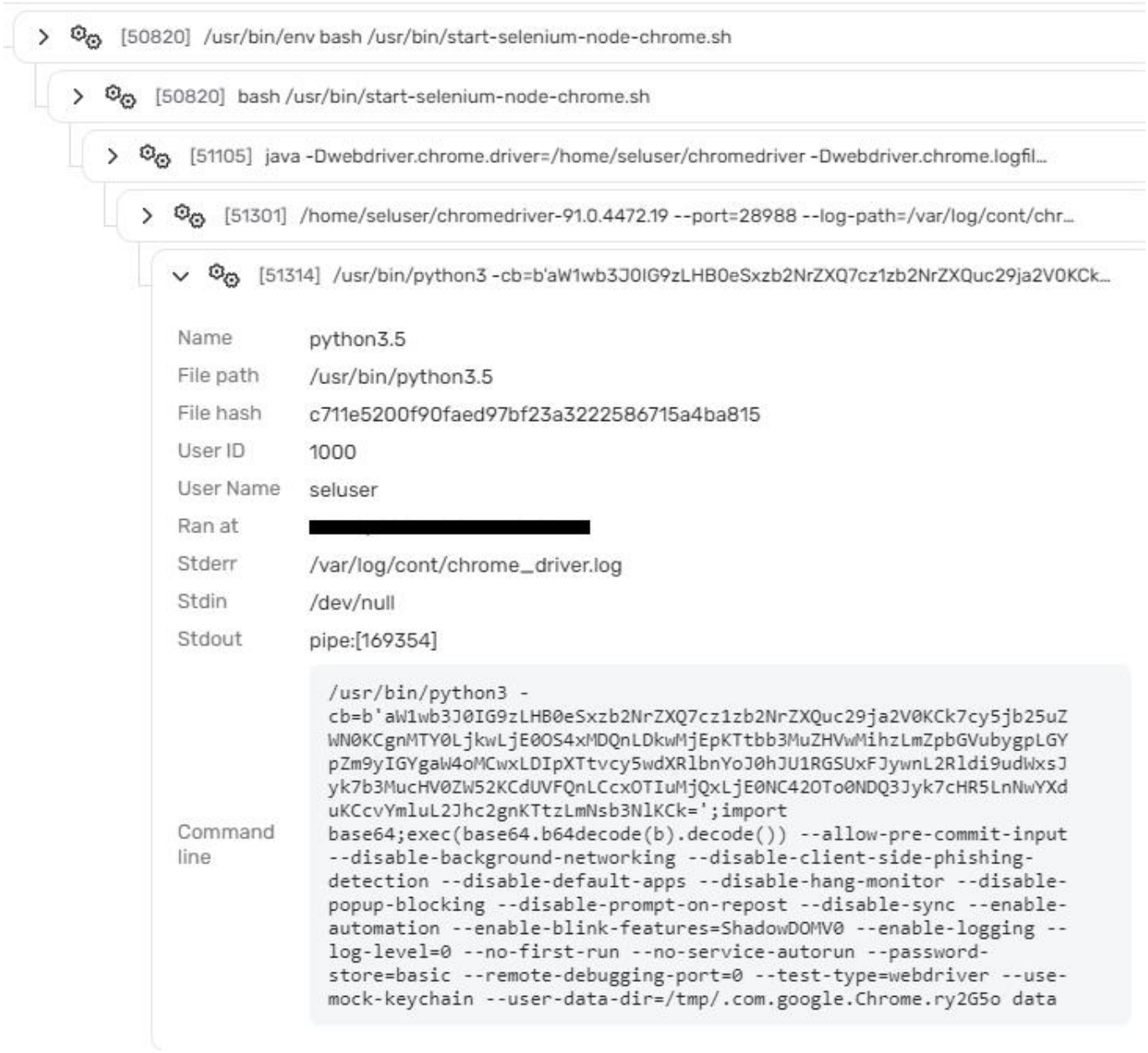
Los investigadores en ciberseguridad están alertando sobre una campaña en curso que está aprovechando los servicios de Selenium Grid expuestos a Internet para la minería ilegal de criptomonedas.

La empresa de seguridad en la nube Wiz está monitoreando esta actividad bajo el nombre SeleniumGreed. Se cree que la campaña, que está dirigida a versiones antiguas de Selenium (3.141.59 y anteriores), ha estado activa desde al menos abril de 2023.

> *«La mayoría de los usuarios no son conscientes de que la API de Selenium WebDriver permite una interacción completa con la máquina, incluyendo la lectura y descarga de archivos, y la ejecución de comandos remotos»,* comentaron los investigadores de Wiz, Avigayil Mechtinger, Gili Tikochinski y Dor Laska.
>
> - *«Por defecto, este servicio no tiene habilitada la autenticación. Esto significa que muchas instancias accesibles públicamente están mal configuradas y pueden ser accedidas por cualquiera y explotadas con fines maliciosos».*

Selenium Grid, parte del marco de pruebas automatizadas Selenium, permite la ejecución paralela de pruebas en múltiples cargas de trabajo, diferentes navegadores y varias versiones de navegadores.



«Selenium Grid debe protegerse del acceso externo utilizando los permisos de firewall adecuados», advierten los mantenedores del proyecto en una documentación de soporte, afirmando que no hacerlo podría permitir que terceros ejecuten binarios arbitrarios y accedan a aplicaciones y archivos web internos.

Actualmente no se sabe exactamente quién está detrás de la campaña de ataque. Sin embargo, implica que el actor de amenazas se dirija a instancias expuestas públicamente de Selenium Grid y haga uso de la API de WebDriver para ejecutar código Python responsable de descargar y ejecutar un minero XMRig.

El proceso comienza cuando el adversario envía una solicitud al centro Selenium Grid vulnerable para ejecutar un programa Python que incluye una carga útil codificada en Base64. Esta carga útil genera un shell inverso en un servidor controlado por el atacante («164.90.149[.] 104») con el fin de obtener la carga útil final: una versión modificada del minero XMRig de código abierto.

> *«En lugar de codificar la IP del grupo en la configuración del minero, la generan dinámicamente en tiempo de ejecución. También establecieron la función de huella dactilar TLS de XMRig dentro del código agregado (y dentro de la configuración), lo que garantiza que el minero solo se comunicará con los servidores controlados por el actor de amenazas»,* explicaron los investigadores.

Se ha informado que la dirección IP en cuestión pertenece a un servicio legítimo que ha sido comprometido por el actor de amenazas, ya que también se ha descubierto que aloja una instancia de Selenium Grid expuesta públicamente.

Wiz señaló que es posible ejecutar comandos remotos en las versiones más recientes de Selenium y que identificó más de 30,000 instancias vulnerables a la ejecución de comandos remotos, por lo que es crucial que los usuarios tomen medidas para corregir la configuración incorrecta.

> *«Selenium Grid no está diseñado para ser expuesto a Internet y su configuración predeterminada no tiene habilitada la autenticación, por lo que cualquier usuario con acceso de red al hub puede interactuar con los nodos a través de la API»*,

> dijeron los investigadores.
>
> *«Esto representa un riesgo de seguridad significativo si el servicio se implementa en una máquina con una IP pública que tiene una política de firewall inadecuada».*