Los hackers detrás de la operación de cryptojacking de Kinsing fueron detectados explotando servidores PostgreSQL mal configurados y expuestos para obtener acceso inicial a los entornos de Kubernetes.

Una segunda técnica de vector de acceso inicial implica el uso de imágenes vulnerables, dijo Sunders Bruskin, investigador de seguridad de Microsoft Defender for Cloud, en un informe de la semana pasada.

Kinsing tiene un historial amplio de apuntar a entornos de contenedores, por lo general aprovechando puertos API abiertos de Daemon Docker mal configurados, así como abusando de exploits recientemente revelados para eliminar software de minería de criptomonedas.

Anteriormente, también se descubrió que el actor de amenazas empleaba un rootkit para ocultar su presencia, además de terminar y desinstalar servicios y procesos de uso intensivo de recursos de la competencia.

Ahora, según Microsoft, las configuraciones erróneas en los servidores PostgreSQL fueron cooptadas por el actor de Kinsing para ganar un punto de apoyo inicial, y la compañía observa una *«gran cantidad de clústeres»* infectados de esta forma.

La configuración incorrecta se relaciona con una configuración de autenticación de confianza, que podría abusare para conectarse a los servidores sin ninguna autenticación y lograr la ejecución del código si la opción se configura para aceptar conexiones desde cualquier dirección IP.

> *«En general, permitir el acceso a una amplia gama de direcciones IP expone el contenedor de PostgreSQL a una amenaza potencial»,* dijo Bruskin.

El vector de ataque alternativo se dirige a servidores con versiones vulnerables de PHPUnit,

Liferay, WebLogic y WordPress, que son susceptibles a la ejecución remota de código para ejecutar cargas maliciosas.

Además, una *«campaña generalizada»* reciente involucró a los atacantes que buscaban el puerto 7001 de WebLogic predeterminado abierto y, de encontrarlo, ejecutaban un comando de shell para iniciar el malware.

> *«Exponer el clúster a Internet sin las medidas de seguridad adecuadas puede dejarlo abierto a ataques de fuentes externas. Además, los atacantes pueden obtener acceso al clúster aprovechando las vulnerabilidades conocidas en las imágenes»,* dijo Bruskin.