Se han descubierto nuevas variantes de un troyano bancario para Android conocido como TrickMo, las cuales incluyen funcionalidades no documentadas previamente que permiten robar el patrón de desbloqueo o el PIN de un dispositivo.

> *«Esta nueva funcionalidad permite que los actores maliciosos operen en el dispositivo incluso cuando está bloqueado»,* comentó Aazim Yaswant, investigador de seguridad de Zimperium, en un análisis publicado la semana pasada.

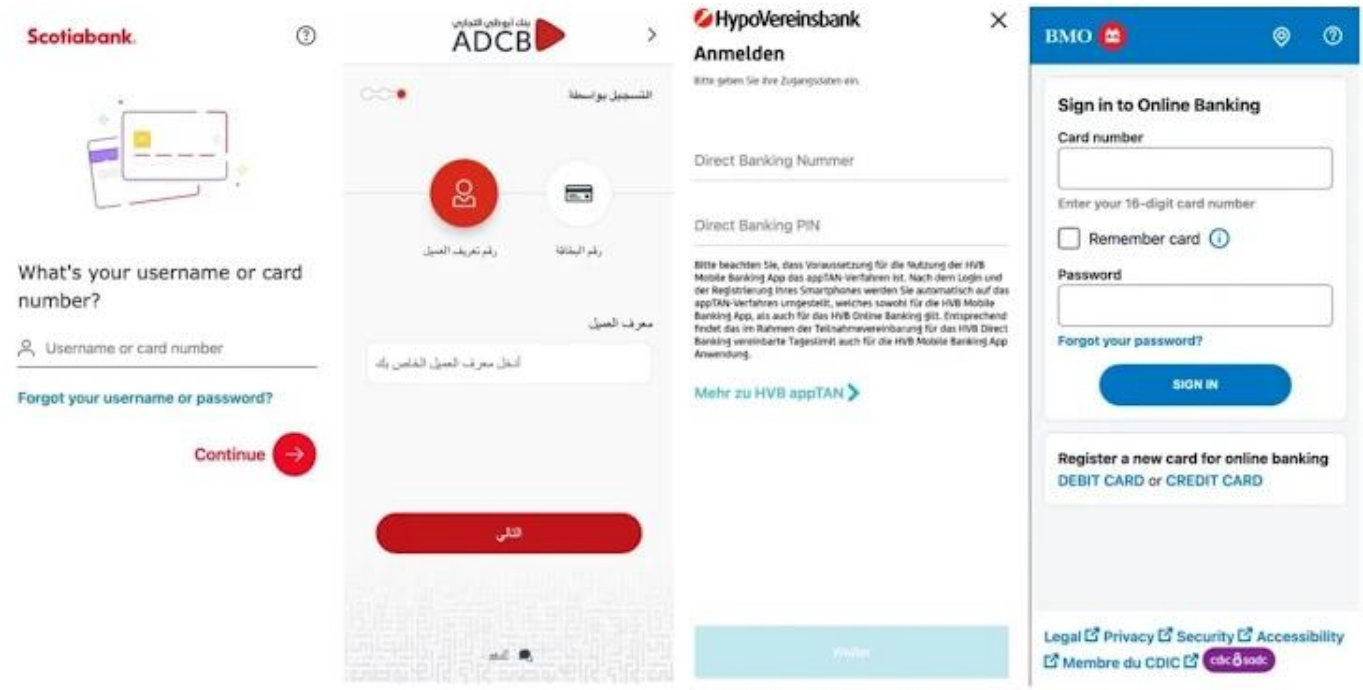
Identificado por primera vez en 2019, TrickMo debe su nombre por su relación con el grupo cibercriminal TrickBot y tiene la capacidad de otorgar control remoto sobre los dispositivos infectados. Además, puede robar contraseñas de un solo uso (OTP) enviadas por SMS y mostrar pantallas superpuestas que capturan credenciales al abusar de los servicios de accesibilidad de Android.

El mes pasado, la empresa italiana de ciberseguridad Cleafy informó sobre versiones actualizadas de este malware móvil, las cuales incluyen mecanismos mejorados para evitar su detección y obtener permisos adicionales para llevar a cabo diversas actividades maliciosas, como realizar transacciones no autorizadas.

Algunas de las nuevas variantes del malware también están diseñadas para capturar el patrón de desbloqueo o el PIN del dispositivo al mostrar una interfaz de usuario falsa que imita la pantalla de desbloqueo real.

Esta interfaz es una página HTML alojada en un sitio web externo y se presenta en modo de pantalla completa, lo que hace que parezca una pantalla de desbloqueo legítima.

Si los usuarios introducen su patrón de desbloqueo o PIN, esa información, junto con un identificador único del dispositivo, se envía a un servidor controlado por los atacantes («android.ipgeo[.]at») a través de una solicitud HTTP POST.



Zimperium señaló que la falta de protecciones de seguridad adecuadas en los servidores de comando y control (C2) permitió obtener información sobre los tipos de datos almacenados en ellos. Entre estos datos se encuentran archivos con alrededor de 13,000 direcciones IP únicas, la mayoría de las cuales están localizadas en Canadá, Emiratos Árabes Unidos, Turquía y Alemania.

> *«Las credenciales robadas no se limitan únicamente a información bancaria, sino que también incluyen aquellas que permiten acceder a recursos corporativos, como VPNs y sitios internos. Esto resalta la importancia crítica de proteger los dispositivos móviles, ya que pueden ser una vía principal para ataques cibernéticos contra organizaciones»*, afirmó Yaswant.

Otro aspecto destacado de TrickMo es su amplio alcance, ya que recolecta datos de aplicaciones que abarcan múltiples categorías, como banca, empresas, empleo, comercio electrónico, redes sociales, entretenimiento, VPNs, gobierno, educación, telecomunicaciones

y salud.

Este avance ocurre en medio del surgimiento de una nueva campaña de un troyano bancario para Android llamado ErrorFather, el cual utiliza una variante del malware Cerberus para cometer fraudes financieros.

> *«La aparición de ErrorFather subraya el peligro persistente de malware reciclado, ya que los cibercriminales siguen aprovechando el código fuente filtrado, incluso años después de que se descubriera el malware Cerberus original»*, explicó Symantec, una empresa propiedad de Broadcom.

De acuerdo con datos de Zscaler ThreatLabz, los ataques móviles motivados por razones financieras que utilizan malware bancario han aumentado un 29% en el período comprendido entre junio de 2023 y abril de 2024, en comparación con el año anterior.

India fue el país más afectado por estos ataques móviles durante ese período, con un 28% del total, seguido por EE. UU., Canadá, Sudáfrica, Países Bajos, México, Brasil, Nigeria, Singapur y Filipinas.