NCR SECURITY UPDATE

FECHA: Junio 22, 2015 **INCIDENT No:** 2015-05 **REV:** #1

Descripción

Nueva variante de ataques con conexiones ilegales al lector de tarjetas.

Resumen

NCR ha estado investigando un nuevo método de captura de datos por medio de conexiones ilegales al lector de tarjetas.

Esta metodología fue confirmada en los Emiratos Arabes Unidos sobre ATMs Personas.

En esta variante del ataque, los delincuentes están atacando ATMs de Lobby (stand-alone), no sobre ATMs modelo de pared (Through the Wall). Acceden al lector de tarjeta logrando abrir la parte superior del ATM. Luego incorporan un dispositivo electrónico similar al observado en ataques previos, para acceder directamente al lector de tarjeta y de esa forma capturar la información de la tarjeta. No se registran perforaciones en la fascia del equipo para realizar el acceso; por lo tanto el ataque no se puede visualizar desde el exterior del ATM una vez que la tapa superior se cierra.

Este ataque es una variante del Modus Operandi observado en ataques previos de conexiones ilegales al lector de tarjetas. (Referencia: Alerta de Seguridad de NCR 2014-14)

En el ataque anterior, la fascia del ATM es perforada cerca del lector de tarjeta con el objetivo de realizar un orificio lo suficientemente grande para que el delincuente pueda acceder al interior del ATM y instalar una conexión directamente sobre el lector de tarjeta y de esa forma copiar la información de la tarjeta que lee el ATM. Un extremo del dispositivo se conecta sobre la parte trasera del cabezal de lectura de la banda magnética del lector de tarjeta, mientras que el otro extremo está unido a un dispositivo de almacenamiento de datos. Una vez instalados los elementos en su lugar, el orificio en la fascia puede ser disimulado ubicando una etiqueta (sticker), u otro tipo de cubierta.

Generalmente para este tipo de ataques la perforación ocurre en el lugar del aviso de orientación de la tarjeta. Esto permite al delincuente el acceso ideal al lector de tarjetas, y el aviso puede ser reemplazado para disimular el orificio.

NCR SECURITY UPDATE

El surgimiento y crecimiento ataques del tipo “Conexión ilegal al lector de tarjeta” se debe a la gran variedad de tecnología “Anti-Skimming” disponible, la cual es exitosa en la prevención de la operación de un “skimmer” tradicional ubicado fuera del ATM. Estos clonadores de conexión ilegal son ubicados en lugares donde la tecnología “Anti-Skimming” de terceros puede no necesariamente proveer protección, dado que el ATM debe tener la capacidad de lectura de la tarjeta.

NCR observa a la fecha que en todos los casos de conexiones ilegales se han realizado sobre ATMs modelo Personas, sin embargo todos los cajeros automáticos deben protegerse de este tipo de ataques.

Orientación y Recomendaciones de NCR

En el caso de los modelos de ATM de la línea SelfServ y Personas, NCR dispone de un kit que evita estas conexiones ilegales. Este kit provee una protección física metálica que envuelve al lector de tarjetas del ATM. Esta barrera provee prevención adicional contra cualquier otra conexión externa realizada en los lectores de tarjeta de los ATMs.

Con el surgimiento de nuevas soluciones anti-skimming más confiables, como ser SPS (Skimming Protection Solution) de NCR –con su malla anti perforaciones, los tradicionales ataques del tipo skimming y las conexiones ilegales al lector de tarjetas que se producen mediante la perforación de las fascia del ATM tienen menos probabilidades de ser exitosos, y que incrementan el riesgo de ataques sobre ATMS de acceso frontal en ambientes públicos.

Es por ello, que NCR recomienda que todos los operadores de ATMs actualicen la parte superior del ATM con una cerradura más segura de nivel UL 437 la cual está disponible para los ATMs de la línea SelfServ.

Por favor contacte a su Ejecutivo de Cuenta de NCR para obtener más información sobre las soluciones.

Cabe destacar que la Solución NCR “Skimming Protection Solution” (SPS), también provee notificación de producirse accesos de la tapa superior; además de estar equipada con una malla anti penetración, la cual permite prevenir y detectar la perforación de la fascia en ésta área alrededor de la boca del lector de tarjeta.

Adicionalmente, NCR recomienda que los empleados del banco o el personal de servicio de mantenimiento de equipos realice regularmente la inspección de la fascia del ATM –al momento de realizar el mantenimiento o recarga del equipo-; con el objetivo de detectar perforaciones u otra evidencia de alteración. En el caso de los equipos de pared (Through The Wall), la inspección se puede realizar desde la parte posterior del ATM; mientras que en los ATMs con acceso frontal cuando se levanta el frente. Los operadores de ATMs deben también asegurarse que sus proveedores de servicio cuenten con la documentación suficiente que los identifique como tal, y que provean al personal que se encuentra en locaciones neutrales con las debidas instrucciones acerca del control de la documentación para confirmar que las personas que tienen acceso al ATM pertenecen a proveedores de servicios autorizados.

Contactos

Denuncia de delitos en cajeros automáticos: global.security@ncr.com
Mejores prácticas y soluciones de seguridad para autoservicio: NCRSelfService.security@ncr.com
Más información sobre esta alerta: owen.wild@ncr.com