PERIÓDICO	PAGINA	FECHA	SECCIÓN
LA CRÓNICA DE HOY	PP-6	21/03/2024	NACIONAL

Al alza, secuestro de datos y correos maliciosos para cometer extorsión

Los grandes cárteles ya incursionan en ese ámbito; Edomex y Colima, las entidades con más incidencia

Ciberfraudes. El secuestro de datos o ransomware --programa malicioso que impide a usuarios acceder a sus archivos personales-- y el envío de correos maliciosos están entre las modalidades más usadas por los delincuentes para extorsionar a personas o empresas. De acuerdo con la consultora Código Verde, especializada en ciberseguridad, los grandes cárteles del narcotráfico en México ya han incursionado en este ámbito.

La información va en sintonía con un informe reciente de la Interpol, el cual ubica al Cártel de Jalisco Nueva Generación en el negocio de los fraudes telefónicos y las estafas por Internet.

Ambas tácticas han sido identificadas en diversas procuradurías o fiscalías locales, en especial en el Estado de México, Colima, Baja California Sur, Nuevo León, Guanajuato, Morelos, Hidalgo, Veracruz y Campeche, entidades con mayor incidencia a nivel nacional, con números superiores a la media nacional en denuncias presentadas y víctimas. **PAG 6**

WEB

PERIÓDICO	PAGINA	FECHA	SECCIÓN
LA CRÓNICA DE HOY	PP-6	21/03/2024	NACIONAL

"Tenemos toda tu información. ¿Quieres la contraseña? Te cuesta 10 mil"...

El secuestro de datos y los correos maliciosos son instrumentos para la extorsión. Nueve estados superan la media nacional de incidencia; Edomex y Colima, casi la triplican

Especial

Daniel Blancas Madrigal
Segunda parte

El secuestro de datos o ransomware, y el envío de correos maliciosos están entre las modalidades más usadas por los delincuentes para extorsionar a personas o empresas…

De acuerdo con la consultora Código Verde, especializada en ciberseguridad, los grandes cárteles del narcotráfico en México ya han incursionado en este ámbito. La información va en sintonía con un informe reciente de la Interpol, el cual ubica al Cártel de Jalisco Nueva Generación en el negocio de los fraudes telefónicos y las estafas por Internet.

Ambas tácticas han sido identificadas en las carpetas de investigación abiertas en diversas procuradurías o fiscalías locales, en especial en el Estado de México, Colima, Baja California Sur, Nuevo León, Guanajuato, Morelos, Hidalgo, Veracruz y Campeche, entidades con mayor incidencia a nivel nacional, con números superiores a la media nacional en denuncias presentadas y víctimas.

DEPÓSITOS

Los casos tienen nombres y rostros, como el de Mauricio, contador en una empresa dedicada a la distribución de materias primas para productos de limpieza, con sede en el Edomex, estado en el cual se triplican los casos en relación al promedio de todo el país.

"Recibí un correo electrónico de una cuenta no identificada en mis contactos, me aseguraban que habían tenido acceso a mi computadora y que tenían la lista de los sitios que solía visitar, así como fotografías almacenadas y enviadas a otras personas. Según ellos, había información y fotografías comprometedoras. Si no quería que las hicieras públicas, tenía que hacer un depósito exprés de 5 mil pesos".

"Le daba vueltas y vueltas al asunto pensando en cuál sería esa información comprometedora. No había mandado nada por el estilo ni había hecho nada ilegal, así que ignoré el correo. A la siguiente semana me llegó otro, en el que ya aludían a la empresa en la cual laboro. La amenaza era que si no depositaba, publicarían datos financieros y listas de clientes. Ya no podía seguir ignorándolo, lo comenté con los directivos y se tomó la decisión de denunciar".

¿Y qué paso?

Nos pidieron fotos, copias y capturas de pantalla de los correos recibidos. Dijeron que era una extorsión, supuestamente intervino la policía cibernética, pero hasta la fecha desconocemos quién estaba detrás.

"Esos correos se los mandan no a una persona sino a decenas o cientos de personas, es un ataque donde te están poniendo lo que crees un cuchillo en la espalda, pero en realidad es un palito de paleta. Si de toda esa masa de mensajes caen dos o tres víctimas, los criminales se dan por bien servidos", señaló a *Crónica* David Schekaiban, uno de los especialistas en ciberseguridad más reconocidos en el país.

Ahí mismo, en el Estado de México, se documentó el caso de Juan Manuel V., otro empresario del ramo textil.

"Me llegó un correo desconocido, pero en el título decía: ´cliente potencial´. Lo abrí pensando que podía ser importante, e incluía un archivo. Le di doble click y, de repente, se comenzó a instalar en la computadora no sé qué cosa. Ya no pude abrir mi inventario ni la base de datos de proveedores y clientes. Me pedía una contraseña que desconocía, ya después supe que era un secuestro de datos y mi información estaba cifrada".

"Al día siguiente llegó otro correo: ´tenemos toda tu información, si quieres la llave o contraseña para acceder, te cuesta 10 mil pesos´. Era como pedir un rescate por mis archivos. Tuve que buscar a un experto en el tema, me sugirió que no pagara nada, y que instalaría unos desencriptadores. Logré recuperar una parte, pero otra muy valiosa se quedó perdida".

Según Schekaiban, el ransomware -programa malicioso que impide a usuarios acceder a sus archivos personales y exige el pago de un rescate para hacerlo-, "le cuesta miles de millones de dólares a las organizaciones y empresas de todo el mundo, ahí se están metiendo los cárteles que antes se dedicaban exclusivamente al tráfico de drogas, como el Cártel de Jalisco Nueva Generación".

¿Cómo lo hacen? -se le cuestionó.

Compran la infraestructura para mandar los correos, desarrollar los programas y cifrar la información: ´dame tanto, o ya no la vuelves a ver´. Esos esquemas son una realidad, es la amenaza más grande que tienen las compañías en la actualidad, porque todo su sistema queda intervenido.

También le pega a personas, gobierno, universidades... Alguien en lo individual no te podrá pagar 5 mil dólares de rescate, pero sí algunas empresas.

MUSCULOSO CONTRA DÉBIL

Sin normatividad específica, muchos de los expedientes se encuadran en el delito de extorsión.

La media nacional, conforme a los datos del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, es de ocho extorsiones por cada 100 mil habitantes, con corte a diciembre de 2023. Sin embargo, los nueve estados ya referidos están por encima de esa referencia.

Sobresalen, por su nivel de incidencia, el Edomex, con 23 extorsiones por cada 100 mil, una problemática creciente en los últimos ocho años.

Y Colima, estado en el cual eran casi inexistentes los casos en 2015. Hoy su proporción es de 19 extorsiones por cada 100 mil habitantes.

"Imagina que dos personas hacen el compromiso de ir al gimnasio todos los días -ejemplifica Schekaiban-. Uno cumple su palabra, y al otro le gana el desinterés. Después de algunos años se vuelven a ver: el primero es un fortachón, y el otro es un obeso en cámara lenta. Es triste decirlo, pero el símil del musculoso cabe para los grupos criminales, que llevan años, más de una década, buscando la manera de hacer más dinero con menos dinero, y han encontrado el camino en la tecnología, desarrollando su mercado ilícito".

Los delincuentes no han dejado de ir al gimnasio...

Exacto, porque si dejan de ir les tumban el negocio. Por eso el uso de radios en la sierra, con un cableado sofisticado; por eso sus cámaras de vigilancia, sus sistemas de monitoreo, sus drones. En cambio, las autoridades siguen peleando como lo hacían hace años, y se han quedado a kilómetros de distancia.

La tecnología para uso delincuencial...

La tecnología magnifica el impacto de los delitos. Si un delincuente utiliza telefonía digital cifrada, si tiene instalado un bloqueador para Internet y redes de radio seguras, será difícil de atrapar.