MAMBA (以MITRE ATT&CK 框架為基礎的惡意行為分析系統)

本院覽號

05A-1100218

公告日期

2024-01-19

智財權狀態

美國臨時案已申請、美國放棄申請、台灣(發明)放棄申請

摘要

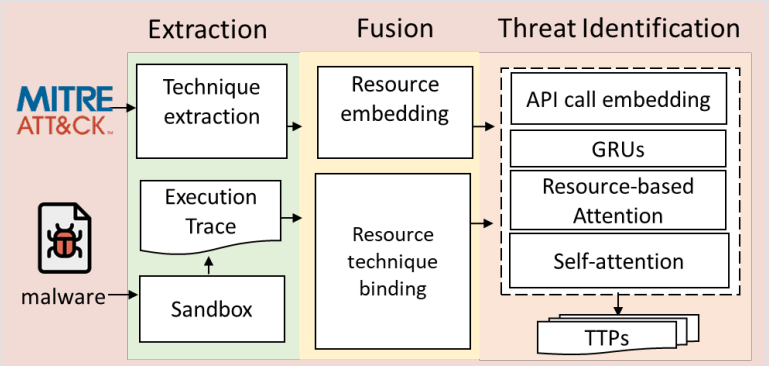
MAMBA是一個類神經網路系統，透過動態分析Windows惡意程式的行為，對應MITRE ATT&CK框架中的自然語言說明、以及指出惡意程式可疑的行為(Windows API calls)。此系統可以自動化分析惡意程式所執行的Windows API calls行為，判斷那些可疑的Windows API calls是惡意行為。這個系統可以解決資安專家在做數位鑑識時，需要人工的判斷Windows程式的執行碼，那些部分是可疑的或是惡意的行為；也可以解決Windows軟體廠商在軟體開發生命週期中，測試程式的安全性。
MAMBA主要的核心技術包含1) 自動化的整合MITRE ATT&CK框架資訊、2) 雙層式類神經網路動態行為分析與3) 自動化定位可疑惡意行為(Windows API calls)。

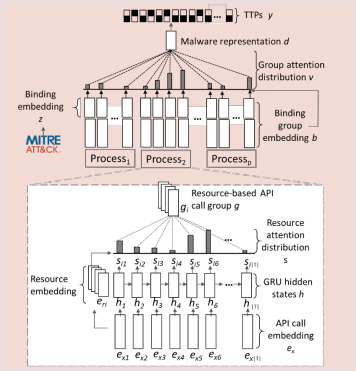
技術優勢

1. 自動化整合MITRE ATT&CK 框架資訊以分析惡意程式操弄的資源態樣
2. 人工智慧基礎的惡意行為分析
3. 自動化對應惡意行為的Windows API calls定位

應用範圍

1. 惡意程式鑑識：可作為惡意程式分析工具，提供惡意行為的高階語意與低階執行碼。
2. 軟體安全查核：可作為軟體開發測試工具，亦可在軟體下載時，檢驗是否有可疑的惡意行為，並顯示其行為的高階語意與低階執行碼。





創作人

陳孟彰、黃意婷

中央研究院
ACADEMIA SINICA