Deep learning model base on API call sequences for ransomware detection

專題編號：113-CSIE-S033
執行期限：112 年第 1 學期至 113 年第 1 學期
指導教授：孫勤昱
專題參與人員： 110820001 吳奕萱
110820015 程邦博
110820052 何穎宣

一、摘要

本專題針對 Windows 可攜式可執行（Portable Executable, PE）檔案進行動態分析，以應用程式介面（Application Programming Interface, API）呼叫序列作為特徵，開發一個基於深度學習的勒索病毒（Ransomware）偵測模型，並將其部屬於網頁平台，方便使用者上傳檔案進行分析。

本專題使用兩種數值化方法處理 API 呼叫序列：直接轉換與四元組語義表示法。接著透過嵌入（Embedding）和卷積（Convolution）技術提取特徵，並利用自然語言處理（Natural Language Processing, NLP）模型—— Transformer 分析 API 呼叫間的關聯，有效辨識勒索病毒。

本專題最終開發的模型準確率達 0.9994、精確率 0.9992、召回率 1.0、F1 Score 0.9996，並成功將其部署於網頁平台。

關鍵詞：勒索病毒偵測、API 呼叫序列、深度學習、自然語言處理。

二、緣由與目的

根據 2023 上半年 FortiGuard Labs 發表的全球威脅情勢報告 [1]，雖然 78% 的企業領袖聲稱其企業已做好應對勒索病毒攻擊的準備，實際上仍有半數成為此類攻擊的受害者。此外，勒索病毒的攻擊未見減緩，相較於 1 月，其在所有被檢測到的惡意軟體中的比例增長了約 13 倍，但成功檢測到勒索病毒的組織卻從 22% 降至 13%，顯示其變得更加複雜。

勒索病毒的威脅持續給企業帶來困擾，其變種更是難以被有效偵測。早期靜態分析偵測技術主要是基於靜態特徵（Signature-based）[2]，不需要執行惡意軟體，這降低了潛在的風險和對系統資源的消耗。然而，此方法對已知特徵（Signature）的過度依賴使之對新型和變種勒索病毒效果不彰。鑑於靜態分析偵測方法存在明顯限制，動態分析方法被提出並廣泛使用。

動態分析透過在虛擬環境中執行病毒樣本，監控並記錄其行為。涵蓋了從軟體的執行過程到註冊表鍵值的變更、系統 API 的呼叫，以及檔案系統的任何變更等 [3]。其中，API 呼叫尤為關鍵，它代表軟體的具體操作，能詳盡呈現其行為模式。

綜上所述，本專題提出一種基於動態分析的方法，將 API 呼叫序列作為特徵，並結合深度學習與自然語言處理技術，開發一個高準確率的勒索病毒偵測模型。

三、研究方法

（一） 研究流程

1. 以沙盒分析 Windows PE 檔案樣本並產生執行報告。
2. 從中提取並預處理 API 呼叫序列。
3. 數值化 API 呼叫序列。
4. 特徵提取。
5. 輸入分類器。
6. 將模型部署於網頁平台。

（二） 實驗環境

使用配備 NVIDIA GeForce RTX 3060 顯卡之主機，在 Ubuntu 16.04.7 LTS 操作系統中，透過開源惡意程式分析沙盒

Cuckoo Sandbox 進行軟體的動態分析，產生執行報告。

（三） API 呼叫序列之資料預處理

1. 刪除連續重複項。
2. 序列長度標準化。
3. 資料標記：勒索病毒為正。
4. 數值化：參考 Li 等人 [4] 提出的方法。

(1) 直接轉換：將 API 呼叫名稱直接轉換為唯一對應的數值 ID。

(2) 四元組語義表示：先將 API 呼叫名稱轉換成四元語義表示（式 1），接著再轉換為數值 ID。

$$< action, object, class, category > \quad (1)$$

其中，$action$ 表示執行的動作，$object$ 表示該動作操作的對象，$class$ 表示對系統的影響程度。$category$ 表示功能類型，參考 Cuckoo Sandbox 提供的分類方法。

5. 分割資料集。

（四） 特徵提取

採用 PyTorch 深度學習框架，透過 Embedding 及 Conv2d 模組，對經過預處理的 API 呼叫序列進行嵌入和卷積。

（五） 使用 Transformer 模型分析語義

（六） 分類器設計

使用兩個搭配 ReLU（Rectified Linear Unit）函數的全連接層與一個搭配 Sigmoid 函數的輸出層進行分類判斷，並結合 Dropout 正則化技術，使模型能學習到更加穩健的特徵。

（七） 實際應用

本專題將訓練好的模型部署至網頁，前端介面採用 TypeScript 及 React 開發，React 具有高度的模組化設計，可以重複利用現有的元件，提升開發效率。後端伺服器使用 Python Flask 框架實作，它是一個輕量化的 Web 應用程式框架，設計簡潔且易於使用。平台設計著重簡潔與直觀，以確保即使是沒有技術背景的使用者也能輕鬆地進行檔案分析。

四、研究成果

- 建立一個具備卓越效能的勒索病毒偵測模型：準確率達 0.9994、精確率 0.9992、召回率 1.0 和 F1 Score 0.9996。

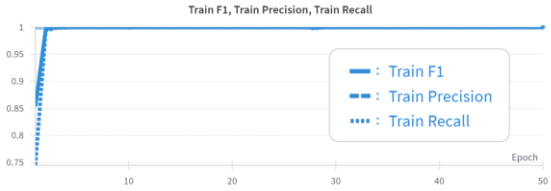

圖 1. 訓練過程各指標趨勢圖

- 將模型部署於網頁平台，提供分析上傳之檔案是否為勒索病毒的功能。

參考文獻

[1] FortiGuard Labs, "Global Threat Landscape Report: A Semiannual Report by FortiGuard Labs," Aug. 7, 2023. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report1h-2023.pdf.

[2] P. Maniriho, A. N. Mahmood, and M. J. M. Chowdhury, "API-MalDetect: Automated malware detection framework for windows based on API calls and deep learning techniques," Journal of Network and Computer Applications, vol. 218, 103704, 2023

[3] P. Maniriho, A. N. Mahmood, and M. J. M. Chowdhury, "A study on malicious software behaviour analysis and detection techniques: Taxonomy, current trends and challenges," Future Generation Computer Systems, vol. 130, pp. 1-18, 2022.

[4] C. Li, Q. Lv, N. Li, Y. Wang, D. Sun, and Y. Qiao, "A novel deep framework for dynamic malware detection based on API sequence intrinsic features," Computers & Security, vol. 116, 102686, 2022.