BOLETÍN DEL GRUPO EGMONT

Fraude que compromete el correo electrónico comercial

Grupo de Trabajo sobre el Intercambio de Información

IEWG

Julio de 2019

- Versión pública -

BOLETÍN PÚBLICO DEL GRUPO EGMONT DE UNIDADES DE INTELIGENCIA FINANCIERA FRAUDE QUE COMPROMETE EL CORREO ELECTRÓNICO COMERCIAL

El objetivo de este boletín es alertar a las autoridades competentes y a los sujetos obligados sobre los riesgos de lavado de dinero y las tipologías clave que se relacionan con los esquemas de fraude que comprometen el correo electrónico comercial (business e-mail compromise, BEC). La información que consta en este documento debe permitir que las autoridades y los sujetos obligados detecten, identifiquen, denuncien e investiguen de mejor manera los esquemas de fraude de BEC, y que desestabilicen estas redes de actividades financieras ilícitas.

BOLETÍN SOBRE EL FRAUDE QUE COMPROMETE EL CORREO ELECTRÓNICO COMERCIAL

Número de identificación: EG-Bulletin-01/2019
Fecha: 30 de julio de 2019
Destinatarios previstos: Autoridades competentes (de reglamentación, supervisión y orden público) y sujetos obligados

Introducción

Evitar que los ciberdelincuentes se aprovechen del sistema financiero mundial es una prioridad fundamental del Grupo Egmont de Unidades de Inteligencia Financiera (UIF) y sus miembros. El Grupo Egmont publica este boletín a fin de alertar a las UIF miembros y a sus jurisdicciones sobre la creciente amenaza que suponen los esquemas de fraude de BEC. Los esquemas de fraude de BEC se encuentran entre las amenazas de ciberdelitos que repercuten negativamente en las instituciones financieras, dado que exponen al sector financiero a pérdidas que ascienden a miles de millones de dólares en todo el mundo. Por ejemplo, en una jurisdicción se detectaron pérdidas potenciales de más de USD 12 000 000 000 en más de 78 000 incidentes de fraude de BEC denunciados, con víctimas en el país y en el mundo, en un período reciente de cinco años.[1] Estos esquemas comprometen las cuentas de correo electrónico personales o comerciales de organizaciones empresariales, profesionales e individuos para enviar instrucciones de pago falsas (o hacer que estas se envíen) y otra información que se utiliza para cometer fraude financiero.

Fraude que compromete el correo electrónico comercial

El fraude de BEC consta de esquemas a través de los cuales los delincuentes comprometen las cuentas de correo electrónico de las víctimas ya sea para (1) enviar instrucciones de pago fraudulentas a instituciones financieras u otros asociados comerciales a fin de malversar fondos o para (2) que los datos se transmitan de manera fraudulenta con el objetivo de cometer fraude financiero.

[1] Consulte el anuncio de servicio público *Business Email Compromise: The 12 Billion Dollar Scam*, de la Agencia Federal de Investigación (*Federal Bureau of Investigation,* FBI), 12 de julio de 2018, disponible en inglés en https://www.ic3.gov/media/2018/180712.aspx.

Las instituciones financieras pueden asumir un rol importante en las iniciativas de identificación, prevención y denuncia de los esquemas de fraude de BEC. Para ello, deben fomentar una mayor comunicación y colaboración entre las unidades internas comerciales, de ciberseguridad, de prevención del fraude y contra el lavado de dinero (ALD).

A fin de combatir la creciente amenaza grave que representa el fraude de BEC para las instituciones financieras y sus clientes, 11 UIF han organizado el equipo del Proyecto BEC de Egmont, que se centra en analizar las metodologías y tendencias de BEC. El objetivo del Grupo Egmont es compartir información clave de este análisis con las UIF, con la esperanza de que estas la transmitan, según corresponda, a las autoridades y sujetos obligados competentes. Con base en esta información clave, este documento presenta indicadores de los esquemas de BEC y las transacciones fraudulentas asociadas. Los sujetos obligados que reciben este boletín pueden utilizarlo para detectar y denunciar posibles transacciones relacionadas con BEC ante las autoridades competentes de reglamentación, de supervisión y del orden público.

Funcionamiento de los esquemas de BEC

En términos generales, en los esquemas de BEC, se suplanta la identidad de las víctimas para enviar instrucciones sobre transacciones aparentemente legítimas a una institución financiera. Si bien existen diferencias en algunos aspectos de los esquemas de BEC, todos se centran en utilizar cuentas de correo electrónico comprometidas para lograr que las instituciones financieras o sus clientes realicen pagos no autorizados o fraudulentos, o que envíen datos confidenciales a un tercero no autorizado, quien los utiliza para cometer fraude financiero. Los esquemas de BEC pueden tener tres fases:

Fase 1: Comprometer la información y las cuentas de correo electrónico de la víctima. En primer lugar, los delincuentes acceden ilegalmente a la cuenta de correo electrónico de la víctima, a menudo a través de ingeniería social[2] o de técnicas de invasión informática. Luego, con esta cuenta, obtienen información en las instituciones financieras de la víctima, los detalles de su cuenta, sus contactos e información relacionada.

Fase 2: Transmitir instrucciones de transacciones de manera fraudulenta. Los delincuentes utilizan la información robada a la víctima para enviar por correo electrónico instrucciones fraudulentas de pago o transmisión de datos a la institución financiera, tal como lo haría la víctima. Con este fin, los delincuentes utilizan la cuenta de correo electrónico vigente de la víctima (que ahora controlan) o crean una cuenta falsa que se le parece. Para sustentar las instrucciones, el delincuente puede adjuntar documentos de respaldo, los cuales se falsifican con este propósito a fin de mejorar su aparente legitimidad.

Fase 3: Ejecutar transacciones no autorizadas. Los delincuentes engañan al empleado o a la institución financiera de la víctima para que realicen transferencias que parecen legítimas pero que, de hecho, no están autorizadas o son fraudulentas.

[2] El término ingeniería social hace referencia a tácticas de interacción humana que se emplean para engañar a un individuo a fin de que revele información. Los delincuentes la utilizan principalmente para facilitar los esquemas de fraude de BEC.

Las instrucciones de la transacción fraudulenta dirigen los pagos a las cuentas de los delincuentes, radicadas en instituciones financieras nacionales o extranjeras. Las instituciones financieras en países del este y sudeste asiáticos, y del este y oeste de Europa, son destinos frecuentes para estas transacciones fraudulentas. Sin embargo, debe destacarse que, a menudo, los delincuentes adaptan sus estrategias y, por ende, los países de destino pueden cambiar rápidamente.

Situaciones hipotéticas de BEC

A menudo, los esquemas de BEC se dirigen a instituciones financieras o a sus clientes, entre los que se incluyen empresas y personas, que realizan grandes transacciones a través de instituciones financieras, entidades prestatarias, compañías inmobiliarias y estudios de abogados. A modo de ejemplo, los esquemas de BEC a menudo asumen las siguientes formas:

Situación hipotética 1: El delincuente suplanta la identidad de un cliente comercial de una institución financiera. Un delincuente accede ilegalmente a la cuenta de correo electrónico de un empleado de la compañía A y la utiliza para enviar instrucciones sobre transferencias fraudulentas a la institución financiera de esta.[3] Según esta solicitud, la institución financiera de la compañía A realiza una transferencia y envía fondos a una cuenta controlada por el delincuente.

En esta situación hipotética, el delincuente, que suplanta la identidad del cliente de la institución financiera, le solicita a esta que realice una transferencia no autorizada.

Situación hipotética 2: El delincuente suplanta la identidad de un ejecutivo (lo cual también se denomina "fraude del CEO"). Un delincuente accede ilegalmente a una cuenta de correo electrónico de un ejecutivo de la compañía B y la utiliza para enviar instrucciones sobre transferencias a un empleado de esta, quien se encarga de procesar y emitir pagos. El empleado cree que las instrucciones enviadas por el ejecutivo son legítimas y ordena a la institución financiera que realice la transferencia.

En esta situación hipotética, el delincuente que suplanta la identidad de un ejecutivo de la compañía engaña a un empleado para que autorice de manera involuntaria una transferencia fraudulenta a una cuenta que controla. Esta situación hipotética puede variar, por ejemplo, cuando un delincuente suplanta la identidad del ejecutivo de una compañía para engañar a un empleado a fin de que envíe información confidencial sobre transacciones o nómina, la cual se podrá utilizar en un futuro fraude financiero.

Situación hipotética 3: El delincuente suplanta la identidad de un proveedor. Un delincuente suplanta la identidad de uno de los proveedores o prestadores de servicios profesionales (como un agente inmobiliario, una compañía de depósito en garantía o un abogado) de la compañía C y le envía a esta un mensaje de correo electrónico para informarle que los pagos de facturas o depósitos futuros deben realizarse a un nuevo número de cuenta, radicada en otro lugar. Según esta información fraudulenta, la compañía C actualiza la información de pago del proveedor en sus registros y envía las nuevas instrucciones sobre transferencias a su institución financiera, la cual realiza los pagos a una cuenta controlada por el delincuente.

[3] En todas estas situaciones hipotéticas, en vez de ingresar ilegalmente en una cuenta, el delincuente también puede falsificar la dirección de correo electrónico o crear una cuenta que se parezca a la dirección legítima de la parte solicitante.

En esta situación hipotética, el delincuente que suplanta la identidad de un proveedor o prestador de servicios envía información de pagos fraudulenta para engañar al empleado de la compañía a fin de que dirija las transacciones a una cuenta que controla.

Situación hipotética 4: El delincuente interviene en servicios inmobiliarios. Un delincuente compromete la cuenta de correo electrónico de un agente inmobiliario o de un individuo que adquiere o vende un inmueble, con el fin de alterar las instrucciones sobre el pago y desviar los fondos de una transacción inmobiliaria (como la ganancia por la venta, el desembolso de un préstamo o los honorarios). De manera alternativa, un delincuente accede ilícitamente a la dirección electrónica de un agente inmobiliario y la utiliza para contactar a una compañía de depósito en garantía, a la cual le indica que redirija las ganancias de la comisión obtenida por el agente inmobiliario por la venta de la propiedad a una cuenta que controla.

En esta situación hipotética, el delincuente suplanta la identidad de un agente inmobiliario o de otro participante principal de la transacción y envía instrucciones fraudulentas sobre el pago, las cuales engañan a la otra parte para que remita los pagos u otros fondos relacionados con la transacción a una cuenta controlada por el delincuente.

Indicadores de fraude de BEC

Poder detectar satisfactoriamente los esquemas de BEC y desestabilizarlos exige realizar un análisis cuidadoso y verificar las instrucciones del cliente sobre la transacción, además de considerar las circunstancias que las rodean. Debido a que algunos indicadores relacionados con el fraude de BEC en realidad pueden reflejar actividades financieras legítimas, se les recuerda a las instituciones financieras que ***un único indicador de transacción no necesariamente implica una actividad sospechosa.*** Antes de determinar que una transacción es sospechosa, las instituciones financieras deben considerar otros indicadores, y los hechos y las circunstancias subyacentes, tales como los antecedentes financieros del cliente, y deben precisar si se manifiestan varios indicadores. Asimismo, deben seguir indagando e investigando, según corresponda.

Los siguientes indicadores pueden señalar un esquema de BEC:

Indicadores relativos a la cuenta de la víctima

Patrones generales de transacciones sospechosas

- Un cliente indica por correo electrónico que se realice un pago directo a un beneficiario conocido. No obstante, la información de la cuenta de este es diferente de la que se utilizó previamente.
- Un cliente indica por correo electrónico que se realice un pago directo a un beneficiario a quien nunca se le había realizado pago alguno y con quien no existe una relación comercial documentada; el monto del pago es similar o superior a los que el cliente realizó a los beneficiarios anteriormente.
- Un cliente indica por correo electrónico que se realicen pagos adicionales inmediatamente después de un pago exitoso a una cuenta que no había utilizado

previamente, para pagarles a sus proveedores/prestadores. Esta conducta puede señalar un intento delictivo de realizar pagos adicionales no autorizados tras determinar que se realizó un pago fraudulento de manera satisfactoria.

- Un cliente indica por correo electrónico que se designe una transacción como "urgente", "secreta" o "confidencial".
- Un cliente envía por correo electrónico instrucciones sobre una transacción, de modo tal que la institución financiera tiene un plazo o una oportunidad limitada para confirmar la autenticidad de la transacción solicitada.
- Un cliente envía por correo electrónico instrucciones sobre una transacción para que se realicen transferencias a la cuenta de una institución financiera que, según quejas documentadas del cliente, se trata de un presunto destino de transacciones fraudulentas.
- Las instrucciones sobre una transacción enviadas por una cuenta de correo electrónico aparentemente legítima contienen texto, plazos y cantidades distintas en comparación con las instrucciones sobre la transacción auténticas y verificadas previamente.
- Las instrucciones sobre transacciones provienen de una cuenta de correo electrónico muy similar a la de un cliente conocido. Sin embargo, se agregaron, cambiaron o borraron uno o más caracteres para alterarla ligeramente. Por ejemplo:

Dirección de correo electrónico legítima	Direcciones de correo electrónico fraudulentas
john-doe@abc.com	john_doe@abc.com john-doe@bcd.com

- Una institución financiera recibe por correo electrónico instrucciones sobre una transacción de parte del empleado de un cliente, que es la nueva persona autorizada para utilizar la cuenta o es una persona autorizada, que no envió todavía ninguna instrucción sobre transferencias.
- El empleado o representante de un cliente envía por correo electrónico a una institución financiera instrucciones sobre una transacción, en nombre del cliente, las cuales se basan exclusivamente en comunicaciones electrónicas provenientes de ejecutivos, abogados o quienes estos designen. No obstante, el empleado o representante del cliente indica que no ha podido verificar las transacciones con dichos ejecutivos, abogados o quienes estos designen.

Jurisdicciones de alto riesgo para fraude de BEC

- La cuenta del beneficiario puede pertenecer a una compañía extranjera o puede estar radicada en una institución financiera de una jurisdicción de alto riesgo, según lo determinen la institución financiera y sus autoridades jurisdiccionales competentes.

Uso de facturas o documentos fraguados

- Los delincuentes envían facturas o documentos fraguados al empleado de una víctima para confirmar la transacción. Las facturas y los documentos fraguados pueden ser de buena calidad e incluir, incluso, documentos genuinos que se modificaron para desviar dinero a la cuenta de una institución financiera del delincuente.

Indicadores relacionados con la cuenta de presuntos delincuentes de fraude de BEC

Patrones generales de transacciones sospechosas

- Tras un ataque a una cuenta o compañía, los fondos se retiran de inmediato de la institución financiera, se transfieren al instante fuera de esta o a varias de sus cuentas.
- Una institución financiera recibe una transferencia por crédito en una cuenta, pero se designa a un beneficiario que no es el titular registrado. Esto puede reflejar instancias donde una víctima envía involuntariamente transferencias a un nuevo número de cuenta, provisto por un delincuente que suplanta la identidad de un proveedor/prestador conocido, y cree que la nueva cuenta pertenece a este, tal como se describe en la situación hipotética de BEC 3. Este indicador puede ser detectado por instituciones financieras que reciben transferencias enviadas por otra como resultado del fraude de BEC.

Monto de la transferencia

- El monto de la transferencia de fondos que se recibe en la cuenta de un beneficiario no concuerda con el perfil del cliente.

Uso de mulas

- El aumento repentino de transacciones de montos elevados y saldos de un cliente intermediario puede indicar la posible intervención de una persona en carácter de mula en un esquema de fraude de BEC. Las mulas que trasladan dinero[4] actúan como intermediarios para los delincuentes y las organizaciones delictivas. En algunos casos, las víctimas desconocen que las están usando para trasladar dinero de manera fraudulenta destinado a los ciberdelincuentes. Con frecuencia, los delincuentes usan mulas que trasladan dinero en el marco de los esquemas de fraude de BEC. Estas mulas generalmente tienen saldos bajos o una actividad financiera limitada antes de intervenir en el esquema.

Mitigación de riesgos

Con un proceso polifacético de verificación de transacciones, las instituciones financieras pueden protegerse contra el fraude de BEC. Por ejemplo, pueden verificar la autenticidad de instrucciones de pago sospechosas que se envían por correo electrónico si se comunican con el cliente por varios medios (p. ej., teléfono o direcciones de correo electrónico alternativas) o si se comunican con otros integrantes de la compañía que estén autorizados a realizar las transacciones. El éxito de los esquemas de BEC depende de que los delincuentes induzcan a las instituciones financieras a realizar transacciones

que parecen legítimas, pero que no están autorizadas. Este tipo de transacciones suelen ser irrevocables, lo cual impide que las instituciones financieras y sus clientes cancelen el pago o recuperen los fondos. Por esta razón, es fundamental detectar las instrucciones de pago de transacciones fraudulentas antes de que se emitan los pagos a fin de prevenir y reducir las transacciones no autorizadas.

Respuesta a los incidentes de BEC y recuperación de fondos

Algunos miembros del Grupo Egmont de UIF trabajan colaborativamente con las instituciones financieras y con los organismos del orden público a fin de recuperar los fondos de las víctimas. Para ello, difunden información del presunto fraude financiero relacionado con BEC. Es fundamental que las víctimas, las instituciones financieras y las autoridades del orden público actúen de inmediato a fin de que puedan recuperarse los fondos. El índice de recuperación de los fondos perdidos disminuye considerablemente tras las primeras 24 horas.

Para colaborar con la investigación de incidentes de BEC y recuperar los fondos del fraude correspondiente, se recomienda a las instituciones financieras poner en práctica estos pasos:[5]

1) **Comunicarse de inmediato con las instituciones del orden público y demás autoridades pertinentes**

   a. *Denunciar el delito:* Es imprescindible que la víctima, las instituciones financieras, las instituciones del orden público y de reglamentación, y las UIF nacionales y extranjeras actúen rápidamente para intentar recuperar los fondos transferidos. Con este fin, la víctima o su institución financiera debe denunciar de inmediato el delito y solicitar la asistencia de la autoridad del orden público y de la UIF.[6]

      Debe tenerse en cuenta que también es importante que las instituciones financieras denuncien no solo las transacciones exitosas, sino también los intentos fallidos, dado que la información relacionada con el intento de fraude puede ser fundamental para que las autoridades competentes puedan investigar las redes delictivas y las actividades ilícitas.

   b. *Alertar a la institución financiera del beneficiario:* La institución financiera donde está radicada la cuenta de la víctima debe comunicarse de inmediato con la institución financiera del beneficiario para informar sobre el presunto fraude.

[4] La identidad de las mulas que transportan dinero permite abrir las cuentas de la institución financiera, obtener tarjetas bancarias con un PIN y códigos personalizados, y lograr acceder a centros de pago en línea. Las mulas deben proporcionar esta información o transferir su acceso a otros miembros del grupo delictivo organizado, a fin de que puedan emplearla con fines ilegales. En general, las mulas ignoran el panorama más amplio del delito en el que participan y solo reciben una pequeña suma por el "servicio" provisto.

[5] Los componentes de cada paso no son necesariamente consecutivos, dado que muchas de estas actividades pueden ocurrir de manera simultánea o con una sucesión cercana. Tal como se indicó, responder de inmediato y colaborar con las autoridades competentes, incluidas las instituciones del orden público y las UIF, es fundamental para lograr recuperar los fondos perdidos en un fraude de BEC.

[6] La autoridad y la operación de las autoridades del orden público, de las UIF y de otras autoridades competentes varían de una jurisdicción a otra. Si bien en esta sección se destaca la importancia de tomar medidas para informar a las autoridades del orden público y a las UIF locales en casos de esquemas de BEC, las personas y las instituciones financieras afectadas deben determinar cuáles son las autoridades relevantes de su jurisdicción a fin de informar a quien corresponda.

c. *Marcar las transacciones sospechosas entrantes:* La institución financiera de la posible víctima o el beneficiario inicial de los fondos obtenidos de manera fraudulenta pueden sospechar el fraude si dudan sobre el origen legítimo de los fondos recibidos. En este caso, la institución financiera debe contactarse de inmediato con las autoridades del orden público o reglamentarias relevantes, y la UIF debe alertarlos sobre la transacción sospechosa.

   La entidad denunciante también debe presentar de inmediato un reporte de operación sospechosa (ROS) ante la UIF relevante, si corresponde. Si la transferencia se realizó en el plazo de las últimas 72 horas, la persona que presenta la queja debe remarcar que la situación es urgente.

2) Detener el movimiento de divisas

a. *No realizar transacciones sospechosas:* La institución financiera del beneficiario que tiene la información (p. ej., el mensaje de suspensión de transferencias SWIFT) de que se realizó una transferencia fraudulenta en la cuenta de uno de sus clientes no debe realizar transacciones que podrían dar lugar a la pérdida de los fondos. A fin de evaluar la validez de la transacción recibida, la institución financiera del beneficiario debe comunicarse con las autoridades del orden público y con la UIF.

3) Confiscar/recuperar los activos

a. *Informar a las autoridades competentes la ubicación de los activos:* A fin de incrementar las probabilidades de recuperar los activos, las instituciones financieras deben proporcionar la información solicitada por las autoridades del orden público y la UIF local. Las instituciones financieras deben informar a la UIF y a las autoridades del orden público antes de realizar cualquier transacción saliente, si los fondos todavía se encuentran en la cuenta, además de notificar el siguiente destino de los fondos que se acaban de transferir desde la cuenta.

b. *Órdenes de bloqueo:* Las instituciones financieras deben cooperar con la UIF o con las autoridades del orden público en caso de que las autoridades competentes emitan órdenes de bloqueo.

Denuncia de transacciones sospechosas según este boletín

En lo que respecta al procedimiento que corresponde a la jurisdicción, los sujetos obligados deben consultar este boletín cuando denuncien posibles transacciones relacionadas con BEC ante las autoridades competentes de sus jurisdicciones, según los indicadores que aquí se presentan. Hacer referencia a este boletín en los ROS permitirá que las autoridades competentes relevantes identifiquen el fraude relacionado con BEC y tomen medidas para colaborar en la recuperación de los fondos y en la correspondiente investigación. Siempre que sea posible, los sujetos obligados deben considerar el siguiente término clave en el ROS para indicar que han consultado este boletín para detectar transacciones sospechosas posiblemente relacionadas con esquemas de BEC:

“Boletín sobre BEC de Egmont”

Se les recuerda a las instituciones que denuncian el fraude que compromete al correo electrónico a través de los ROS que se debe incluir toda la información relevante y detallada posible, en especial, la siguiente:

Detalles de la transacción:

- Fechas y montos de las transacciones sospechosas.
- Información identificatoria del emisor, número de cuenta e institución financiera.
- Información identificatoria del beneficiario, número de cuenta e institución financiera.
- Información de las instituciones financieras intermediarias y del corresponsal, si corresponde.

Detalles del esquema:

- Ciberindicadores, tales como direcciones de correo electrónico relevantes, encabezados de correo electrónico y direcciones de protocolo de Internet (IP) asociadas, con sus respectivas marcas de tiempo.
- Descripción e intervalos de las comunicaciones electrónicas sospechosas.