En las últimas semanas, se han descubierto múltiples paquetes maliciosos en los repositorios de npm, PyPI y RubyGems que afectan gravemente la seguridad de los entornos de desarrollo. Estas amenazas incluyen robo de fondos en billeteras de criptomonedas, exfiltración de datos sensibles como tokens de la API de Telegram, eliminación de bases de código completas, y uso de modelos de aprendizaje automático para ocultar cargas maliciosas. Todo esto pone de relieve la diversidad de ataques a la cadena de suministro en los ecosistemas de código abierto.

Informes de firmas como Checkmarx, ReversingLabs, Safety y Socket detallan cómo estos paquetes maliciosos fueron diseñados para infiltrarse en sistemas de desarrollo CI/CD y explotar herramientas ampliamente utilizadas por los desarrolladores.

Socket, por ejemplo, identificó *gems* maliciosas que se hacían pasar por el plugin legítimo de Fastlane *fastlane-plugin-telegram*. Estas bibliotecas fueron publicadas por un actor malicioso bajo los alias Bùi nam, buidanhnam y si_mobile, justo después de que Vietnam prohibiera el uso de Telegram a nivel nacional.

> *"Estas gems exfiltran silenciosamente todos los datos enviados a la API de Telegram redirigiendo el tráfico a un servidor de comando y control (C2) controlado por el atacante. Esto incluye tokens de bots, IDs de chats, contenido de mensajes y archivos adjuntos",* explicó Kirill Boychenko, investigador de Socket.

La modificación introducida por los atacantes cambiaba el punto de conexión de red por uno codificado (*rough-breeze-0c37.buidanhnam95.workers[.]dev*), que actuaba como intermediario entre la víctima y Telegram, capturando datos sensibles sin levantar sospechas.

> *"Esta campaña ilustra cuán rápido pueden los actores de amenazas aprovechar eventos geopolíticos para lanzar ataques dirigidos a la cadena de suministro"*, añadió Boychenko. *"Al disfrazar funcionalidades de robo de credenciales como una 'función proxy', el atacante explotó la confianza en los ecosistemas de paquetes para infiltrarse en entornos CI/CD".*

En npm también se descubrió un paquete llamado *xlsx-to-json-lh* que imitaba al legítimo *xlsx-to-json-lc*. Este paquete contenía una carga que, una vez activada, podía borrar directorios completos del proyecto sin advertencia ni posibilidad de recuperación.

> *"Este paquete contiene una carga oculta que establece una conexión persistente con un servidor C2",* explicó el investigador Kush Pandya. *"Cuando se activa, puede eliminar directorios completos de proyectos sin aviso ni opciones de recuperación".*

La acción destructiva se desencadenaba cuando el servidor enviaba la orden en francés *«remise à zéro»* (reinicio), eliminando archivos fuente, configuraciones, datos de control de versiones y todos los activos del proyecto.

Asimismo, se identificaron otros paquetes npm como *pancake_uniswap_validators_utils_snipe*, *pancakeswap-oracle-prediction*, *ethereum-smart-contract* y *env-process*, que usaban JavaScript ofuscado para sustraer entre el 80 % y el 85 % de los fondos en billeteras Ethereum o BSC y redirigirlos a direcciones controladas por los atacantes.

En el ecosistema Python, se detectó un segundo lote de 11 paquetes maliciosos enfocados en el ecosistema Solana, subidos a PyPI entre el 4 y el 24 de mayo de 2025, según la empresa Safety. Estos paquetes robaban archivos de scripts Python desde los sistemas de los desarrolladores y los enviaban a servidores externos. Uno de ellos, *solana-live*, incluso tenía como objetivo específico los Jupyter Notebooks, aunque se presentaba como una biblioteca para obtener precios.

También se documentó una campaña basada en *typosquatting*, donde se subieron paquetes que imitaban a *colorama* (biblioteca Python) y *colorizr* (biblioteca JavaScript en npm), combinando nombres de distintos ecosistemas para atacar a usuarios de PyPI.

> "*La táctica de usar el nombre de un ecosistema (npm) para atacar a usuarios de otro (PyPI) es inusual"*, indicó Checkmarx. *"Las cargas útiles permiten acceso remoto persistente, control total de escritorios y servidores, así como la recolección y exfiltración de datos sensibles".*

Esta campaña tenía variantes tanto para sistemas Windows como Linux, lo que le permitía conectarse a un servidor C2, exfiltrar variables de entorno e información de configuración, y evadir soluciones de seguridad. Aún no se sabe si ambas variantes provienen del mismo autor o si se trata de campañas separadas con tácticas similares.

El auge de la inteligencia artificial también está siendo aprovechado como nuevo vector de ataque. En mayo de 2024 se detectaron paquetes como *aliyun-ai-labs-snippets-sdk*, *ai-labs-snippets-sdk* y *aliyun-ai-labs-sdk*, que fingían ser SDKs de Python para interactuar con servicios de Aliyun AI Labs.

Aunque estuvieron disponibles en PyPI por menos de 24 horas, se descargaron más de 1.700 veces antes de ser eliminados.

> *"Una vez instalado, el paquete malicioso entrega una carga tipo infostealer oculta*

> *dentro de un modelo PyTorch cargado desde el script de inicialización”,* explicó Karlo Zanki, investigador de ReversingLabs. *“La carga maliciosa exfiltra información básica sobre la máquina infectada y el contenido del archivo .gitconfig”.*

Este modelo recolectaba datos como el usuario conectado, la dirección de red, el nombre de la organización (obtenido desde la configuración de la app china AliMeeting) y otros archivos de configuración.

Además, esta técnica revela los riesgos de los formatos de modelos de aprendizaje automático como *Pickle*, que permiten la ejecución de código arbitrario durante la deserialización.

> *“Los atacantes siempre buscan nuevas formas de ocultar sus cargas maliciosas ante las herramientas de seguridad — y los analistas”,* advirtió Zanki. *“Esta vez usaron modelos de aprendizaje automático, un enfoque novedoso para distribuir malware a través de la plataforma PyPI. Es una estrategia inteligente, ya que las herramientas de seguridad apenas están comenzando a detectar funcionalidades maliciosas dentro de modelos de ML”.*