En lo que se considera un asalto continuo al ecosistema de código abierto, más de 15,000 paquetes de spam inundaron el repositorio de npm en un intento de distribuir enlaces de phishing.

> *«Los paquetes se crearon utilizando procesos automatizados, con descripciones de proyectos y nombres generados automáticamente que se parecían mucho entre sí»,* dijo el investigador de Checkmarx, Yehuda Gelb.

> *«Los atacantes se refirieron a sitios web minoristas utilizando ID de referencia, y así se beneficiaron de las recompensas de referencia que obtuvieron».*

La forma en que operan los ciberdelincuentes consiste en envenenar el registro con paquetes maliciosos que incluyen enlaces a campañas de phishing en sus archivos *README.md,* que evocan una campaña similar que la empresa de seguridad de la cadena de suministro de software expuso en diciembre de 2022.

Los módulos falsos se hicieron pasar por trucos y recursos gratuitos, con algunos paquetes llamados *«free-tiktok-followers», «free-xbox-codes» y «instagram-followers-free».*

El objetivo final de la operación es atraer a los usuarios para que descarguen los paquetes y hagan clic en los enlaces a los sitios de phishing con falsas promesas de más seguidores en las plataformas de redes sociales.

> *«Las páginas web engañosas están bien diseñadas y, en algunos casos, incluyen chats interactivos falsos que parecen mostrar a los usuarios que reciben los trucos del juego o los seguidores que les prometieron»,* explicó Gelb.

Los sitios web instan a las víctimas a completar las encuestas, que después allanan el camino

para encuestas adicionales o, de forma alternativa, las redirigen a portapapeles de comercio electrónico legítimos como AliExpress.

Al parecer, los paquetes se cargaron en npm desde varias cuentas de usuario en cuestión de horas entre el 20 y el 21 de febrero de 2023, usando un script de Python que automatiza todo el proceso.

Además, el script Python también está diseñado para agregar enlaces a los paquetes npm publicados en los sitios web de WordPress operados por los hackers que aseguran ofrecer trucos de Family Island.

Esto se logra mediante el uso del paquete Python de Selenium, para interactuar con los sitios web y realizar las modificaciones necesarias.

En total, el uso de la automatización permitió al adversario publicar una gran cantidad de paquetes en un corto período de tiempo, sin mencionar la creación de varias cuentas de usuario para ocultar la escala del ataque.

> *«Esto demuestra la sofisticación y determinación de estos atacantes, que estaban dispuestos a invertir importantes recursos para llevar a cabo esta campaña»*, dijo Gelb.

Los hallazgos demuestran una vez más los desafíos para asegurar la cadena de suministro de software, ya que los hackers siguen adaptándose con *«técnicas nuevas e inesperadas».*