Los actores maliciosos están aprovechando interfaces expuestas del Java Debug Wire Protocol (JDWP) para obtener capacidades de ejecución de código y desplegar mineros de criptomonedas en sistemas comprometidos.

> *"El atacante utilizó una versión modificada de XMRig con una configuración codificada de forma fija, lo que le permitió evitar argumentos sospechosos en la línea de comandos, que usualmente son detectados por los defensores. La carga útil empleaba proxies de pools de minería para ocultar la dirección de su billetera de criptomonedas, impidiendo así que los investigadores rastrearan su origen»,* señalaron los investigadores de Wiz, Yaara Shriki y Gili Tikochinski, en un informe publicado esta semana.

La empresa de seguridad en la nube —que está en proceso de adquisición por Google Cloud— indicó que detectó esta actividad a través de sus servidores honeypot con TeamCity, una herramienta popular para integración y entrega continua (CI/CD).

JDWP es un protocolo de comunicación utilizado en Java con fines de depuración. Permite a los desarrolladores usar un depurador para trabajar con una aplicación Java que se ejecuta en otro proceso, ya sea en la misma máquina o de forma remota.

Sin embargo, dado que JDWP carece de mecanismos de autenticación o control de acceso, exponer este servicio a Internet representa un vector de ataque que puede ser explotado como punto de entrada, permitiendo el control total sobre el proceso Java en ejecución.

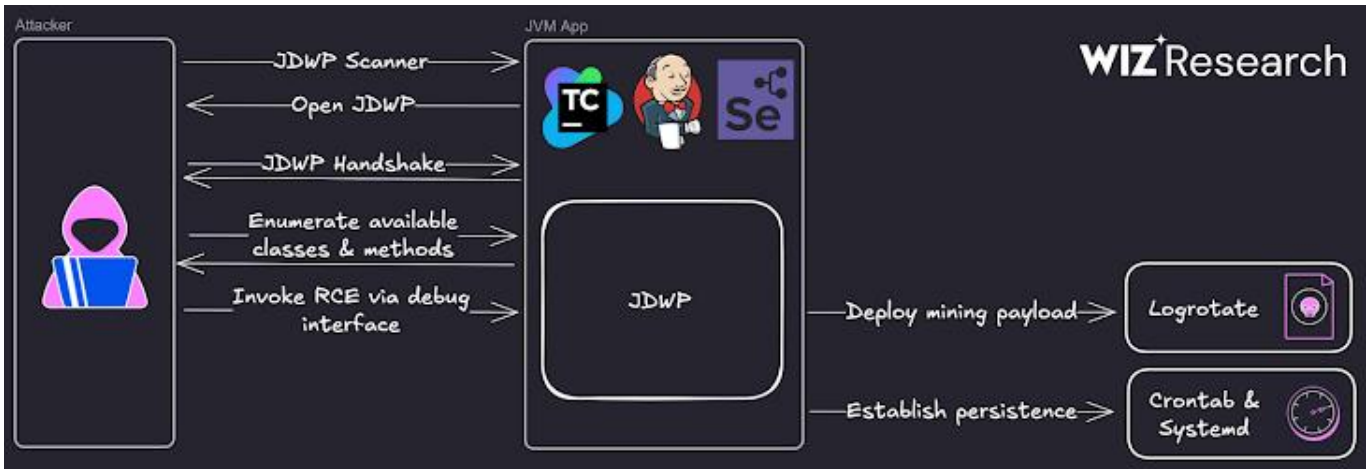
En resumen, esta mala configuración puede ser usada para inyectar y ejecutar comandos arbitrarios, establecer persistencia y ejecutar cargas maliciosas.

> *"Aunque JDWP no está activado por defecto en la mayoría de las aplicaciones Java, sí es ampliamente utilizado en entornos de desarrollo y depuración. Muchas aplicaciones populares inician automáticamente un servidor JDWP al ejecutarse en*

> *modo debug, frecuentemente sin advertir al desarrollador sobre los riesgos. Si no se protege adecuadamente o se deja expuesto, puede permitir vulnerabilidades de ejecución remota de código (RCE)»*. explicó Wiz.

Algunas de las aplicaciones que pueden activar un servidor JDWP en modo debug incluyen TeamCity, Jenkins, Selenium Grid, Elasticsearch, Quarkus, Spring Boot y Apache Tomcat.

Datos de GreyNoise muestran que más de 2,600 direcciones IP han estado escaneando endpoints JDWP en las últimas 24 horas, de las cuales más de 1,500 son clasificadas como maliciosas y otras 1,100 como sospechosas. La mayoría de estas direcciones provienen de China, Estados Unidos, Alemania, Singapur y Hong Kong.



En los ataques monitoreados por Wiz, los actores maliciosos explotan el hecho de que la Máquina Virtual de Java (JVM) escucha conexiones del depurador en el puerto 5005, lo que les permite escanear la red en busca de puertos JDWP abiertos. En la siguiente etapa, se envía una solicitud JDWP-Handshake para verificar si la interfaz está activa y así establecer una sesión.

Una vez confirmada la exposición e interactividad del servicio, los atacantes ejecutan un

comando curl para descargar y ejecutar un script shell de tipo dropper que realiza una serie de acciones:

- Elimina procesos de minería competidores o que usen alto CPU.
- Descarga una versión modificada del minero XMRig desde un servidor externo ("awarmcorner[.]world") a la ruta `~/.config/logrotate`, adaptado a la arquitectura del sistema.
- Establece persistencia mediante tareas cron, asegurando que la carga se vuelva a descargar y ejecutar al iniciar sesión, reiniciar o en intervalos de tiempo programados.
- Se elimina a sí mismo al finalizar.

> *"Al ser de código abierto, XMRig facilita a los atacantes su personalización. En este caso, eliminaron toda la lógica de análisis de argumentos y codificaron la configuración directamente. Este ajuste no solo simplifica la distribución, sino que también permite que la carga se haga pasar por el proceso logrotate de forma más convincente».* explicó Wiz.

Aparece el nuevo botnet Hpingbot

Este hallazgo coincide con el análisis de NSFOCUS sobre un nuevo y ágil malware escrito en Go, llamado Hpingbot, capaz de infectar sistemas Windows y Linux para convertirlos en parte de una botnet que lanza ataques DDoS, utilizando hping3, una herramienta de red que permite enviar paquetes ICMP/TCP/UDP personalizados.

Una característica destacada de este malware es que, a diferencia de otros troyanos basados en familias conocidas como Mirai o Gafgyt, Hpingbot es una cepa completamente nueva. Desde al menos el 17 de junio de 2025, se han emitido varios cientos de comandos DDoS, apuntando principalmente a Alemania, Estados Unidos y Turquía.

> *"Es una nueva familia de botnets desarrollada desde cero, que demuestra una gran*

> *capacidad de innovación y eficiencia en el uso de recursos existentes, como distribuir las cargas a través de Pastebin y lanzar ataques DDoS con hping3, lo que mejora su sigilo y reduce considerablemente los costos de desarrollo y operación,"* señaló la empresa china de ciberseguridad.

Hpingbot se propaga aprovechando configuraciones débiles en SSH, mediante un módulo autónomo que realiza ataques de fuerza bruta por medio de "password spraying" para obtener acceso inicial.

Los comentarios de depuración en alemán presentes en el código fuente indican que la versión más reciente aún podría estar en pruebas. El ataque, en términos generales, implica el uso de Pastebin como punto de referencia para obtener una dirección IP ("128.0.118[.]18"), la cual se emplea para descargar un script.

Ese script detecta la arquitectura del CPU del sistema infectado, finaliza versiones previas del troyano y recupera la carga principal encargada de iniciar ataques DDoS por medio de TCP y UDP. También implementa persistencia y elimina el historial de comandos para ocultar la infección.

En un giro interesante, desde el 19 de junio, los atacantes han comenzado a usar nodos infectados por Hpingbot para distribuir otro componente DDoS en Go, que, aunque comparte el mismo servidor C2, ya no usa Pastebin ni hping3, sino que implementa funciones integradas de inundación UDP/TCP.

Otro detalle relevante es que, aunque la versión de Windows no puede utilizar hping3 para lanzar ataques DDoS —ya que se instala mediante el comando de Linux `apt -y install`—, la capacidad del malware de descargar y ejecutar cargas adicionales sugiere que los atacantes podrían estar buscando más que solo interrumpir servicios, convirtiendo la botnet en una red de distribución de malware.

> *"Es importante destacar que la versión para Windows de Hpingbot no puede utilizar*

> *directamente hping3 para lanzar ataques DDoS, pero su actividad sigue siendo muy frecuente, lo que indica que los atacantes no se están limitando a los ataques de denegación de servicio, sino que también buscan aprovechar su funcionalidad para descargar y ejecutar cargas arbitrarias.”*