NCR SECURITY UPDATE

FECHA: 17 de Febrero de 2015 **INCIDENTE N°:** 2015-02 **REV:** #1

Ataques mediante inserción de Malware en la Red a Computadoras de Instituciones Financieras (Malware: Carbanak)

Resumen

NCR ha sido notificada y se encuentra actualmente analizando el reporte liberado por Kaspersky en relación a los ataques registrados recientemente mediante la inserción de malware en la red de los bancos. El reporte está captando la atención de los medios; quienes ya lo denominan como “el mayor robo contra instituciones bancarias de la historia”.

El camino que sigue este tipo de ataque es diferente de aquellos ataques sobre los que NCR ya le ha alertado a Usted en el pasado. Se trata de un ataque que se ha gestado desde hace bastante tiempo y tiene como objetivo la infraestructura informática, insertando malware en la red y utilizando los sistemas del banco para robar dinero según los siguientes métodos:

- Transfiriendo dinero a cuentas bancarias fraudulentas que pertenecen a los hackers
- Utilizando un sistema electrónico de pagos para enviar dinero a cuentas fraudulentas fuera del país
- Provocando en los ATMs el dispensado de dinero en determinados horarios y ubicaciones.

Orientación y Recomendaciones de NCR

NCR continúa investigando este reporte y obteniendo más información acerca del método y canales utilizados en este ataque. NCR recomienda a todos sus clientes revisar sus controles de seguridad de la red según las mejores prácticas de la industria. Los segmentos de la red que se utilizan para controlar la red de ATMs son especialmente atractivos para los delincuentes; dado que los consideran una fuente para obtener dinero. Es por ello que se debe tener mayor cuidado en estos segmentos e implementar medidas de seguridad.

NCR quiere señalar especialmente que este alerta **no está relacionado** en absoluto con el alerta recientemente liberado bajo el nombre “Man in the Middle Attack in Latin America” (Alerta: 2015-01). Mientras que ambos ataques se produjeron en la red, el ataque lógico del tipo “Man in the Middle” se trató específicamente de un ataque a la funcionalidad de dispensador del ATM; por lo que es necesario tomar medidas de precaución para proteger el equipo de este tipo de ataque.

NCR SECURITY UPDATE

Tampoco este alerta tiene relación con Alertas de NCR anteriores acerca de ataques a cajeros automáticos mediante el uso de malware o del tipo “Black Box”. Cabe nuevamente destacar que este tipo de ataques se produjeron específicamente sobre la funcionalidad de dispensado del ATM; por lo que es necesario tomar medidas de precaución para proteger el equipo de este tipo de ataque.

Para conocer en detalle la guía de recomendaciones de NCR para proteger los equipos de ataques del tipo “Black Box”, “Man in the Middle attacks” y uso de malware para ATMs; le sugerimos que revise los Alertas de Seguridad de NCR liberados anteriormente.

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