Resumen de la solución

Protección frente a las aplicaciones móviles en colusión

En la actualidad es necesario que las aplicaciones móviles puedan comunicarse de forma fácil. Desgraciadamente, la presencia de estos canales de comunicación tan útiles también favorece la aparición de comportamientos insidiosos. Es posible que cuando dos o más apps se analizan por separado, cada una de ellas parezca totalmente inofensiva. Sin embargo, cuando se instalan en el mismo dispositivo, pueden intercambiar información y cometer actos maliciosos.

En el *Informe de McAfee Labs sobre amenazas: junio de 2016*, examinamos detenidamente las aplicaciones en colusión, que son un nuevo método que emplean las apps maliciosas para complicar su detección. Por motivos de seguridad, los sistemas operativos para móviles recluyen sus aplicaciones en entornos aislados, limitan sus funciones y controlan con claridad los permisos que tienen. Sin embargo, los sistemas operativos para móviles también incluyen muchos métodos para que estas aplicaciones se comuniquen entre sí e intercambien información fuera de los límites de los entornos aislados.

Para evitar la detección, los agresores pueden emplear varias aplicaciones que tengan funciones y permisos diferentes y que, combinadas, les permitan conseguir sus objetivos. Por ejemplo, la App A tiene permisos para acceder a información confidencial y la App B tiene acceso a Internet. Cuando se instalan por separado, la App A no puede enviar información fuera del dispositivo y la App B no puede acceder a la información confidencial. Sin embargo, instaladas en el mismo dispositivo, la App A envía la información confidencial a la App B que, a su vez, transmite esa información a un destino en el exterior.

Al actuar en colusión, las aplicaciones móviles consiguen llevar a cabo acciones maliciosas como las siguientes sin ser detectadas:

- **Robo de información:** cuando una app con acceso a información sensible o confidencial colabora (de manera activa o pasiva) con una o más aplicaciones para enviar información fuera del dispositivo.
- **Robo financiero:** cuando una app envía información a otra que puede realizar transacciones financieras o llamadas a API financieras.

intel Security

- **Uso indebido del servicio:** cuando una app es capaz de controlar el servicio de un sistema y recibe información o comandos de una o varias aplicaciones.
- **Elevación de privilegios:** cuando una app proporciona sus privilegios más ventajosos a otras aplicaciones con el fin de obtener datos confidenciales y realizar otras acciones delictivas.

Protección frente a las aplicaciones móviles en colusión

Intel® Security recomienda lo siguiente para protegerse contra las aplicaciones móviles en colusión:

- **Utilizar apps de tiendas y marcas de confianza**, ya que las fuentes autorizadas realizan análisis de malware rutinarios de las aplicaciones de sus catálogos.
- **Desactivar la opción para instalar apps de "fuentes desconocidas"** para evitar que se instalen aplicaciones que no han sido autorizadas.
- **Evitar el software con publicidad incrustada**, ya que el exceso de anuncios puede ser indicativo de la presencia de varias bibliotecas de anuncios, lo que aumenta la posibilidad de colusión.
- **Consultar las puntuaciones y reseñas de una aplicación móvil antes de instalarla** a fin de verificar que otros usuarios de la app no hayan experimentado problemas de seguridad.
- **No desbloquear ("jailbreak" o "root") el dispositivo**, ya que esto permitiría a las aplicaciones obtener acceso a nivel de sistema con la posibilidad de llevar a cabo actividades maliciosas.
- **Desplegar una solución de administración de móviles** como mecanismo para controlar qué apps pueden instalar los usuarios.

Cómo puede ayudarle Intel Security a protegerse de las aplicaciones móviles en colusión

McAfee® Mobile Security for Android

Cuando descarga nuevas apps, navega por Internet o realiza transacciones bancarias online, McAfee Mobile Security for Android protege su dispositivo móvil frente a amenazas. McAfee Mobile Security for Android utiliza la inteligencia que le proporcionan los investigadores de amenazas de McAfee Labs para identificar aplicaciones maliciosas, incluidas las apps en colusión, y las detiene antes de que se ejecuten en su dispositivo móvil. Con McAfee Mobile Security for Android, su móvil está protegido y puede utilizar cualquier aplicación sola o combinada con otra con total confianza.

McAfee Mobile Security for Android ofrece las siguientes funciones:

- Utiliza análisis en tiempo real para analizar automáticamente mensajes de correo electrónico, mensajes de texto, adjuntos y archivos con el fin de detectar si contienen contenido malicioso.
- Realiza análisis completos programados mediante Smart Scheduler.
- Permite ejecutar actualizaciones automáticas para garantizar que cuente con la información más actualizada de los investigadores de amenazas para protegerse contra todo tipo de ataques, incluidos los provocados por aplicaciones móviles en colusión.
- Informa y alerta automáticamente si una aplicación viola la privacidad y le permite desinstalar aplicaciones que no son seguras.
- Bloquea sitios web peligrosos que pueden contener amenazas maliciosas.

Otros documentos para ampliar la información

Towards Automated Android App Collusion Detection (Hacia la detección automatizada de colusión de aplicaciones para Android), un informe de investigación que es fruto de la colaboración de McAfee Labs e investigadores de varias universidades de Reino Unido.

Colluding Apps: Tomorrow's Mobile Malware Threat (Aplicaciones en colusión: la amenaza del malware para móviles del futuro), un artículo de la revista IEEE Security & Privacy.

Analysis of the Communication Between Colluding Applications on Modern Smartphones (Análisis de la comunicación entre aplicaciones en colusión en los smartphones modernos), Actas de la 28.ª conferencia anual de aplicaciones de seguridad informática.

A Survey on Application Collusion Attacks on Android Permission-Mechanism (Estudio de los ataques por colusión de aplicaciones al mecanismo de permisos de Android), International Journal for Scientific Research & Development.

Towards a Systematic Study of the Covert Channel Attacks in Smartphones (Hacia un estudio sistemático de los ataques a smartphones a través de canales ocultos), International Conference on Security and Privacy in Communication Networks.

Automatic Detection of Inter-Application Permission Leaks in Android Applications (Detección automática de fugas de permisos entre aplicaciones Android), IBM Journal of Research and Development.

McAfee. Part of Intel Security.
Avenida de Bruselas n.º 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8500
www.intelsecurity.com