Investigadores de seguridad cibernética revelaron ayer detalles sorprendentes sobre una campaña generalizada de malware para Android en la que los atacantes reemplazaron de forma silenciosa las apps legítimas instaladas por sus versiones maliciosas en casi 25 millones de teléfonos móviles.

Dichas apps van desde JioTV, AppLock, HotStar, Flipkart, Opera Mini, TrueCaller, hasta apps como WhatsApp o Telegram.

Según los investigadores de Check Point, los atacantes están distribuyendo un nuevo tipo de malware para Android, que se disfraza de edición de fotos de aspecto inocente, entretenimiento para adultos o aplicaciones de juegos y está disponible por medio de las tiendas de aplicaciones de terceros ampliamente utilizadas.

El malware, apodado como Agent Smith, aprovecha múltiples vulnerabilidades de Android, como la falla de Janus y la falla de Man-in-the-Disk, e inyecta código malicioso en los archivos APK de aplicaciones específicas instaladas en un dispositivo comprometido y luego vuelve a aparecer de forma automática.

> *«No es suficiente para esta familia de malware intercambiar solo una aplicación inocente con un doble infectado. Lo hace para todas y cada una de las aplicaciones en el dispositivo, siempre y cuando los nombres de los paquetes estén en su lista de presas. Con el tiempo, esta campaña también infectará el mismo dispositivo, repetidamente, con los últimos parches maliciosos. Esto nos lleva a estimar que hay más de 2.8 mil millones de infecciones en total, en alrededor de 25 millones de dispositivos únicos, lo que significa que, en promedio, cada víctima habría sufrido aproximadamente 112 intercambios de aplicaciones inocentes»,* dijeron los investigadores.

Los investigadores creen que el malware está vinculado a una compañía con sede en China, y ha sido diseñado para obtener ganancias financieras al ofrecer anuncios maliciosos a las víctimas.

Después de la instalación de aplicaciones falsas, el malware Agent Smith aprovecha una cadena de infección de tres etapas y contiene diferentes módulos para cada paso, su funcionamiento es el siguiente:

1.- Módulo del cargador: la aplicación inicial que distribuye el malware contiene un módulo llamado Loader, cuyo único propósito es descifrar, extraer y ejecutar el módulo de la segunda etapa, llamado Core.

2.- Módulo Core: una vez ejecutado, el módulo Core se comunica con el servidor C&C de los atacantes para recibir una lista de aplicaciones populares que deben ser dirigidas.

Si se encuentra una coincidencia instalada en el dispositivo de la víctima, el módulo Core intenta infectar el APK objetivo utilizando la vulnerabilidad de Janus o simplemente recompilando el APK con una carga útil maliciosa.

Además, para instalar automáticamente el APK modificado y reemplazar su versión original sin el consentimiento de los usuarios, los atacantes utilizan una serie de vulnerabilidades de 1-Day, incluido el ataque man-in-the-disk.

3.- Boot Module: Este módulo (de inicio), se incluye en la carga maliciosa que se empaquetó con la aplicación original y funcionó igual que el módulo del cargador. Extrae y ejecuta una carga útil malintencionada, llamada módulo de parches, cuando una víctima ejecuta la aplicación modificada.

4.- Módulo de parches: el módulo de parches se diseñó para evitar que las aplicaciones modificadas obtengan actualizaciones legítimas que, de ser instaladas, revertirían todos los cambios maliciosos.

> *«Mientras invierte muchos recursos en el desarrollo de este malware, el actor detrás de Agent Smith no quiere una actualización real para eliminar todos los cambios realizados, por lo que aquí es donde entra en juego el módulo Patch. Con el*

> *único propósito de deshabilitar las actualizaciones automáticas para la aplicación infectada, este módulo observa el directorio de actualización de la aplicación original y elimina el archivo una vez que aparece».*

5.- Módulo AdSDK: esta es la carga útil real que muestra los anuncios a las víctimas con fines de lucro y también infecta el dispositivo con otras familias de software publicitario.

Sin embargo, los investigadores advierten que este malware modular podría adaptarse fácilmente para fines mucho más intrusivos y dañinos, como el robo de información confidencial, desde mensajes privados hasta credenciales bancarias y mucho más.

Los investigadores se encontraron inicialmente con el malware Agent Smith a inicios de 2019, que se encontraba principalmente en dispositivos Android en la India y en otros países asiáticos cercanos como Pakistán, Bangladesh, Indonesia y Nepal.

Sin embargo, el malware también afectó a un número considerable de dispositivos en Estados Unidos (más de 300,000), Australia (más de 140,000), y el Reino Unido (más de 135,000).

Además de las tiendas de aplicaciones de terceros, los investigadores también encontraron al menos 11 aplicaciones infectadas en Google Play Store en los últimos meses, que contienen componentes malintencionados pero inactivos de Agent Smith.

Esto indica de cierta manera, que los actores de amenazas detrás de la campaña de malware también quieren encontrar una forma en la plataforma de descarga de apps de Google para difundir su adware. Google por su parte ya eliminó todas las aplicaciones de su tienda.

Debido a que el Agent Smith ha infectado principalmente a los usuarios que descargaron aplicaciones de tiendas de aplicaciones de terceros, se recomienda siempre a los usuarios que descarguen aplicaciones de tiendas confiables para minimizar el riesgo de infección.