Análisis de Malware

MISP y VIPER

Gerard Díaz Hoyos

KeepCoding
Bootcamp de Ciberseguridad
5a edición

MISP (*Malware Information Sharing Platform*):

Plataforma de intercambio de información sobre malware y amenazas.

Vamos a añadir un reporte a la base de datos de MISP (función que, cada vez más, va a ser requerida por todas las compañías que manejen cierto volumen de datos).

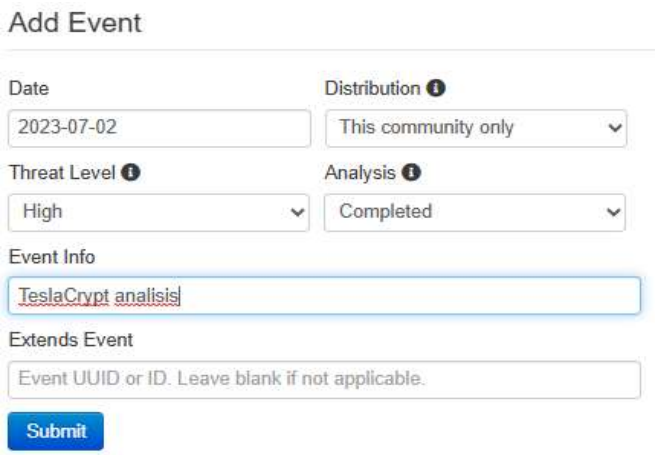
Usuario: alumno14@keepcoding.io

Event ID: 16

UUID: 6a9e8a0f-46cc-4c00-b2d9-57401e6c7a01

Los pasos que tendremos en cuenta serán:

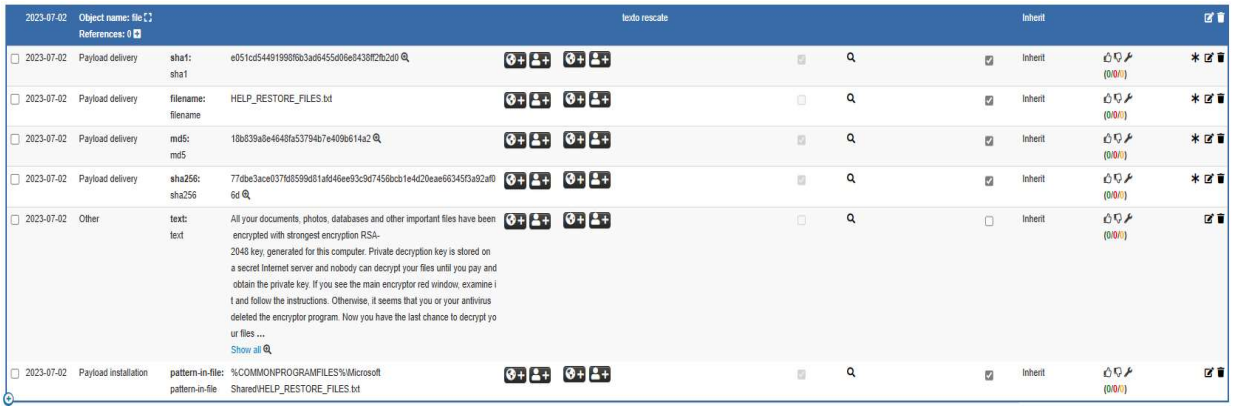
1.Creación de un nuevo evento



2.Adición de archivos relevantes

Con estos 2 botones, situados en el panel lateral, añadiremos el archivo principal del malware, los dropper, mutex, comandos relevantes, etc.

A modo de ejemplo, se visualizarían del siguiente modo:



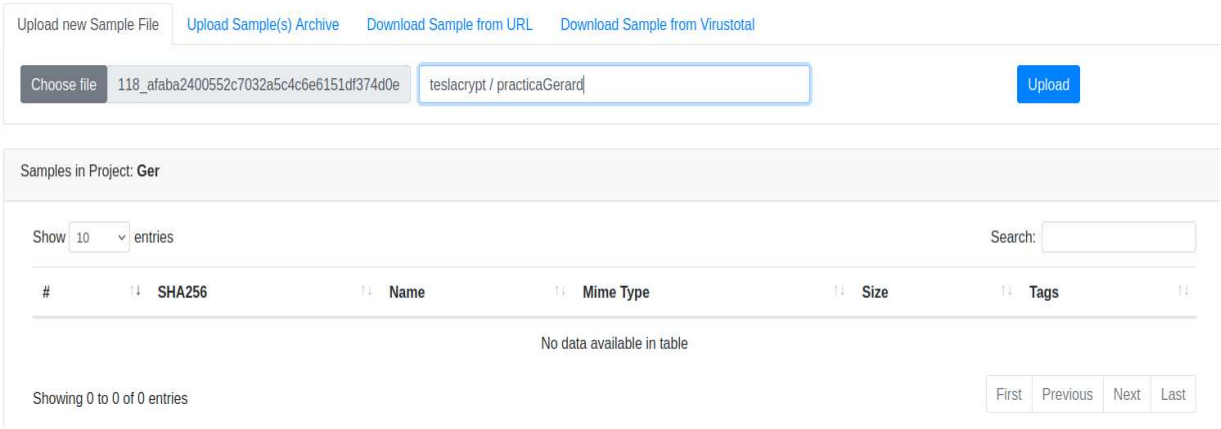
VIPER

Plataforma para subida y descarga de archivos maliciosos de forma segura.

Usuario: alumno14

Proyecto: Ger

Tan sólo se debe subir el archivo que queramos:



Y ya estará disponible para la descarga: