Comunidad de Madrid

Medios de Comunicación

Ha sido creada por investigadores del IMDEA Software e identifica las conexiones con operadores de actividades ilícitas

La Comunidad de Madrid desarrolla una herramienta para rastrear el cibercrimen de Bitcoins

- Han analizado más de 7.500 direcciones que pertenecen a 30 familias de programas maliciosos como el secuestro de datos o el robo de información
- Facilitaría a los Cuerpos de Seguridad del Estado evidencias para obtener una orden judicial y conocer los destinatarios finales del dinero obtenido de manera ilegal

4 de enero de 2023.- La Comunidad de Madrid, a través de su Instituto de Investigaciones Avanzadas IMDEA Software, ha desarrollado una herramienta capaz de rastrear las operaciones financieras de cibercrimen en la moneda digital Bitcoin. Se trata de un sistema automatizado de código abierto, cuyos derechos no son exclusivos de los autores, que ayuda identificar relaciones con entidades maliciosas que abusan de esta tecnología.

Esta iniciativa favorece la investigación de los delitos digitales como estafas, suplantación de identidad, robo de datos personales o fraudes informáticos, entre otros. Para ello han analizado más de 7.500 direcciones que pertenecen a 30 familias de *malware* (programas maliciosos), entre ellos relacionados con *ransomware* (secuestro de datos), *clippers* (hurto de criptomonedas), técnicas de engaño para la extorsión sexual o *infostealers* (sustracción de información).

El dispositivo utiliza el método *back-and-forth exploration* (seguimiento de un movimiento hacia adelante y hacia atrás), cuya principal ventaja es que permite rastrear todas las transacciones producidas por una dirección de manera indefinida. De esta forma, la herramienta del IMDEA de la Comunidad de Madrid, además de servir a los usuarios, podría ser especialmente útil para los Cuerpos de Seguridad del Estado. Así, les permitiría identificar rutas completas, entre ellas los lugares de depósito como podrían ser las casas de cambio de criptomonedas que son utilizadas, en ocasiones, por operadores de actividades ilícitas.

Los efectivos policiales, por ejemplo, podrían utilizar dichos itinerarios como evidencia para obtener una orden judicial para requerir a una entidad los datos de identificación personal asociados a las direcciones involucradas y así

conocer quiénes son los destinatarios finales del dinero obtenido de manera fraudulenta.

Este pionero programa, realizado por los investigadores del IMDEA Software Gibran Gómez, Pedro Moreno-Sánchez y Juan Caballero, está basado en el estudio *Watch Your Back: Identifying Cybercrime Financial Relationships in Bitcoin through Back-and-Forth Exploration*.