Una nueva plataforma de malware como servicio (MaaS) para Android, llamada SuperCard X, permite realizar ataques de retransmisión de comunicación de campo cercano (NFC), facilitando a los ciberdelincuentes la realización de retiros fraudulentos.

Según la empresa de prevención de fraude Cleafy, la campaña activa está dirigida a clientes de bancos y emisores de tarjetas en Italia, con el objetivo de comprometer datos de tarjetas de pago. Hay indicios de que este servicio se promociona en canales de Telegram.

SuperCard X utiliza un enfoque en varias etapas, combinando ingeniería social (a través de smishing y llamadas telefónicas), instalación de aplicaciones maliciosas e interceptación de datos NFC para cometer fraudes de manera muy efectiva, según los investigadores de seguridad Federico Valentini, Alessandro Strino y Michele Roviello.

Este malware, desarrollado por un actor de amenazas de habla china, se ha difundido mediante tres aplicaciones falsas que engañan a las víctimas para que las instalen usando técnicas de ingeniería social, como mensajes SMS o de WhatsApp engañosos:

- Verifica Carta (io.dxpay.remotenfc.supercard11)
- SuperCard X (io.dxpay.remotenfc.supercard)
- KingCard NFC (io.dxpay.remotenfc.supercard)

Los mensajes se hacen pasar por alertas de seguridad bancaria e inducen una sensación de urgencia, solicitando a los usuarios que llamen a un número para disputar una transacción.

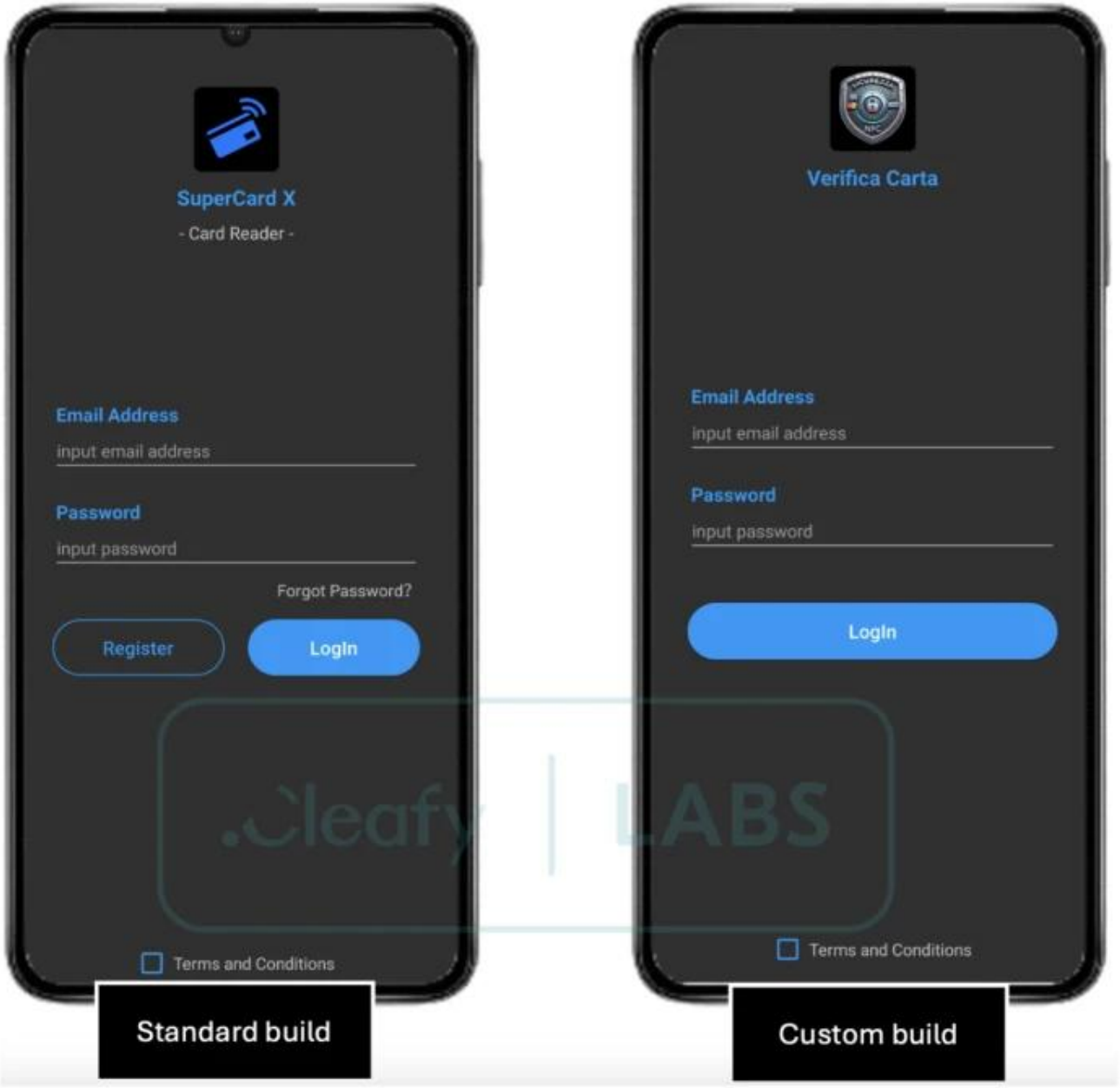
La cadena de infección continúa con lo que se llama un ataque de entrega orientado por teléfono (TOAD), donde los atacantes manipulan a las víctimas para que instalen la app haciéndose pasar por soporte técnico. También usan tácticas persuasivas para obtener los PIN y pedir que eliminen los límites de sus tarjetas, facilitando el robo de fondos.

El núcleo de la operación es una técnica de retransmisión NFC no documentada anteriormente, que permite a los atacantes autorizar pagos en puntos de venta (PoS) y retiros en cajeros automáticos interceptando y retransmitiendo comunicaciones NFC desde

dispositivos infectados.

Para ello, los atacantes piden a las víctimas que acerquen su tarjeta al teléfono móvil, lo que permite al malware SuperCard X capturar los datos NFC y enviarlos a un servidor externo. Esa información es luego usada por los atacantes en un dispositivo bajo su control para realizar transacciones no autorizadas.

La aplicación usada para capturar datos NFC en el teléfono de la víctima se llama Reader, mientras que una app llamada Tapper se instala en el dispositivo del atacante para recibir la información. La comunicación entre Reader y Tapper usa HTTP y requiere que los atacantes inicien sesión.



Por tanto, los atacantes deben crear una cuenta en la plataforma SuperCard X antes de distribuir las apps, y las víctimas deben introducir las credenciales que se les dan por teléfono.

Este paso es clave porque enlaza el dispositivo de la víctima con el Tapper del atacante, permitiendo retransmitir los datos de la tarjeta para realizar retiros. Tapper también puede emular la tarjeta robada para engañar a los terminales PoS o cajeros automáticos.

Los investigadores de Cleafy notaron que las variantes del malware Reader tienen diferencias sutiles en la pantalla de inicio de sesión, lo que sugiere que son versiones personalizadas por afiliados para campañas específicas. Además, SuperCard X utiliza TLS mutuo (mTLS) para proteger su comunicación con los servidores de control (C2).

El hecho de que los atacantes puedan manipular a los usuarios para cambiar configuraciones críticas no ha pasado desapercibido para Google, que estaría desarrollando una función en Android que bloquea la instalación de apps desde fuentes desconocidas y el otorgamiento de permisos sensibles.

Aunque no hay pruebas de que SuperCard X esté en la Google Play Store, se recomienda a los usuarios revisar cuidadosamente las descripciones, permisos y reseñas de las apps antes de instalarlas. También se aconseja mantener activado Google Play Protect para protegerse contra amenazas emergentes.

> “Esta nueva campaña representa un riesgo financiero importante que va más allá de los bancos y afecta también a emisores de tarjetas y proveedores de pago”, dijeron los investigadores.
> “La combinación innovadora de malware y retransmisión NFC permite realizar retiros fraudulentos con tarjetas de débito y crédito, siendo especialmente eficaz en cajeros automáticos sin contacto.”