13/04/2019

Las estafas suponen ya el 75 por ciento de la ciberdelincuencia

El tocomocho y el timo de la estampita se han reconvertido en fraudes con lingotes de oro y criptomonedas



Los ladrones de casas han dado paso a los ladrones de datos. El crimen organizado vinculado a los delitos contra el patrimonio se ha reconvertido. Lo dicen los expertos y lo avalan las cifras. La ciberdelincuencia no para de crecer, copada por los fraudes: **las estafas suponen ya el 75 por ciento de todos los delitos que se cometen en la red** . Son datos que maneja la Policía Nacional, que se enfrenta, como el resto de cuerpos policiales, no a una tendencia «sino a un fenómeno», explica el inspector jefe Raúl López, al frente de la Sección de Fraude de Comercio Electrónico de la **Unidad Central de Ciberdelincuencia.**

Más que de modalidades hay que referirse a qué queda fuera del alcance de los malos: prácticamente nada. La razón principal es la oferta casi infinita que existe «online». Todo lo que necesitamos se puede conseguir a golpe de click de ratón o pantalla de teléfono. «Los delincuentes lo saben y lo explotan a su antojo», afirma López. «Se trata de vender algo a través de Internet y mediante engaño obtener un beneficio que suele ser enorme».

El fraude tiene un elevadísimo impacto en la criminalidad. Más datos que lo refrendan. **En 2012 la Policía recibía unos veintidós correos al día en las pestañas que tiene habilitadas en su página web para denunciar estafas; ahora, la media diaria es de entre 200 y 300 alertas, más de 30.000 denuncias al año solo en la web** . «Son alertas en las que el perjudicado nos lo comunica, pero luego hay que denunciar», aclara Nacho San Segundo, policía del Grupo de Fraude en comercio en Internet, uno de los expertos dedicado a perseguir a los cibercriminales para los que no hay barreras.

Del alquiler a la consola

A medida que se generaliza el uso de las tecnologías, se disparan las estafas. La relación es clara y la preocupación internacional cada vez mayor. «Las modalidades son infinitas, se trata de aguzar el ingenio», continúa San Segundo que aporta razones sociológicas. «El estrés, las prisas y la comodidad crean un caldo de cultivo perfecto para los delincuentes. Estás comprando una entrada para un espectáculo y a medida que ves que se van agotando en la pantalla te provoca ansiedad y no reparas en detalles que deberías y en tomar todas las precauciones».

Otro ejemplo que trae de cabeza a las Fuerzas y Cuerpos de Seguridad: los alquileres vacacionales o las ventas de artículos de segunda mano a través de portales, utilizados sin su consentimiento por los delincuentes.

Hace tres semanas la Policía de Cádiz acabó con una organización que acumula más de 800 denuncias. Vendían desde thermomix hasta carritos de bebé, pasando por videoconsolas, drones, móviles y alquileres falsos de viviendas. Con su sofisticado método y

tirando de ingeniería social consiguieron que cientos de personas les enviaran sus carnés de identidad. Las víctimas no solo han perdido el dinero que pagaron, sino que además se enfrentan ahora a procedimientos judiciales, impagos y amenazas porque esos datos fueron utilizados para engañar a otros como ellos.

La banda usurpaba anuncios reales de los portales de compra-venta entre particulares como Wallapop, Milanunicos, eBay, etc. y llegaron a crear cientos de perfiles falsos en redes sociales. Entre las víctimas hay abogados, miembros de las Fuerzas y Cuerpos de Seguridad, carteros y todo tipo de profesiones. Abrieron más de 200 cuentas bancarias gracias a una prolija red de «muleros», colaboradores que a cambio de dinero se prestaban a cobrar y a abrir las citadas cuentas.

«Ya no estamos tanto ante organizaciones verticales, estructuradas, hay muchas que trabajan de manera horizontal y a veces ni se conocen entre ellos», aclara Nacho San Segundo. Han detectado cómo un grupo de hackers, por ejemplo, venden un virus o datos de tarjetas de crédito a una mafia; los responsables las utilizan y contratan a su vez a «mulas» que a cambio de entre 50 y 300 euros abren hasta cuatro o cinco cuentas bancarias en un día. Ahí se recibe el dinero de las estafas y en cuestión de minutos esos fondos se transfieren a cuentas extranjeras, casi siempre en paraísos fiscales o fuera de control.

«Hacker» de 15 años

«El hacker puede ser un chaval de 15 años, que se lo toma como un reto. La organización lo ficha en la red oscura y a partir de ahí entra en una cadena de hoteles o en un banco, crea un progama malicioso y se hace con cientos de credenciales de tarjetas de crédito mientras la víctima descubre cómo le han hecho cargos y no ha usado su tarjeta físicamente», detalla el inspector jefe Raúl López. Se conoce con el nombre de «carding» y con este método se despluma a miles de personas a diario. El «skimming» precisa que se esté haciendo una transacción en ese momento y está casi en desuso. «Disparan contra todo», admite López de forma gráfica.

La reconversión criminal es clara. «Para robar una vivienda necesito herramientas, apoyo y especialistas, es arriesgado y no es extraño que tenga que recurrir a la violencia. Si en lugar de eso publicito pisos internacionalmente, despliego a mis lugartenientes y los pongo a trabajar el beneficio será mayor, arriesgo menos y es complicado armar una causa y no hablemos ya de conseguir un ingreso en prisión», aseguran los agentes.

Las organizaciones de países del Este (rumanos, rusos) y africanas, sobre todo nigerianos, monopolizan parte del ciberfraude. Estos últimos, los reyes de la conocida estafa de las «cartas nigerianas» son ahora los jefes del «Love Scam» o el «Premio de la Lotería». Para la primera buscan a sus víctimas en webs de citas o redes sociales, personas solas o necesitadas de cariño a las que embaucan hasta entablar una relación sentimental. Una vez camelados, el siguiente paso es conseguir dinero. «Algunos vienen a denunciar obligados por la familia y se niegan a aceptar que la rubia despampante que les habla de amor a través de su móvil es un maromo de dos metros en un cíber de Nigeria», dice López. En «el soldado americano», otra variante, un marine herido en cualquier antigua guerra simula tener oro que necesita recuperar y pide dinero para ese rescate.

La ingeniería social, hacerse con el mayor número de datos de la víctima elegida, es clave. Los nuevos tocomochos y timos de la estampita son ahora estafas con lingotes de oro, criptomonedas o diamantes. Inversiones en páginas inexistentes que dejan a la víctima sin dinero y sin producto.

Hay estafas burdas y otros sofisticadísimas que dejan a empresas al borde de la bancarrota. **El llamado «fraude del CEO» está devorando compañías en todo el mundo**. La organización suplanta la identidad del consejero delegado o de alguno de los jefes con capacidad ejecutiva tras acceder a sus comunicaciones privadas y conocer su actividad con proveedores y clientes. El pago que hace el responsable por alguna operación concertada llega a una cuenta bancaria preparada para el delito. Así estafó ocho millones de euros una red rumana el año pasado tras dar de alta 700 cuentas.

«Internet no tiene fronteras y los sistemas judiciales las tienen todas» , dice el inspector jefe. Una comisión rogatoria para bloquear una cuenta puede tardar meses, pero el dinero en esa cuenta dura minutos. Los 2,5 millones que habían llegado desde España a una cuenta de Hong Kong, cuyo bloqueo pidieron, se habían reducido a 30 cuando la maquinaria echó a andar.

Fuente: ABC

https://www.abc.es/espana/abci-estafas-suponen-75-ciento-ciberdelincuencia-201904070200_noticia.html