xHelper es una pieza misteriosa de malware para Android que se reinstala en dispositivos aún después de que los usuarios lo eliminan o restablecen los dispositivos de fábrica.

Según los informes, xHelper infectó a más de 45 mil dispositivos el año pasado, y desde entonces, los investigadores de seguridad cibernética estuvieron tratando de descubrir cómo el malware sobrevive al restablecimiento de fábrica y cómo ha infectado a tantos dispositivos en primer lugar.

En una publicación de hoy, Igor Golovin, analista de malware de Kaspersky, finalmente resolvió el misterio al revelar detalles técnicos acerca del mecanismo de persistencia utilizado por el malware, y finalmente también descubrió cómo eliminar completamente xHelper de un dispositivo infectado.

Como el vector de ataque inicial y para su distribución, la aplicación de malware se disfraza como una aplicación de optimización de velocidad y limpiador popular para teléfonos inteligentes, que afecta principalmente a los usuarios en Rusia (80.56%), India (3.43%) y Argelia (2.43%).

> *«Pero en realidad, no existe nada útil al respecto: luego de la instalación, el limpiador simplemente desaparece y no se ve en ninguna parte ni en la pantalla principal ni en el menú del programa. Puede verlo solo inspeccionando la lista de aplicaciones instaladas en la configuración del sistema»,* dijo Golovin.

Una vez instalada por un usuario desprevenido, la aplicación maliciosa se registra a sí misma como un servicio en primer plano y luego extrae una carga útil cifrada que recopila y envía información de identidad del dispositivo objetivo a un servidor web remoto controlado por el atacante.

En el siguiente paso, la aplicación maliciosa ejecuta otra carga útil ofuscada que desencadena un conjunto de exploits de rooteo de Android e intenta obtener acceso administrativo al sistema operativo del dispositivo.

> *«El malware puede obtener acceso a la raíz principalmente en dispositivos con versiones de Android 6 y 7 de fabricantes chinos (incluidos los ODM)»*, dijo Golovin.

El malware se encuentra en silencio en el dispositivo y espera los comandos de los atacantes. Según un análisis previo del mismo malware realizado por investigadores de Symantec, utiliza la fijación de certificados SSL para evitar que su comunicación sea interceptada.

> *«El malware instala una puerta trasera con la capacidad de ejecutar comandos como superusuario. Proporciona a los atacantes acceso total a todos los datos de la aplicación y también puede ser utilizado por otro malware, por ejemplo, CookieThief».*

Si el ataque tiene éxito, la aplicación maliciosa luego abusa del privilegio de root para instalar silenciosamente xHelper copiando directamente los archivos de paquetes maliciosos en la partición del sistema (/system/bin folder) después de volver a montarlo en el modo de escritura.

> *«A todos los archivos en las carpetas de destino se les asigna en el atributo inmutable, lo que dificulta la eliminación del malware porque el sistema ni siquiera permite que los superusuarios eliminen archivos con este atributo»*, dijo Golovin.

Algo interesante, es que aunque una aplicación de seguridad legítima o un usuario afectado podrían simplemente volver a montar la partición del sistema, de la misma forma, para eliminar de permanentemente el archivo de malware, xHelper también modifica una biblioteca del sistema (libc.so) con la intención de prevenir la infección y volver a montar la partición del sistema en el modo de escritura.

> *«Además de eso, el troyano descarga e instala varios programas maliciosos más y*

> *elimina las aplicaciones de control de acceso de root, como Superuser»,* dijo Golovin.

Según Kaspersky, reemplazar la biblioteca modificada con la del firmware original para un teléfono inteligente Android podría volver a habilitar la partición del sistema de montaje en el modo de escritura para eliminar permanentemente el malware xHelper para Android.

Sin embargo, en lugar de seguir un procedimiento tan complicado para deshacerse del malware, se aconseja a los usuarios afectados que simplemente vuelvan a flashear sus teléfonos con una copia nueva del firmware descargado del sitio web oficial de los proveedores o instalando un dispositivo diferente pero compatible.