los sistemas empresariales y causar estragos en sus datos.

Recientemente, el IBM X-Force Application Security Research Team descubrió una vulnerabilidad en Dropbox SDK para Android que permite a los atacantes conectar aplicaciones en dispositivos móviles a una cuenta de Dropbox controlada por el intruso sin la autorización ni el conocimiento de la víctima.[9] Esta vulnerabilidad, llamada DroppedIn, se puede utilizar de dos maneras a través de una aplicación malintencionada que se instala en el dispositivo del usuario o de manera remota con técnicas de descargas no autorizadas desde un sitio web.

Este fue un error grave en el mecanismo de autenticación dentro de la aplicación para Android con las versiones 1.5.4 hasta 1.6.1 de Dropbox SDK. Sin embargo, luego de que IBM Security Team divulgó el problema a Dropbox, este fue resuelto en Dropbox SDK para Android v1.6.2 en solo 4 días. Puede leer un resumen de la vulnerabilidad de seguridad DroppedIn en una publicación de blog (nota al pie de referencia 9) en SecurityIntelligence.com.

Piratas informáticos lograron utilizar la vulnerabilidad DroppedIn debido a la facilidad de instalar una aplicación malintencionada en un dispositivo con Android. Los ciberdelincuentes están continuamente probando maneras nuevas y creativas de atacar las vulnerabilidades de las plataformas de los sistemas operativos móviles, que son diferentes a los de las PC.

Si bien es posible que Android continúe enfrentando una cantidad de desafíos en relación a la adopción por parte de las empresas, los últimos avances en seguridad de Google y de los fabricantes de dispositivos, y el respaldo de los proveedores de soluciones de gestión de movilidad empresarial (EMM) líderes están contribuyendo a su expansión en empresas y agencias gubernamentales. Cuando los consumidores, y por lo tanto sus empleados, eligen dispositivos con Android, su organización necesita habilitar la seguridad y protección necesarias para evitar el malware móvil.

iOS No Es Vulnerable

Los dispositivos con iOS dominaron el mercado empresarial por muchos motivos clave. Cuando el iPhone hizo su primer debut en 2007, los profesionales comenzaron a utilizar sus iPhones personales para trabajar, en vez de sus viejos smartphones corporativos. La arquitectura de espacio aislado y el comportamiento de las aplicaciones para iOS dieron como resultado seguridad por diseño en la plataforma, lo que dificulta a los piratas informáticos infectar todo el dispositivo y las aplicaciones, a menos que los usuarios eviten intencionalmente sus sistemas de seguridad.

Luego de enfocarse inicialmente solo en el mercado para consumidores, Apple rápidamente percibió el potencial del mercado empresarial. Comenzó a incorporar controles que permitían a los líderes de TI asegurar y gestionar los dispositivos, las aplicaciones y los datos de una manera más eficiente con la ayuda de proveedores de soluciones de gestión de dispositivos móviles (MDM).

A diferencia de la arquitectura y del ecosistema abiertos de las aplicaciones para Android, Apple tiende a contar con un entorno de aplicación y dispositivo mucho más cerrado. Las aplicaciones para iOS públicas solo pueden descargarse e instalarse a partir de la iTunes App Store, a menos que un dispositivo con iOS se haya descodificado. Las aplicaciones que se cargan a iTunes pasan por un proceso de análisis profundo antes de que Apple las publique oficialmente. Además, son necesarios certificados digitales para firmar las aplicaciones para iOS, por lo tanto, pueden rastrearse hasta el desarrollador de la aplicación.

Todos estos motivos contribuyeron para que los iPhones y iPads tuvieran una gran aceptación por parte de las empresas, los gobiernos y las instituciones educativas a través de los años. Sin embargo, estas amplias medidas de seguridad no detuvieron a los ciberdelincuentes en sus intentos por piratear los dispositivos con iOS. De hecho, ocurrieron incidentes en los que los piratas informáticos infectaron de una manera creativa iPhones y iPads, que incluyeron malwares nuevos llamados WireLurker y ataque enmascarado.

WireLurker es un nuevo tipo de malware cuyo blanco son los dispositivos con iOS y Mac OS.[10] Lo que diferencia a WireLurker es que logra infectar dispositivos con iOS que no fueron descodificados cuando se conectan a dispositivos con Mac OS infectados a través de cables USB.

Así funciona generalmente WireLurker para atacar dispositivos:

- El usuario descarga e instala una aplicación para el sistema operativo X infectada con malware en su dispositivo con Mac OS, seguramente desde una tienda de aplicaciones no oficial de terceros.
- A continuación, el usuario ejecuta la aplicación infectada y le otorga permisos de raíz, que implica saber la contraseña de administrador del dispositivo con Mac OS.
- Una vez que se encuentra en ejecución, la aplicación para el sistema operativo X infectada con malware descarga varias aplicaciones para iOS y espera a que un dispositivo con iOS, que confía en la computadora, se conecte a través de un cable USB.
- Después de que un dispositivo con iOS, que confía en el dispositivo con Mac OS infectado, se conecta, la aplicación con malware cargará las aplicaciones para iOS malintencionadas en el iPhone o iPad.
- Las aplicaciones para iOS son en sí mismas aplicaciones firmadas por empresas, lo que significa que los ciberdelincuentes pusieron en peligro la cuenta de otra organización o lograron que Apple aprobara sus propias aplicaciones para iOS. Estas aplicaciones también cuentan con perfiles de aprovisionamiento, lo que hace que los dispositivos con iOS confíen en ellas.

Una vez que las aplicaciones para iOS malintencionadas se cargan en los dispositivos con iOS no descodificados, son capaces de robar información y comunicarse con frecuencia con los servidores de los atacantes.

Tal vez aún más nefasto que WireLurker sea el malware descubierto recientemente llamado ataque enmascarado,[11] que también logra infectar dispositivos con iOS sin descodificar, pero sin la necesidad de conectarse a un dispositivo con Mac OS infectado. Con este ataque, una aplicación para iOS instalada con aprovisionamiento ad-hoc/empresarial podría reemplazar una aplicación aprobada de la iTunes App Store, siempre y cuando ambas aplicaciones utilicen el mismo identificador de paquete.

Esta es la manera en la que el ataque enmascarado puede reemplazar aplicaciones auténticas de los usuarios y robar información:

- El usuario hace clic en un enlace de cualquier sitio web para descargar e instalar la aplicación malintencionada que está firmada con un certificado empresarial y podría llamarse algo así como “Nuevo Angry Bird”.
- La aplicación malintencionada reemplaza la aplicación legítima, que puede ser una aplicación de e-mail o de un banco, que tiene el mismo identificador de paquete.
- Los atacantes pueden simular la interfaz de inicio de sesión de la aplicación original para robar las credenciales del usuario.
- La aplicación también puede utilizar memorias caché para imitar la funcionalidad de la aplicación reemplazada, como los e-mails recientes de una aplicación de e-mails.

Una vez que los ciberdelincuentes logran obtener credenciales de inicio de sesión y datos en caché locales, los datos confidenciales de los usuarios y la información financiera son vulnerables a ataques y pérdida de datos.

La Gestión de Movilidad Empresarial abarca La Protección contra Malware

IBM MaaS360 Mobile Threat Management

IBM ofrece una nueva capa de seguridad para EMM con la integración de IBM Security Trusteer para proteger contra malware móvil y dispositivos en peligro, tales como tablets o smartphones descodificados o descifrados.

La integración y sinergia diferenciadas crean una defensa eficiente contra piratas informáticos y ladrones que están trabajando para obtener información personal y corporativa para lograr beneficios ilícitos.

Detecte y analice aplicaciones con iOS y Android con firmas de malware a partir de una base de datos continuamente actualizada.

Trusteer, que es utilizado por cientos de millones de usuarios para proteger sus organizaciones de actos ilícitos y violaciones de datos, ofrece conocimiento de riesgos e inteligencia de seguridad a MaaS360.

Detección y resolución de malware móvil:

- Detecte y analice aplicaciones con iOS y Android con firmas de malware a partir de una base de datos continuamente actualizada.
- Agregue excepciones de aplicaciones para personalizar el uso de aplicaciones aceptables.
- Establezca controles normativos pormenorizados para tomar las acciones necesarias.
- Utilice un motor de reglas de conformidad casi en tiempo real para automatizar la resolución.
- Alerte a los usuarios y a las partes responsables cuando se detecte malware.
- Visualice los dispositivos en peligro en My Alert Center y los eventos de detección en los tableros de My Activity Feed.
- Desinstale las aplicaciones con malware automáticamente (en determinados dispositivos con Android, como Samsung SAFE).
- Bloquee accesos y elimine los datos de los dispositivos de manera parcial o total.
- Recopile y observe los atributos de amenazas del dispositivo, incluidos:
  - Malware detectado
  - Configuraciones de sistema sospechosas encontradas, como escucha de SMS o paquete de inicio
  - Conexión a una zona activa de Wi-Fi insegura
  - Permiso para instalar aplicaciones fuera de las tiendas
  - Versión de sistema operativo
- Verifique el historial de auditorías de eventos de detección de malware.

Figura 3: MaaS360 trabaja junto con Trusteer para detectar, analizar y resolver malware móvil y dispositivos en peligro.

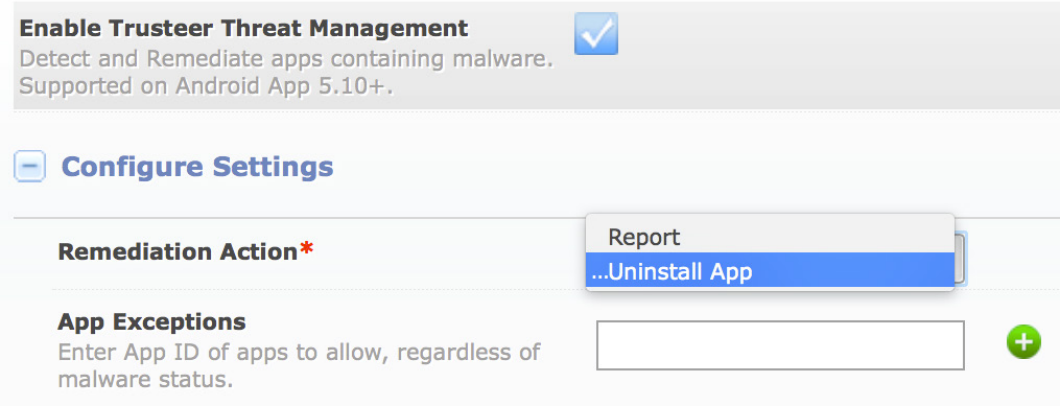

Figura 4: algunos de los valores de configuración de MaaS360.

Detección suplementaria de descodificaciones y descifrados:

- Detecte dispositivos móviles vulnerables o en peligro.
- Protéjase de dispositivos con iOS descodificados o con Android descifrados que podrían brindar a los atacantes privilegios adicionales en el sistema operativo, lo que habilita varios vectores de ataque.
- Busque amenazas y técnicas ocultas activas que intenten esconder la detección de dispositivos descodificados o descifrados.
- Implemente una lógica de detección actualizada móvil sin actualizaciones de aplicaciones para lograr una mayor capacidad de respuesta para los atacantes más rápidos.
- Establezca políticas de seguridad y reglas de conformidad para automatizar las resoluciones.
- Bloquee accesos, elimine los datos de los dispositivos de manera parcial o total o suprima el control del dispositivo.

Los dispositivos y la información del usuario también se pueden proteger con esta capa de seguridad, que no es de fácil acceso para los consumidores.

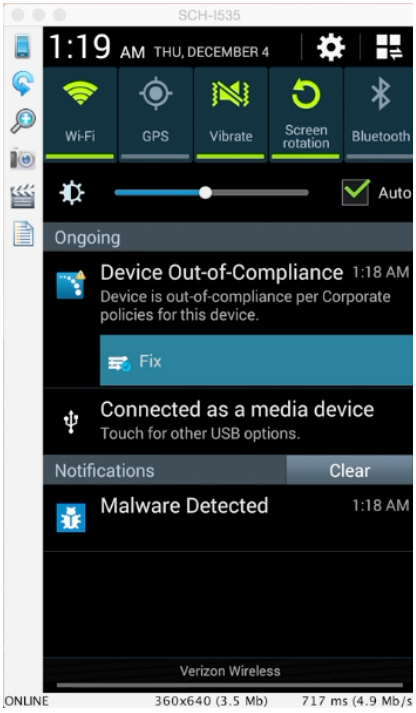

Figura 5: captura de pantalla que muestra malware móvil detectado y un dispositivo que no se ajusta al cumplimiento normativo.

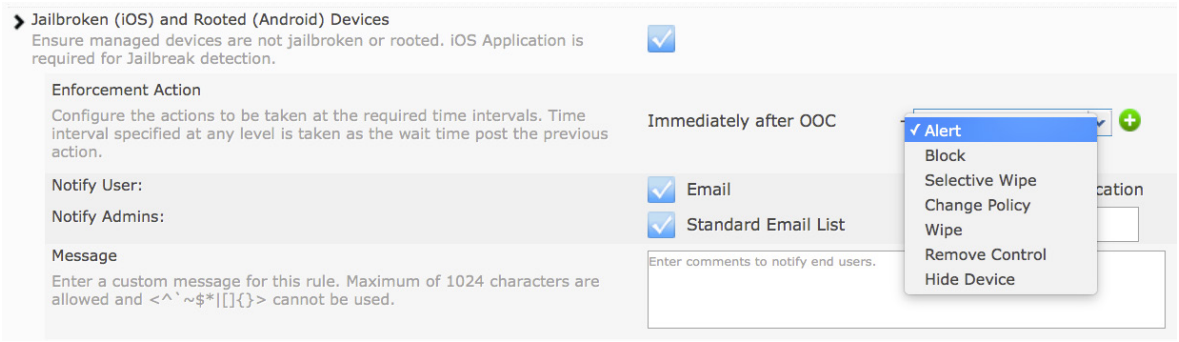

Figura 6: configure acciones de ejecución de cumplimiento para dispositivos descodificados o descifrados.

Trusteer Mobile Risk Engine habilita capas de protección e inteligencia de ciberdelincuencia para la prevención flexible de malware para detectar y adaptarse con mayor velocidad a los más recientes comportamientos de ataques y que el malware esté prácticamente inhabilitado para cometer actos ilícitos. Actualizado continuamente para brindar las verificaciones de malware, descodificación y descifrado, el motor realiza evaluaciones de riesgo móvil casi en tiempo real en base a factores de riesgo de aplicaciones y dispositivos.

Principales Beneficios

Los beneficios de la solución MaaS360 Mobile Threat Management van más allá de simplemente proteger los datos y los dispositivos corporativos. Los dispositivos y la información del usuario también se pueden proteger con esta capa de seguridad, que no es de fácil acceso para los consumidores.

Las organizaciones pueden tomar más acciones para ayudar a educar a los usuarios y proteger sus datos.

- Brinde respaldo tanto a dispositivos BYOD como corporativos
- Proteja los datos personales como un beneficio adicional para el empleado en relación a BYOD
- Gestione las amenazas móviles de una manera proactiva casi en tiempo real
- Reduzca el riesgo de las filtraciones de datos confidenciales de información personal y corporativa
- Haga que la adopción de Android sea más aceptable en la empresa, especialmente a través de BYOD
- Implemente acciones automáticas para resolver los riesgos de seguridad móviles cuando ocurran

Educar y Proteger a los Usuarios

Además de contar con la solución MaaS360 Mobile Threat Management, las organizaciones pueden tomar más acciones para ayudar a educar a los usuarios y proteger sus datos.

Las organizaciones deberían considerar implementar las siguientes actividades relacionadas con la seguridad móvil:

- Educar a los empleados acerca de la seguridad de las aplicaciones: informar acerca de los peligros de descargar aplicaciones de terceros y los peligros potenciales que resultan de los permisos de dispositivo demasiado flexibles.
- Proteja los dispositivos BYOD: implemente capacidades de gestión de movilidad empresarial para permitir que los empleados utilicen sus propios dispositivos al mismo tiempo que conserva la seguridad de la organización.
- Permita a los empleados realizar descargas a partir de tiendas de aplicaciones autorizadas únicamente: autorice a los empleados a descargar aplicaciones solamente de tiendas de aplicaciones autorizadas, como Google Play, Apple App Store y la tienda de aplicaciones de su organización, si corresponde.
- Actúe rápidamente cuando un dispositivo está en peligro: establezca políticas automáticas en smartphones y tablets que tomen acciones automáticas si se descubre un dispositivo en peligro o una aplicación malintencionada. Este método protege los datos de su organización mientras se soluciona el problema.

¿Por qué MaaS360?

MaaS360 es la protección contra malware avanzada e integrada de IBM con seguridad y gestión de movilidad empresarial líder en la industria. Es ágil y fácil de configurar y usar para proteger los datos confidenciales en los dispositivos móviles personales y corporativos.

Acerca de IBM MaaS360

IBM MaaS360 es la plataforma de gestión de movilidad empresarial que permite proteger datos y productividad para la manera en la que trabajan las personas. Miles de organizaciones confían en MaaS360 como la base de sus iniciativas de movilidad. MaaS360 ofrece gestión integral con controles sólidos de seguridad para usuarios, dispositivos, aplicaciones y contenido para respaldar cualquier despliegue móvil. Para obtener más información acerca de IBM MaaS360 y para empezar a usar una versión de evaluación sin costo de 30 días, visite **ibm.com**/maas360

Acerca de IBM Security

La plataforma de seguridad de IBM ofrece inteligencia en seguridad para ayudar a las organizaciones a proteger de manera integral a las personas, los datos, las aplicaciones y la infraestructura. IBM ofrece soluciones para gestión de acceso e identificación, gestión de eventos e información de seguridad, seguridad de base de datos, desarrollo de aplicaciones, gestión de riesgos, gestión de puntos terminales, protección contra intrusiones de última generación, y más. IBM opera una de las organizaciones de suministro, investigación y desarrollo de seguridad más grandes del mundo. Para obtener más información, visite **ibm.com**/security

IBM de Colombia S.A.
Cra 53 No. 100 – 25
Bogotá – Colombia

Puede encontrar la página de inicio de IBM en:
ibm.com

Considere el medio ambiente antes de imprimir

1 World to have more cell phone accounts than people by 2014, enero de 2013 International Telecommunications Union, http://www.siliconindia.com/magazine_articles/World_to_have_more_cell_phone_accounts_than_people_by_2014-DASD767476836.html

2 State of Mobile App Security, noviembre de 2014, Arxan Technologies, https://www.arxan.com/wp-content/uploads/assets1/pdf/State_of_Mobile_App_Security_2014_final.pdf

3 Bring Your Own Device: The Facts and the Future, mayo de 2013, Gartner, http://www.gartner.com/newsroom/id/2466615

4 Motive Security Labs Malware Report, segundo semestre de 2014, Motive Security Labs, http://www.gartner.com/newsroom/id/2466615

5 2014 Cost of Data Breach Study: Global Analysis, mayo de 2014, Ponemon Institute, http://www-03.ibm.com/security/data-breach/

6 State of Mobile App Security, noviembre de 2014, Arxan Technologies, https://www.arxan.com/wp-content/uploads/assets1/pdf/State_of_Mobile_App_Security_2014_final.pdf

7 The State of Mobile Application Insecurity, febrero de 2015, Ponemon Institute, https://www-01.ibm.com/marketing/iwm/iwm/web/signup.do?source=swg-WW_Security_Organic&S_PKG=ov33432&S_TACT=102PW2CW

8 IDC Worldwide Quarterly Mobile Phone Tracker, febrero de 2015, IDC, http://www.idc.com/getdoc.jsp?containerId=prUS25450615

9 DroppedIn: Remotely Exploitable Vulnerability in the Dropbox SDK for Android, marzo de 2015, IBM Security, http://securityintelligence.com/droppedin-remotely-exploitable-vulnerability-in-the-dropbox-sdk-for-android/#.Vb-1_SisG8W

10 Wirelurker: A new Era in OS X and iOS Malware; Blog, PaloAlto Networks, 5/11/14; http://researchcenter.paloaltonetworks.com/2014/11/wirelurker-new-era-os-x-ios-malware/

11 Xue, H., Wie, T., Yulong, Z.; Masque: All Your iOS Apps Belong to Us; Fire Eye; 10/11/14; https://www.fireeye.com/blog/threat-research/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html

WGW03150-COES-01