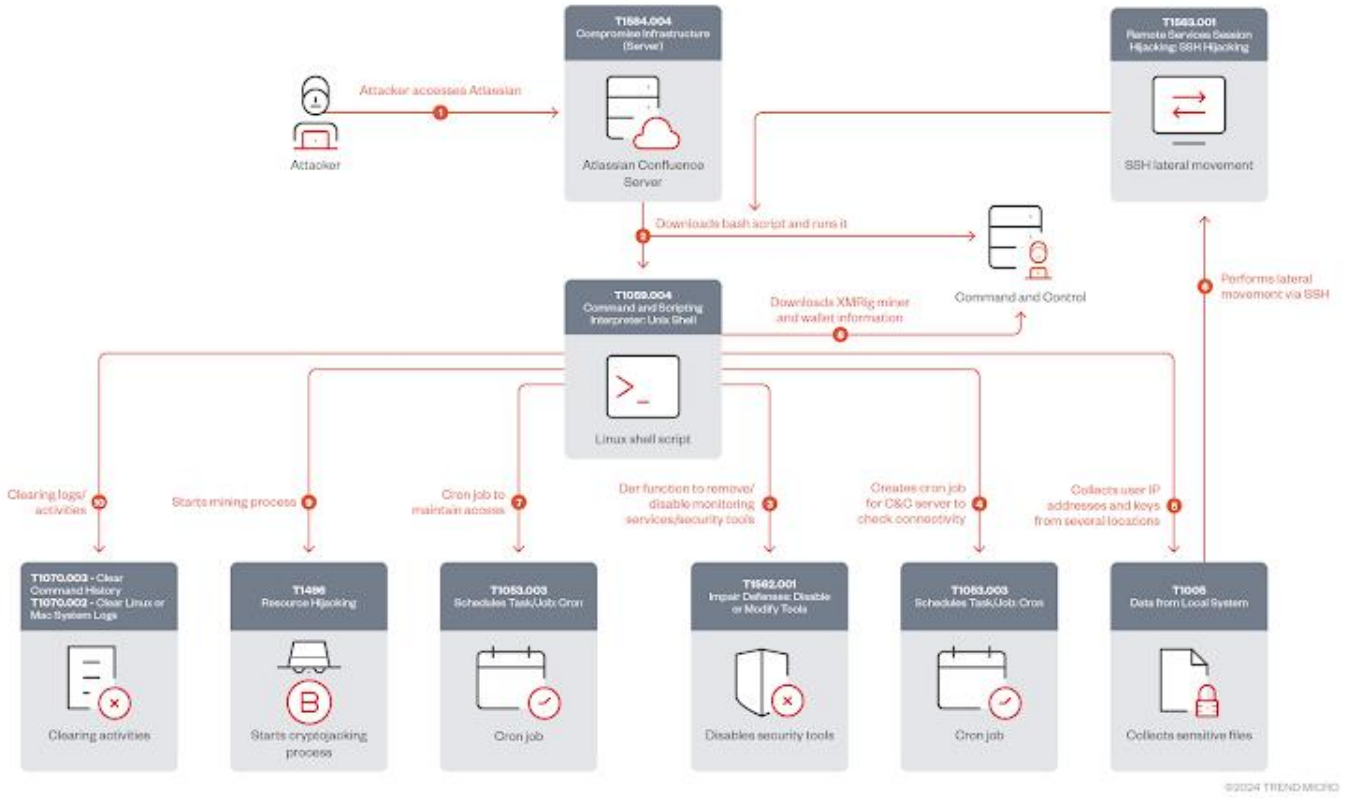
Los actores maliciosos están aprovechando de manera activa una vulnerabilidad crítica de seguridad, ahora corregida, que afecta a Atlassian Confluence Data Center y Confluence Server para realizar minería ilegal de criptomonedas en instancias vulnerables.

> *«Los ataques involucran a actores que emplean métodos como la ejecución de scripts shell y mineros XMRig, la explotación de puntos de acceso SSH, la terminación de procesos de minería de criptomonedas competidores y el mantenimiento de la persistencia mediante trabajos cron,»* explicó Abdelrahman Esmail, investigador de Trend Micro.

La vulnerabilidad de seguridad explotada es CVE-2023-22527, un fallo de máxima gravedad en versiones anteriores de Atlassian Confluence Data Center y Confluence Server, que podría permitir a atacantes no autenticados ejecutar código de manera remota. Esta vulnerabilidad fue resuelta por la empresa de software australiana a mediados de enero de 2024.



Trend Micro reportó un elevado número de intentos de explotación de esta vulnerabilidad entre mediados de junio y finales de julio de 2024, en los que se utilizó para instalar el minero XMRig en sistemas no parcheados. Se cree que al menos tres actores maliciosos diferentes están detrás de esta actividad ilegal:

- Desplegar el minero XMRig a través de un archivo ELF utilizando solicitudes especialmente diseñadas.
- Utilizar un script shell que primero elimina campañas de criptojacking competidoras (por ejemplo, Kinsing), borra todos los trabajos cron existentes, desinstala herramientas de seguridad en la nube de Alibaba y Tencent, y recopila información del sistema, antes de configurar un nuevo trabajo cron que verifica la conectividad con el servidor de comando y control (C2) cada cinco minutos y lanza el minero.

> *«Dada su continua explotación por parte de actores maliciosos, CVE-2023-22527 representa un riesgo significativo para las organizaciones a nivel mundial»,* comentó Esmail.
>
> *«Para mitigar los riesgos y amenazas asociados con esta vulnerabilidad, los administradores deben actualizar sus versiones de Confluence Data Center y Confluence Server a las versiones más recientes disponibles lo antes posible».*