PRÁCTICA 3: Analizando la RAM 3 - Reto INCIBE

Sospechamos que el volcado de memoria adjunto se corresponde con una máquina que ha sido infectada de forma persistente por algún tipo de malware, posiblemente un dropper. Nos gustaría identificar el dominio dañino utilizado por el mismo.

Objetivo:

- Investigar y averiguar la forma de infección y el dominio dañino.
- Hacer investigaciones avanzadas mediante el uso de plugins específicos para procesar artefactos específicos del SO.

Recursos necesarios:

- Volatility (https://www.volatilityfoundation.org/26)
- Plugins Volatility
- Descarga la práctica aquí