Un actor de amenazas denominado RED-LILI, se vinculó a una campaña de ataques a la cadena de suministro a gran escala, ahora en curso, al repositorio de paquetes NPM mediante la publicación de casi 800 módulos maliciosos.

> *«Habitualmente, los atacantes usan una cuenta NPM desechable anónima desde la cual lanzan sus ataques. Como parece esta vez, el atacante ha automatizado completamente el proceso de creación de cuentas NPM y ha abierto cuentas dedicadas, una por paquete, lo que hace que su nuevo lote de paquetes maliciosos sea más difícil de detectar»,* dijo la compañía de seguridad israelí Checkmarx.

Estos hallazgos se basan en informes recientes de JFrog y Sonatype, que detallaron cientos de paquetes de NPM que aprovechan técnicas como la confusión de dependencias y los errores tipográficos para apuntar a los desarrolladores de Azure, Uber y Airbnb.

Según un análisis detallado del modus operandi de RED-LILI, se cree que la evidencia más temprana de actividad anómala ocurrió el 23 de febrero de 2022, con el grupo de paquetes maliciosos publicados en *«ráfagas»* en el lapso de una semana.

Específicamente, el proceso de automatización para cargar las bibliotecas no autorizadas en NPM, que Checkmarx describió como una *«fábrica»,* implica el uso de una combinación de código Python personalizado y herramientas de prueba web como Selenium para simular las acciones del usuario necesarias para replicar el proceso de creación de usuarios en el registro.

Para superar la barrera de verificación de la contraseña de un solo uso (OTP) establecida por NPM, el atacante aprovecha una herramienta de código abierto llamada Interactsh para extraer la OTP enviada por los servidores NPM a la dirección de correo electrónico proporcionada durante el registro, lo que permite efectivamente la solicitud de creación de cuenta para tener éxito.

Armado con esta nueva cuenta de usuario de NPM, el actor de amenazas crea y publica un

paquete malicioso, solo uno por cuenta, de forma automática, pero no antes de generar un token de acceso para publicar el paquete sin requerir el desafío de un correo electrónico OTP.

> *«A medida que los atacantes de la cadena de suministro mejoran sus habilidades y dificultan la vida de sus defensores, este ataque marca otro hito en su progreso. Al distribuir los paquetes a través de múltiples nombres de usuario, el atacante hace que sea más difícil para los defensores correlacionarlos y derribarlos a todos con un 'golpe'. Por eso, por supuesto, aumentan las posibilidades de infección»,* dijeron los investigadores.