Los investigadores en ciberseguridad han desarrollado lo que es el primer minero de criptomonedas basado en la nube que resulta completamente indetectable, aprovechando los servicios de Automatización de Microsoft Azure sin generar ningún gasto.

La empresa de ciberseguridad SafeBreach informó que descubrió tres métodos distintos para llevar a cabo esta operación minera, incluyendo uno que puede ejecutarse sigilosamente dentro del entorno informático de un objetivo, evitando cualquier forma de detección.

> El investigador de seguridad Ariel Gamrian, quien realizó el estudio, afirmó: *«Si bien esta investigación tiene profundas implicaciones para la minería de criptomonedas, también conlleva consecuencias significativas para diversos otros ámbitos, ya que estos métodos podrían emplearse para realizar tareas que requieran la ejecución de código en la plataforma Azure».*

El objetivo principal de la investigación era identificar la solución definitiva de cripto-minería que ofreciera acceso ilimitado a recursos informáticos, requiriera un mantenimiento mínimo, fuera rentable y permaneciera completamente indetectable.

Es aquí donde entra en juego la Automatización de Azure. Desarrollada por Microsoft, representa un servicio de automatización basado en la nube que permite a los usuarios automatizar la creación, implementación, monitoreo y mantenimiento de recursos dentro del marco de Azure.

SafeBreach descubrió una vulnerabilidad en la calculadora de precios de Azure, lo que permitía la ejecución ilimitada de tareas sin generar costos, aunque esto ocurría dentro del entorno del atacante. Microsoft lanzó posteriormente un parche para corregir este problema.

Otro enfoque implica la iniciación de un trabajo de prueba para la minería, marcándolo como «Fallido» y luego creando un trabajo de prueba ficticio adicional, aprovechando la limitación de que solo un trabajo de prueba puede ejecutarse simultáneamente. El resultado final oculta completamente la ejecución de código dentro del entorno de Azure.

Un actor de amenazas podría aprovechar estos métodos al establecer una shell inversa hacia un servidor externo y luego autenticarse en el punto final de Automatización para lograr sus objetivos.

Además, se descubrió que la ejecución de código se podía llevar a cabo aprovechando la capacidad de Automatización de Azure de cargar paquetes personalizados de Python.

> *«Podríamos generar un paquete malicioso con el nombre 'pip' y cargarlo en la Cuenta de Automatización. El proceso de carga reemplazaría el 'pip' existente en la cuenta de Automatización. Una vez que nuestro 'pip' personalizado estuviera guardado en la cuenta de Automatización, el servicio lo utilizaría cada vez que se cargara un paquete»*, explicó Gamrian.

SafeBreach también proporcionó un concepto de prueba llamado CoinMiner, diseñado para adquirir poder informático gratuito a través de los servicios de Automatización de Azure mediante la explotación del mecanismo de carga de paquetes de Python.

Ante las divulgaciones, Microsoft ha considerado este comportamiento como *«por diseño»*, lo que indica que el método aún puede aprovecharse sin generar cargos.

Si bien el alcance de la investigación se refiere al uso indebido de la Automatización de Azure para la minería de criptomonedas, la empresa de ciberseguridad advirtió que los mismos métodos podrían ser adaptados por actores de amenazas para llevar a cabo cualquier tarea que requiera la ejecución de código dentro de la plataforma Azure.

> *«Como clientes de servicios en la nube, las organizaciones individuales deben supervisar de manera proactiva cada recurso y cada acción que ocurra dentro de su entorno. Recomendamos encarecidamente que las organizaciones se informen sobre los métodos y flujos que los actores maliciosos pueden emplear para crear recursos indetectables y supervisar de manera proactiva la ejecución de código que*

> *sea indicativa de tal comportamiento»,* enfatizó Gamrian.