經濟部 111 年度
主動式資安情資與智能偵防技術計畫(2/4)
合作研究計畫

《攻擊狙殺鏈實務應用》

建議書徵求文件

財團法人資訊工業策進會

中華民國 111 年 03 月

111年度合作研究計畫建議書徵求文件

一、 簡介

針對 APT 攻擊特性，駭客於網路與主機層級發動組合式攻擊狙殺鏈，以往對特定攻擊制訂的偵測規則，已不足以獵捕攻擊鏈行為，亟需研發攻擊狙殺鏈告警事件關聯技術，將不同層級 (如：網路或主機)、不同範圍 (如：網際網路、區域網路、VLAN 等) 及不同攻擊手法之異質資安防護設備 (如：IDS、IPS、Firewall、Anti-Virus、APT 防護等) 偵測告警進行整體考量，為每個攻擊偵測規則對應與標示 ATT&CK 之戰術、手法、程序及應變。接著即可從點 (如：CVE Exploit、Malware)、線 (如：Attack Path) 到面 (如：Cross-Layer Kill Chain) 各個角度進行資安偵防，以利獵捕攻擊狙殺鏈過程相關行為，並作為後續人工智慧偵防技術的參考與訓練。

於人工智慧偵防技術中，藉由使用知識圖 (Knowledge Graph/Vault) 技術輔助追緝偵防，並經由遷移式學習 (Transfer Learning) 和主動式學習 (Active Learning) 提升偵防模型之準確率，以因應攻擊手法的多樣性。此外，基於 MITRE ATT&CK 定義之狙殺鏈進行攻擊步驟的推估建模，一來在日誌/流量資料不完整的情況或規則無法發揮預期效用時，可透過本技術進行人工智慧輔助推估。二來事先定義/訓練 (Pre-define/Pre-train) 的狙殺鏈模型，其攻擊組合(例如：新增、刪除及複數個攻擊行為)或順序偏差像是攻擊行為序列偏移或含有雜質，舊有規則無法發揮預期效用時，亦可透過本技術進行人工智慧輔助推估。

本案即以第三方協助驗證的角度，模擬符合ATT&CK框架之攻擊狙殺鏈攻手法(如：APT40、APT41 等) ，設計資料集和狙殺鏈中網路相關攻擊手法之偵測規則，透過本案提供的攻擊樣本，我方可進行人工智慧偵防模型的訓練、測試與實驗，以及偵測規則的驗證。

二、 計畫目標

本計畫的主要目標可分為四個部分：

1. 建置仿真場域模擬環境

   設計的攻擊狙殺鏈 (Cyber Kill Chain) 進行仿真場域之樣本資料生成與模擬，藉由多階層多面向之監控與日誌稽核部署所取得的日誌與行為軌跡，即可取得內網流量、外網流量、伺服器服務、本機運行等因攻擊鏈施作所產生的威脅軌跡，產出企業網路模擬環境中的正常與威脅異常特徵模式。

2. 蒐集網路流量、應用層日誌等攻擊手法資料樣本

   蒐集仿真環境正常運作流量、被攻擊網路流量及應用層日誌資料，標記特徵值且解決格式不一致和環境差異等問題，確保後續分析結果之可靠性。

3.攻擊狙殺鏈設計和施作腳本規劃

建立威脅監控端網路仿真環境，透過 MITRE ATT&CK 框架描述企業內攻擊的複雜性，可用於企業進行攻防演練，以協助本案人工智慧偵防模型之訓練與測試。攻擊狙殺鏈 (Cyber Kill Chain) 入侵設計應包含攻擊手法、攻擊技術工具、攻擊程序 (Tactics, Techniques, and Procedures, TTPs)。

4.攻擊狙殺鏈相關之偵測特徵生成

研製並彙整攻擊鏈中與網路或主機相關之攻擊手法、步驟、工具及 TTP（Techniques, Tactics, Procedures）等，包含可輔助偵測識別之攻擊特徵與樣態（如：Traffic Pattern、System Log Pattern），須提供相關之原始資料（如：PCAP封包檔、受害系統日誌等）、攻擊標記（TTP）及攻擊特徵與樣態。

三、 計畫範圍

本計畫範圍即以第三方檢測的角度，模擬設計至少3種駭客攻擊手法，透過實際場域樣本、測試樣本與實驗數據，分析與評估本計畫人工智慧偵防模組的穩定性及有效性，主要研究範圍說明如下：

1.網路攻擊鏈設計與施作腳本規劃

設計攻擊鏈腳本，能夠針對過去出現的威脅情境分析，建議參考MITRE提出的ATT&CK框架，將入侵期間可能發生的情況，做出網路攻擊鏈(Cyber Kill Chain)入侵手法共通性描述：

- 基礎於以下入侵階段進行網路攻擊鏈設計與腳本設計：入侵初期(Initial Access)、執行(Execution)、持續性潛伏(Persistence)、權限提升(Privilege Escalation)、防禦迴避(Defense Evasion)、憑證存取(Credential Access)、情資探索與收集(Discovery & Collection)、橫向擴散(Lateral Movement)、命令控制(Command and Control)、資料盜取(Exfiltration)等。
- 統整各個網路攻擊鏈之關鍵入侵階段，描述說明並設計對應腳本，例如：以橫向擴散為關鍵階段，設計APT40、APT41等不同攻擊鏈之模擬腳本。
- 基於人工智慧偵防模組可偵測攻擊步驟，使用框架呈現攻擊者所使用的策略與手法，建立標準化、架構化的資訊，有一致的過程來確定威脅的階段，檢視網路安全事件的全貌。

2.執行AI分析模型評測機制，做為技術商品化的參考依據

- 設計攻擊鏈的每一個階段所使用的手法與工具技術，必須在企業網路模擬環境或威脅監控端網路模擬環境中有一個鑑識點，並同時充分說明鑑識點的取證位置、如何運用工具或其他方法取證、取證之內容與惡意行為的相關性。

- 根據樣本資料之資料來源、攻擊階段與攻擊類型探討威脅偵測AI分析模組，即時觸發警示網路安全事件全貌的涵蓋率，評估AI分析模組的穩定性及有效性。
- 透過鑑識點資訊來評估AI模組的偵測效率，並依據評估結果循環修正AI分析模組。

四、 預期成果

本計畫的預期成果應包含以下：

1.驗證演算法模組並應用實際場域之期中及期末報告

2.駭客模擬之攻擊情境與腳本，包含：

- 攻擊情境：建立各攻擊階段技法的結構化參照矩陣(如：MITRE ATT&CK 框架)，藉此描繪攻擊者的手法與行為，透過一致性過程確定威脅階段之說明文件。
- 腳本設計：規劃偵測類別、偵測能力與覆蓋範圍之腳本設計，內容須含偵測描述所提供的連結及記錄測試實況截圖之說明文件。

3.攻擊軌跡資料樣本集。

- 提供於評測過程中，完整攻擊軌跡標示資料樣本集。
- 包括執行攻擊過程之完整網路封包、應用程式日誌及主機日誌等相關紀錄資料。

4.建立可解釋性評測報告

- 執行攻擊情境與腳本，從技術的角度去截圖描述過程中的觀察（包含攻擊時間點及攻擊結果的截圖），應給予每個階段已定義的偵測類別標籤(Detection Categories)，如：以一致性指標說明 AI 分析模組防禦能量。

五、 執行方式

本計畫預計將結合學界在理論面以及本會在資安偵防技術研發實務經驗，透過雙方合作討論方式來進行，本計畫亦需提供教育訓練及經驗分享機制，藉此增進本會研究人員的專業能力，以提升本合作案成果之效益，相關執行方式步驟如下：

1.建置攻擊模擬環境並蒐集狙殺鏈威脅行為之軌跡

依企業場域之內外部網路拓撲架構，設計建置攻擊狙殺鏈（Cyber Kill Chain）模擬環境，在環境中的端點及網路層蒐集內外網流量、日誌資料等，並與正常環境所產生的軌跡進行比較，作為後續分析狙殺鏈威脅行為樣本。

2.攻擊狙殺鏈腳本實作及威脅行為特徵說明

依 APT40、APT41 之威脅情資，參照 MITRE ATT&CK 框架所定義的攻擊手法、戰術及步驟 （Tactics, Techniques, and Procedures, TTPs），設計實作狙

殺鏈攻擊腳本，並依 TTPs 說明對應的威脅行為及特徵，作為後續威脅分析及偵測規則之參考。

六、 計畫期程及預估計畫總經費

計畫執行區間：111 年 01 月 01 日 至 111 年 12 月 15 日

總經費：1,000,000元

七、 驗收標準(含教育訓練)

1. 期中驗收報告預計於 111 年 09 月 10 日交付，內容包含
   - 攻擊模擬環境規劃及環境建置
     i.含攻擊模擬環境之網路拓撲、架構、系統版本等說明文件
     ii.依上述攻擊模擬環境，提供內外網流量、日誌資料監控之部署建議
   - 攻擊狙殺鏈情境設計文件
     iii.含 APT40、APT41 預計實作腳本內容（TTPs 說明列表）
2. 期末驗收報告預計於 111 年 12 月 10 日交付，內容包含
   - 攻擊狙殺鏈實作文件
     i.以期中預計實作的 APT40、APT41 攻擊腳本內容，提供各項 TTPs 實作方法及說明
     ii.提供 APT40、APT41 攻擊實作結果，包含時間點、TTPs、工具、執行檔名稱、攻擊結果的截圖等
3. 期末驗收資料集預計於 111 年 12 月 10 日交付，內容包含
   - 正常運作流量、被攻擊網路流量及系統日誌資料樣本集（原始檔案）
   - 執行 APT40、APT41 攻擊狙殺鏈所需的攻擊腳本、工具及程式
4. 期末教育訓練預計於 111 年 12 月 10 日舉辦，內容包含
   - 攻擊手法之腳本工具操作演練
5. 進度討論會議：每月召開一次進度研討會議

八、 技術能力需求

1. 資訊安全相關背景：須瞭解作業系統核心底層運作原理、惡意程式偵防技術與資安滲透測試等各項技術，並熟悉相關資安分析工具與虛擬化平台的使用，方能掌控本計畫研發所需核心技術。