1 Objetivos

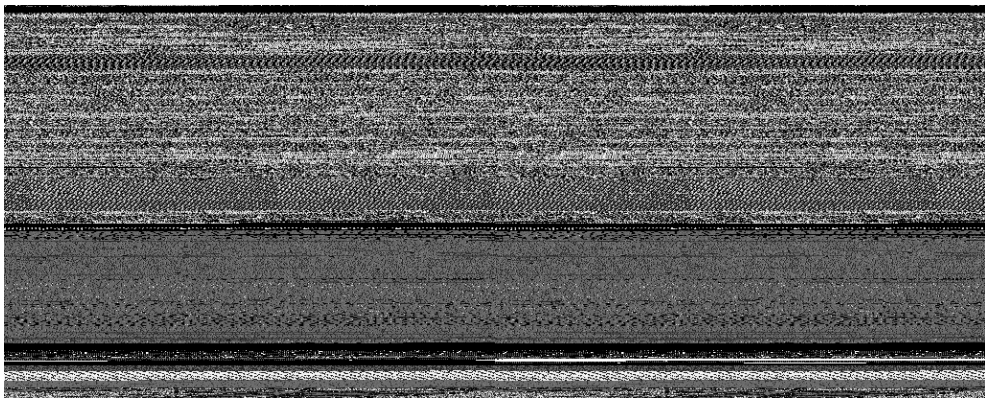
- Aplicar los conocimientos de Deep Learning y las redes neuronales en ciberseguridad.
- Investigar y adquirir conocimientos sobre el uso de redes convolucionales para la clasificación de imágenes de malware.

2 Preámbulo

La clasificación de malware es una tarea que involucra diversos retos. Cada tipo de análisis estático y dinámico tiene ventajas y limitaciones. Del lado del análisis estático la velocidad de análisis es su principal característica y su mayor reto consiste en diferenciar las llamadas a las DLLs y APIs sospechosas, de llamadas benignas. En el análisis dinámico la principal ventaja es registrar el comportamiento del malware con todo detalle, pero la preparación del entorno y ejecución requiere una inversión de tiempo y recursos técnicos considerables.

Las redes neuronales convolucionales se usan normalmente en la clasificación de imágenes, y de aquí surge la idea: ¿qué sucede si los bytes de un malware se pasan a una imagen? (artículo “Malware Images: Visualization and Automatic Classification”).

Las siguientes imágenes son dos ejemplares distintos de malware que pertenecen a la familia Adialer.C:



Los hashes de estos ejemplares son:

- 00bb6b6a7be5402fcfce453630bfff19
- 000bde2e9a94ba41c0c111ffd80647c2

Podemos observar a simple vista que las imágenes son bastante similares, y podemos determinar que ambos pertenecen a la misma familia. Entonces podemos considerar convertir los ejemplares de malware a imágenes y entrenar a la red neuronal con estas para clasificarlos.

3 Desarrollo

Este laboratorio es obligatorio, ya que es la base para los últimos laboratorios (sobre este modelo se trabajarán modelos de ataque y defensa). Se deberá desarrollar de forma individual o en parejas.

La entrega del laboratorio se realizará el miércoles 26 de abril a las 11:59 p.m. Se deberá entregar un jupyter notebook con el modelo implementado.

Para este laboratorio se utilizará el dataset contenido en el archivo malimg_dataset.zip que se encuentra en CANVAS. Este dataset contiene imágenes en formato .PNG de 25 familias distintas de malware.

1. En el preprocesamiento debe mostrar cuantos ejemplares hay por cada familia. En base a estos datos debe determinar si considera pertinente prescindir de ejemplares que tengan pocas observaciones.
2. Plotee las imágenes de los ejemplos de malware.
3. Utilizando Keras y Tensorflow construya una red neuronal con las capas, funciones de activación y el optimizador que considere conveniente.
4. Muestre el resumen del modelo.
5. Divida el dataset en un 70% entrenamiento y un 30% de pruebas.
6. Entrene el modelo con el número de épocas que considere conveniente.
7. Muestre las métricas de su modelo.
8. Evalúe el modelo con el dataset de pruebas y muestre las métricas obtenidas. Discuta los resultados obtenidos.