Una entidad de habla turca llamada Nitrokod fue atribuida a una campaña activa de minería de criptomonedas que implica hacerse pasar por una aplicación de escritorio para Google Translate para infectar a más de 111 mil víctimas en 11 países desde 2019.

> *«Cualquiera puede usar las herramientas maliciosas. Se pueden encontrar mediante una simple búsqueda en la web, se pueden descargar desde un enlace y la instalación es un simple doble clic»,* dijo Maya Horowitz, vicepresidenta de investigación de Check Point.

La lista de países con víctimas incluye Reino Unido, Estados Unidos, Sri Lanka, Grecia, Israel, Alemania, Turquía, Chipre, Australia, Mongolia y Polonia.

La campaña implica servir malware por medio de software gratuito alojado en sitios populares como Softpedia y Uptodown. Pero en una táctica interesante, el malware pospone su ejecución durante semanas y separa su actividad maliciosa del software falso descargado para evitar la detección.

A la instalación del programa infectado le sigue la implementación de un ejecutable de actualización en el disco que, a su vez, inicia una secuencia de ataque de cuatro etapas, con cada cuentagotas pavimentado para la siguiente, hasta que el malware real se elimina en la séptima etapa.

Después de la ejecución del malware, se establece una conexión a un servidor remoto de comando y control (C2) para recuperar un archivo de configuración para iniciar la actividad de extracción de monedas.

Un aspecto notable de la campaña de Nitrokod es que el software falso que se ofrece de forma gratuita es para servicios que no tienen una versión de escritorio oficial, como Yandex Translate, Microsoft Translate, YouTube Music, MP3 Download Manager y Pc Auto Shutdown.

Además, el malware se elimina casi un mes después de la infección inicial, cuando se elimina

el rastro forense, lo que dificulta descifrar el ataque y rastrearlo hasta el instalador.

> *«Lo más interesante para mí es el hecho de que el software malicioso es tan popular, pero pasó desapercibido durante tanto tiempo. El atacante puede elegir fácilmente alterar la carga útil final del ataque, cambiándolo de un criptominero a, por ejemplo, ransomware o troyano bancario»,* dijo Horowitz.