Una campaña en curso está atacando a desarrolladores de npm mediante cientos de versiones *typosquatting* de paquetes legítimos, en un esfuerzo por engañarlos para que ejecuten malware multiplataforma.

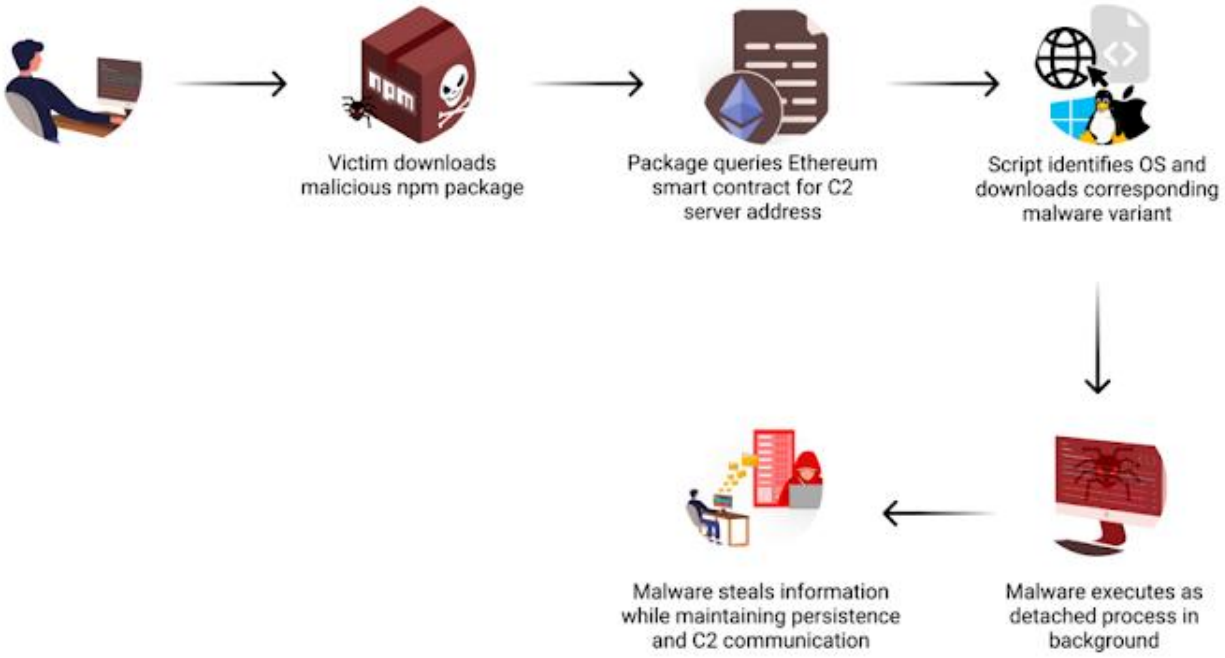
Este ataque es notable por emplear contratos inteligentes de Ethereum para distribuir las direcciones del servidor de comando y control (C2), según hallazgos recientes de Checkmarx, Phylum y Socket publicados en los últimos días.

La actividad fue detectada por primera vez el 31 de octubre de 2024, aunque se estima que comenzó al menos una semana antes. Hasta ahora, se han registrado no menos de 287 paquetes *typosquat* en el repositorio de npm.

> *«A medida que esta campaña comenzó a revelarse, quedó claro que el atacante estaba en las primeras etapas de una campaña de typosquatting dirigida a desarrolladores que intentaban usar las bibliotecas populares Puppeteer, Bignum.js y varias librerías de criptomonedas,»* dijo Phylum.

Estos paquetes incluyen JavaScript ofuscado que se ejecuta durante (o después) de la instalación, lo cual conduce a la descarga de un binario de segunda fase desde un servidor remoto, dependiendo del sistema operativo.

Dicho binario establece persistencia en el sistema y extrae información sensible de la máquina comprometida para enviarla de vuelta al mismo servidor.



En un giro particular, el código JavaScript se comunica con un contrato inteligente de Ethereum usando la biblioteca *ethers.js* para obtener la dirección IP. Es relevante señalar que una campaña conocida como *EtherHiding* usó una táctica similar empleando contratos en Binance Smart Chain (BSC) para avanzar en la cadena de ataque.

La naturaleza descentralizada del blockchain hace que esta campaña sea más difícil de bloquear, ya que el actor malicioso puede actualizar las direcciones IP asociadas al contrato con el tiempo, permitiendo que el malware se conecte fácilmente a nuevas direcciones a medida que las antiguas son bloqueadas o eliminadas.

> *«Al aprovechar la cadena de bloques de esta manera, los atacantes obtienen dos ventajas clave: su infraestructura se vuelve casi imposible de eliminar debido a la inmutabilidad de la blockchain, y la arquitectura descentralizada hace que sea extremadamente difícil bloquear estas comunicaciones,»* explicó el investigador de

> Checkmarx, Yehuda Gelb.

Todavía no está claro quién está detrás de la campaña, aunque el equipo de investigación de amenazas de Socket informó haber encontrado mensajes de error en ruso en el manejo de excepciones y los registros, lo cual sugiere que el autor de la amenaza podría hablar ruso.

Este evento destaca nuevamente las nuevas estrategias que los atacantes están utilizando para comprometer el ecosistema de código abierto, subrayando la necesidad de que los desarrolladores sean cautelosos al descargar paquetes de repositorios de software.

> *«El uso de la tecnología blockchain para la infraestructura C2 representa un enfoque diferente en los ataques a la cadena de suministro dentro del ecosistema npm, haciendo que la infraestructura de ataque sea más resistente a intentos de eliminación y complicando los esfuerzos de detección,»* concluyó Gelb.