III Bootcamp Full Stack Cibersecurity Módulo 7 - Malware Analysis



Caso práctico Ticketing FAME | VIPER | MISP

Marcos Alonso González

alonsogonzalezmarcos@gmail.com https://github.com/magalorn

7 de mayo de 2022

Índice

1. VIPER	3
2. FAME	4
3. MISP	•

1. VIPER

Se han subido dos muestras al gestor de malware VIPER:

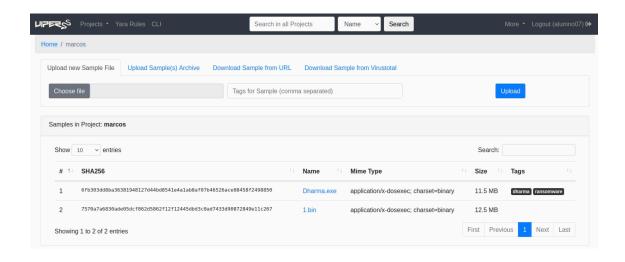
alumno07

Project marcos

http://3.133.116.136:8000/project/marcos/

- · Dharma.exe
- 1.bin

La segunda muestra se ha subido ya que en los últimos meses se ha asociado este malware a Dharma. Podríamos estar ante una muestra modificada del malware de Dharma, por lo que sería interesante analizar más en profundidad 1.bin más adelante, si bien en este informe nos centramos en el análisis de Dharma.exe.



2. FAME

Se ha lanzado sobre **FAME** análisis tanto del fichero Dharma.exe como de la botnet http://epoolsoft.com con todos los módulos disponibles.

El funcionamiento de la plataforma es sencillo, para el análisis, en el apartado "Submit" se ofrecen las siguientes opciones:

- Subir una muestra del fichero a analizar
- · Analizar una url
- · Analizar un hash

En este caso, se ha subido el fichero Dharma.exe y se ha analizado http://epoolsoft.com, la URL de la botnet hallada en el análisis con el resto de herramientas.



Sin embargo no se ha encontrado información de interés diferente a la extraída con el resto de herramientas utilizadas en el análisis. Puede verse la información obtenida en estos enlaces:

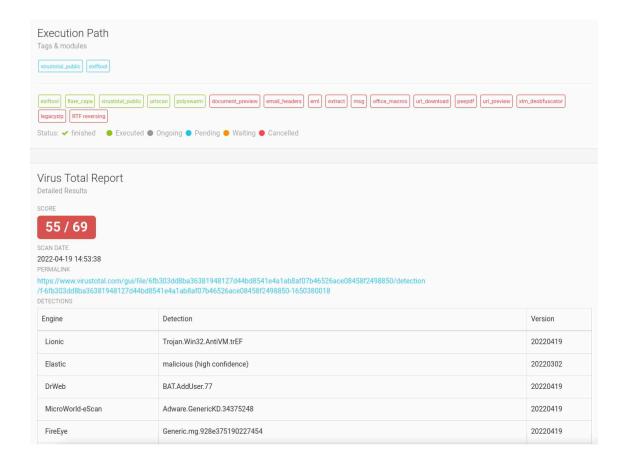
alumno07@keepcoding.io

Dharma.exe: http://13.58.26.224/analyses/62769d93b4ee101273de0f8f/

http://epoolsoft.com: http://13.58.26.224/analyses/62769f1db4ee101273de0f96/

A destacar, es que FAME no detecta la URL de la botnet como maliciosa.

FAME incluye integración con Virus Total, muestra como en el caso de Dharma.exe, la herramienta detecta en la mayoría de marcas de AVs la muestra como malware.



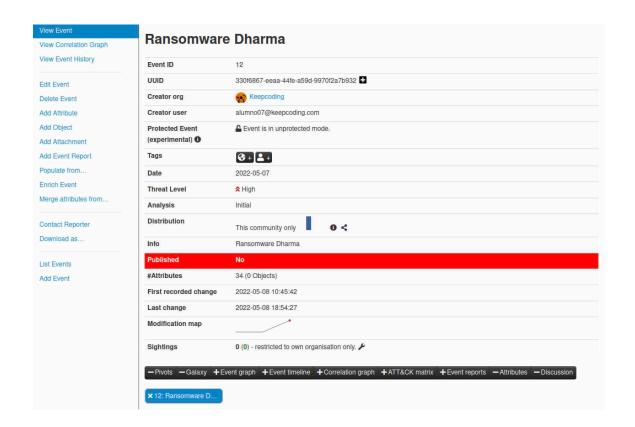
3. MISP

Plataforma utilizada por la comunidad de analistas de malware para compartir la información de las muestras analizadas.

Cuenta con un sistema de cumplimentación de campos y diferentes apartados donde se puede incluir información para crear eventos.

Alumno07 Event ID 12

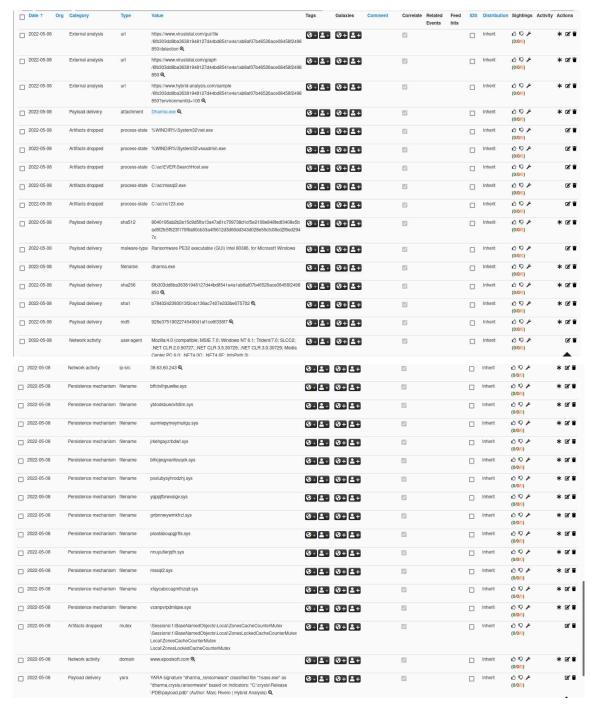
https://18.119.159.89/events/view/12



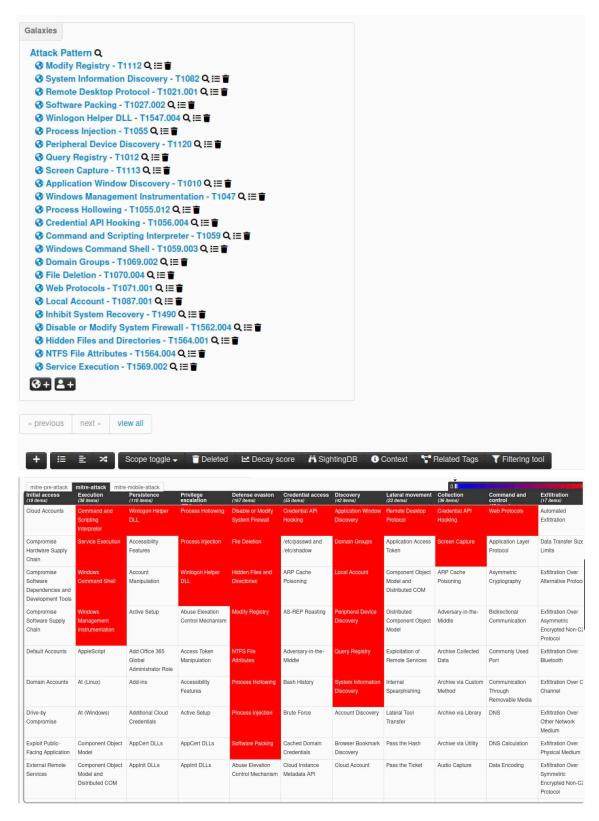
En este caso, con la muestra Dharma.exe, se ha incluido en el evento, entre otra, la siguiente información:

 Atributos: Se ha añadido información de las categorías External Analysis, Payload delivery, Artifacts Dropped, Network Activity, Persistance mechanism.

Para incluir información de atributos, basta con pulsar "Add Atribute" en el menu lateral izquierdo y posteriormente elegir categoria, tipo e incluir la información.



 Galaxies: En la Attack Pattern Galaxy, se incluyen las tácticas de la. Matriz MITRE ATT&CK que se han encontrado en el análisis del malware. Se han encontrado en este caso 24 coincidencias.



Se han incluido en este ticketing una pequeña parte de la información que puede subirse a la plataforma sobre la muestra analizada, ya que MISP cuenta con un gran abanico de posibilidades para incluir información de diferentes maneras, incluso con la subida del fichero que contiene la muestra sobre la que se ha compartido la información.

Una vez finalizado el evento, puede publicarse para compartirlo con la comunidad de usuarios de MISP.