

RANSOMWARE EN ANDROID

Víctor Manuel Pedraza Moreno

Nicolás Rojas Henao

Universidad Santo Tomás - Tunja

1. Introducción

Un virus es un programa informático que tiene como objetivo alterar el funcionamiento de una computadora o dispositivo móvil de forma que el usuario no se dé cuenta. El malware Ransomware es un virus que afecta distintos Sistemas Operativos principalmente a Android y a Windows, este se encarga de encriptar información para luego extorsionar a la víctima. De la misma forma se pretende explicar su comportamiento, sus características y formas de detección y prevención.

Durante el transcurso de esta investigación se aborda en primer lugar la definición exacta de Ransomware que otorgan diferentes autores, en la segunda parte se expone su comportamiento y características en Android, posteriormente se muestran algunas de las investigaciones realizadas para la prevención y tratamiento del virus en dispositivos móviles. Por último, se plantean unas recomendaciones a tener en cuenta y finalmente las conclusiones.

2. Ransomware

Según el artículo de investigación - *Uncovering the Face of Android*

Ransomware: Characterization and Real-Time Detection - (Chen , y otros, 2018) afirman: “*Ransomware, como su nombre lo indica, es cualquier tipo de malware que exija una suma de dinero de los usuarios afectados al impedirles el acceso a sus dispositivos o datos.*”(p.1)

Para ello usa algunos métodos como pueden ser el cifrado de archivos y bloqueo de la pantalla, en algunas ocasiones Ransomware muestra mensajes amenazantes o con alguna acusación de forma que las víctimas se sientan más intimidadas y así paguen el rescate. Algunas víctimas comunes han sido hospitales, escuelas, gasolineras, etc. En Junio de 2017 McAfee Lab afirmó que el número de víctimas había alcanzado 10 millones.

Para reforzar el concepto anterior en el artículo -*Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization*- (Monika, Zavarsky, & Lindskog, 2016) afirman:

Ransomware es una forma de código malicioso o malware que infecta una computadora y se propaga rápidamente para encriptar los datos o bloquear la máquina. Este malware hace que los datos sean inaccesibles para los usuarios, y los atacantes exijan el pago del usuario para

tener sus archivos sin cifrar y accesibles. (p.2)

Este malware es más común en dispositivos móviles especialmente en Android, ya que en la actualidad se manejan volúmenes de información importantes en este tipo de dispositivos como transacciones bancarias, fotos privadas, archivos de nómina, entre otros. (Song, Bongjoon, & Sangjun, 2016) afirman: *“El rápido crecimiento del mercado móvil ha sido el principal objetivo de los hackers para obtener ganancias ilegales mediante el uso de Ransomware” (p.1)*

3. Comportamiento y características en Android

Debido a que existen gran cantidad de aplicaciones y diferentes sitios donde se pueden descargar las apk¹ es más fácil para los autores del malware propagar el virus. Para entender mejor el comportamiento de este virus es necesario conocer algunos conceptos básicos sobre los componentes de Android, (Chen , y otros, 2018) afirman: *“Una aplicación de Android puede tener cuatro tipos de componentes: actividad, servicio, receptor de Broadcast y proveedor de contenido” (p.2)*. Una actividad define una interfaz gráfica de usuario y sus interacciones con las acciones de los usuarios, por otra parte, un servicio es un componente que se ejecuta en segundo plano y sus operaciones suelen tener una larga ejecución, debido a esto los autores del malware siempre utilizan el componente de servicio ya que así pueden evitar que el usuario se percate de algo

sospechoso. El receptor Broadcast es el componente encargado de permitir que las aplicaciones se registren para eventos de sistemas o aplicaciones. Por último, un proveedor de contenido proporciona un mecanismo desde el cual los datos almacenados por una aplicación pueden ser accesibles para otras aplicaciones. Por lo tanto (Chen , y otros, 2018) manifiestan:

Para realizar operaciones confidenciales (por ejemplo, tareas que pueden costar dinero o acceder a datos privados), las aplicaciones necesitan permisos específicos. Los permisos necesarios se definen en un archivo de manifiesto (es decir, AndroidManifest.xml), que se almacena en el archivo de la aplicación. Además, Android Debug Bridge (ADB) es un conjunto de herramientas incluidas en el paquete de Android SDK. Consiste en programas de cliente (es decir, PC) y del lado del servidor (es decir, dispositivo móvil) que se comunican entre sí. A través de la interfaz de línea de comando de ADB, los usuarios pueden controlar el dispositivo móvil para realizar muchas operaciones, por ejemplo, instalar o desinstalar aplicaciones, transmitir datos e incluso rootear el dispositivo. (p.2)

Los creadores del malware adquieren el control total del dispositivo encriptando información valiosa para posteriormente extorsionar a la víctima. Es importante distinguir algunas de las características metódicas de este malware:

- **Pantalla de bloqueo:** Se puede efectuar debido a varias estrategias como pueden ser

¹ **Android Application Package-Paquete de Aplicación Android:** Es un formato que se usa para distribuir e instalar componentes para el Sistema Operativo Android.

actividades de secuestro, configurando parámetros específicos y deshabilitando ciertos botones. Para esto se necesitan de algunos permisos solicitados al AndroidManifest.xml. Según el trabajo de (Chen , y otros, 2018) se obtuvo:

Entre las 2.721 muestras de Ransomware en nuestra colección, 2.544 de ellas (es decir, 14/15 familias) intentan bloquear el dispositivo de la víctima. Esto muestra que muchos autores de Ransomware obligan a las víctimas a pagar dinero por el uso normal de su dispositivo bloqueando la pantalla. (p.4)

- **Encriptación de archivos:** Los autores del malware pueden utilizar criptosistemas personalizados para evitar ser descifrados. Algunas de las actividades que utiliza Ransomware en la encriptación son: sobrescribir los contenidos del archivo original por los datos cifrados, determinar si el archivo original es valioso o no, eliminar el archivo original y crear un nuevo archivo que contenga los datos encriptados.
- **Usos de permisos:** Ransomware a diferencia de otros malware tiene una característica única y es que sus comportamientos son muy similares a los de aplicaciones benignas, por ejemplo abrir cuadros de dialogo o encriptar algunos archivos. Para esto ransomware necesita de varios

permisos que nos son muy solicitados por otros malware, algunos ejemplos de estos permisos son WALK_LOCK, DISABLE_KEYGUARD y SYSTEM_ALERT_WINDOW.

- **Método de pago:** A diferencia de otros malware, Ransomware utiliza métodos de pago electrónico como BitCoin, MoneyPack, PaySafeCard y CashU, los cuales son anónimos lo que dificulta el seguimiento de su origen y el destino final de los pagos. El método de pago más usado por los autores de Ransomware es el BitCoin.
- **Mensajes con amenazas:** Muchos malware tratan de ser sigilosos mientras que Ransomware necesita responsabilizarse de sus comportamientos maliciosos, es por esto que muestra un texto a sus víctimas donde amenazan con distribuir contenido privado como fotos intimas o material protegido por derechos de autor. En muchos casos el mensaje amenazante bloquea directamente el dispositivo.

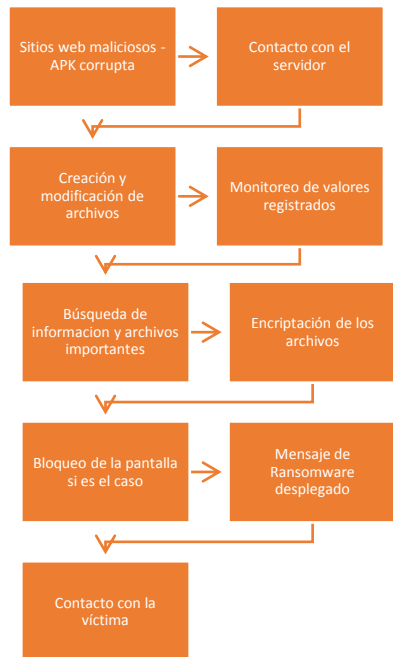


Ilustración 1 Ciclo de vida de Ransomware (Adaptación de: (Monika, Zavorsky, & Lindskog, 2016)

En la Ilustración 1 se puede evidenciar el ciclo de Ransomware en un dispositivo con Sistema Operativo Android y como las características mencionadas anteriormente son aplicadas a través de este proceso.

4. Técnicas de prevención

4.1. RansomProber

Esta aplicación notifica a los usuarios antes de realizar cualquier acción que pueda ser sensible y permita que Ransomware actúe. RansomProber cuenta con 3 pasos importantes para detectar amenazas como la anteriormente nombrada, los cuales son: El análisis de encriptación, análisis en primer plano y por último el análisis de diseño, (Chen , y otros, 2018) afirman:

En primer lugar, RansomProber detecta si algunos archivos han sido encriptados por el módulo de Análisis de encriptación. Luego, el módulo Análisis de primer plano decide si el proceso de encriptación pertenece a la aplicación con la que el usuario está interactuando. Finalmente, se analizarán los widgets UI de las actividades relacionadas y las coordenadas de operación del usuario, esto es realizado por el módulo de Análisis de diseño. Si el cifrado del archivo es desconocido para el usuario e irrelevante para las expectativas del usuario, este comportamiento puede definirse como no intencionado por el usuario y la aplicación correspondiente puede etiquetarse como encriptación del ransomware. (p.6)

Muchos autores de Ransomware no muestran interés en archivos temporales ya que no tienen información valiosa por lo tanto los autores de RansomProber filtran estos para que la herramienta no tenga mucha sobrecarga a la hora de realizar el análisis. Algunas rutas que contienen información valiosa y suelen ser objetivo del malware son: /Android/data, /data/system/accounts.db, /data/.../contacts2.db, /data/.../mmsms.db, /sdcard/Pictures, y /sdcard/Downloads.

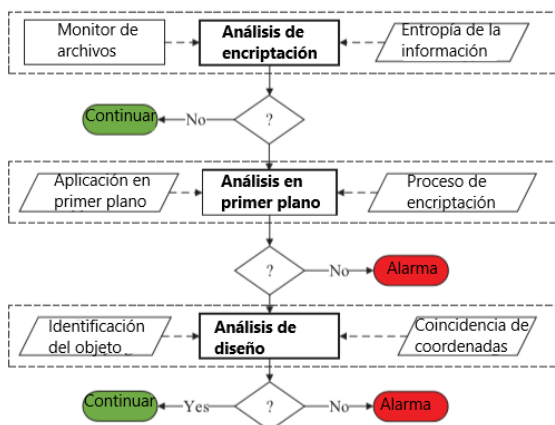


Ilustración 2 Traducción del proceso de RansomProber

De acuerdo a la ilustración 2, se puede observar que el primer proceso es el análisis de encriptación, donde se pueden utilizar varias técnicas como pueden ser monitorear archivos, de acuerdo a la entropía de la información, si se presenta una entropía muy grande puede ser que Ransomware esté actuando. (Chen , y otros, 2018) afirman:

Desde la perspectiva de los datos, la entropía de la información de un archivo tendría una enorme diferencia antes y después de que se encriptara. Mediante el examen de varios archivos diferentes (incluidos los archivos cifrados y no cifrados), encontramos que cualquier archivo se puede caracterizar por las propiedades de sus datos. Por ejemplo, uno puede considerar qué tan bien ordenados están los datos o cuánto espacio ocupan los datos. Cada archivo difiere no solo en tamaño, sino también en el nivel de entropía de la información. Normalmente, un archivo encriptado parece "aleatorio",

mientras que un archivo no encriptado contiene información bien "estructurada". Por lo tanto, la entropía de los archivos cifrados es más alta que la de los archivos no cifrados. (p.6)

El segundo paso es realizar el análisis en primer plano donde RansomProber detecta si el archivo ha sido encriptado, además este comportamiento puede ser normal o no, esto también lo determina esta herramienta. Para este análisis hay que tener en cuenta el comportamiento de los Widgets y las actividades de la aplicación que está siendo examinada. (Chen , y otros, 2018) afirman “*El objetivo del análisis en primer plano es asegurarse de que la aplicación en primer plano active el proceso de cifrado. Si la operación de cifrado es irrelevante para la aplicación en primer plano, el comportamiento puede ser desconocido para el usuario*” (p.7). Esto significa que el comportamiento es sospechoso

Por último se realiza el análisis de diseño donde se realiza el análisis exhaustivo de tres indicadores UI, los cuales son fundamentales para entender el comportamiento de Ransomware, estos son: Botones, Lista de Archivos y Textos Ocultos. (Chen , y otros, 2018) mencionan: “*RansomProber registra las coordenadas de pulsación del usuario y la información de diseño de las actividades relacionadas de forma persistente. Si no hay ninguna operación de pulsación durante el proceso de encriptación, podemos inferir directamente que la operación es sin intención del usuario.*” (p.7). RansomProber implementa unos

indicadores de detección, donde se tratan de descartar los falsos positivos.

4.2. Análisis automático:

(Kanwal, Thakur, & Lashkari, 2017) afirman:

Existen varias técnicas y herramientas desarrolladas para detectar diferentes tipos de Ransomware. Los autores informan acerca de la técnica de detección conocida como Análisis automático que es la combinación de: Análisis estático y Análisis dinámico. (p.1)

Análisis estático: Se realiza en el código no ejecutable en tiempo de compilación

Análisis dinámico: Se comprueba y controla el comportamiento de la aplicación ejecutora.

Algunas fuentes donde se puede propagar el malware son las cuentas, los correos electrónicos, los contactos, el calendario, bases de datos, archivos, registros de ubicación, entre otros. Usualmente se da a través de internet, tarjetas de memoria, transmisión de SMS, comunicación entre procesos, etc.

Para el desarrollo de una aplicación encargada de buscar una solución para Ransomware, se utilizó una aplicación con Google Firebase, (Kanwal, Thakur, & Lashkari, 2017) lo definen como: *“Firebase es una aplicación web y una plataforma móvil con infraestructura y herramientas diseñadas para ayudar a los desarrolladores a crear aplicaciones de alta calidad” (p.2)*

(Kanwal, Thakur, & Lashkari, 2017) manifiestan:

En firebase, todos los datos se almacenan en formato JSON, los cambios realizados en los datos se reflejan inmediatamente en todos los dispositivos que utilizan la operación de sincronización. Firebase también permite al usuario acceder a los datos fuera de línea En la base de datos, estamos almacenando el nombre del paquete único de todas las aplicaciones que hemos encontrado hasta la fecha y con el nombre del paquete hay una etiqueta que nos dice si la aplicación es segura o no. Cuando se inicia la aplicación obtenemos la lista de todas las aplicaciones instaladas en el dispositivo, también obtenemos la lista de todos los archivos .apk presentes en el dispositivo. Luego diferenciamos las aplicaciones instaladas en función de si se instaló desde Google Play Store o por cualquier otra fuente. (p.2).

Con esos autores descartan las aplicaciones descargadas desde Google Play ya que estas suelen estar libres de malware y se centran en las que no fueron descargadas desde allí. En la base de datos en Firebase se encuentran muestras de paquetes que contienen las aplicaciones presentes en el dispositivo y tienen unas etiquetas que muestran si la aplicación es segura, está en proceso, o no es segura. Ahora se conecta con esta base de datos y se compraran los paquetes allí disponibles con el de la aplicación que está siendo analizada, si existe el paquete,

se obtiene su etiqueta y en caso de que no sea segura se pide al usuario que desinstale la aplicación.



Ilustración 3. Muestra de la base de datos en Firebase. Tomada De: Kanwal, M., Thakur, S., & Lashkari, R. (2017). An app based on static analysis for android ransomware. Scopus

4.3. Sdguard app

Esta aplicación implementa permisos para detectar si un Ransomware está encriptando archivos de la memoria externa del teléfono.

Una desventaja de esta aplicación es que a la hora de instalar es necesario que el teléfono este rooteado y tenga el sistema de archivos FUSE en la SD.

Sdguard tiene una arquitectura que consta de dos componentes de servicio (monitor de pila de actividad y analizador de registro de E / S) y una lista de control de acceso. Cuando una aplicación crea un

archivo, el demonio FUSE personalizado modifica el propietario y el grupo del archivo. Por otro lado si una aplicación lee o escribe un archivo, el módulo del comprobador de permisos verifica su UID y el permiso para determinar la acción de acceso (permitir o rechazar). La grabadora de E / S es capaz de registrar todas las operaciones de E / S en la SD, y luego escribir el registro en un archivo. El analizador de registro de E / S analiza este último archivo e intenta encontrar acciones maliciosas. (Hong, Liu, Ren, & Chen, 2017) declaran:

También creamos algunos archivos señuelo a los que pueden acceder las aplicaciones instaladas. Podemos encontrar un tipo de ransomware que encripta el archivo. El usuario puede establecer algunas reglas de acceso específicas para las aplicaciones instaladas a través de la lista de control de acceso (...). El servicio de monitoreo de la pila de actividades se encarga de supervisar la pila de actividad del sistema Android (...). Al encontrar una actividad de determinada aplicación, (...), podemos pensar que la aplicación es Ransomware que puede bloquear la pantalla del usuario, por lo tanto matamos su proceso para eliminar la amenaza. (p.1)

5. Recomendaciones y conclusiones

Evitar descargar aplicaciones de terceros o ingresar a sitios web de extraña procedencia, de ser posible únicamente a través de Google Play Store o tiendas

certificadas ya que estas suelen revisar el código fuente de todas las aplicaciones.

En caso de manejar información valiosa (Cuentas bancarias, archivos privados, entre otros) por medio de cualquier dispositivo móvil o computadora, es recomendable contar con la ayuda de aplicaciones que detectan posibles amenazas como Ransomware.

Contar con copias de seguridad de la información sensible en caso de que no se haya detectado la amenaza a tiempo.

Los antivirus pueden detectar amenazas como Ransomware, así que de ser posible es recomendable instalar un antivirus confiable y estar al tanto de sus actualizaciones y notificaciones de posibles amenazas.

Tener cuidado a la hora de otorgar permisos a las aplicaciones desconocidas o poco confiables, ya que algunas solicitan el permiso de acceso a archivos para así encriptar y robar la información.

Reforzar la seguridad de las aplicaciones agregando métodos como el envío de correos o códigos de seguridad que permitan la confirmación de identidad del usuario evitando así el envío y manipulación de información sensible.

6. Bibliografía

- Chen , J., Wang, C., Zhao , Z., Chen, K., Du, R., & Ahn, G. (2018). Uncovering the Face of Android Ransomware: Characterization and Real-Time Detection. *Scopus*, 14.
- Ferrante, A., Malek, M., Martinelli, F., Mercaldo, F., & Milosevic, J. (2018). Extinguishing ransomware - a hybrid approach to android ransomware detection. *Scopus*.
- Gharib, A., & Ghorbani, A. (2017). DNA-Droid: A real-time android ransomware detection framework. *Scopus*.
- Hong, S., Liu, C., Ren, B., & Chen, J. (2017). Poster: Sdguard - An android application implementing privacy protection and ransomware detection. *Scopus*.
- Kanwal, M., Thakur, S., & Lashkari, R. (2017). An app based on static analysis for android ransomware. *Scopus*.
- Monika, Zavorsky, P., & Lindskog, D. (2016). Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization . *Scopus*, 7.
- Song, S., Bongjoon, K., & Sangjun, L. (2016). The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform. *Scopus*, 10.
- Yang, T., Yang, Y., Qian, K., Lo, D.-T., Qian, Y., & Tao, L. (2015). Automated detection and analysis for android ransomware. *Scopus*.