**Grupo 4 – Ejercicio Amenazas**

Nota: <https://www.welivesecurity.com/la-es/2021/02/02/kobalos-amenaza-linux-afecta-infraestructuras-informaticas-alto-rendimiento/>

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Kobalos es una amenaza para Linux que afecta a infraestructuras informáticas de alto rendimiento. En la mitología griega, un Kobalos es una criatura pequeña y traviesa. Es un malware multiplataforma, al cual llamaron Kobalos, que persigue clusters informáticos de alto rendimiento (HPC) y otros objetivos de alto perfil. El mismo es una amenaza que representa es un malware backdoor del tipo troyano.
2. Para infectar el sistema objetivo lo que se hace es se embebe Kobalos en OpenSSH, y cuando OpenSSH se ejecuta en el sistema entonces infecta al mismo con Kobalos.
3. Al momento no se encontró ningún otro malware, excepto por el ladrón de credenciales SSH. La forma en que Kobalos está contenido en una sola función y el uso de un puerto abierto existente para llegar a Kobalos hace que esta amenaza sea más difícil de encontrar.
4. Factor de doble autentificación que podria mitigarlo y también podríamos chequear el hash del software para chequear que sea el original.