Los ciberdelincuentes están adoptando cada vez más una nueva técnica que explota la comunicación de campo cercano (NFC) para sustraer fondos de las víctimas de manera masiva.

Esta estrategia, denominada Ghost Tap por la firma ThreatFabric, permite a los atacantes extraer dinero de tarjetas de crédito robadas que están vinculadas a servicios de pago móvil como Google Pay o Apple Pay, aprovechando la retransmisión del tráfico NFC.

> *«Los delincuentes ahora pueden utilizar Google Pay y Apple Pay para enviar la información de pago sin contacto (tap-to-pay) a nivel global en cuestión de segundos. Esto significa que, incluso sin tener físicamente tu tarjeta o tu teléfono, pueden realizar transacciones desde tu cuenta en cualquier parte del mundo»*, afirmó la empresa de ciberseguridad holandesa.

El modus operandi comienza engañando a las víctimas para que instalen malware bancario en sus dispositivos móviles. Este malware puede capturar credenciales bancarias y contraseñas temporales mediante técnicas como ataques de superposición de pantalla o registradores de teclas (*keyloggers*). Otra variante incluye el uso de llamadas de suplantación de identidad (*vishing*).

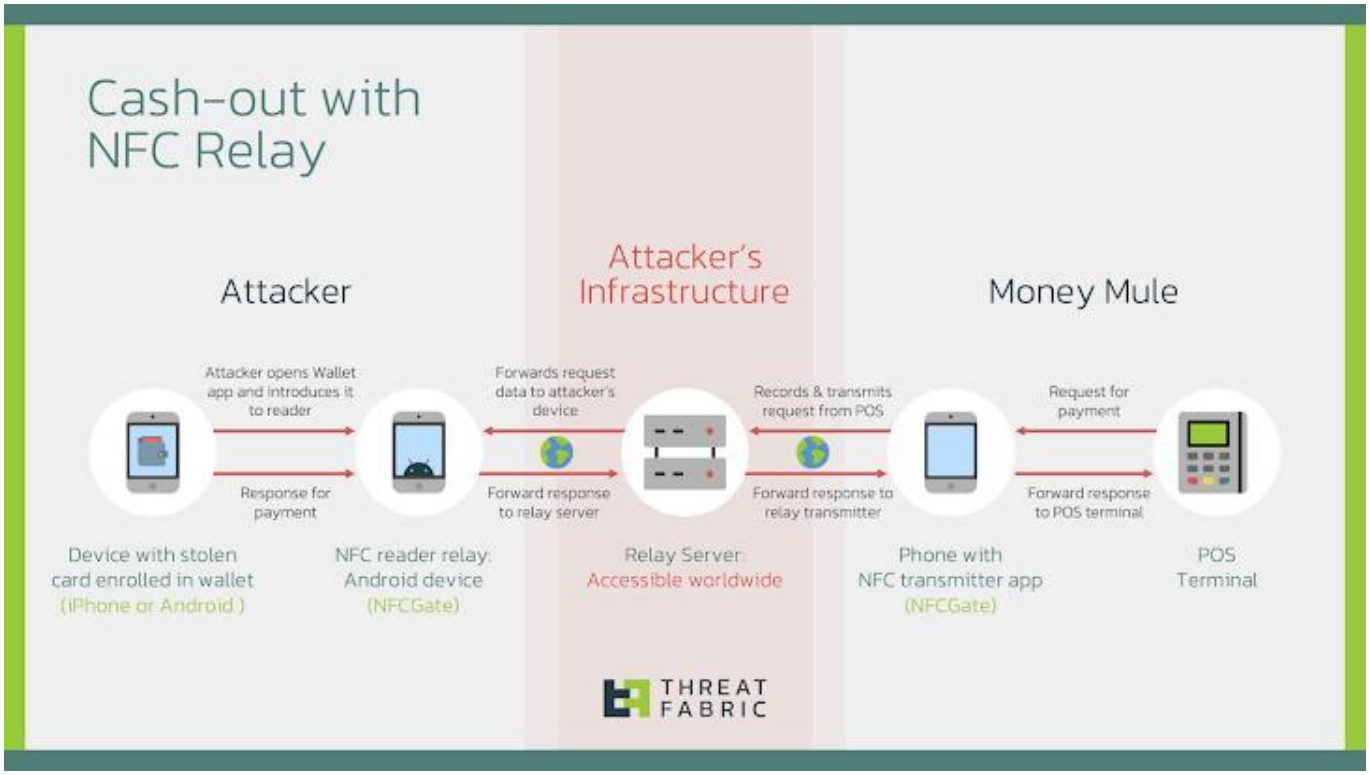
Con los datos de la tarjeta en su poder, los atacantes buscan vincularla a Google Pay o Apple Pay. Sin embargo, para evitar que el emisor de la tarjeta bloquee las operaciones, retransmiten la información de pago sin contacto a un intermediario, conocido como «mula», encargado de realizar compras fraudulentas en tiendas.

Para esto, los delincuentes emplean una herramienta legítima llamada NFCGate, diseñada para capturar, analizar y modificar tráfico NFC. Esta herramienta también permite retransmitir el tráfico NFC entre dos dispositivos mediante un servidor.

> *«Un dispositivo actúa como lector que escanea una etiqueta NFC, mientras que el*

> *otro emula una etiqueta NFC utilizando la tecnología de Emulación de Tarjeta en el Host (HCE)»,* explican investigadores del Laboratorio de Redes Móviles Seguras de la Universidad Técnica de Darmstadt.

Aunque en el pasado NFCGate había sido utilizada por criminales para extraer datos NFC de dispositivos de las víctimas, como documentó ESET en agosto de 2024 con el malware NGate, esta es la primera vez que se emplea para retransmitir la información en tiempo real.



> *«Los ciberdelincuentes pueden establecer un enlace entre un dispositivo con una tarjeta robada y un terminal de punto de venta (PoS), manteniéndose en el anonimato y llevando a cabo retiros masivos»,* señaló ThreatFabric.

> *«El atacante con la tarjeta robada no necesita estar en el lugar de la transacción. Puede encontrarse en otro país mientras la tarjeta es utilizada en varios puntos de venta en un corto lapso de tiempo».*

La técnica ofrece ventajas adicionales, como la posibilidad de comprar tarjetas de regalo en tiendas físicas sin que los delincuentes estén presentes. Además, permite escalar el esquema mediante la coordinación de varias «mulas» en distintas ubicaciones de manera simultánea.

La detección de los ataques Ghost Tap se complica porque las transacciones aparentan originarse desde el mismo dispositivo, evadiendo los sistemas antifraude. Asimismo, el dispositivo vinculado puede estar en modo avión, lo que dificulta rastrear su ubicación real y comprobar que no fue utilizado físicamente en el terminal.

> *«Creemos que el avance de las redes con mayor velocidad de comunicación, combinado con la ausencia de sistemas de detección basados en el tiempo en cajeros automáticos o terminales PoS, ha hecho posibles estos ataques. En ellos, los dispositivos con las tarjetas se encuentran lejos del lugar donde se realiza la operación (sin presencia física en el terminal)»,* explicó ThreatFabric.

> *«Con la capacidad de expandirse rápidamente y operar de manera anónima, este método de extracción de efectivo supone un gran desafío para las instituciones financieras y los comercios».*