Un actor de amenazas desconocido está utilizando paquetes npm maliciosos para atacar a desarrolladores con el objetivo de robar código fuente y archivos de configuración de las máquinas de las víctimas, lo que demuestra cómo las amenazas acechan constantemente en repositorios de código abierto.

> *«El responsable de esta campaña de amenazas ha sido vinculado a actividades maliciosas que datan desde el 2021. Desde entonces, han estado publicando de manera continua paquetes maliciosos»,* declaró la empresa especializada en seguridad de cadenas de suministro de software, Checkmarx

Este informe más reciente es una continuación de la misma campaña que Phylum expuso a principios de mes, en la cual se desarrollaron varios módulos npm con el fin de extraer información valiosa hacia un servidor remoto.

Estos paquetes, por diseño, están configurados para ejecutarse inmediatamente después de su instalación mediante un *«hook postinstall»* definido en el archivo package.json. Esto desencadena el inicio de preinstall.js, que inicia index.js para capturar los metadatos del sistema y recolectar código fuente y secretos de directorios específicos.

El ataque finaliza con el script creando un archivo ZIP con los datos y enviándolo a un servidor FTP previamente definido.

Una característica común que conecta todos los paquetes es el uso de *«lexi2»* como autor en el archivo package.json, lo que permite a Checkmarx rastrear los orígenes de esta actividad hasta el 2021.

Aunque no está claro cuáles son los objetivos exactos de la campaña, el uso de nombres de paquetes como binarium-client, binarium-crm y rocketrefer sugiere que el enfoque está dirigido al sector de las criptomonedas.

> *«El sector de las criptomonedas sigue siendo un objetivo candente, y es importante reconocer que no solo nos enfrentamos a paquetes maliciosos, sino también a adversarios persistentes cuyos ataques continuos y cuidadosamente planeados se remontan a meses o incluso años atrás»*, afirmó el investigador de seguridad Yehuda Gelb.