Hace unos meses, cientos de usuarios de Android se quejaron en Internet por una nueva pieza de malware misterioso que se esconde en los dispositivos infectados, y que según los informes, puede reinstalarse aún después de que los usuarios eliminen la aplicación o restablezcan sus dispositivos de fábrica.

Nombrado como Xhelper, el malware ya ha infectado más de 45 mil dispositivos Android en los últimos seis meses, y sigue propagándose infectando al menos 2400 dispositivos en promedio cada mes, según el último informe publicado hoy por Symantec.

Aunque los investigadores de Symantec no encontraron la fuente exacta de donde proviene la aplicación maliciosa empaquetada con el malware Xhelper, la compañía de seguridad cibernética sospechó que una aplicación del sistema malicioso preinstalada en dispositivos Android de ciertas marcas es el que descarga el malware.

> *«Ninguna de las muestras que analizamos estaba disponible en Google Play Store, y aunque es posible que el malware Xhelper sea descargado por usuarios de fuentes desconocidas, creemos que puede no ser el único canal de distribución»*, dijeron los investigadores en su reporte.
>
> *«Desde nuestra telemetría, hemos visto que estas aplicaciones se instalan con más frecuencia en ciertas marcas de teléfonos, lo que nos lleva a creer que los atacantes pueden centrarse en marcas específicas»*, agregaron.

En un reporte separado, publicado hace dos meses por Malwarebytes, los investigadores creyeron que el malware Xhelper se estaba propagando por medio de *«redireccionamientos web»* u *«otros sitios web sospechosos»* que incitan a los usuarios a descargar aplicaciones de fuentes externas no confiables.

¿Cómo trabaja Xhelper?

Una vez instalado, Xhelper no proporciona una interfaz de usuario normal, sino que se instala como un componente de aplicación que no aparece en el iniciador de aplicaciones del dispositivo en un intento por permanecer oculto para los usuarios.

Xhelper se basa en algunos eventos externos activados por los usuarios, como conectar o desconectar el dispositivo infectado de una fuente de alimentación, reiniciar un dispositivo o instalar y desinstalar aplicaciones.

Una vez lanzado, el malware se conecta a su servidor remoto de comando y control por medio de un canal encriptado y descarga cargas adicionales como cuentagotas, clickers y rootkits en los dispositivos Android comprometidos.

> *«Creemos que el conjunto de malware almacenado en el servidor de C&C tiene una funcionalidad amplia y variada, que ofrece al atacante múltiples opciones, incluido el robo de datos o incluso la toma completa del dispositivo»*, dicen los investigadores.

Los investigadores creen que el código fuente de Xhelper sigue siendo un trabajo en progreso, ya que algunas de sus *«variantes más antiguas incluyen clases vacías que no se implementaron en ese momento, pero la funcionalidad ahora está totalmente habilitada».*

Se ha visto que el malware Xhelper está dirigido a usuarios de teléfonos inteligentes Android principalmente en India, Estados Unidos y Rusia.

Aunque muchos productos antivirus para Android pueden detectar el malware Xhelper, aún no lo pueden eliminar permanentemente ni bloquear su reinstalación en los dispositivos infectados.