Un grupo de hackers brasileños detrás de un malware de punto de venta (PoS) avanzado y modular conocido como Prilex, volvieron a asomar la cabeza con nuevas actualizaciones que le permiten bloquear transacciones de pago sin contacto.

La compañía rusa de seguridad cibernética Kaspersky dijo que detectó tres versiones de Prilex (06.03.8080, 06.03.8072 y 06.03.8070), que son capaces de apuntar a tarjetas de crédito habilitadas para NFC, lo que lleva su esquema criminal a un nivel superior.

Habiendo evolucionado el malware centrado en cajeros automáticos al malware de PoS a lo largo de los años desde que entró en funcionamiento en 2014, el actor de amenazas incorporó constantemente nuevas funciones diseñadas para facilitar el fraude con tarjetas de crédito, incluyendo una técnica llamada transacciones GHOST.

Aunque los pagos sin contacto han tenido un gran auge, en parte debido a la pandemia de COVID-19, el motivo subyacente detrás de la nueva funcionalidad es deshabilitar la función para obligar al usuario a insertar la tarjeta en el teclado PIN.

Con ese fin, se descubrió que la última versión de Prilex, que Kaspersky descubrió en noviembre de 2022, implementa una lógica basada en reglas para determinar si capturar o no la información de la tarjeta de crédito junto con una opción para bloquear transacciones basadas en NFC.

> *«Esto se debe al hecho de que las transacciones basadas en NFC a menudo generan una identificación única o un número de tarjeta válido para una sola transacción»,* dijeron los investigadores.

Si una transacción basada en NFC de este tipo es detectada y bloqueada por el malware instalado en el terminal PoS infectado, el lector de PIN muestra un mensaje de error falso: *«Error sin contacto, inserte su tarjeta».*

Esto lleva a la víctima a utilizar su tarjeta física insertándola en el lector de PIN, lo que

permite que los hackers cometan fraude. Otra característica nueva agregada a los aparatos es la capacidad de filtrar tarjetas de crédito por segmentos y crear reglas adaptadas a esos niveles.

> *«Estas reglas pueden bloquear NFC y capturar datos de la tarjeta solo si la tarjeta es Black/Infinite, Corporate u otro nivel con un límite de transacción alto, lo que es mucho más atractivo que las tarjetas de crédito estándar con un saldo/límite bajo»,* agregaron los investigadores.

> *«Debido a que los datos de transacción generados durante un pago sin contacto son inútiles desde la perspectiva de un ciberdelincuente, es comprensible que Prilex necesite obligar a las víctimas a insertar la tarjeta en el terminal PoS infectado».*