31/10/2024

Así funciona TrickMo: el virus bancario que también roba el PIN y el patrón de desbloqueo del móvil

Las herramientas que tienen los ciberdelincuentes también evolucionan con el desarrollo tecnológico



En un ciberataque tenemos que ser conscientes de que el objetivo principal de los estafadores es hacerse tanto con nuestros datos personales como los bancarios. Para ello suelen acudir a técnicas como hacernos rellenar un falso formulario con toda esta información haciéndose pasar por una entidad conocida que no levante sospechas, ya sea Hacienda o la DGT.

Pero para que su engaño funcione, es fundamental que la víctima pique y sea ella misma quien entregue esta información. Pero ha medida que la tecnología evoluciona y desarrolla nuevas funciones y capacidades, **las herramientas que tienen los ciberdelincuentes también lo hacen y se vuelven todavía más eficaces y sofisticadas**.

Ahora, como han identificado las firmas de seguridad Cleafy y Zimperium, han descubierto una variante de el troyano bancario conocido como TrickMo, el cual ha ampliado sus capacidades para permitir a los ciberdelincuentes acceder y controlar el dispositivo móvil incluso si está bloqueado al poder robar el código PIN y el patrón de desbloqueo.

Originalmente, TrickMo ha sido siempre**un troyano diseñado para acceder sin autorización a las cuentas bancarias y transacciones financieras de sus víctimas**, con el objetivo de robar su dinero. Para ello, es capaz de **grabar la pantalla, interceptar los códigos de un solo uso** (OTP, por sus siglas en inglés)**y conceder permisos de manera automática** en las notificaciones emergentes.

El troyano tiene múltiples variantes, y esta última, además, ha compartido nuevas capacidades encontradas en las variantes que ha analizado, que**apuntan** al control del dispositivo móvil incluso cuando está bloqueado.

En concreto, algunas muestran tenían la capacidad de**robar el PIN o patrón de desbloqueo con una interfaz falsa que simula ser la del dispositivo móvil**. De esta forma, de manera inadvertida, la víctima introduce su información de desbloqueo y esta se transmite a los cibercriminales.

El análisis de Zimperium ha permitido ubicar a las víctimas principalmente en Canadá, Emiratos Árabes Unidos, Turquía y Alemania, aunque su principal objetivo son las credenciales de las cuentas bancarias, no es el único, puesto que **también se dirige contras las que dan acceso a recursos empresariales**, **como las VPN.**

Fuente: https://www.eleconomista.es/

LINK DE LA NOTICIA