red seguridad

Revista especializada en Seguridad de la Información

Nº 80 primer trimestre 2018 Época II

Los nuevos enemigos silenciosos de Android

Fernando Carrazón
COO de GoNetFPI

Los teléfonos móviles se han convertido en un elemento imprescindible para la mayoría de los españoles, y es que, en la actualidad, ya nadie puede pasar un día entero sin ellos. Dentro de este panorama, es innegable que Android se ha convertido en el sistema operativo líder en el mundo; con él opera el 72 por ciento de los terminales. En el caso de España, nueve de cada 10 dispositivos tienen el sistema operativo de Google, lo que los ha convertido en un objetivo prioritario para los ciberdelincuentes.

Durante 2017 hemos podido apreciar una migración de los *malwares* bancarios hacia los terminales móviles Android. Los ciberdelincuentes son conscientes de que cada día crece el número de personas que sustituyen su ordenador por su teléfono móvil o tablet. En los últimos meses, se han localizado distintos *malwares* que afectan a entidades bancarias españolas, entre los que destacan Marcher, Maza-bot y Charger (que luego analizaremos más detenidamente). Además de éstos últimos, destinados al robo, se empiezan a ver varias familias de *malware* destinadas a minar criptomonedas.

La realidad es que la tecnología avanza sin descanso en dos sentidos: hacia la innovación para mejorar en el desarrollo de nuestra sociedad y, por otro lado, hacia la sofisticación de la ciberdelincuencia como consecuencia de la proliferación de la conectividad de los dispositivos. Por este motivo, la innovación constante es una obligación para estar a la vanguardia de la seguridad en lo que a temas de fraude se refiere. En este panorama de amenazas sofisticadas y en constante crecimiento es donde toman especial relevancia los Android Forensics Analytics, análisis en profundidad de los dispositivos a través de los cuáles se puede saber si han estado expuestos a un ataque o vulnerabilidad y que permite tomar las medidas oportunas para evitar incidentes futuros.

El análisis forense

Siempre que un dispositivo tenga un comportamiento anómalo, debemos actuar. Es muy importante realizar un análisis forense remoto que permitirá proteger al equipo frente a:

- Incidentes de código malicioso.
- Incidentes de acceso no autorizado.
- Incidentes por uso inapropiado.
- Filtración de documentos confidenciales.
- Comportamientos anómalos de los sistemas.
- Destrucción de datos.
- Futuros ataques.
- A ataques contra la propiedad intelectual y el derecho a la intimidad.
- Sabotajes y fraude informático.

Pero la primera pregunta que se nos viene a la cabeza es ¿cómo se realiza un forense remoto?, ¿cuánto tiempo dura el análisis?, ¿podré disponer de mi dispositivo?

Antes de nada, es importante no utilizar el dispositivo para conservar las huellas que ha podido dejar el incidente, analizarlo y extraer información que será de gran utilidad para prevenir futuros ataques. Por lo tanto, la cuarentena del equipo hasta que el forense complete su análisis es muy relevante.

Para el proceso de búsqueda y análisis por parte del forense, se instala un *software*, proporcionado siempre por el analista, que permite obtener todas las evidencias ocultas en el equipo. En el caso de Android, el usuario debe abrir la aplicación manualmente y conectar el cargador al dispositivo. En ese momento se realiza una conexión con el servidor forense sin que el usuario tenga que intervenir más. De hecho, es conveniente no llevar a cabo ninguna acción mientras se realiza el análi-

sis forense, que suele durar poco más de tres horas. No obstante, el dispositivo se encuentra totalmente operativo mientras se realiza el mismo. Transcurrido el tiempo de análisis se realiza un dictamen y se elabora un detallado informe forense sobre el mismo, tras el cual ya se puede desinstalar la aplicación del dispositivo.

Pero, ¿qué debemos hacer si el resultado del forense determina que nuestro terminal está infectado? Dependiendo del tipo de *malware* que haya infectado nuestro dispositivo, éste actuará de una forma u otra. Si es de tipo bancario, normalmente nos suele solicitar los datos de nuestras tarjetas de crédito o cuentas bancarias. Es muy importante desconfiar siempre de pantallas mal diseñadas o cuando notemos una superposición de pantallas entre las aplicaciones de tipo bancario.

Aunque los ataques son cada vez más sofisticados, siempre existen conductas que nos permiten evitarlos y mantener los dispositivos libres de *malware*, como son:

- Instalar solo *apps* de sitios oficiales, en el caso de Android.
- Desconfiar de las aplicaciones que solicitan permisos excesivos.
- Instalar solo las aplicaciones que vamos a utilizar.
- Es muy importante mantener actualizadas las aplicaciones y el software del fabricante.
- No está de más usar un antivirus en tu dispositivo. Los hay gratuitos y la instalación es inmediata.
- Cuidado con las páginas de dudosa legalidad, como pueden ser las webs para ver el futbol online, descargas de *torrents* o sitios con calificación para adultos.

Marcher, Maza-bot y Charger

Antes hicimos referencia a tres *malwares* que afectaban a entidades bancarias: Marcher, Maza-bot y Charger. Este tipo de *malwares*, localizados a través de Android Forensics Analytics, se han convertido en los enemigos silenciosos de los dispositivos Android. Todos ellos tienen un funcionamiento similar: buscan una sobreposición sobre una aplicación legítima mostrando un *phishing*. A pesar de que las entidades bancarias envían mensajes de texto a los móviles de sus clientes con las OTP (contraseñas de un solo uso), estos *malwares* tienen implementadas diferentes soluciones que logran su objetivo: leer esa clave OTP remotamente. En los análisis se detecta que los teléfonos infectados envían datos a sus respectivos paneles de control, con localizaciones normalmente en Europa del Este.

Marcher y Maza-bot tienen en su código los nombres de las aplicaciones a las que van a suplantar. En el *command and control* (C&C) existen páginas web de *phishing* para cada uno de sus objetivos, que se cargan al iniciar la aplicación que se desea infectar. Al mismo tiempo, el móvil infectado deja de recibir SMS de cara al usuario y los mensajes recibidos son interceptados por el *malware* y reenviados al C&C sin dejar rastro de ellos en el terminal, por lo que pasa totalmente inadvertido.

Sin embargo, Charger actúa de una forma diferente. Este *malware* realiza una recopilación de las aplicaciones instaladas en el móvil y las envía al C&C. Posteriormente, se envía al móvil el código para mostrar el *phishing* y, tras recibir a través de esta técnica fraudulenta las credenciales, se inserta una pantalla de bloqueo (habitualmente una pantalla con el muñeco de Android y la excusa de actualizar las aplicaciones en el móvil) que impide al usuario realizar cualquier tipo de acción mientras los ciberdelincuentes realizan las operaciones bancarias.

Dependiendo del *malware*, existen distintas tendencias para lograr la instalación en los dispositivos. Si nos referimos a Marcher y Maza-bot, lo más habitual es encontrarlos en páginas de dudosa legalidad. En estos casos, las aplicaciones llevan nombres destinados a confundir al usuario con actualizaciones, juegos gratuitos o cualquier otro tipo de nombre capaz de engañar a la víctima, como por ejemplo: Flash Player 10 Update, MobileConnect o Android Security Update 16.2.1.

En los casos detectados de Charger, la infección resulta mucho más sencilla. Estos *malwares* son capaces de evadir los sistemas de detección de Play Store, por lo que estas aplicaciones, que tienen un tiempo de vida estimado de alrededor de 15 días, están disponibles y cualquier usuario las puede descargar. En los casos analizados de Charger, se ha observado que entre 1.000 y 5.000 usuarios han descargado e instalado estas aplicaciones, según los datos que ofrece Play Store. La mayoría de las aplicaciones disponibles en esta plataforma con el *malware* Charger suele estar relacionada con linternas. Normalmente, estas aplicaciones nos piden unos permisos de ejecución que poco tienen que ver con su funcionalidad. Por ejemplo, en el caso de las linternas, suelen pedir el acceso a la lectura y envío de SMS, cosa que debería hacernos sospechar de su legitimidad.

Por lo tanto, ante estos nuevos *malwares*, lo principal es usar el sentido común y siempre desconfiar de cualquier cosa que nos resulte sospechosa o fuera de lo normal. ■