Investigadores de ciberseguridad han identificado una biblioteca de Python maliciosa en el repositorio Python Package Index (PyPI), la cual permite la descarga no autorizada de música desde la plataforma de streaming Deezer.

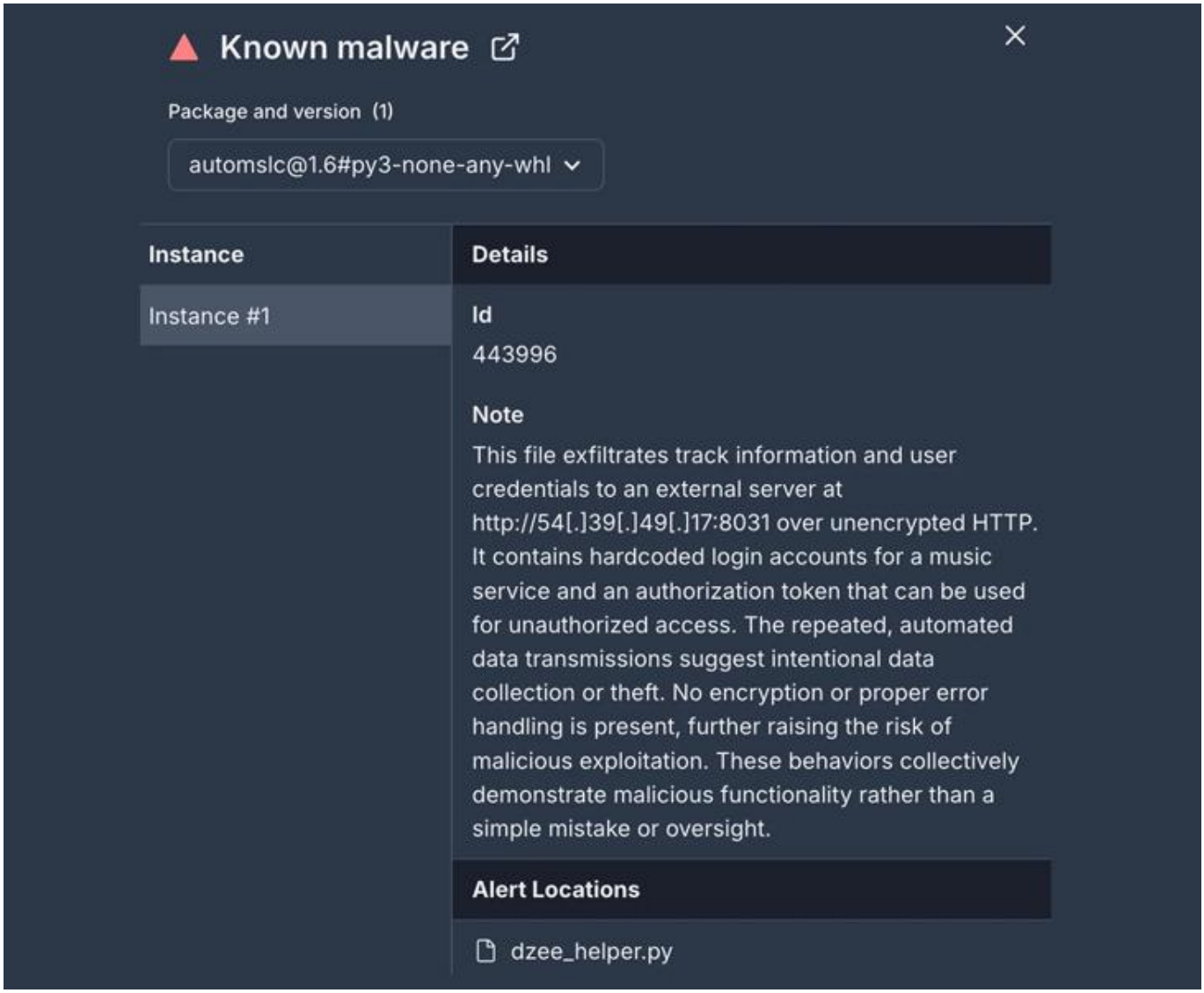
El paquete en cuestión, llamado automslc, ha sido descargado más de 104,000 veces hasta el momento. Lanzado originalmente en mayo de 2019, aún sigue disponible en PyPI.

> *«A pesar de que automslc, con más de 100,000 descargas, se promociona como una herramienta para la automatización musical y la recuperación de metadatos, en realidad evade las restricciones de acceso de Deezer al incluir credenciales incrustadas y conectarse a un servidor remoto de comando y control (C2)»,* explicó Kirill Boychenko, investigador de seguridad en Socket, en un informe publicado hoy.

Este paquete ha sido diseñado para acceder a la plataforma francesa de streaming utilizando tanto credenciales ingresadas por el usuario como credenciales preconfiguradas, recopilar información sobre las pistas y descargar archivos de audio completos, infringiendo así las políticas de uso de la API de Deezer.

Además, automslc se comunica regularmente con un servidor remoto en la dirección «54.39.49[.]17:8031», proporcionando actualizaciones sobre el estado de las descargas y permitiendo al atacante mantener un control centralizado sobre la operación de piratería musical.

Dicho de otra manera, este paquete convierte los dispositivos de sus usuarios en una red clandestina que facilita la descarga masiva de música de manera ilegal. La dirección IP mencionada está vinculada a un dominio llamado «automusic[.]win», el cual es utilizado por el atacante para gestionar la distribución de las descargas.



> *«Las normas de la API de Deezer prohíben el almacenamiento local o sin conexión de archivos de audio completos. Sin embargo, automslc descarga y desencripta canciones enteras, evitando esta restricción y exponiendo a los usuarios a posibles consecuencias legales»,* advirtió Boychenko.

Este hallazgo coincide con la identificación de un paquete malicioso en npm, denominado

@ton-wallet/create, el cual se ha descubierto sustrayendo frases mnemotécnicas de desarrolladores y usuarios del ecosistema TON, haciéndose pasar por el paquete legítimo @ton/ton.

Dicho paquete fue subido al registro de npm en agosto de 2024 y ha sido descargado 584 veces hasta la fecha, permaneciendo aún disponible para su descarga.

La biblioteca contiene una función maliciosa capaz de extraer la variable de entorno process.env.MNEMONIC, permitiendo a los atacantes obtener acceso total a las billeteras de criptomonedas de las víctimas y potencialmente vaciar sus fondos digitales. La información obtenida es enviada a un bot de Telegram bajo el control del atacante.

> *«Este tipo de ataque representa una amenaza significativa para la seguridad de la cadena de suministro de software, afectando a desarrolladores y usuarios que integran billeteras TON en sus aplicaciones. Es fundamental llevar a cabo auditorías regulares de dependencias y utilizar herramientas automatizadas para detectar posibles comportamientos maliciosos en paquetes de terceros antes de implementarlos en entornos de producción»*, advirtió Socket.