MÁSTER EN ANÁLISIS DE MALWARE Y REVERSING

MÓDULO 2. ENTORNOS DE ANÁLISIS DE MALWARE – TAREA 2

MÁSTER EN *ANÁLISIS DE MALWARE Y REVERSING*

Campus Internacional CIBERSEGURIDAD

ENIIT INNOVA IT BUSINESS SCHOOL

UCAM Universidad Católica de Murcia

Tabla de contenido

1. INTRODUCCIÓN

Hola. Esta es la **segunda evaluación** práctica de la asignatura de Entornos de Análisis de Malware.

1.1. Requisitos técnicos

Te vale cualquier sistema operativo Linux que esté soportado (es decir, que puedas instalar paquetes actualizados). Virtualiza aquel con el que prefieras trabajar. Por ejemplo, Ubuntu, Debian, Arch e incluso una Kali Linux.

Vamos a hacer uso extensivo de Python. **Recuerda que en la guía de apéndices tienes una sección dedicada a montarte tus entornos virtuales Python**. No obstante, si tienes un método mejor o con el que prefieras trabajar, adelante.

1.2. Formato de entrega

Utiliza un archivo comprimido en formato zip.

Dicho archivo comprimido contendrá un documento en formato pdf con las respuestas y los archivos con el código fuente.

El nombre del archivo zip vendrá dado por:

NOMBREALUMNO_EAM_EVAL_2.zip

Dentro del comprimido, la estructura deberá ser similar a esta:

```
.
├── documento_entrega.pdf
├── paquete_stix.json
└── paquete_stix.py
```

1.3. Consejos

- Por favor, escribe con buena ortografía, es necesario para hacerte comprender bien.

- Utiliza un lenguaje apropiado, profesional. Imagina que es un informe que van a leer las personas que trabajan en una empresa u organización.
- **Estas prácticas están pensadas para que empieces ya a poner a trabajar tus habilidades como reverser. Es bastante probable que tengas que encender el IDA Pro o Ghidra, un depurador o un editor hexadecimal para avanzar.**

1.4. Usa una máquina virtual desechable o con snapshots

Es importante respetar la siguiente norma:

LOS ARCHIVOS SOLO SE ABREN Y PROCESAN DENTRO DE UNA MÁQUINA VIRTUAL DESECHABLE

2. EVALUACIÓN

2.1. Introducción

A lo largo de esta evaluación nos vamos a centrar en trabajar sobre el estudio de una campaña APT desde el punto de vista técnico. Trabajaremos en la creación de un paquete STIX con los datos que vamos extrayendo de la investigación y su relación con ATT&CK.

2.2. Materiales

La campaña está basada en el artículo publicado por el TAG (Threat Analysis Group) de Google disponible en esta URL:

https://blog.google/threat-analysis-group/internet-explorer-0-day-exploited-by-north-korean-actor-apt37/

En los materiales de descarga disponéis de una copia PDF del artículo por si el mismo no está disponible en línea.

2.3. Entregables

Documento PDF con tus respuestas, capturas de pantalla y descripciones o razonamientos.

Script Python que produzca el paquete STIX

El paquete STIX en formato de salida json.

Todo ello en un archivo zip tal y como se indica en el punto 1.2 de este mismo documento.

2.4. Instrucciones

Vamos a modelar la amenaza descrita en el artículo reseñado. Es una operativa habitual en cualquier SOC, el trabajo de un analista de malware o producto del automatismo que tengamos implementado en nuestra cadena de análisis de malware.

En primer lugar, lee el artículo con vista de analista. Observa de que partes se compone. Separa los distintos implicados: grupo apt, exploit, vulnerabilidad,

productos, etc.

A continuación, empleando un script Python y usado la librería STIX2 modela el APT con los distintos componentes que están relacionados y descritos en el artículo.

No te agobies. **Haz los que puedas o creas convenientes. Cuanto más exacto y completo sea tu paquete STIX mayor nota obtendrás**.
Dado que el trabajo se centra en tu script y la salida proporcionada por este, el documento PDF tan solo se usará para que anotes el razonamiento que has empleado para detectar los distintos componentes y relacionarlos.

Lo que si debe llevar el documento pdf es una captura de pantalla del grafo de tu paquete STIX generado en:

https://oasis-open.github.io/cti-stix-visualization/

NOTA: Aunque se incluya el archivo json, se evaluará la ejecución del script porporcionado.

PUNTOS EXTRA:

Se darán puntuación extra si enlazas correctamente las diferentes categorías ATT&CK con los componentes de tu STIX.

No enlazar correctamente no baja la nota. Se proporcionará en el feedback los comentarios apropiados para tu valoración.