Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

ATAQUE DE CRIPTOJACKING USA LA RED TOR Y LAS API DE DOCKER PARA INFECTAR SERVIDORES

10/ 09/2025

CONTENIDO

INTRODUCCIÓN

Una nueva y compleja campaña de cryptojacking, que utiliza la red anónima de Tor, ha sido descubierta. El ataque se dirige a APIs de Docker mal configuradas y, según investigadores, tiene un potencial preocupante para la creación de una red de bots masiva.

ATAQUE DE CRIPTOJACKING USA LA RED TOR Y LAS API DE DOCKER PARA INFECTAR SERVIDORES

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_09_10_2
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	10/09/2025
Es día cero (0 day):	No

RESUMEN

Una nueva y compleja campaña de cryptojacking, que utiliza la red anónima de Tor, ha sido descubierta. El ataque se dirige a APIs de Docker mal configuradas y, según investigadores, tiene un potencial preocupante para la creación de una red de bots masiva.

¿Cómo funciona la cadena de ataque?

La cadena de ataque es sofisticada y se aprovecha de la falta de seguridad en los servidores.

- Compromiso inicial: Los atacantes escanean internet en busca de APIs de Docker expuestas públicamente. Una vez que encuentran una, la comprometen para ejecutar un nuevo contenedor malicioso basado en la imagen de Docker Alpine. Este contenedor monta el sistema de archivos del servidor, dándoles acceso directo a los archivos.
- Descarga del malware: Una vez dentro, se ejecuta una carga útil codificada en Base64 que descarga un script malicioso desde un dominio.onion de la red Tor. Este método hace que sea extremadamente difícil rastrear la infraestructura de los atacantes.
- Persistencia y comunicación: El script modifica las configuraciones de SSH para asegurar su persistencia. Además, instala herramientas de reconocimiento como masscan, libpcap y torsocks para mapear la red comprometida y establecer comunicación con un servidor de comando y control (C2).
- Propagación: El script descarga un binario comprimido desde un segundo dominio. onion. Este "dropper", escrito en Go, lanza la herramienta de escaneo Masscan para buscar otras máquinas con APIs de Docker abiertas en el puerto 2375 y repite el ciclo de infección.

El objetivo oculto

Lo más preocupante de esta nueva variante es su potencial futuro. Aunque el malware se enfoca en el cryptojacking, el binario incluye lógica para escanear y explotar otros servicios, como los puertos 23 (Telnet) y 9222 (depuración remota de navegadores Chromium).

- La funcionalidad para Telnet está diseñada para realizar ataques de fuerza bruta, robar credenciales y exfiltrar datos.
- La lógica para el puerto 9222 permitiría al malware interactuar con sesiones de navegador para recopilar información y transmitirla al servidor C2.

Esto sugiere que los atacantes están preparando una infraestructura para formar una red de bots que podría ser utilizada para ataques de denegación de servicio (DDoS) o robo de datos a gran escala en el futuro.

RECOMENDACIONES

- No expongas la API de Docker a internet: Esta es la principal puerta de entrada para este ataque. Asegúrate de que el puerto de la API de Docker (el 2375 o 2376) no sea accesible desde la red pública.
- Implementa reglas estrictas de firewall: Configura tu firewall para que solo permita el tráfico necesario a tus servidores.
- Utiliza la autenticación con TLS/SSL: Configura tu demonio de Docker para que requiera autenticación a través de certificados TLS.

NOTICIA COMPLETA

https://devel.group/blog/ataque-de-criptojacking-usa-la-red-tor-y-las-api-de-docker-para-infectar-servidores/

CONTACTOS DE SOPORTE

Correo electrónico: cti@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group