FRAUDE BEC & EAC: una metodología de ciberdelito muy costosa para los bancos

Lavadodinero.com®

Entrenamiento y Prevención del Crimen Financiero

La unidad de inteligencia financiera de Estados Unidos emitió una advertencia al sistema bancario sobre una nueva metodología de fraude a través de correos electrónicos, que es considerada una de las tendencias más notorias de ciberdelitos desde el año 2013 al haber sido utilizada para estafar unos US$ 3.100 millones.

La Red de Control de Crímenes Financieros (FinCEN por sus iniciales en inglés) detalla en la Advertencia FIN-2016-A003 que los criminales controlan las cuentas de correos electrónicos de los clientes, a través de las cuales solicitan transferencias cablegráficas de fondos sin que los verdaderos propietarios se enteren. Esta metodología se conoce como Fraude de Email Comprometido (*Email Compromised Fraud*) y se clasifica en dos versiones:

a) Cuentas de Email de Negocios Comprometidas (BEC por sus iniciales en inglés): las víctimas son entidades comerciales clientes del banco afectado. Usualmente las víctimas son empresas -grandes o pequeñas- que realizan muchas transferencias y/o que trabajan con entidades extranjeras. Algunos datos de interés manejados por el Centro de Quejas de Crímenes en Internet del Buró Federal de Inteligencia (Internet Crimen Complaint Center – IC3 / FBI):

- **Desde enero de 2015 se ha producido un incremento de 1.300% en el número de reportes de casos asociados a esta metodología.**
- **Entre octubre de 2013 y mayo de 2016 unas 15.668 personas jurídicas se han visto afectadas, de las cuales 1.636 son empresas con sede fuera de Estados Unidos.**
- **Clientes de 100 países se han visto afectados.**
- **Las transferencias fraudulentas han sido realizadas para 79 países.**
- **La mayoría de las transferencias han sido efectuadas para bancos ubicados en China y Hong Kong.**

b) Cuentas de Email Comprometidas (EAC por sus iniciales en inglés): las cuentas defraudadas son personales. Las víctimas son incitadas a realizar pagos a destinatarios fraudulentos. Durante el año 2015, el IC3 recibió 281 denuncias de personas que fueron víctimas de este fraude y que perdieron en conjunto más de US$ 11 millones.

¿CÓMO FUNCIONAN EL FRAUDE BEC & EAC?

Básicamente es un fraude que consiste en dos etapas: primero la obtención de los datos de la víctima; segundo, la solicitud de transferencias electrónicas de fondos de forma fraudulentas. Si no se logra el primer nivel de fraude es imposible ejecutar la segunda etapa. Los pasos son los siguientes:

1) Acceso a la información de las víctimas: la primera parte del proceso consiste en obtener los datos de las futuras víctimas. En tal sentido, los criminales buscan acceder a las cuentas de correos electrónicos (personales y/o de negocios) de las víctimas, para lo cual utilizan dos procesos:

a. Técnicas de intrusión de los equipos (laptops, tabletas, etc.): las principales son:

i. **Pishing emails:** el delincuente envía correos electrónicos que simulan ser de una empresa o un banco con la intención de engañar a la víctima y obtener la información sensible que pueda ser usada para el fraude, como datos de acceso a las cuentas de banca en línea, tarjetas de crédito, contraseñas de cuentas, datos filiatorios, etc.

ii. **Scareware:** es una técnica mediante la cual los estafadores instalan en los equipos de las víctimas software maliciosos que anuncian falsos virus o fallas, generando miedo en los usuarios, quienes son incitados a instalar supuestos software para resolver los problemas. Las amenazas suelen ser falsas, pero el software instalado transmite luego la información personal a los estafadores.

iii. **Ransomware:** literalmente es un secuestro de una parte o la totalidad de los discos de almacenamiento de los equipos, impidiendo el acceso de los usuarios a su información. El software posteriormente pide un "rescate" para liberar la información comprometida, la cual igual puede haber sido robada por los ciberdelincuentes.

b. Técnicas de ingeniería social: se refiere a las tácticas de interacción humana que se utilizan para engañar a una persona para que revele información. Pueden utilizar llamadas telefónicas, emails o cualquier contacto directo con la víctima, quien es considerado el "eslabón más débil" en los sistemas de seguridad.

2) Transmisión de instrucciones de transacciones fraudulentas: los criminales utilizan la información robada para girar instrucciones de transferencia bancaria fraudulenta a la institución financiera de una manera que parece ser de la víctima, quien es el titular de la cuenta o la persona autorizada. El email es enviado desde cualquiera de las cuentas de correo electrónico reales de la víctima, preferiblemente la que está registrada ante el banco, aunque también pueden ser usadas cuentas falsas que asemejan el correo electrónico de la víctima.

3) La ejecución de transacciones no autorizadas: los empleados de la víctima (en caso de ser un negocio) o de la institución financiera realizan las transferencias electrónicas que parecen ser legítimas. Las instrucciones indican que el dinero sea enviado a cuentas bancarias nacionales o extranjeras controladas por los criminales. Los bancos en Asia y particularmente en China y Hong Kong son destinos comunes para estas transacciones fraudulentas.

BANDERAS ROJAS (RED FLAGS)

- Instrucciones de transacciones enviadas por el cliente mediante un correo electrónico que contienen un lenguaje diferente, plazos de tiempo y/o cantidades atípicas que no han sido previamente verificadas.

- Instrucciones para realizar una transacción que se originan a partir de una cuenta de correo electrónico que se parece mucho a la cuenta de correo electrónico típicamente usada por el cliente. La dirección de e-mail puede haber sido ligeramente alterada mediante la adición, cambio o supresión de uno o más caracteres.
  Por ejemplo:

  Cuenta de email legítima:
  john-doe@abc.com
  Cuentas de email fraudulentas:
  juan_perez@abc.com /
  john-doe@bcd.com

- Instrucciones por email para realizar una transacción de pago directo a un beneficiario conocido; Sin embargo, la información de la cuenta del beneficiario es diferente de la utilizada anteriormente.

- Instrucciones por email para realizar transferencias electrónicas directas a una cuenta bancaria extranjera que ha sido previamente el destino de transacciones fraudulentas.

- Instrucciones por email para realizar una transacción de pago directo a un beneficiario con el que el cliente no tiene historial de pagos o relación comercial documentada, y el pago es de una cantidad similar o superior a los enviados a los beneficiarios conocidos históricamente.

- Instrucciones de transacción por correo electrónico que incluyen marcas, afirmaciones o palabras que clasifican el requerimiento como "Urgente", "Secreto" o "Confidencial".

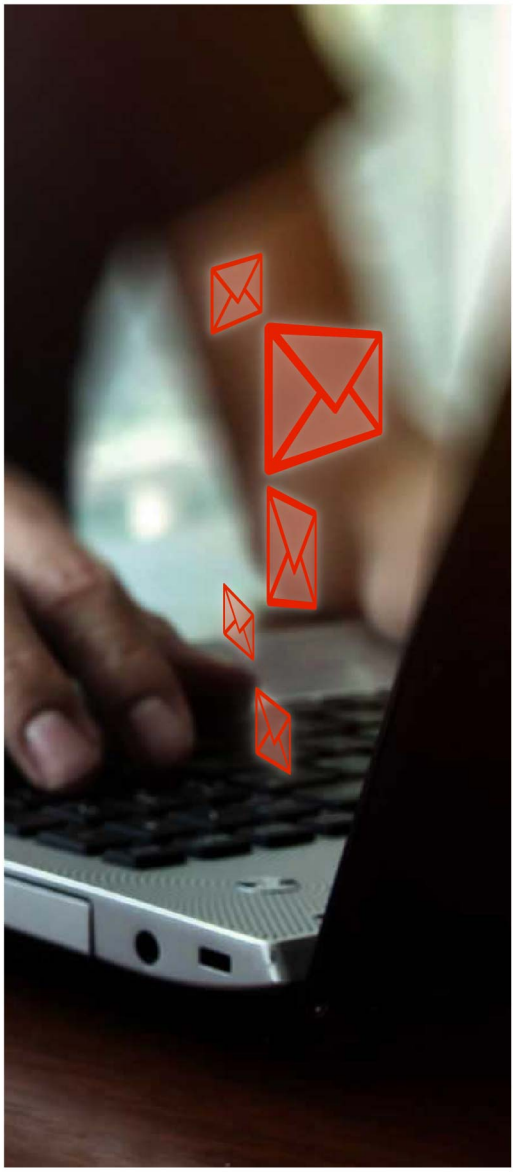
- Instrucciones por correo electrónico para realizar una transacción que son realizadas de una manera que no le da tiempo suficiente o la oportunidad a la institución financiera de confirmar la autenticidad de la transacción solicitada.

- Instrucciones por correo electrónico para realizar una transacción enviadas por un empleado de un cliente que es una persona recientemente autorizada en la cuenta o es una persona autorizada que no ha enviado previamente instrucciones de transferencia bancaria.

- Un empleado del cliente o un representante envía por correo electrónico instrucciones para una transacción. Dicha instrucción se basa exclusivamente en las comunicaciones de correo electrónico procedentes de los ejecutivos, abogados o representantes del cliente. Sin embargo, el empleado o representante del cliente que envía el requerimiento indica que no ha podido contactar al remitente original para verificar la transacción ordenada.

- Un email solicitando pagos adicionales inmediatamente después de un pago hecho a una cuenta que nunca antes había sido utilizada por el cliente para pagar a sus proveedores / vendedores. Tal comportamiento puede ser compatible con un criminal que intenta emitir pagos no autorizados adicionales al enterarse de que un primer pago fraudulento se ha realizado exitosamente.

- Una transferencia bancaria es acreditada a una cuenta, sin embargo, el nombre del beneficiario de la transferencia no coincide con el titular de la cuenta. Esto puede reflejar los casos en que una víctima envía inadvertidamente transferencias electrónicas a un nuevo número de cuenta, proporcionado por un criminal que se hizo pasar por un distribuidor/proveedor conocido. Esta señal de alerta puede ser vista por las instituciones financieras que reciben las transferencias electrónicas enviadas por otra institución financiera como resultado de correo electrónico fraudulentos.



Título: **FRAUDE BEC & EAC: una metodología de ciberdelito muy costosa para los bancos**
Producción: **Departamento de Producción de Lavadodinero.com**
Coordinación General: **Juan Alejandro Baptista**
Diseño: **Andrés Alvarado**
Edición: **octubre de 2016**

Copyright@2016. Se prohíbe la reproducción parcial o total de este material sin la previa autorización por escrito de Lavadodinero.com / Ideas Publishing Solutions. Las violaciones de los derechos de autor y de la propiedad intelectual de este contenido serán consideradas violaciones de las leyes federales de Estados Unidos.

BST
Global Consulting

Risk Managment
Antilavado
Consultoría Integral
Auditorías

www.bst.consulting

ESTADOS UNIDOS - MÉXICO - PANAMÁ - PARAGUAY - PERÚ - REPÚBLICA DOMINICANA - URUGUAY

Lavadodinero.com®

Entrenamiento y Prevención del Crimen Financiero

SOMOS UN CENTRO DE CAPACITACIÓN CONTRA LOS CRÍMENES FINANCIEROS

ajustado a los presupuestos de las empresas y profesionales regulados