El equipo de seguridad de npm (Node Package Manager), el administrador de paquetes de facto para el ecosistema JavaScript, eliminó hoy un paquete malicioso que fue detectado robando información confidencial de sistemas UNIX.

El paquete malicioso se llama 1337qq-js y se cargó en el repositorio npm el 30 de diciembre de 2019. El paquete fue descargado al menos 32 veces, y hoy fue descubierto por el equipo de investigación de vulnerabilidades de Microsoft.

Según un análisis realizado por el equipo de seguridad de npm, el paquete extrae información confidencial por medio de scripts de instalación y solo se dirige a sistemas UNIX.

Entre los datos que recopila se encuentran:

- Variables de entorno
- Procesos en ejecución
- /etc/hosts
- uname -a
- archivo npmrc

El hecho de robar variables de entorno se considera como una violación de seguridad importante debido a que cierta información, como contraseñas codificadas o tokens de acceso a la API, por lo general se almacena como variables de entorno en algunas aplicaciones web o móviles de JavaScript.

El equipo de npm recomienda que todos los desarrolladores que descargaron o utilizaron este paquete de JavaScript en sus proyectos eliminen el paquete de sus sistemas y roten las credenciales comprometidas.

Este sería el sexto incidente de un paquete malicioso que aparece en el índice del repositorio npm, aunque este es el menos grave, principalmente porque los analistas de seguridad de Microsoft capturaron la biblioteca dos semanas después de su publicación y antes de que obtuviera un seguimiento serio.