Investigadores en ciberseguridad han descubierto una nueva variante de un troyano bancario para Android llamado TrickMo, que presenta nuevas capacidades para evitar el análisis y mostrar pantallas de inicio de sesión falsas con el fin de capturar las credenciales bancarias de las víctimas.

> *«Los métodos incluyen el uso de archivos ZIP mal formateados junto con JSONPacker. Además, la aplicación se instala a través de una aplicación dropper que emplea los mismos métodos de evasión de análisis»*, señalaron los investigadores de Cleafy, Michele Roviello y Alessandro Strino.
>
> *«Estas características están diseñadas para eludir la detección y complicar los esfuerzos de los expertos en ciberseguridad para analizar y neutralizar el malware.»*

TrickMo, que fue detectado por primera vez en el entorno real por CERT-Bund en septiembre de 2019, ha sido conocido por atacar dispositivos Android, particularmente apuntando a usuarios en Alemania para robar contraseñas de un solo uso (OTPs) y otros códigos de autenticación de dos factores (2FA) para facilitar el fraude financiero.

Este malware orientado a móviles se considera parte del trabajo del ahora desaparecido grupo de cibercrimen TrickBot, que ha ido mejorando continuamente sus técnicas de ofuscación y evasión para mantenerse bajo el radar.

Entre sus características más destacadas se encuentran la capacidad para registrar la actividad de la pantalla, capturar las pulsaciones de teclas, recolectar fotos y mensajes SMS, controlar remotamente el dispositivo infectado para llevar a cabo fraudes en el dispositivo (ODF), y abusar de la API de servicios de accesibilidad de Android para realizar ataques de superposición HTML y ejecutar clics y gestos en el dispositivo.

La aplicación dropper descubierta por la empresa de ciberseguridad italiana se hace pasar por el navegador web Google Chrome, que, al ser abierto después de la instalación, solicita a

la víctima actualizar Google Play Services haciendo clic en el botón Confirmar.

Si el usuario procede con la actualización, un archivo APK que contiene la carga útil de TrickMo se descarga en el dispositivo bajo el nombre de *«Servicios de Google,»* tras lo cual se le pide al usuario que habilite los servicios de accesibilidad para la nueva aplicación.

> *«Los servicios de accesibilidad están diseñados para asistir a usuarios con discapacidades ofreciendo formas alternativas de interactuar con sus dispositivos. Sin embargo, cuando son utilizados por aplicaciones maliciosas como TrickMo, estos servicios pueden otorgar un control extensivo sobre el dispositivo»,* explicaron los investigadores.
>
> *«Este permiso elevado permite a TrickMo realizar diversas acciones maliciosas, como interceptar mensajes SMS, manejar notificaciones para interceptar u ocultar códigos de autenticación, y ejecutar ataques de superposición HTML para robar credenciales de usuario. Además, el malware puede desactivar bloqueos de pantalla y aceptar permisos automáticamente, integrándose sin problemas en las operaciones del dispositivo.»*

Asimismo, el abuso de los servicios de accesibilidad permite al malware desactivar funciones de seguridad importantes y actualizaciones del sistema, otorgar permisos automáticamente a su voluntad y prevenir la desinstalación de ciertas aplicaciones.

El análisis de Cleafy también reveló configuraciones incorrectas en el servidor de comando y control (C2) que permitieron acceder a 12 GB de datos sensibles exfiltrados de los dispositivos, incluidos credenciales y fotos, sin necesidad de autenticación.

El servidor C2 también alberga los archivos HTML utilizados en los ataques de superposición. Estos archivos incluyen páginas de inicio de sesión falsas para varios servicios, incluyendo bancos como ATB Mobile y Alpha Bank, así como plataformas de criptomonedas como

Binance.

La brecha de seguridad no solo destaca el error de seguridad operacional (OPSEC) por parte de los actores de amenaza, sino que también expone los datos de las víctimas al riesgo de explotación por otros actores de amenaza.

La gran cantidad de información expuesta desde la infraestructura C2 de TrickMo podría ser utilizada para cometer robo de identidad, infiltrar diversas cuentas en línea, realizar transferencias no autorizadas de fondos e incluso hacer compras fraudulentas. Peor aún, los atacantes podrían secuestrar las cuentas y bloquear a las víctimas al restablecer sus contraseñas.

> *«Usando información personal y fotos, el atacante puede crear mensajes convincentes que engañen a las víctimas para que divulguen aún más información o lleven a cabo acciones maliciosas,»* señalaron los investigadores.
>
> *«Explotar datos personales tan detallados resulta en daños financieros y reputacionales inmediatos y consecuencias a largo plazo para las víctimas, haciendo que la recuperación sea un proceso complicado y prolongado.»*

Esta divulgación se produce mientras Google ha estado cerrando brechas de seguridad relacionadas con la carga lateral, permitiendo a los desarrolladores de terceros verificar si sus aplicaciones están cargadas lateralmente mediante la API de Integridad de Play y, de ser así, exigir a los usuarios que descarguen las aplicaciones desde Google Play para seguir utilizándolas.