Investigadores en ciberseguridad han identificado una nueva campaña de malware dirigida a entornos Linux con el objetivo de realizar minería de criptomonedas de manera ilegal y distribuir malware de botnets.

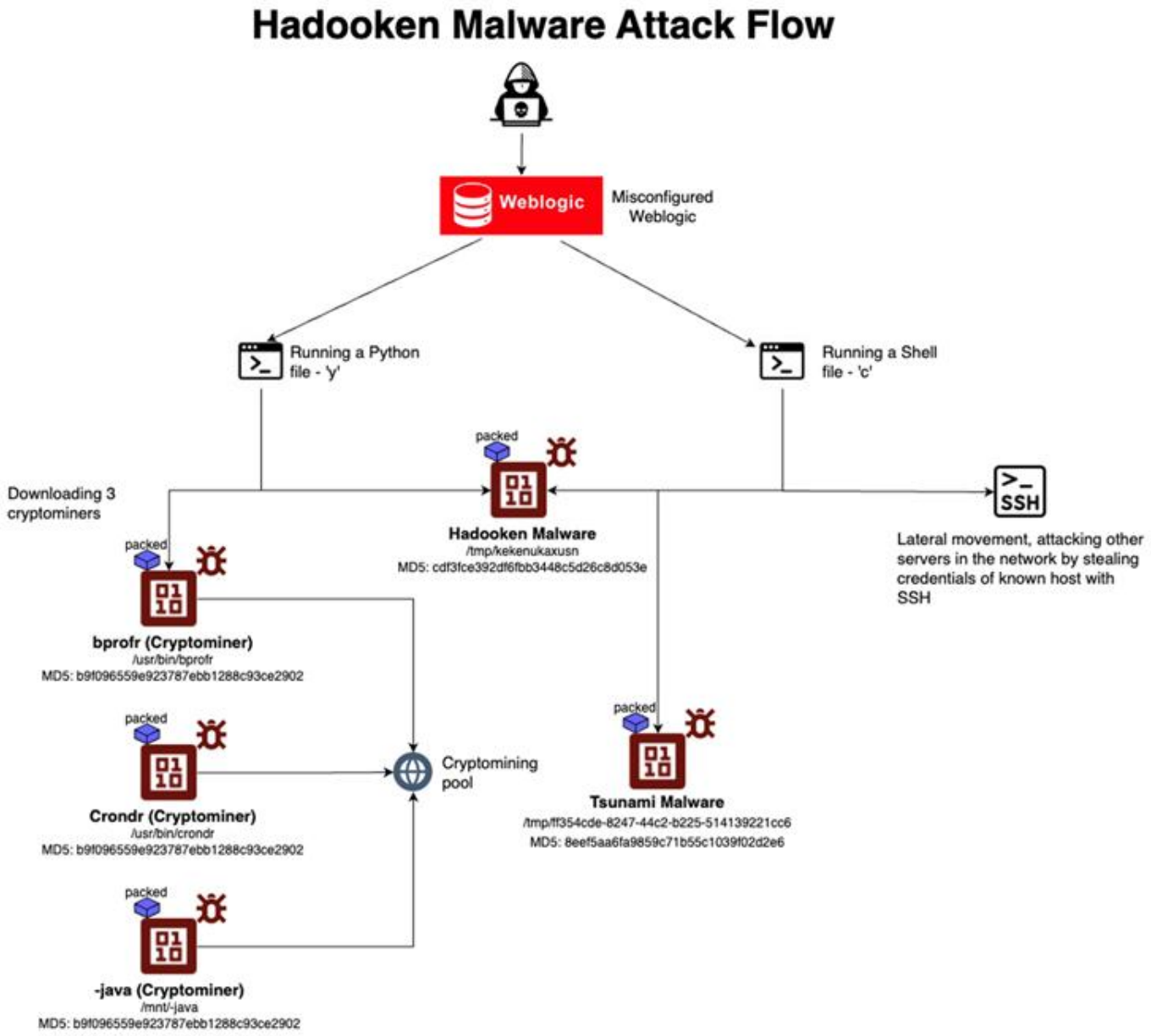
Esta actividad, que apunta específicamente al servidor Oracle Weblogic, está diseñada para desplegar una variante de malware llamada Hadooken, según la empresa de seguridad en la nube Aqua.

> *«Cuando Hadooken se ejecuta, instala el malware Tsunami y lanza un criptominero»,* explicó el investigador de seguridad Assaf Moran.

Las secuencias de ataque aprovechan vulnerabilidades de seguridad conocidas y configuraciones incorrectas, como contraseñas débiles, para obtener acceso inicial y ejecutar código arbitrario en sistemas vulnerables.

Esto se lleva a cabo mediante el despliegue de dos cargas maliciosas casi idénticas, una escrita en Python y la otra en un script de shell, ambas responsables de descargar el malware Hadooken desde un servidor remoto («89.185.85[.]102» o «185.174.136[.]204«).

> *«Además, la versión en shell script intenta recorrer diferentes directorios que contienen datos SSH (como credenciales de usuarios, información del host y claves secretas), y utiliza esa información para atacar servidores conocidos»,* señaló Morag.
>
> *«Después, se propaga lateralmente a través de la organización o en los entornos conectados para continuar diseminando el malware Hadooken.»*



Hadooken incluye dos componentes principales: un minero de criptomonedas y una botnet de denegación de servicio distribuido (DDoS) conocida como Tsunami (también llamada Kaiten), que previamente ha atacado servicios de Jenkins y Weblogic instalados en clústeres de Kubernetes.

Además, el malware garantiza su persistencia en el sistema al crear trabajos cron que ejecutan el criptominero de manera periódica con diferentes frecuencias.

Aqua señaló que la dirección IP 89.185.85[.]102 está registrada en Alemania bajo la empresa de alojamiento Aeza International LTD (AS210644). Un informe anterior de Uptycs de febrero de 2024 la vincula a una campaña de criptomonedas del grupo 8220 que explotaba fallos en Apache Log4j y Atlassian Confluence Server y Data Center.

La segunda dirección IP, 185.174.136[.]204, actualmente inactiva, también está relacionada con Aeza Group Ltd. (AS216246). Según informes de Qurium y EU DisinfoLab de julio de 2024, Aeza es un proveedor de alojamiento a prueba de fallos con presencia en Moscú M9 y dos centros de datos en Frankfurt.

> *«El modelo operativo de Aeza y su rápido crecimiento pueden explicarse por la contratación de jóvenes desarrolladores vinculados a proveedores de alojamiento a prueba de fallos en Rusia, que ofrecen refugio a actividades cibercriminales»,* indicaron los investigadores en su informe.