Los investigadores descubrieron una serie de paquetes de Python maliciosos en el repositorio oficial de software de terceros que están diseñados para filtrar las credenciales de AWS y las variables de entorno a un punto final expuesto públicamente.

La lista de paquetes incluye módulos loglib, módulos pyg, pygrata, pygrata-utils y hkg-sol-utils, según el investigador de seguridad de Sonatype, Ax Sharma. Los paquetes y el punto final ahora se eliminaron.

> *«Algunos de estos paquetes contienen código que lee y extrae sus secretos o utilizan una de las dependencias que harán el trabajo»,* dijo Sharma.

El código malicioso inyectado en *«loglib-modules» y «pygrata-utils»* permite recopilar credenciales de AWS, información de interfaz de red y variables de entorno y exportarlas a un punto final remoto: *«hxxp://graph.pygrata[.]com:8000/upload».*

De forma preocupante, los puntos finales que alojan esta información en forma de cientos de archivos .txt no estaban protegidos por ninguna barrera de autenticación, lo que permitía efectivamente que cualquier parte en la web accediera a las credenciales.

Cabe mencionar que paquetes como «pygrata» utilizan uno de los dos paquetes mencionados antes como dependencia y no albergan el código en sí mismos. La identidad del actor de la amenaza y sus motivos siguen sin estar claros.

> *«¿Las credenciales robadas se expusieron intencionalmente en la web o fueron una consecuencia de las malas prácticas de OPSEC?. Si se trata de algún tipo de prueba de seguridad legítima, seguramente no existe mucha información en este momento para descartar la naturaleza sospechosa de la actividad»,* dijo Sharma.

Esta no es la primera vez que se descubren paquetes maliciosos de este tipo en repositorios

de código abierto. Exactamente hace un mes, se descubrieron dos paquetes troyanizados de Python y PHP, llamados ctx y phpass, en otro caso de un ataque a la cadena de suministro de software.

Posteriormente, un investigador de seguridad con sede en Estambul, Yunus Aydin, se atribuyó la responsabilidad de las modificaciones no autorizadas y afirmó que simplemente *«quería mostrar cómo este simple ataque afecta a más de 10 millones de usuarios y empresas».*

En una línea similar, una compañía alemana de pruebas de penetración llamada Code White admitió el mes pasado cargar paquetes maliciosos en el registro de NPM en un intento por imitar de forma realista los ataques de confusión de dependencia dirigidos a sus clientes en el país, la mayoría de los cuales son destacados medios de comunicación, logística y firmas industriales.