Se ha detectado que un grupo de hackers está explotando las configuraciones incorrectas en los contratos inteligentes para crear tokens de criptomonedas maliciosos con el objetivo de robar fondos de usuarios.

Los casos de fraude de tokens en la naturaleza incluyen la ocultación de funciones de tarifa del 99% y ocultar rutinas de puerta trasera, según informes de Check Point.

Los contratos inteligentes son programas almacenados en la cadena de bloques que se ejecutan automáticamente cuando se cumplen condiciones predeterminadas según los términos de un contrato o acuerdo. Permiten realizar transacciones y acuerdos de confianza entre partes anónimas sin necesidad de una autoridad central.

Al examinar el código fuente de Solidity utilizado para implementar contratos inteligentes, la compañía de seguridad cibernética israelí encontró instancias de tarifas ocultas y codificadas que no se pueden cambiar, al mismo tiempo que permite que los actores malintencionados ejerzan control sobre *«quién puede vender».*

En otro caso, un contrato legítimo llamado Levyathan, fue hackeado después de que sus desarrolladores subieran inadvertidamente la clave privada de la billetera de su repositorio de GitHub, lo que permitió al hacker acuñar una cantidad infinita de tokens y robar fondos del contrato en julio de 2021.

Un rug pull es un tipo de estafa que sucede cuando los creadores retiran el dinero de los inversores y abandonan el proyecto luego de que se asigna una gran cantidad a lo que parece ser un proyecto criptográfico legítimo.

Finalmente, los controles de acceso deficientes implementados por los mantenedores de Zenon Network, permitieron que un hacker abusara de la función de grabación sin protección dentro del contrato inteligente para aumentar el precio de la moneda y drenar fondos por una suma de $814,570 dólares en noviembre de 2021.

Estos hallazgos se producen cuando se han observado campañas de ciberataques que

aprovechan esquemas de phishing basados en señuelos, que rodean tokens criptográficos que pronto se lanzarán, aunque sean falsos, para finalmente engañar a las víctimas para que paguen con su propia criptomoneda.

> *«Además de eso, para involucrar a otras víctimas y perpetuar la estafa, el sitio web ofreció un programa de referencial para amigos y familiares. Al hacer esto, los actores de amenazas crearon un nuevo canal confiable por medio del cual las víctimas actuales se referían a otros objetivos potenciales»,* dijo Or Katz, investigador de Akamai.

> *«La implicación es que los usuarios de criptomonedas seguirán cayendo en estas trampas y perderán su dinero. Para evitar las monedas fraudulentas, recomiendo a los usuarios de criptomonedas que diversifiquen sus billeteras, ignoren los anuncios y prueben sus transacciones»*, dijo Oded Vanunu.