El paquete de npm denominado «tensorlake«, un kit de desarrollo de software (SDK) basado en TypeScript para aplicaciones, entornos aislados y servicios en la nube de Tensorlake, fue comprometido como parte de un ataque a la cadena de suministro conocido como ChainDrop / Shai-Hulud.

La versión maliciosa 0.5.144 *«contiene malware ofuscado que recopila credenciales, extrae secretos, establece mecanismos de persistencia y ejecuta código proporcionado de forma remota»*, señaló Socket. La versión 0.5.144 ya no está disponible para su descarga desde el registro de paquetes de npm.

El análisis de la versión comprometida revela que incluye un enlace de preinstalación destinado a ejecutar un archivo JavaScript («package/lib/setup.mjs»). Este archivo funciona como un cargador ofuscado que inicia el componente principal encargado de robar credenciales y propagarse por sí mismo («package/lib/Math_Symbol.js») mediante el entorno de ejecución Bun.

El malware de extracción está diseñado para recopilar credenciales desde archivos locales, entornos de integración y entrega continuas (CI), Kubernetes y fuentes de Vault. Además, descarga el binario HackBrowserData, extrae la información recopilada, establece persistencia en el equipo afectado y permite ejecutar código enviado de manera remota.

«Esta combinación amplía el riesgo más allá del simple robo de una clave API», explicó Socket. *«Cualquier secreto al que tenga acceso el proceso que ejecuta el malware podría quedar expuesto, mientras que los mecanismos de persistencia pueden conservar el acceso del atacante incluso después de eliminar la dependencia comprometida.»*

Los tipos de información que puede sustraer el malware incluyen:

- Tokens de npm
- Tokens de GitHub
- Credenciales y secretos de Amazon Web Services (AWS)
- HashiCorp Vault

- Credenciales de Kubernetes
- Claves SSH
- Archivos .env
- Carteras de criptomonedas
- Datos de aplicaciones de mensajería
- Archivos de configuración y archivos MCP relacionados con Anthropic Claude, Cursor, Kiro, Windsurf y Zed

«Para propagarse, el gusano identifica los paquetes vinculados con la identidad de publicación de la víctima, genera información de procedencia mediante Sigstore y vuelve a publicar las versiones comprometidas», explicó Socket. *«Las cadenas de texto relacionadas con un flujo de trabajo falso de Copilot/Dependabot indican que también podría instalar flujos de trabajo de GitHub Actions.»*

El malware también emplea un contrato de Ethereum para determinar su punto de conexión de comando y control (C2) («iseekaigogo[.]com»). Como mecanismo alternativo, utiliza GitHub para almacenar los datos robados y cifrados en un repositorio público cuya descripción es «Shai-Hulud: Here We Go Again».

Asimismo, se identificó un componente denominado *«hostage token»*, que utiliza un monitor basado en PowerShell para consultar repetidamente «api.github.com/user» mediante el token de GitHub sustraído, con el objetivo de comprobar si este continúa siendo válido. Si la víctima intenta revocar el token, el monitor ejecuta un controlador proporcionado por el atacante mediante el cmdlet «Invoke-Expression», lo que permite ejecutar código PowerShell diseñado, aparentemente, para activar una rutina destructiva, una técnica que ya había sido observada en campañas anteriores de Shai-Hulud.

De acuerdo con StepSecurity, los archivos maliciosos fueron introducidos en la rama principal del repositorio tensorlakeai/tensorlake utilizando el nombre de uno de sus mantenedores. Posteriormente, el paquete fue publicado desde ese mismo repositorio. El primer commit malicioso se realizó el 7 de octubre de 2026 a la 01:20 a. m. UTC. Un día después, el flujo de publicación del repositorio lanzó la versión 0.5.144 en npm.

«El malware también crea los archivos .claude/settings.json y .vscode/tasks.json dentro de los repositorios a los que consigue acceder, de modo que vuelve a ejecutarse cuando alguien abre el proyecto en Claude Code o VS Code», afirmó Ashish Kurmi, de StepSecurity.

ChainDrop fue documentado por primera vez a comienzos de agosto de 2026, después de que cientos de paquetes de npm, entre ellos Keyv y Cacheable, fueran comprometidos. Estos paquetes contenían una variante de Mini Shai-Hulud que incorporaba un gusano capaz de propagarse y robar credenciales mediante una carga útil de JavaScript basada en Bun y fuertemente ofuscada.

Este nuevo incidente amplía el alcance del ataque a la cadena de suministro hacia la infraestructura de agentes de inteligencia artificial (IA), y vuelve a demostrar que los actores maliciosos están dirigiendo cada vez más sus ataques contra herramientas y servicios de IA con el propósito de obtener información de alto valor perteneciente a las empresas. Se recomienda a los usuarios que hayan instalado la versión maliciosa eliminarla de inmediato y renovar sus credenciales.