Detectan un malware para MacOS para el robo de criptomonedas

Un campaña maliciosa vinculada al grupo Lazarus utiliza el ‘malware’ denominado KandyKorn para infectar los ordenadores de Apple de ingenieros de ‘blockchain’ de una comunidad de criptomonedas y robarles sus divisas.

KandyKorn es un nuevo ‘malware’ para MacOS descubierto por Elastic Security Labs que se distribuye en una campaña dirigida contra ingenieros de ‘blockchain’, a quienes, mediante ingeniería social en un servidor público de Discord, se les engaña para que descarguen un supuesto ‘bot’ de arbitraje de criptomonedas, con la promesa de beneficios económicos.

En lugar de dicho ‘bot’, estos ingenieros lo que acaban descargando es una aplicación python que se distribuye como un archivo .zip, y que tras ejecutarse y conectarse a un servidor de comando y control, instala una carga útil y crea una aplicación que simular ser Discord.

Esta aplicación es obra de HLOADER, que ha podido ser identificado por una técnica de firma de código binario de macOS vista anteriormente en la actividad de Grupo Lazarus, como señalan desde la firma de ciberseguridad. En Elastic Security Labs destacan, sin embargo, el secuestro de flujo de ejecución, una novedad en este grupo para lograr persistencia en MacOS.

En lo que respecta a la carga útil, esta se refiere a KandyKorn y sucede en la última etapa de esta cadena de ejecución. Con este ‘malware’, Lazarus logra acceder y extraer datos del ordenador de sus víctimas con el objetivo de robar criptomonedas.

Con información de PortalTic.