

Mesa 4: Kobalos

- 1) Kobalos es un troyano cuyo objetivo es infectar computadoras de alto rendimiento (HPC) y robar las credenciales SSH de los usuarios legítimos del sistema.
- 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) Es una sola amenaza pero puede infectar otros sistemas que se comuniquen con el sistema infectado.
- 4) Recomendaría chequear el hash de todos los instaladores/binarios de programas que van a ser utilizados en el sistema en cuestión para asegurarse que coinciden con el software “original” y no se encuentra adulterado con este malware.