BANCO DE MÉXICO

Información sobre los Ataques a Participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI)

Extracto del Informe Trimestral Enero – Marzo 2018, Recuadro 6, pp. 51-53, Mayo 2018

Introducción

Entre la segunda mitad de abril y la primera mitad de mayo del año en curso, cinco participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI) experimentaron ataques a los aplicativos que utilizan para preparar sus órdenes de pago y conectarse con el SPEI.

Es importante resaltar que, a pesar de los ataques mencionados, el sistema central del SPEI no se ha visto afectado y no ha sido blanco de ataque. Asimismo, los recursos de los clientes de las instituciones financieras están seguros y no están en peligro.

En respuesta a estos eventos, el Banco de México emprendió una serie de medidas para contener los posibles daños derivados de esos ataques sobre los participantes afectados, así como en el sistema de pagos en general. Entre estas medidas destacan: (i) la migración de los participantes afectados, así como aquellos con un mayor perfil de riesgo, hacia una plataforma de operación contingente; (ii) la implementación de alertas en el SPEI central para detectar anomalías en los mensajes de pago y la implementación de controles adicionales en los aplicativos que proveen los servicios de conexión al SPEI a los participantes; y (iii) la emisión de regulación para proporcionar espacio con el fin de que las entidades que otorgan el servicios de transferencias de fondos implementen medidas de control para fortalecer sus sistemas de detección de transferencias irregulares, verificar la integridad de sus operaciones y verificar la seguridad en los retiros de efectivo.

Resumen de los Eventos Operativos Registrados Durante Abril y Mayo

El 17 de abril, el Banco de México registró la vulneración de un participante en el SPEI derivada de ataques cibernéticos. A partir de esa fecha se han identificado cuatro eventos adicionales: dos el 24 de abril, uno el 26 de abril y uno más el 8 de mayo.

Los ataques que se han presentado se han focalizado en diversos elementos que componen los aplicativos que usan los participantes para preparar sus órdenes de pago y conectarse con el SPEI y en la infraestructura de cómputo y telecomunicaciones de los bancos en la que se operan estos aplicativos.

Al respecto, es importante mencionar que el Banco de México no ofrece estos aplicativos a los participantes, ni tampoco los certifica o valida, sino que cada participante es responsable de contar con el servicio, ya sea proporcionado por terceros (en la mayoría de los casos) o desarrollar los propios. Cabe destacar que en todos los casos identificados y reportados como un evento de ciberseguridad, los aplicativos de conexión han sido desarrollados por un tercero (ver Tabla 1). No obstante, la vulnerabilidad pudo estar asociada tanto a los sistemas, como a la infraestructura en la que fue instalado.

Si bien las investigaciones de los ataques siguen en curso, el “modus operandi” identificado hasta el momento se describe a continuación:

- Los atacantes vulneran la infraestructura tecnológica de los participantes e insertan transacciones ilegítimas en alguna etapa del proceso que realizan los aplicativos de conexión al SPEI (ver Gráfica 2).
- Las transacciones ilegítimas incluyen una cuenta emisora inexistente y una cuenta receptora real.

- Los participantes firman y envían al SPEI estas transacciones ilegítimas a través de sus aplicativos, con lo que las validan.
- El SPEI revisa que las operaciones estén firmadas por los participantes, las procesa y se abonan en la cuenta del participante receptor.
- El participante receptor hace el correspondiente abono a las cuentas de sus clientes, en este caso los receptores de los recursos ilegítimos.
- Finalmente, los recursos ilegítimos son retirados mediante disposiciones de efectivo.

Tabla 1
Proporción de Mercado de los Diferentes Participantes del SPEI
Porcentaje del total

	Número de operaciones	**Monto de operaciones[1/]**
Instituciones directamente atacadas: 5	13.1	7.6
Instituciones afectadas y con un perfil de riesgo superior[2/]	19.5	28.8
Instituciones no afectadas con proveedor externo	7.2	14.7
Instituciones no afectadas con desarrollo propio	73.4	56.5

1/ Los montos de las operaciones excluyen al sistema de liquidación de valores por no tener instrucciones directas del público en general.
2/ Incluye instituciones directamente atacadas.
Fuente: Banco de México

Los participantes afectados se han percatado de estas instrucciones ilegítimas por dos vías: (i) mediante alertas internas producto de sus procesos de validación de operaciones y (ii) por medio de alertas por parte de otros participantes receptores de operaciones sospechosas. Debido a estos mecanismos de alerta, algunas de las transacciones identificadas fueron detenidas por los participantes receptores, con lo que se evitó la disposición indebida de parte de los recursos de procedencia fraudulenta.

Los recursos de los clientes no han estado en riesgo. Los atacantes han buscado vulnerar las conexiones de los participantes con el SPEI, lo cual involucra únicamente recursos de la institución afectada. De hecho, los recursos de los clientes radican en un sistema separado con validaciones de autenticidad individuales por operación de las cuales no se cuenta con indicio alguno de que hayan sido vulneradas. La afectación a los clientes ha sido la ralentización de los pagos para aquellas transacciones en las que participa alguna institución afectada o con perfil de riesgo alto para el envío de órdenes de pago a través del SPEI.

Protocolo de Reacción ante Eventos de Ciberseguridad

En cada caso de evento relacionado con ciberseguridad, se aplica un protocolo que implica la desconexión de la institución atacada y el inicio de operación a través de esquemas de contingencia.

Para este fin, el Banco de México cuenta con un sistema paralelo para hacer transacciones en el SPEI, el Cliente de Operación Alterna (COAS) del SPEI. La operación a través de este esquema de contingencia reduce los riesgos al tratarse de una infraestructura distinta a la que se ha visto afectada. Sin embargo, la operación en este esquema es semiautomática, lo que hace que las transferencias no se envíen y/o abonen en tiempo real.

Una vez identificados los casos de ataques a alguna institución, se identifican elementos de riesgo que pueden resultar comunes a otros participantes. Con base en esta información, se emite un comunicado avisando a aquellos participantes, en los que se identificó un mayor riesgo, que tendrán que conectarse al SPEI a través del COAS desde sus instalaciones en fecha futura.

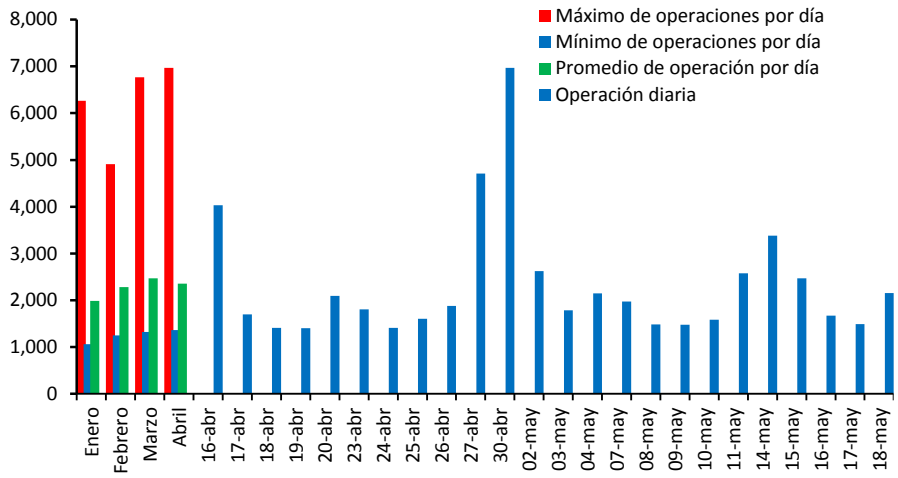
Pese a los ataques, el SPEI ha continuado brindando sus servicios de manera segura y procesando grandes cantidades de pagos. Cabe resaltar que el 30 de abril, este sistema de pagos alcanzó su máximo histórico diario al procesar más de 6.8 millones de pagos. De igual forma, los participantes que han sido afectados han recuperado el nivel de operación en el SPEI una vez que se estabilizaron sus procesos contingentes (ver Gráfica 1).

Requerimientos de Ciberseguridad Aplicables a los Participantes

Entre estos requerimientos destacan aquellos relacionados con la seguridad de los aplicativos de conexión al SPEI y con el esquema de operación alterna COAS, tales como:

- Contar con procedimientos para evaluar los protocolos de comunicación utilizados en la infraestructura tecnológica y prescindir de aquellos que se consideren inseguros.

Gráfica 1
Número de Operaciones Procesadas por SPEI durante la Contingencia Operativa
Millones de operaciones



- Contar con procedimientos que permitan administrar las vulnerabilidades de seguridad informática derivadas de, entre otros factores, cambios, actualizaciones o errores en la infraestructura tecnológica.
- Contar con procedimientos para detectar y gestionar incidentes de seguridad informática en la infraestructura tecnológica, que aseguren su identificación, contención y la adecuada recolección y resguardo de evidencia de seguridad.
- Contar con procedimientos que aseguren que los componentes que brindan seguridad a sus sistemas informáticos se encuentren vigentes.
- Todos los participantes del SPEI deben de cumplir con requerimientos estrictos en materia de ciberseguridad informática y continuidad operativa.

- Estos requerimientos se dieron a conocer a los participantes del SPEI y entidades que pretenden incorporarse al sistema mediante la Circular 14/2017 emitida en julio de 2017 y los cuales entraron en vigor el 31 de enero del presente año, tiempo considerado por el Banco de México como suficiente para que los participantes hicieran las modificaciones necesarias a sus sistemas de cómputo y demás modificaciones necesarias para el cumplir con la regulación.
- Los participantes debían ser evaluados por un auditor externo respecto al cumplimiento de los estándares técnicos en la Circular 14/2017 y respecto al Banco de México en febrero (se extendieron prorrogas a diversos participantes).
- Los requerimientos de ciberseguridad y de continuidad operativa contenidos en la Circular 14/2017 incluyen medidas preventivas encaminadas a prevenir y evitar ataques como los presentados en las últimas semanas.
- El cabal cumplimiento de todas las disposiciones requeridas para la conexión al SPEI son un elemento indispensable para todos los participantes del SPEI.
- El incumplimiento de las disposiciones por parte de algunos participantes vulnera a todo el sistema, incrementando la probabilidad de ocurrencia de ataques como los descritos, con claras afectaciones a los todos los usuarios de los servicios de transferencias electrónicas. Los procesos de supervisión están siendo reforzados para asegurar el cabal cumplimiento de la norma por todos los participantes.
- Requerimientos relacionados con la seguridad de los aplicativos de conexión al SPEI y con el esquema de operación alterna COAS (cont.):
    - ✓ Contar con procedimientos que permitan vigilar, auditar y rastrear todas las operaciones realizadas por los sistemas informáticos;
    - ✓ Contar con procedimientos de contratación y capacitación del personal para asegurar que aquel relacionado con la operación con el SPEI, cuente con las habilidades, competencias y conocimientos requeridos para el puesto que desempeña; y
    - ✓ Acreditar que pueden continuar con su operación ante la activación del “Procedimiento de Operación Alterno SPEI” (POA-SPEI), así como operar mediante el procedimiento de contingencia denominado “Cliente de Operación Alterno SPEI” (COA-SPEI).
- Derivado de los procesos de supervisión iniciados desde 2017 a los participantes del SPEI y otros sistemas de pagos operados por el Banco de México, se detectó un nivel de cumplimiento heterogéneo en los requerimientos de ciberseguridad y continuidad operativa.
- Es importante mencionar que el Banco de México intensificará sus procesos de supervisión en esta materia.

Comunicación con los Participantes y con el Público

Comunicación con los participantes

Se generaron comunicados hacia todos los participantes para incrementar el monitoreo y vigilancia en las operaciones y reducir la probabilidad de que se presentaran ataques adicionales:

- El 17 de abril se reporta la detección de vulnerabilidades en una institución y se pide extremar precauciones.
- El 24 de abril se reporta el segundo evento especificando elementos de preocupación y solicitando medidas y controles adicionales.
- El 8 de mayo se les pide establecer controles en sus conexiones con todas las infraestructuras.

- El 10 de mayo se les reitera a las instituciones que por seguridad debe hacerse la conexión a COAS.

Adicionalmente, se generaron comunicados dirigidos hacia los participantes con riesgos más elevados los días 26 de abril y 7 y 8 de mayo instruyéndoles acciones particulares.

Comunicación al público

Se emitieron los siguientes comunicados de prensa:

- El 27 de abril se informa de eventos operativos en 3 instituciones y la ralentización del sistema para clientes.
- El 30 de abril se brinda mayor detalle sobre el comunicado anterior y se explican algunas de las medidas preventivas que han adoptado las instituciones (conjunto con la SHCP y la CNBV).
- El 14 de mayo se hacen del conocimiento del público las acciones emprendidas por Banco de México en los ámbitos de ciberseguridad, operativo y regulatorio.
- El 16 de mayo se publica en la página del Banco de México un micrositio con Información importante sobre la situación del SPEI que agregará información de manera continua.

Mitigación de Riesgos

Acciones tecnológicas

- Los participantes en los que se detectaron los incidentes, operan por vías alternas y mantienen su capacidad para enviar órdenes de transferencias a la infraestructura del SPEI.
- Se establecieron alertas en el SPEI central para detectar algunas anomalías en los mensajes.
- Se ha mantenido un soporte técnico reforzado 24/7 para los participantes.
- Se exigió a los proveedores de servicios de conexión al SPEI que incorporen controles adicionales en sus aplicativos.
- Se solicitó a los participantes hacer un análisis profundo de sus infraestructuras para detectar software durmiente.

Acciones operativas

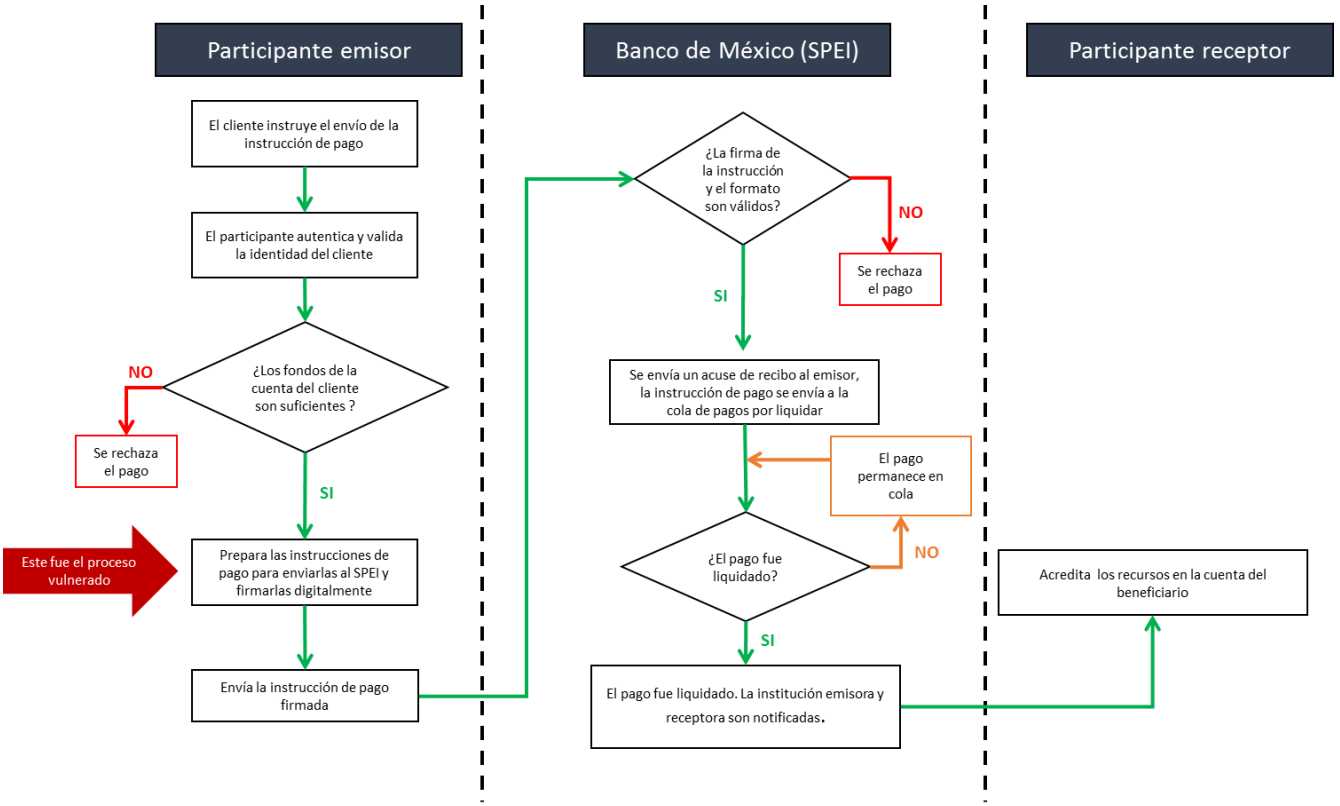
- Se requirió a los participantes cuyos aplicativos e infraestructura de cómputo para conectarse al SPEI resultaron afectados, tomar medidas para renovar los elementos de seguridad de sus operadores para autenticarse en los sistemas de pagos operados por el Banco de México, al tiempo que este Instituto Central ha ampliado y fortalecido el esquema de soporte a todos los participantes del sistema.
- El Banco de México reforzó el monitoreo de su infraestructura y sistemas para detectar cualquier comportamiento anómalo.

Acciones regulatorias

- El Banco de México emitió disposiciones (Circular 4/2018 y Circular 5/2018) que otorgan a las instituciones de crédito y demás entidades que prestan el servicio de transferencias de fondos, espacio para que estas implementen medidas de control adicionales encaminadas a fortalecer sus sistemas de detección de transferencias irregulares, verificar la integridad de sus operaciones y evitar posibles afectaciones a dichas instituciones, al resto de los participantes y al sistema en su conjunto.

- Adicionalmente, estas disposiciones consideran espacios para verificar la seguridad en los retiros de efectivo.

Gráfica 2
Diagrama de flujo de envío y recepción de una transferencia de fondos a través de SPEI



Fuente: Banco de México