Hash cargado en ChromaDB

- **Smoke Loader:** 076abc443c05871e2e638ec146f791b06084aafb9dc200410c6aaaacef934239

Prompt 0 (Informe Sintetizado)

Actúa como analista experto en ciberseguridad, ayúdame creando un informe en el que indiques lo siguientes rubros:

- explícame 3 tácticas y técnicas de MITRE ATT&CK
- explícame 3 comportamientos críticos (MBC Behavior)
- explícame 3 habilidades maliciosas

El hash: sha256 076abc443c05871e2e638ec146f791b06084aafb9dc200410c6aaaacef934239 es el que debes analizar, finalmente dame 3 recomendaciones para poder detectar este malware en mi infraestructura.

Prompt 1 (MITRE ATT&CK)

Eres un analista experto en ciberseguridad, así que utiliza el marco MITRE ATT&CK e identifica las tácticas, técnicas que son utilizadas por el siguiente hash:

- sha256 076abc443c05871e2e638ec146f791b06084aafb9dc200410c6aaaacef934239

finalmente dame el resultado en un formato de lista con la descripción de cada una de estas.

Prompt 2 (MBC Objective - MBC Behavior)

Como analista experto en ciberseguridad, te pediré que utilices el catálogo de objetivos (MBC Objective) y comportamientos de malware (MBC Behavior) así que te daré el siguiente hash:

- 076abc443c05871e2e638ec146f791b06084aafb9dc200410c6aaaacef934239

Muéstrame una descripción detallada de estos comportamientos afín de poder identificar qué es lo que intenta hacer este malware al infectar a sus víctimas.

Prompt 3 (Capacidades Maliciosas)

Eres un analista experto en ciberseguridad, así que te daré el siguiente hash:

- 076abc443c05871e2e638ec146f791b06084aafb9dc200410c6aaaacef934239

Ayúdame a identificar las capacidades maliciosas que han sido utilizados por el hash, además selecciona 5 de ellas y dame una descripción detallada de estas, finalmente ayúdame a identificar el objetivo de la muestra de malware.