Se ha detectado una nueva botnet peer-to-peer (P2P) basada en Golang que apunta activamente a servidores Linux en el sector educativo desde su aparición en marzo de 2022.

Nombrado Panchan por Akamai Security Research, el malware *«utiliza sus funciones de concurrencia integradas para maximizar la capacidad de propagación y ejecutar módulos de malware y recopila claves SSH para realizar movimientos laterales».*

El botnet, que se encuentra lleno de funciones, se basa en una lista básica de contraseñas SSH predeterminadas para llevar a cabo un ataque de diccionario y expandir su alcance, funciona principalmente como un cryptojacker diseñado para secuestrar los recursos de una computadora para extraer criptomonedas.

La compañía de seguridad cibernética y servicios en la nube dijo que detectó por primera vez la actividad de Panchan el 19 de marzo de 2022, y atribuyó el malware a un probable actor de amenazas japonés en función del idioma utilizado en el panel administrativo integrado en el binario para editar la configuración de minería.

Se sabe que Panchan implementa y ejecuta dos mineros, XMRig y nbhash, en el host durante el tiempo de ejecución, la novedad es que los mineros no se extraen al disco para evitar dejar un rastro forense.

> *«Para evitar la detección y reducir la trazabilidad, el malware elimina sus criptomineros como archivos mapeados en memoria, sin presencia de disco. También elimina los procesos del criptominero si detecta algún proceso de monitoreo»,* dijeron los investigadores.

De los 209 pares infectados detectados hasta ahora, se cree que 40 están actualmente activos. La mayoría de las máquinas comprometidas se encuentran en Asia (64), seguidas de Europa (52), América del Norte (45), América del Sur (11), África (1) y Oceanía (1).

Una pista interesante sobre los orígenes del malware es el resultado de una vulnerabilidad de

OPSEC por parte del atacante, que revela el enlace a un servidor Discord que se muestra en el panel de administración «*godmode*».

> *«El chat principal estaba vacío excepto por un saludo de otro miembro que ocurrió en marzo. Podría ser que otros chats solo estén disponibles para miembros con mayores privilegios del servidor»,* dijeron los investigadores.