LITORALPRESS

Fecha: 14-07-2024
Medio: El Mercurio
Supl. : El Mercurio - Cuerpo B
Tipo: Noticia general
Título: OTRA VEZ LAS FACTURAS... el nuevo fraude que acecha a las empresas vía hackers y el SI

Pág. : 4
Cm2: 1.162,8
VPE: $ 15.274.294

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

Antofagasta Minerals, Cantabria y Microsoft, algunos de los afectados:

OTRA VEZ LAS FACTURAS... el nuevo fraude que acecha a las empresas vía *hackers* y el SII

A través de compañías, en un día y en horarios insólitos. Emiten facturas, suplantan identidad de gerentes en el SII y las aprueban, para luego venderlas. Un mecanismo que afecta en cientos de millones a grandes firmas. Hoy, hay casos en la justicia, que piden oficiar a Impuestos Internos para tener más antecedentes. • **MARÍA JOSÉ TAPIA**

El 16 de mayo, la gerenta corporativa de riesgo de Antofagasta Minerals (AMSA) recibió una notificación virtual del Servicio de Impuestos Internos (SII). Le señalaban que su clave de acceso había sido modificada.

La ejecutiva inició el proceso de recuperación de su contraseña. Sin embargo, al otro día recibió una nueva notificación... su clave había sido cambiada nuevamente. Y luego ocurriría lo mismo con sus datos personales —como *mail* y teléfono— asociados al organismo. Se alertó tanto al Servicio como a la empresa. Y si inicialmente no encontraron ninguna vulneración a sus sistemas informáticos, luego aparecieron facturas emitidas que no estaban asociadas a proveedores de AMSA. Eran seis autorizadas en la misma plataforma del SII. Incluso, cuatro de ellas habían sido aceptadas suplantando la identidad del gerente general del *holding*, Iván Arriagada. En total fueron $373 millones, se lee en la querella por fraude informático que presentaron el 3 de junio pasado.

El caso de la minera del grupo Luksic no es aislado. Desde hace un año han aparecido varios que dan cuenta de un nuevo tipo de delito con facturas. Ya no es solo la emisión de documentos falsos entre compañías, sino que ahora serían *hackers* que logran entrar a las plataformas de las empresas en el SII y aprobar los documentos. Una compañía tiene 8 días para visar una factura, cuando ocurre pasa a ser un título ejecutivo que solo puede ser pagado.

Según relatan en el mundo privado, en general la nueva dinámica opera así: se trata de firmas creadas en un día, que emiten facturas a compañías de renombre —en algunos casos a las 4 de la mañana—, y *hackers* ingresan en la plataforma de esas firmas en el SII y las aprueban. Con ese documento, las venden a *factoring* medianos o pequeños, con descuentos atractivos, y luego estas las ceden a *factoring* grandes. "Estamos hablando de una factura de una compañía *premium*, confirmada. O sea, no hay nada mejor en el sistema. Y luego te llama un *factoring*, diciéndole a la empresa que debe plata, miras tus sistemas y te das cuenta de que te enteraste 30 días después", dicen fuentes al tanto. Y agregan: "El tipo que hizo la empresa en un día era con identidad robada, y el que le robó la *password* a los gerentes generales era un *hacker*".

Desde el entorno de las facturas reconocen que han recibido algunas alertas, pero no es generalizado, "aunque no por eso, deja de ser preocupante".

Hace un año, le ocurrió lo mismo a la matriz de las cadenas Emporio de la Rosa, Cory y Bonafide, Cantabria, de propiedad de la familia Bofill, controladores de Carozzi.

El 18 de abril de 2023, la administrativa contable de la empresa envió un correo pidiendo apoyo en relación con un número de proveedores que aparecían emitiendo facturas, pero que no estaban registrados. Solicitaba que se les creara un perfil para evitar atrasos en los pagos. El gerente de Operaciones revisó los movimientos y concluyó que era un fraude.

Se trataba de 10 documentos por $155 millones emitidos por dos empresas de transportes, una de seguridad y una comercializadora; todas constituidas a través de Empresas en un día.

Las facturas fueron aceptadas utilizando la clave o el certificado digital del jefe de Contabilidad de Cantabria. Y cedidas algunas a Tanner, por la cual pagó $24,6 millones, y a Factotal, que canceló $19,9 millones. De hecho, fuentes conocedoras precisan que finalmente el perjuicio fue por unos $30 millones, ya que el resto alcanzó a pararse.

"Esto perjudica a Cantabria, pues con la declaración de que los servicios fueron efectivamente recibidos, se crea una obligación cedible en su contra (...). Y en algunos casos se perjudicó también a las empresas de *factoring*, en la medida en que entregan una suma de dinero a cambio de un crédito que no descansa en operaciones reales, y eventualmente, puede ser discutido", señala la querella por estafa, acceso ilícito a datos informáticos y receptación de los mismos presentada por la firma el 24 de mayo de 2023.

Medidas de control falibles

Hoy, las compañías cuentan con sistemas que procesan las facturas. Uno de ellos es Artikos, que las recibe, autoriza, rechaza y paga. Este programa está asociado a la cuenta del SII, asegurando que los documentos han sido emitidos por proveedores registrados y cuyos servicios han sido prestados. Generalmente, el *software* revisa las facturas todos los días a las 6:00 de la mañana. Sin embargo, en estas estafas, el sistema no ha podido frenarlas porque son facturas aceptadas en forma manual a través del propio Servicio, suplantando identidades de altos ejecutivos. En el caso de AMSA, por ejemplo, del gerente general y del gerente de Finanzas.

Además, en todos los ejemplos, los montos son pequeños en comparación con los tamaños de las compañías en cuestión, justamente para evitar sospechas.

Un *modus operandi* similar afectó recientemente a una empresa importante del país, que fue defraudada en unos $500 millones y pagó los documentos sin percatarse de que era una estafa. Lo mismo le pasó a Microsoft.

El 23 de enero, un cliente frecuente de la tecnológica recibió una orden de compra por $15 millones. Era de una persona con un correo que emulaba el *mail* de Microsoft (pero sin la t) y con un e-RUT obtenido en el portal del SII con los datos de la compañía. El cliente encendió la alerta. Luego, otro *partner* de Microsoft los contactó por lo mismo. Pero era aún peor: la casilla de correo del suplantador era @portalmicrosoftchile-.com, sabiendo que la correcta es @marcomkt.com; sin embargo, al acceder a www.portalmicrosoftchile.com, redirecciona al sitio web de Microsoft, sin ser un portal de ellos.

La firma interpuso primero una denuncia ante la Fiscalía Oriente. Y luego empezaron a aparecer las facturas. Fue el estudio de abogados DNPV el que los contactó por una deuda de $17,6 millones con una factura emitida por una empresa de transporte. "La factura fue recepcionada y aceptada el mismo 21 de febrero de 2024 a solo horas de haber sido emitida", se lee en la acción judicial.

> AMSA, Microsoft y Cantabria le pidieron al Ministerio Público que oficie al SII para que entregue las direcciones IP desde las que se aceptaron las facturas falsas.

Según agregan en todas las órdenes de compra referidas se establece que las facturas deben ser enviadas a una casilla que no es de dominio de Microsoft. "Como las personas naturales tenían acceso de forma ilícita al portal del SII de Microsoft, al momento de recibir el correo electrónico de la factura emitida, las daban por recepcionadas y las aceptaban en cuestión de minutos", se lee en la acción judicial. "Este *modus operandi* puso a mi representada en la imposibilidad de conocer lo que estaba pasando y de impedir que siguiera sucediendo", agrega.

En total son 19 documentos por $212 millones, aunque admite que el monto podría incrementarse. Fueron órdenes de compra de suplantadores dirigidos a comercios reconocidos como Sodimac, Cencosud, Latam, quienes luego emitían la factura a Microsoft por servicios que nunca contrató.

Además, hubo una factura suya cedida a Security, la cual —dice la acción judicial— emitió una nota de crédito y están reclamando el pago total a la tecnológica.

En el mercado estiman que si bien los casos aún son menores, deben estarse multiplicando con rapidez. "Creemos que hay bastantes más, porque es algo tan jugoso que es imposible que los *hackers* estén esperando meses para hacer otra estafa", asegura una firma afectada.

"Lo clave es que las empresas pagadoras y las entidades financieras que anticipan el pago de facturas tengan mecanismos de control y detección de situaciones anómalas", subraya el gerente general de la Bolsa de Productos, Christopher Bosler.

AMSA pagó US$ 5 mil millones en 2023 a más de 300 proveedores y contratistas, efectuando compras por más de US$ 600 millones a proveedores de Coquimbo y Antofagasta, "de tal manera que una factura supuestamente emitida a nombre de una compañía tan solvente y prestigiosa como Antofagasta Minerals o alguna de sus filiales, y aceptadas por estas, son muy codiciadas en el mercado de los *factorings*, por cuanto representan un pago seguro", dice la firma en su acción judicial.

En la minera las facturas han terminado en manos de Penta Financiero, Eurocapital, entre otros. AMSA alertó a los *factoring* de que los documentos eran falsos.

Buscando soluciones

El fundador de Btrust Finance —que transa facturas—, Patricio Cortés, creó hace algunos meses la plataforma de inteligencia artificial The Merlyn IA justamente a raíz de estos casos. Según cuenta, le llegaron alertas de lo que estaba ocurriendo, sobre todo ejemplos de facturas fraudulentas que se habían aprobado a las 4 de la mañana desde la plataforma del SII.

Diseñó una plataforma que está en línea mirando todo el proceso desde el origen de la orden de compra hasta el pago. Y cada vez que hay un cambio en un patrón, a la hora que sea, se alerta a la compañía vía *mail*, WhatsApp o llamado telefónico para alcanzar a frenarla. Ya han alertado a empresas y una eléctrica les acaba de comprar el servicio. "Les decimos a las compañías 'piensa que esto puede ocurrir. Lo importante es que tú no te enteres cuando te llame el fondo para cobrarte'", destaca.

Todo ello, considerando, además, que la problemática se dificulta si esto ocurre en el SII. Y con un mercado de grandes magnitudes: se emiten 24 millones de facturas mensualmente, de ellas ceden 410.000, lo que equivale a más de US$ 3.000 millones. "Todo el mercado de facturas depende del SII", señala un actor del mercado.

"Es relevante el rol del SII, actor esencial para el funcionamiento del mercado de facturas, en cuanto a inversión en tecnología, seguridad y procesos de control", añade Christopher Bosler, de la Bolsa de Productos.

AMSA, Microsoft y Cantabria le pidieron al Ministerio Público que oficie al SII para que entregue las direcciones IP desde las cuales fueron aceptadas las facturas falsas. Y se indague la ubicación de las mismas.

Desde el SII aseguraron haber tomado conocimiento de algunos de estos casos; puso en alerta a la autoridad tributaria, que está monitoreando el tema a través de equipos especializados de la Subdirección de Fiscalización y del área de Asistencia al Contribuyente. Paralelamente, a través de la Subdirección Jurídica, se está atentos a accionar penalmente con la presentación de querellas frente a la comisión de delitos tributarios.