Investigadores de seguridad cibernética descubrieron un malware para Linux completamente indetectable, que explota técnicas indocumentadas para permanecer bajo el radar y apuntar a servidores Docker de acceso público alojados en plataformas de nube populares, incluidas AWS, Azure y Alibaba Cloud.

Docker es una solución popular de plataforma como servicio (PaaS), para Linux y Windows, diseñada para facilitar a los desarrolladores la creación, prueba y ejecución de sus aplicaciones en un entorno aislado llamado contenedor.

Según la última investigación de Intezer, una campaña de bots de minería de Ngrok que escanea Internet en busca de puntos finales de API Docker mal configuradas, ya ha infectado muchos servidores vulnerables con el nuevo malware.

Aunque la botnet de minería Ngrok ha estado activa por los últimos dos años, la nueva campaña se centra principalmente en tomar el control de los servidores Docker mal configurados y explotarlos para configurar contenedores maliciosos con criptomineros que se ejecutan en la infraestructura de las víctimas.

Nombrado Doki, el nuevo malware multiproceso aprovecha un *«método no documentado para contactar a su operador al abusar de la cadena de criptomonedas Dogecoin de una forma única para generar dinámicamente su dirección de dominio C2 a pesar de que las muestras estén disponibles de forma pública en VirusTotal».*

Según los investigadores, el malware:

- Fue diseñado para ejecutar comandos recibidos de sus operadores
- Utiliza un explorador de bloques de criptomonedas Dogecoin para generar su dominio C2 en tiempo real de forma dinámica
- Utiliza la biblioteca embedTLS para funciones criptográficas y comunicación de red
- Crea URL únicas con una vida útil corta y las usa para descargar cargas útiles durante el ataque

> *«El malware utiliza el servicio DynDNS y un Algoritmo de Generación de Dominio (DGA) único basado en la cadena de bloques de criptomonedas Dogecoin para encontrar el dominio de su C2 en tiempo real».*

Además, los atacantes detrás de la nueva campaña, también lograron comprometer las máquinas host al vincular los contenedores recién creados con el directorio raíz del servidor, lo que les permite acceder o modificar cualquier archivo en el sistema.

> *«Al usar la configuración de enlace, el atacante puede controlar la utilidad cron del host. El atacante modifica el cron del host para ejecutar la carga útil descargada cada minuto. Este ataque es muy peligroso debido al hecho de que el atacante usa técnicas de escape de contenedores para obtener el control total de la infraestructura de la víctima».*

Una vez hecho, el malware también aprovecha los sistemas comprometidos para escanear aún más la red en busca de puertos asociados con Redis, Docker, SSH y HTTP, utilizando una herramienta de escaneo como zmap, zgrap y jq.

Doki logró permanecer bajo el radar durante más de seis meses a pesar de haber sido cargado en VirusTotal el 14 de enero de 2020, y escaneado varias veces desde entonces. Sorprendentemente, hasta ahora no es detectable por 60 principales motores de detección de malware.

A fines del mes pasado, se encontraron actores maliciosos apuntando a puntos finales expuestos de la API de Docker e imágenes infestadas de malware para facilitar ataques DDoS y minar criptomonedas.