Se ha observado que actores maliciosos cargaron un conjunto de ocho paquetes en el registro npm que se hacían pasar por integraciones dirigidas a la plataforma de automatización de flujos de trabajo n8n, con el objetivo de robar credenciales OAuth de desarrolladores.

Uno de estos paquetes, denominado "n8n-nodes-hfgjf-irtuinvcm-lasdqewriit", simula ser una integración de Google Ads y solicita a los usuarios vincular su cuenta publicitaria mediante un formulario aparentemente legítimo, para luego transferir esas credenciales a servidores controlados por los atacantes.

"El ataque representa una nueva escalada en las amenazas a la cadena de suministro", señaló Endor Labs en un informe publicado la semana pasada. *"A diferencia del malware tradicional en npm, que suele centrarse en credenciales de desarrolladores, esta campaña abusó de plataformas de automatización de flujos de trabajo que funcionan como bóvedas centralizadas de credenciales, almacenando tokens OAuth, claves API y datos sensibles de decenas de servicios integrados como Google Ads, Stripe y Salesforce en un solo lugar."*

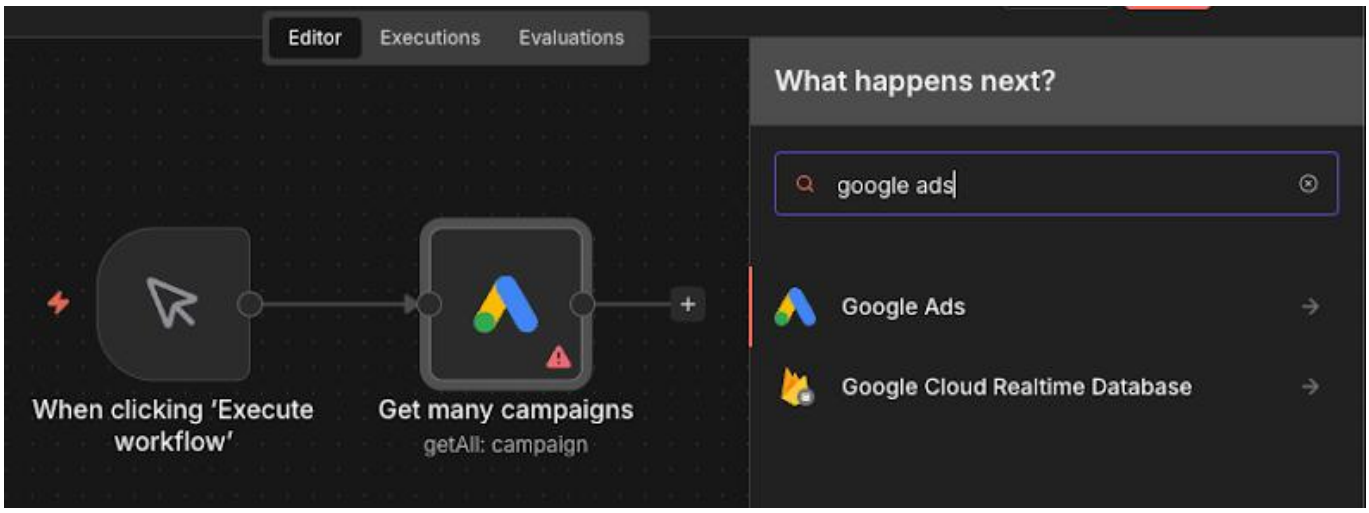
La lista completa de los paquetes identificados, que ya han sido eliminados, es la siguiente:

- n8n-nodes-hfgjf-irtuinvcm-lasdqewriit (4,241 descargas, autor: kakashi-hatake)
- n8n-nodes-ggdv-hdfvcnnje-uyrokvbkl (1,657 descargas, autor: kakashi-hatake)
- n8n-nodes-vbmkajdsa-uehfitvv-ueqjhhhksdlkkmz (1,493 descargas, autor: kakashi-hatake)
- n8n-nodes-performance-metrics (752 descargas, autor: hezi109)
- n8n-nodes-gasdhgfuy-rejerw-ytjsadx (8,385 descargas, autor: zabuza-momochi)
- n8n-nodes-danev (5,525 descargas, autor: dan_even_segler)
- n8n-nodes-rooyai-model (1,731 descargas, autor: haggags)
- n8n-nodes-zalo-vietts (4,241 descargas, autores: vietts_code y diendh)

Los usuarios "zabuza-momochi", "dan_even_segler" y "diendh" también han sido asociados con otras bibliotecas que, al momento de redactar este informe, aún permanecen disponibles para su descarga:

- n8n-nodes-gg-udhasudsh-hgjkhg-official (2,863 descargas)
- n8n-nodes-danev-test-project (1,259 descargas)
- @diendh/n8n-nodes-tiktok-v2 (218 descargas)
- n8n-nodes-zl-vietts (6,357 descargas)

No está claro si estos paquetes contienen funciones maliciosas similares. No obstante, un análisis de los tres primeros paquetes mediante ReversingLabs Spectra Assure no detectó problemas de seguridad. En el caso de "n8n-nodes-zl-vietts", la evaluación señaló que la biblioteca incluye un componente con historial de malware.



De forma llamativa, una versión actualizada del paquete "n8n-nodes-gg-udhasudsh-hgjkhg-official" fue publicada en npm hace apenas tres horas, lo que sugiere que la campaña podría seguir activa.

El paquete malicioso, una vez instalado como nodo comunitario, se comporta como cualquier otra integración de n8n, mostrando pantallas de configuración y almacenando los tokens OAuth de Google Ads en formato cifrado dentro del repositorio de credenciales de n8n. Cuando el flujo de trabajo se ejecuta, el código descifra los tokens usando la clave maestra de n8n y los exfiltra hacia un servidor remoto.

Este desarrollo marca la primera ocasión en la que una amenaza a la cadena de suministro apunta de manera explícita al ecosistema n8n, aprovechando la confianza en integraciones comunitarias para cumplir sus objetivos.

Los hallazgos subrayan los riesgos de seguridad asociados a la integración de flujos de trabajo no confiables, los cuales amplían la superficie de ataque. Se recomienda a los desarrolladores auditar los paquetes antes de instalarlos, revisar cuidadosamente los metadatos en busca de anomalías y utilizar integraciones oficiales de n8n.

N8n también ha advertido sobre los riesgos de seguridad derivados del uso de nodos comunitarios obtenidos desde npm, ya que estos pueden ejecutar acciones maliciosas en el sistema donde se ejecuta el servicio. En instancias de n8n autoalojadas, se aconseja deshabilitar los nodos comunitarios configurando N8N_COMMUNITY_PACKAGES_ENABLED en false.

"Los nodos comunitarios se ejecutan con el mismo nivel de acceso que n8n. Pueden leer variables de entorno, acceder al sistema de archivos, realizar solicitudes de red salientes y, lo más crítico, recibir claves API y tokens OAuth descifrados durante la ejecución de los flujos de trabajo", explicaron los investigadores Kiran Raj y Henrik Plate. *"No existe ningún mecanismo de aislamiento o sandbox entre el código de los nodos y el entorno de ejecución de n8n."*

"Debido a esto, un solo paquete npm malicioso es suficiente para obtener una visibilidad profunda de los flujos de trabajo, robar credenciales y comunicarse externamente sin levantar sospechas inmediatas. Para los atacantes, la cadena de suministro de npm ofrece un punto de entrada silencioso y altamente efectivo en los entornos n8n."