Kippel01

TECNOLOGÍA

Bancos y plataformas de intercambio de criptomonedas, principales víctimas de los ciberdelincuentes

Los criminales optan por dirigir sus ataques a las operaciones interbancarias, los cajeros, los trabajadores y el personal directivo mediante phishing o a través de los encaminadores, utilizados como puerta de entrada de malware.

17 DIC 2018 — 04:51

POR DANIEL LÓPEZ

La lucha contra la ciberdelincuencia es continua. Cuanto más se fortalecen tecnológicamente las empresas y las administraciones, más perfeccionistas se vuelven los delincuentes a la hora de ejecutar sus ataques. **Los piratas informáticos se adaptan rápidamente al mercado** y buscan nuevas maneras de lucrarse, y en ese contexto han decidido centrar sus esfuerzos en derribar directamente a las entidades financieras y a las plataformas de intercambio de criptomonedas.

Así lo remarca el Centre de Seguretat de la Informació de Catalunya (Cesicat) en su último *Informe de Tendències de Ciberseguretat* al que ha tenido acceso Kippel01. Según la entidad, los ataques dirigidos a los bancos se concentraron en las operaciones interbancarias, los cajeros, los trabajadores y el personal directivo mediante *phishing* en el tercer trimestre. También a través de los encaminadores (*routers*), utilizados como puerta de entrada de *malware* o para redirigir

fraudulentamente las comunicaciones.

En este ámbito, **el uso de troyanos se convirtió en una tendencia al alza**, siendo el tipo de *malware* más difundido. Desde el inicio de 2018, se ha incrementado un 60% la detección de este tipo de programas informáticos. Asimismo, **el número de troyanos bancarios detectados en terminales móviles se ha triplicado**, debido a la proliferación del uso de estos dispositivos para realizar operaciones financieras.

La caída del valor de las criptomonedas estimuló el descenso de la minería ilegal

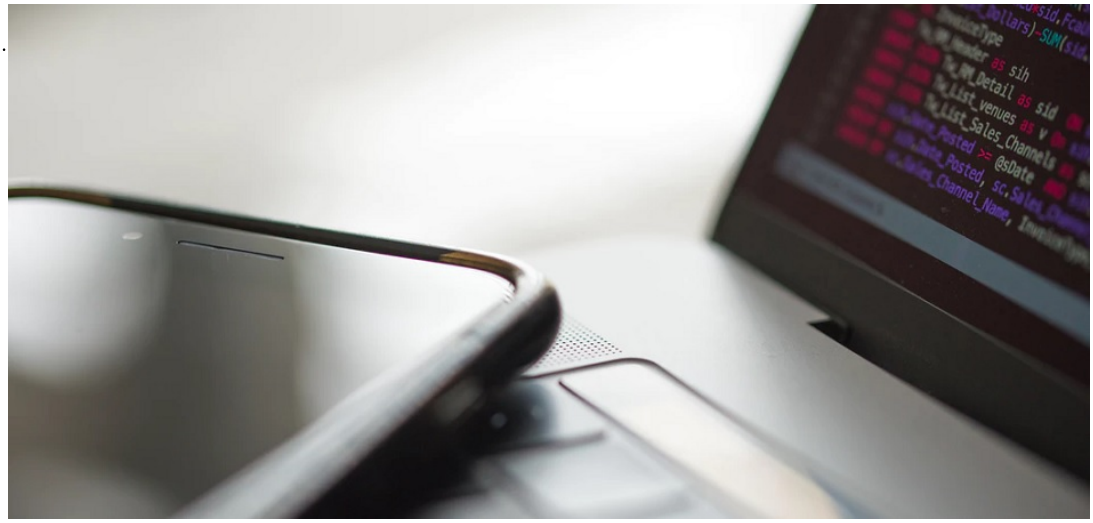
En cuanto a las criptomonedas, el estudio indica que se trata de un campo donde la ciberdelincuencia "se mueve con relativa comodidad". **Los ataques dirigidos a plataformas de intercambio de criptodivisas no dejaron de aumentar a lo largo del año**. Durante la primera mitad de 2018, los robos en este segmento ascendieron a 800 millones de dólares (704 millones de euros), casi el triple respecto al mismo periodo del año pasado.

Por contra, **en el tercer trimestre de este año, la minería ilegal dirigida a empresas descendió un 26%**, mientras que cayó un 32% en la de consumidores. El también llamado *cryptojacking* decreció, de acuerdo con el Cesicat, por "la caída del valor de las criptomonedas y la incerteza que provocan las nuevas regulaciones".

Eso no quiere decir, sin embargo, que no surgieran nuevas modalidades para minar criptodivisa de forma ilegal. El informe destaca la detección de una nueva variante del *ransomware* Rakhni que, examinando la configuración del dispositivo de la víctima, decide si es bueno para minar o para ejecutar el programa. Se distribuye mediante emails de *phishing* con un archivo en formato PDF que, al clicarse, descarga el *payload*. Esto último hace referencia a la parte del *malware* que realiza la acción maliciosa y se aprovecha de las vulnerabilidades del sistema.

Kippel01

TECNOLOGÍA



Las ofertas iniciales de moneda (ICO, por sus siglas en inglés), que actúan a modo de rondas de financiación virtuales vía *blockchain*, también aparecen en el foco de los ciberdelincuentes. Es remarcable el robo de 7,7 millones de dólares (6,8 millones de euros) a la plataforma singapurense Kickico el pasado julio. Tras asumir el control de una cuenta de administrador, se transfirieron criptomonedas a cuarenta direcciones falsas. El estudio alerta sobre cómo **estos incidentes de seguridad pueden afectar a la confianza de los usuarios**, lo que también acaba repercutiendo en el valor de las divisas digitales.

En los últimos meses, también se ha observado como usuarios de criptomonedas se han visto afectados por el llamado secuestro de la tarjeta SIM, que tiene como objetivo saltarse la seguridad de los sistemas basados en la autenticación doble. Este ataque consiste en contactar con la operadora de la víctima y, mediante técnicas de ingeniería social, obtener una réplica de su tarjeta SIM. Una vez conseguida, el criminal puede reiniciar las contraseñas en otro dispositivo y consumar el robo. Esta clase de ciberataque no es habitual y suele ir dirigido a un individuo concreto.

Además, desde la aplicación del Reglamento General de Protección de Datos (Rgpd) el pasado 25 de mayo, los incidentes que antes se desconocían o se informaban con meses de retraso, ahora se deben comunicar en un término de 72 horas una vez se han detectado. Por tanto, ahora las empresas afectadas no pueden ocultar información.