TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 17. No. 2, mayo-agosto, 2018, p.52- 59 ISSN 1729-3804

SEGURMÁTICA SEGURIDAD MÓVIL: MÁS ALLÁ DE LA DETECCIÓN DE MALWARE ANDROID

Ailin de la Caridad Prieto Quiñones [1], Pablo Hernández Valdés [2]

[1]Segurmática, Calle Zanja No.651 esq. A Soledad, Centro Habana, La Habana, Cuba., [2]Segurmática, Calle Zanja No.651 esq. A Soledad, Centro Habana, La Habana, Cuba.
[1]ailin@segurmatica.cu

RESUMEN

Desde hace algún tiempo Android se ha ido convirtiendo en el sistema operativo móvil más utilizado y por ese motivo para los creadores de programas malignos les resulta atractivo. El número de aplicaciones malignas está aumentando constantemente y con la introducción paulatina en Cuba de dispositivos con este sistema operativo resulta importante estar protegidos. Con ese objetivo en Segurmática se ha trabajando para incorporar al motor antivirus la capacidad de detección de aplicaciones malignas orientadas a esta plataforma. En adición, se ha desarrollado una aplicación para detectar aplicaciones malignas en los dispositivos con sistema operativo Android.

PALABRAS CLAVES: Android, Programas malignos, Detección, Seguridad.

ABSTRACT

Android has become one of the most used mobile operating system. In this regard, developers for malicious programs find out an attractive platform on Android Operating Systems. The total number of malicious applications is constantly increasing and considering the gradual introduction in Cuba of devices with this operating system it is important to be protected. Segurmática has been working to incorporate the detection capability of Android malware to the antivirus engine. Additionally, the company has developed applications to detect malicious softwares on devices by using Android.

KEY WORDS: Android, Malware, Detection, Security.

1. INTRODUCCIÓN

El desarrollo de los dispositivos móviles viene de conjunto con los sistemas operativos móviles, los cuales se han ido transformando de ser una simple interfaz para los servicios básicos como era en los teléfonos iniciales a ser un sistema operativo completo personalizable, con aplicaciones y con facilidades para los desarrolladores. Uno de estos sistemas operativos es Android, desarrollado por Google, el cual ha ido aumentando su uso y desde hace varios años es el más utilizado [1].

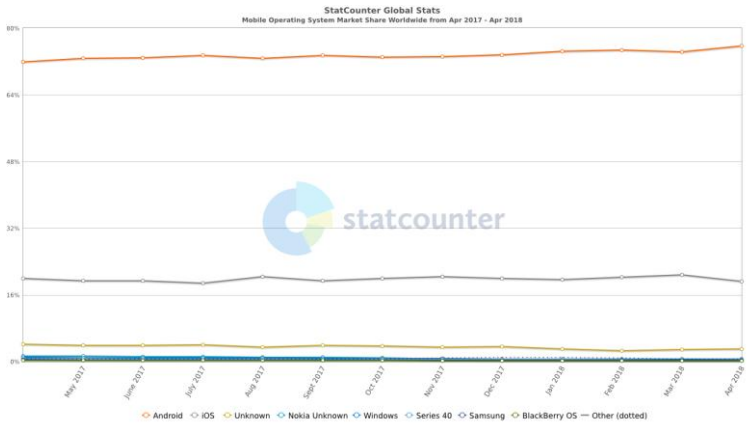

Figura 1: Uso de los sistemas operativos móviles

Con el uso generalizado de los teléfonos inteligentes, la cantidad de malware ha aumentado de manera exponencial. Entre los dispositivos inteligentes, los dispositivos Android son los dispositivos más atacados por malware debido a su alta popularidad [2].
De la misma manera que el uso del sistema operativo crece, también aumenta el interés dentro de los creadores de programas malignos para convertirlo en objetivo de su ataque. En la actualidad casi la totalidad de las aplicaciones malignas móviles están orientadas a Android [3].

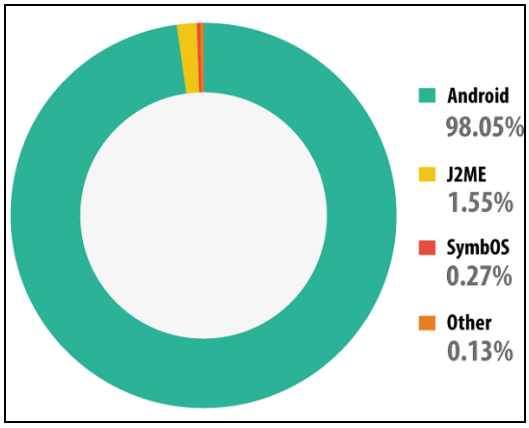

Figura 2: Distribución de las aplicaciones malignas

En Cuba el desarrollo de la telefonía móvil está atrasado con respecto a otras partes del mundo, pero a pesar de eso es común encontrarse a personas con un móvil Android, y esta tendencia va creciendo. La empresa Segurmática tiene entre sus objetivos garantizar la protección de todos sus usuarios. Por ese motivo la empresa se dio a la tarea de incorporar al motor antivirus la capacidad de detección de aplicaciones malignas hechas para Android y el desarrollo de una aplicación orientada a este sistema.

2. DESCRIPCIÓN DE APLICACIONES ANDROID

Una aplicación para Android es un fichero con extensión APK, aunque internamente es un fichero ZIP con la estructura siguiente [4]:

- [assets]
- [lib]
- [META-INF]
- [res]
- AndroidManifest.xml
- classes.dex
- resources.arsc

Hay carpetas y ficheros que contienen recursos (assets, res, resources.arsc), otros que contienen código (lib, classes.dex) y otros que contienen información descriptiva de la aplicación (META-INF, AndroidManifest.xml). Una aplicación se identifica por un nombre de paquete único, por ejemplo com.google.android.email, todas las versiones de la misma aplicación tienen que estar firmadas con el mismo certificado, garantizando de esta manera que sean creadas por la misma persona o equipo de desarrolladores.

Una característica interesante es que en el AndroidManifest.xml es obligatorio especificar todos los permisos que la aplicación requiera. Un permiso puede ser acceder a la cámara, conectarse a Internet, ver o modificar contactos, acceder a los SMS, entre muchos otros (hay más de 150) [5].

APLICACIONES MALIGNAS

Las aplicaciones malignas se pueden dividir en dos grandes grupos [6]:

- Independientes: Son aplicaciones creadas completamente para ser malignas.

- Re-empaquetadas: Son aplicaciones legítimas que fueron desensambladas, se les adicionó código maligno y se volvieron a empaquetar.

Una característica común en las aplicaciones malignas es que solicitan una gran cantidad de permisos, necesarios para realizar su actividad maligna, pero que no son necesarios para una aplicación normal. A continuación se muestran los ejemplos de una tabla y una figura:

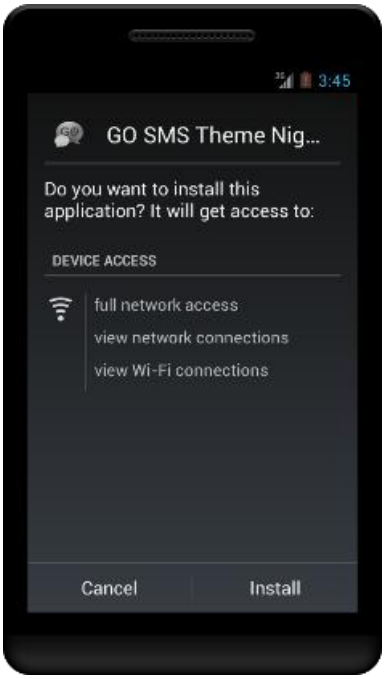

Figura 3: Permisos de una aplicación legítima.

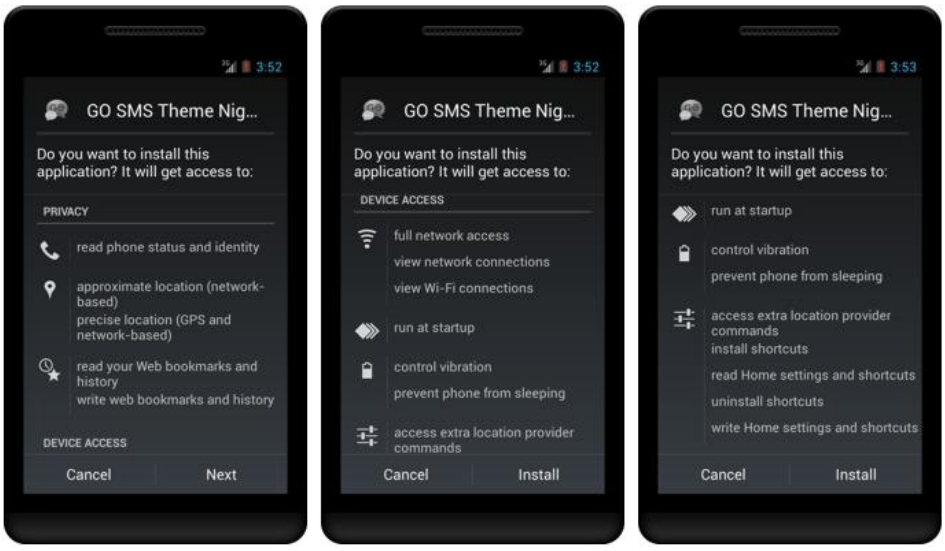

Figura 4: Permisos de la misma aplicación re-empaquetada con código maligno.

3. SITUACIÓN EN CUBA

En Cuba el uso de teléfonos inteligentes y tabletas ha aumentado considerablemente, en parte por los servicios del correo Nauta y los puntos Wifi para la conexión a Internet. Este incremento del número de dispositivos hace que circulen una gran cantidad de aplicaciones, la mayoría obtenida fuera de la tienda oficial Google Play. Por su parte, es también conocido que los sitios alternativos para descargas incluyen gran cantidad de aplicaciones que han sido modificadas para incorporarles códigos malignos.

En Segurmática se han analizado las aplicaciones que están circulando en el país por diferentes vías. El número de códigos malignos que se han encontrado ha crecido considerablemente como aprecia en el gráfico de la Figura 5.

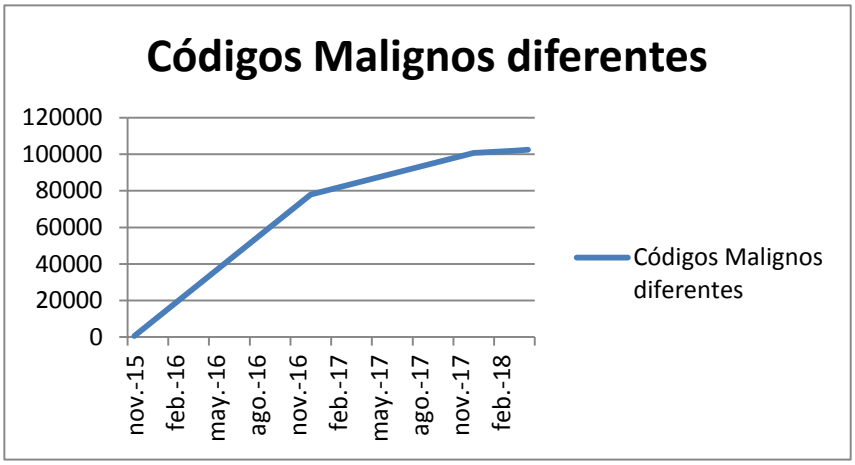

Figura 5: Códigos malignos detectados en Segurmática 2015-2017.

También se han encontrado códigos malignos desarrollados en Cuba. Por ejemplo, la aplicación EtecsaDroyd en su versión 4.2.5 fue modificada para incorporarle un código maligno que se queda "leyendo" los SMS que se reciben y cuando el texto del mensaje es Cola se activa el código. Entre otras acciones sobrescribe los ficheros que están en la tarjeta de memoria. De esta variante maliciosa se han encontrado hasta 10 paquetes de instalación diferentes con el mismo código maligno. Esta modificación no fue realizada por el programador original de la aplicación.

DETECCIÓN

Para la incorporación de la detección de aplicaciones malignas al motor antivirus se utilizan dos métodos principalmente [7]:

- Por firmas:
  - Es rápido.
  - Es necesario tener una firma por cada aplicación maligna.
- Con algoritmos complejos:
  - Es más lento.
  - Busca identificar dentro de la aplicación características, clases, métodos, correspondientes a códigos malignos. Generalmente esta se realiza analizando la estructura interna del classes.dex.
  - Un algoritmo puede identificar una gran cantidad de aplicaciones infectadas (modificadas) con un código maligno correspondiente a una misma familia.

Con la incorporación de la detección al motor antivirus, los productos Segurmática Antivirus y SAVUnix, para Windows y Linux respectivamente, son capaces de analizar los paquetes de instalación de Android (APK) y detectar aplicaciones infectadas. Estos productos son muy útiles en un PC pero tienen la desventaja de que no pueden analizar las aplicaciones ya instaladas en un dispositivo móvil. Por este motivo en Segurmática se inició el desarrollo de una aplicación orientada específicamente a los dispositivos con Android.

4. SEGURMÁTICA SEGURIDAD MÓVIL

Segurmática Seguridad Móvil es una aplicación orientada a la detección de aplicaciones malignas para el sistema operativo Android. Está diseñada para soportar versiones de Android a partir de la 4.0, y las arquitecturas ARM y x86. Tiene como características el bajo consumo de recursos, no necesita privilegios de root para ejecutarse, con interfaz optimizada para móviles y tabletas, y disponible en inglés y en español. La aplicación mantiene un diseño basado en material design, con criterios de accesibilidad visual y navegación Dpad. La Figura 6 muestra la interfaz de esta aplicación Segurmática para la seguridad móvil.

Figura 6: Pantalla inicial de la aplicación.

Entre las funcionalidades principales de la aplicación se encuentran el análisis automático de las nuevas aplicaciones que se instalen o se actualicen, el análisis en demanda de las aplicaciones instaladas y del almacenamiento, tanto la memoria interna como la SD. Además de permitir al usuario actualizar la misma tanto desde internet como desde una carpeta en el dispositivo. La Figura 7 muestra un ejemplo de detección de aplicación maligna.

Otra de las funcionalidades de la aplicación es la de visualizar los permisos de las aplicaciones instaladas [8]. En este caso se realizó una selección de los permisos más recurrentes dentro de las aplicaciones malignas o permisos más peligrosos para Android [9], de forma tal que el usuario tenga la posibilidad de visualizar cuales aplicaciones de las que tiene instaladas en su dispositivo tienen acceso a cada uno de estos permisos. Esta aplicación da la posibilidad al usuario de visualizar o no las aplicaciones del sistema, iniciar un nuevo análisis para alguna de las aplicaciones listadas e incluso ir a la información de la aplicación en el sistema. Pese a que esta funcionalidad puede parecer trivial es de gran importancia puesto que en muchísimas ocasiones como usuarios a la hora de instalar nuevas aplicaciones no nos detenemos a analizar que permisos les estamos otorgando a las aplicaciones que instalamos.

La aplicación también cuenta con la funcionalidad Bloqueo de Llamadas [10], la cual está personalizada para nuestro país donde se destacan opciones como "Bloquear llamadas con *99" y "Bloquear llamadas desde números fijos". Además, puede agregar números manualmente a la lista de bloqueo o bien importarlos desde el registro de llamadas o desde los contactos. Dentro de esta misma funcionalidad también cuenta con la opción de agregar excepciones a las reglas de bloqueo creadas y mantiene un registro de las llamadas realizadas y recibidas en el dispositivo, así como el estado de estas llamadas según el contacto (Si el contacto está bloqueado o no). La Figura 8 muestra un ejemplo de pantalla de configuración de estas opciones.

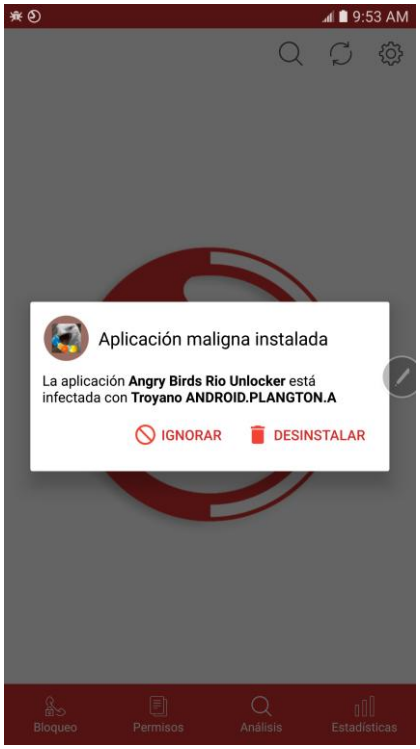

Figura 7: Detección de la instalación de una aplicación maligna

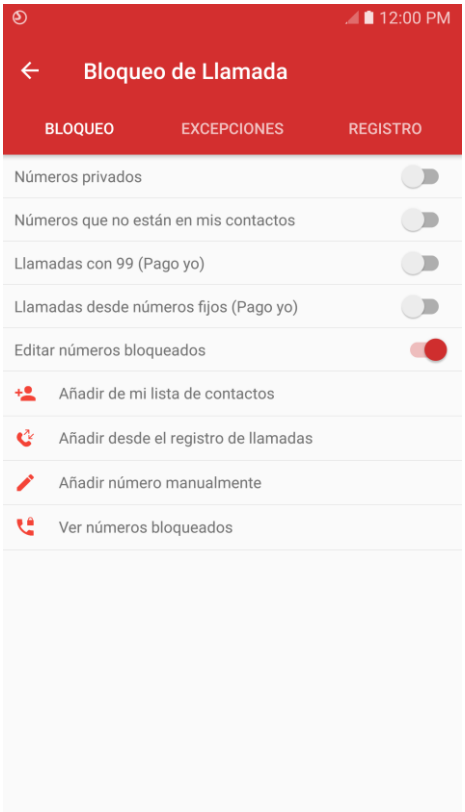

Figura 8: Pantalla Bloqueo de Llamadas.

Otra funcionalidad importante es el Cortafuegos (Firewall), el cual crea una VPN en el dispositivo, que permite controlar el tráfico de entrada y salida de las redes Wifi y Datos Móviles [11]. La interfaz muestra un listado de

las aplicaciones instaladas en el dispositivo, de forma tal que el usuario puede seleccionar si permite o deniega el acceso para ambos casos, bien sea general para todas las aplicaciones instaladas o para alguna aplicación específica. De igual forma se pueden crear filtros con un determinado puerto y host definiendo el acceso (permitido o denegado), el tipo (entrante y/o saliente) y la red (Wifi o Datos), ver Figura 9.

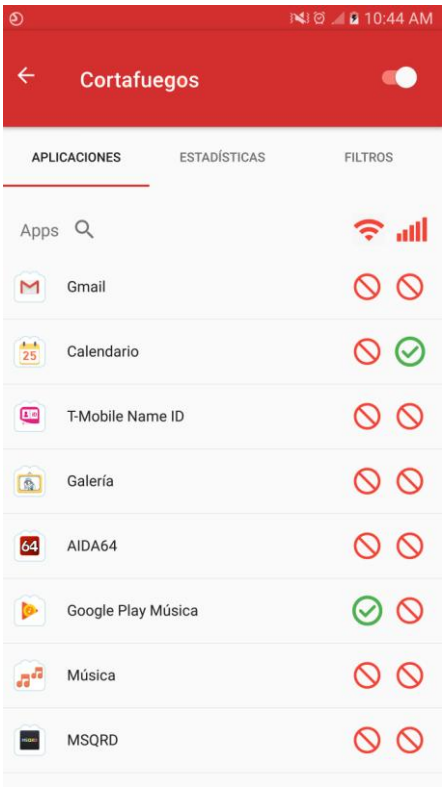

Figura 9: Pantalla Cortafuegos

3. CONCLUSIONES

El empleo de Android como sistema operativo móvil en Cuba va en ascenso, y a pesar de que no tiene el nivel de penetración que tienen otros países no estamos exentos a ser afectados por aplicaciones malignas, incluyendo las que son hechas en Cuba o para Cuba. Con la aplicación Segurmática Seguridad Móvil, la empresa Segurmática, garantiza a sus usuarios la protección en todos sus dispositivos móviles y les brinda nuevas opciones para proteger sus datos y su privacidad, de manera tal que el desarrollo de las nuevas tecnologías y el acceso a internet, tan novedoso para los cubanos, sea un punto a favor en nuestro día a día.

REFERENCIAS

[1] StatCounter Global Stats.
[2] T. Kim, B. Kang, M. Rho, S. Sezer, y E. G. Im, «A Multimodal Deep Learning Method for Android Malware Detection Using Various Features», IEEE Transactions on Information Forensics and Security, vol. 14, n.º 3, pp. 773-788, mar. 2019.
[3] Kaspersky Lab, Mobile Malware Evolution: 2013. https://blog.kaspersky.com/mobile-malware-evolution-2013/
[4] J. Lalande, V. V. T. Tong, M. Leslous, y P. Graux, «Challenges for Reliable and Large Scale Evaluation of Android Malware Analysis», en 2018 International Conference on High Performance Computing Simulation (HPCS), 2018, pp. 1068-1070.
[5] System Permissions. http://developer.android.com/reference/android/Manifest.permission.html
[6] L. Onwuzurike, M. Almeida, E. Mariconti, J. Blackbum, G. Stringhini, y E. De Cristofaro, «A Family of Droids-Android Malware Detection via Behavioral Modeling: Static vs Dynamic Analysis - IEEE Conference Publication», presentado en 2018 16th Annual Conference on Privacy, Security and Trust (PST), 2018.

[7] H. Cai, N. Meng, B. Ryder, y D. Yao, «DroidCat: Effective Android Malware Detection and Categorization via App-Level Profiling - IEEE Journals & Magazine», IEEE Transactions on Information Forensics and Security.
[8] «Manifest.permission», Android Developers. [En línea]. Disponible en: https://developer.android.com/reference/android/Manifest.permission. [Accedido: 05-dic-2018].
[9] L. Sun, «SIGNIFICANT PERMISSION IDENTIFICATION FOR ANDROID MALWARE DETECTION», Degree of Master of Science, University of Nebraska, 2016.
[10] «Implementing Block Phone Numbers», Android Open Source Project. [En línea]. Disponible en: https://source.android.com/devices/tech/connect/block-numbers. [Accedido: 05-dic-2018].
[11] «Explained: Absolute Best way to Limit Data on Android», www.infopackets.com, 30-abr-2018. [En línea]. Disponible en: https://www.infopackets.com/news/10327/explained-absolute-best-way-limit-data-android. [Accedido: 05-dic-2018].