Masterhacks – Investigadores descubrieron un nuevo ransomware que secuestra toda la información de un teléfono con Android, cambiando el código PIN y cifrando todos los archivos con el objetivo de que la víctima pague un rescate.

Se trata de DoubleLocker, uno de los ransomwares más elaborados y sofisticados en la historia de Android.

Según Lukas Stefanko, miembro del equipo de investigadores de seguridad en ESET, es el primer ataque de ransomware que puede cifrar los datos de la víctima, además de impedir el acceso al dispositivo móvil. *«Jamás habíamos visto una combinación de ataques como esta en el ecosistema Android».*

El usuario se infecta mediante una descarga falsa de Adobe Flash Player, y aprovechando los servicios de accesibilidad de Android, bloquea el acceso al teléfono cambiando el código PIN.

Este ransomware puede afectar a cualquier usuario de Android, ya que no requiere que se haya hecho root al dispositivo. Cuando la víctima se infecta, el malware se convierte en el launcher Android por defecto para el control del acceso a dispositivo y mostrar la pantalla de bloqueo cuando el usuario presiona el botón de home.

DoubleLocker también cifra los datos de la víctima, por lo que no es posible recuperar los archivos sin pagar el rescate a los piratas.

Para retomar el control del teléfono, es necesario realizar un pago de 0.0130 bitcoins, equivalente a unos 74 dólares, para poder desbloquear el teléfono y recuperar los datos. En caso de no querer pagar, simplemente se realiza un hard reset al dispositivo, teniendo en mente que se perderá toda la información almacenada.