BANCO DE MÉXICO

29 de agosto de 2018

Reporte de análisis forenses

Versión Pública

Hace algunos días, concluyeron los análisis forenses realizados a la infraestructura informática de las instituciones financieras cuyos sistemas de conexión al Sistema de Pagos Electrónicos Interbancarios (SPEI) fueron vulnerados en abril pasado. Estos análisis forenses fueron practicados por terceros especializados contratados por dichas instituciones. Con base en las evidencias recolectadas como parte de los citados análisis, es posible determinar algunas características comunes de los ataques:

Objetivo: El objetivo del ataque fue generar transferencias electrónicas de fondos hacia cuentas bancarias específicas, con el fin de sustraer ilegítimamente recursos monetarios. No se trató de un ataque al sistema central del SPEI operado por el Banco de México, ni a alguna infraestructura del mismo, sino de un ataque en el que se comprometieron elementos de los sistemas de las instituciones financieras vulneradas, y dirigido particularmente a vulnerar los sistemas para la generación y envío de órdenes de transferencias. Para ello, se aprovecharon de las funcionalidades y el procesamiento expedito de este sistema de pagos, de tal manera que la tramitación automatizada de las órdenes ilegítimas de transferencias se pudiera llevar a cabo antes de que pudieran detectarlas a tiempo las instituciones financieras de donde estas se originaron. En consecuencia, el ataque no tuvo como propósito volver inoperante al SPEI o penetrar las defensas del Banco Central.

Modus operandi general:

1. **Inserción de operaciones apócrifas**. En estos ataques, se utilizaron distintas técnicas para insertar, en el flujo de las operaciones que las instituciones vulneradas procesan en sus sistemas, órdenes de transferencias simuladas que no fueron generadas por los sistemas de manejo de cuentas de los clientes, por lo que estas no quedaron referidas a ninguna de dichas cuentas. Cabe señalar que los recursos de los cuentahabientes no estuvieron en ningún momento en riesgo, toda vez que únicamente fueron vulnerados los sistemas de envío de órdenes de transferencias de las instituciones, y con cargo a las cuentas concentradoras que estas mantienen para el procesamiento de todas las transferencias realizadas por este sistema de pagos.
2. **Uso de cuentas beneficiarias válidas**. Las transferencias correspondientes a estos ataques se generaron por montos y hacia destinatarios válidos. En consecuencia, tales transferencias se liquidaron conforme a los procedimientos del sistema. Las instituciones receptoras de dichas transferencias cuentan con los datos y, en su caso, documentos de identificación de los titulares de las cuentas en las que se realizaron los abonos respectivos. Toda esta información es susceptible de utilizarse en las investigaciones a cargo de la Procuraduría General de la República.
3. **Eliminación de evidencias**. Una vez concluidas las transferencias apócrifas, los atacantes borraron muchos de sus rastros en los sistemas de las instituciones financieras vulneradas. Esto

indica un ataque profesional, que aprovechó las vulnerabilidades en los controles de seguridad informática de dichas instituciones.

Conclusiones: El modus operandi descrito requirió contar, por parte de los atacantes, con un conocimiento profundo de la infraestructura tecnológica y los procesos de las instituciones vulneradas; así como del acceso a ellas.

Para estos ataques, se utilizaron técnicas comunes como robo de credenciales, escalamiento de privilegios, movimientos laterales entre servidores, inserción de archivos o ejecución de instrucciones y borrado de bitácoras. Con las conclusiones específicas derivadas de los análisis forenses, se están instrumentando las medidas correspondientes para evitar ataques similares y fortalecer la interacción con el Banco de México de las instituciones que participan en los sistemas de pagos que aquel opera. Cabe destacar que dichas medidas ya están consideradas en la regulación aplicable a los participantes en dichos sistemas de pagos.