視覺化系統事件日誌攻擊調查

楊明翊
國立臺灣科技大學電機工程學系
M11207517@mail.ntust.edu.tw

黃意婷
國立臺灣科技大學電機工程學系
ythuang@mail.ntust.edu.tw

摘要

傳統的主機式入侵檢測系統透過系統日誌進行分析與鑑識，因日誌內容數量龐大，不易資安專家人工分析與進行關聯。因此本研究提出一個互動式攻擊視覺化平台－Cloversmith，用於協助資安分析師調查系統日誌。透過使用者研究驗證平台有效性，結果顯示 TTP Attack Path 模式能有效提升攻擊事件的發現能力。本研究的貢獻為，提出以攻擊場景為核心的可視化平台。從結合 MITRE ATT&CK TTP 自動化生成更高層次攻擊場景，並在互動介面中提供多種協助攻擊調查的功能，目的在幫助資安分析師從大量的資訊中，快速理解攻擊的完整脈絡。

關鍵詞：數位鑑識、進階持續性威脅、攻擊調查、可視化、多階段攻擊。

Abstract

Traditional host-based intrusion detection systems analyze system logs, but the massive volume of data makes manual analysis and correlation difficult for security experts. This study presents Cloversmith, an interactive attack-visualization platform that assists analysts in investigating system logs. A user study validates its effectiveness: the TTP Attack Path mode effectively improves the discovery of attack events. Our contribution is a visualization platform centered on attack scenarios that integrates MITRE ATT&CK TTPs to automatically construct higher-level attack scenarios and provides multiple investigation aids in an interactive interface, enabling analysts to quickly grasp the complete context of attacks amid large volumes of information.

Keywords: MITRE ATT&CK, Digital Forensics, Advanced Persistent Threat, Visualization, Attack Investigation.

1. 前言

在網路普及的時代，資訊安全扮演相當重要的角色。許多公家機關以及企業正面臨多樣的攻擊，從傳統的惡意程式到進階持續性威脅（Advanced Persistent Threat）。例如2025年6月，資安業者 Seqrite 揭露同時針對臺灣與日本等中國東部海域國家的 APT 攻擊行動 Swan Vector，藉由假的履歷表、財務文件作為誘餌來接觸受害者[1]。為了調查攻擊發生的來源，許多資安人員嘗試分析系統日誌（Audit log）。然而，如何從大量的日誌中，有效率地萃取出有價值的攻擊情報，已成為當前資安領域面臨的挑戰。

儘管有許多日誌分析與威脅偵測的方法[2], [3]，但資安分析師仍面臨著許多問題。首先是攻擊場景重建的高耗時與高人力成本。當攻擊警報發生，資安專家須針對大量的警報做關聯，嘗試還原並分析攻擊情境。其次，當我們利用現有的工具建立溯源圖時，容易面臨依賴性爆炸的問題。最後是現有的可視化工具存在著解釋性不足的問題，M²ASK[4] 提到有些方法僅以攻擊生命週期的階段來標記事件（如偵察、橫向移動、資料外洩），導致攻擊描述無法聚焦於具體行為。

本研究的目的是將已標記攻擊的日誌事件自動化產生攻擊場景圖，並結合 MITRE ATT&CK TTP[5] 摘要攻擊場景以提供語意標籤，幫助資安分析師分析與關連攻擊事件發生的脈絡。

MITRE ATT&CK 是由 MITRE 組織所建立的威脅知識庫，TTP 定義了攻擊者的策略（Tactics）、技術（Techniques）與詳細過程（Procedures）。相較於僅以攻擊生命週期的階段（如：橫向移動、資料外洩）來標記事件，這種做法過於籠統，無法揭露具體的攻擊手法。而 ATT&CK TTP 的優勢在於，它能以具體的技術描述攻擊行為，且不只提供字面描述，ATT&CK 更對每一項 TTP 提供了常見作法、使用工具、可觀測證據與資料來源等詳細情資，提升了攻擊事件的可解釋性。

2. 文獻探討

為了檢測與分析進階持續性威脅（APT），基於稽核日誌的研究分為三類：攻擊情境重建、摘要攻擊情境、使用者行為特徵分析。

2.1 攻擊情境重建

RapSheet[6]導入了戰術溯源圖（Tactical Provenance Graph, TPG）的概念，針對端點偵測與回應（EDR）系統產生的警報進行因果關聯分析，然而，其成果並未提供面向分析師的互動式視覺分析。同樣地，HOLMES[7]提出了高階場景圖（High-level Scenario Graph, HSG）的概念，將低階的稽核日誌流映射至與 APT 生命週期各階段，更偏向偵測與告警摘要，較少支援分析師在視覺介面中對實體互動細節進行逐步探索。M²ASK[4]則展示了另一種基於攻擊關聯的方法，透過關聯分析來建立多步驟的攻擊場景，重心在 TTP 的序列關聯而非可操作的溯源圖視覺化；其輸出較少提供結合共享實體的互動關聯，需要額外的視覺分析功能來落實人員調查流程。

2.2 摘要攻擊情境

WATSON[8]提出透過聚合上下文語義來從稽核日誌中抽象出高層次的行為。它使用基於翻譯

的嵌入模型（ TransE）來學習稽核日誌中的語義表示，並進行聚類。挑戰在於，聚類方法可能會將表面相似但本質不同的正常行為與異常行為歸為一類，影響檢測的精確度。

2.3 使用者行為特徵分析

早期研究如 Salem[9]等人從命令列的歷史中萃取多種特徵，如指令與參數使用頻率、打字錯誤率等，為每位使用者建模來識別內部威脅。Tuor 等人[10]將資料擴展至網路流量與系統日誌，蒐集工作時段、存取頻率等特徵，揭露可疑行為[10]。整體而言，行為特徵分析能在攻擊早期偵測偏離常態的操作，補足僅依單一事件判斷的不足。

3. 方法

圖 1介紹 Cloversmith 的系統流程以及兩種分析模式下的功能。系統以已標記的稽核日誌為輸入，Parser 由日誌擷取事件欄位：srcNode、dstNode、relation、timestamp、label，並建立溯源圖。視覺化分析在兩種模式下進行：TTP Attack Path 依共享實體與時序串聯形成攻擊鏈；System Resource Analysis 呈現完整溯源圖來支援細節回溯。

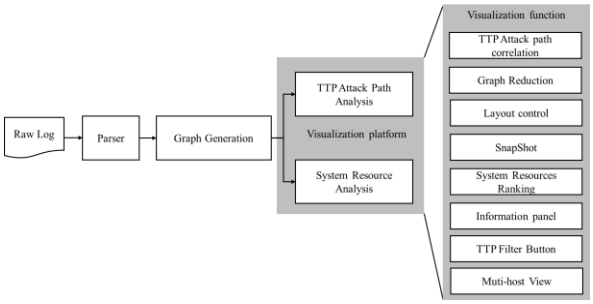

圖 1 Cloversmith 系統流程圖。

3.1 前處理

3.1.1 Raw Log

事件日誌紀錄 Process 與系統資源之間的互動。由 Procmon 或 Sysmon 所收集的日誌能用於安全監控和事後取證。稽核日誌中一筆紀錄稱為日誌事件（event），包含事件來源、類型、時間戳記與 Process ID，如**圖 2** 所示，Discord.exe （PID 8672）正在系統上執行，並開啟和查詢指定的鍵值。

Time ...	Process Na...	PID	Operation	Path
下午 02...	Discord.exe	8672	RegOpenKey	HKCU\Software\Valve\Steam\Apps\1097150
下午 02...	Discord.exe	8672	RegQueryValue	HKCU\Software\Valve\Steam\Apps\1097150\Installed
下午 02...	Discord.exe	8672	RegCloseKey	HKCU\Software\Valve\Steam\Apps\1097150

圖 2 Procmon 中 Raw log 範例

3.1.2 Parser

在生成攻擊圖之前，系統透過 **Parser** 階段從原始日誌事件中萃取關鍵欄位資訊，並移除冗餘系統資訊。如**圖 3** 所示，我們定義了兩種類型的節點：來源節點（srcNode）與目標節點（dstNode）。其中，節點包含檔案（File）、Process、註冊表（Registry）與網路（Network）等系統資源。節點之間的關係則為邊（黑色箭頭），用來描述節點之間的交互關係，並附帶事件發生的時間戳記與標記（label）。

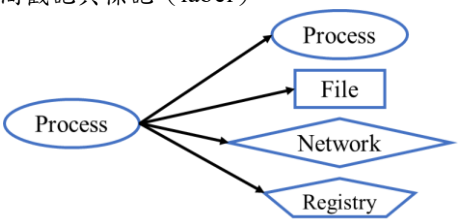

圖 3 節點類型與邊的定義

3.1.3 Graph Generation

Parser 階段後，Cloversmith 會進入 Graph Generation 階段。首先，使用 NetworkX[11]將事件轉換為有向圖（如**圖 4**），並將結果以 .pkl 格式儲存用於後續的載入。最後格式化為 Cytoscape.js 可讀取的結構，作為前端互動式可視化界面的輸入。

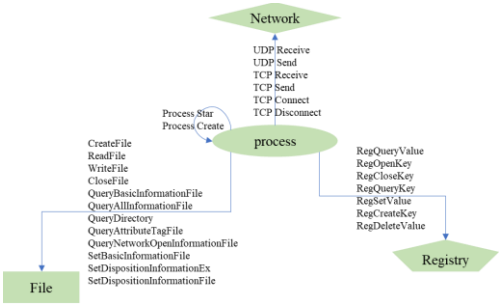

圖 4 有向圖示例

3.1.4 TTP 攻擊路徑關聯（TTP Attack Path Correlation）

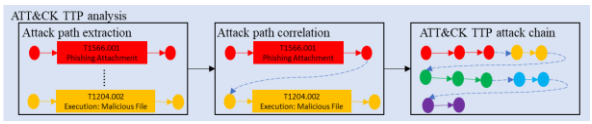

圖 5 TTP 攻擊路徑關聯流程示意圖

為了串聯日誌中標記為 ATT&CK TTP 的事件，Cloversmith 依系統實體的共享關係串接成一條完整的攻擊鏈，協助分析人員觀察攻擊過程。如**圖 5** 所示。首先是攻擊路徑萃（Attack Path Extraction），系統從完整的溯源圖，篩選出帶有 TTP 標記的事件，讓後續關聯專注在攻擊相關部分。攻擊事件關聯 （Attack Path Correlation）此步驟系統會判斷不同攻擊事件之間是否共享同一個系統實體（如相同的檔案）。若存在共享實體，則視為可建立的關聯。此方法近似於 HOLMES[7] 透過資訊流的依賴串接高層次場景圖（HSG）、以及 M²ASK[4]透

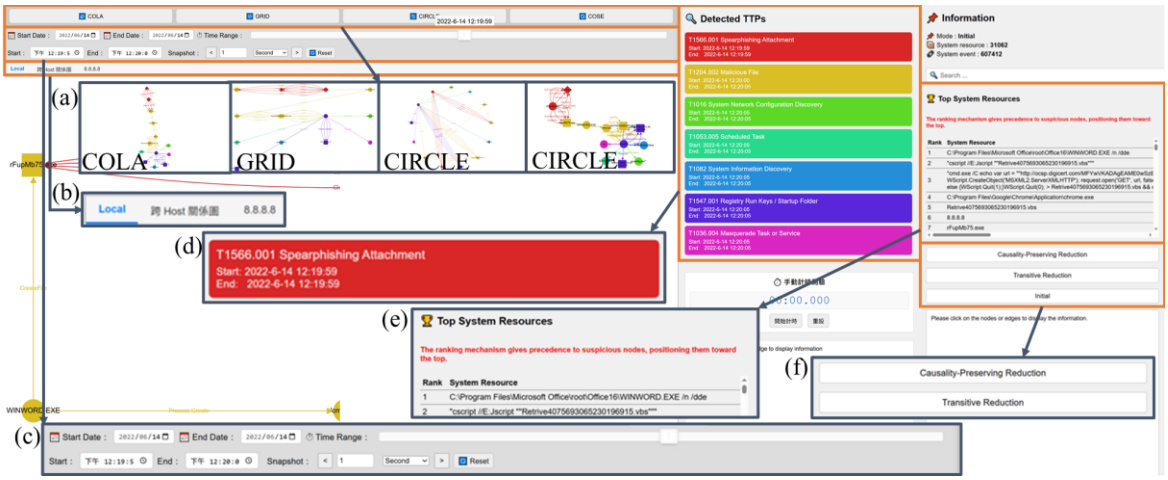

圖 6 Cloversmith 系統介面

過共享節點合併攻擊序列，皆是利用攻擊在系統中接觸的共同實體建立事件間的連結。完整攻擊鏈（ATT&CK TTP Attack Chain）為攻擊事件關聯建立完成後，Cloversmith 將所有關聯的 TTP 事件依照時間排序，生成一條攻擊鏈。

3.2 攻擊可視化工具

Cloversmith 以日誌事件作為輸入，分析人員可依需求選擇不同模式進行視覺化探索。TTP Attack Path Analysis 模式聚焦於 MITRE ATT&CK TTP 的關聯與攻擊路徑追蹤；而 System Resource Analysis 模式著重於系統資源的互動，觀察不同實體間的關係與關鍵節點。為方便理解兩種模式與功能的關聯性，本研究將可視化功能整理如**表 1**。

表 1 可視化平台功能對照表

功能模組	TTP Attack Path Analysis	System Resource Analysis
Graph Reduction	✗	✓
Layout Control	✓	✓
Snapshot	✓	✓
System Resources Ranking	✗	✓
Information Panel	✓	✓
TTP Filter Button	✓	✗
Multi-host View	✓	✗

3.2.1 系統資源排序（System Resources Ranking）

在攻擊調查中，大型攻擊圖可能包含數百甚至數千個系統實體與事件。資安分析師需耗費大量時間檢視，容易錯過攻擊的核心位置。**圖 6（e）**區塊顯示 Cloversmith 對節點的評分與排名，引導資安分析師鎖定相對可疑的系統實體展開調查。

此功能的排序核心為一套評分演算法，我們採用度中心性（Degree Centrality）作為基礎分數計算依據，因其能以極低計算成本即時反映節點的活躍度。此外，我們將攻擊標記（TTP 標籤）作為額外加權，確保低活躍度但高威脅性的節點不會被忽略。整體流程如**演算法**，分為兩階段：

1. 計算每個節點的基礎分數並檢測是否為攻擊節點。
2. 正規化分數並加權攻擊節點後排序。

演算法 1 System Resource Scoring and Ranking

Algorithm 1 System Resource Scoring and Ranking Algorithm

Input: Graph $G = (V, E)$
Output: Ranked list of nodes L_{ranked}
$node\_info\_list \leftarrow$ new List()
$max\_base\_score \leftarrow 0$
for each node n in V **do**
  $base\_score \leftarrow \text{in\_degree}(n) + \text{out\_degree}(n)$
  $max\_base\_score \leftarrow \max(max\_base\_score, base\_score)$
  $is\_attack \leftarrow$ any edge e adjacent to n has non-benign label
  $node\_info\_list.add(\{node : n, base : base\_score, attack : is\_attack\})$
end for
for each info in $node\_info\_list$ **do**
  $normalized\_score \leftarrow info.base / \max(1, max\_base\_score)$
  if $info.attack$ is True **then**
    $info.final\_score \leftarrow normalized\_score + 1$
  else
    $info.final\_score \leftarrow normalized\_score$
  end if
end for
$L_{ranked} \leftarrow$ sort $node\_info\_list$ by $final\_score$ descending
return L_{ranked}

3.2.2 可視化分析介面

為協助資安分析師應對複雜的攻擊調查，Cloversmith 提供整合多種分析功能的可視化介面（如**圖 6**）。此介面將原始系統日誌轉化為可操作的分析環境。透過一系列輔助功能，分析師得以多角度探索。以下將詳述各項主要功能。

首先，因稽核日誌生成的溯源圖節點與邊數量龐大，我們設計圖形簡化（Graph Reduction）功能。Cloversmith 提供兩種圖形簡化演算法（如

圖 6（f))，讓分析人員根據當前調查需求即時切換。第一種演算法 Causality-Preserving Reduction（CPR）[12] 合併重複或冗餘的事件，但在簡化圖形的同時，仍保留所有節點之間完整的因果關係。第二種 Transitive Reduction（TR）[13]僅保留節點之間最直接的依賴關係，呈現最簡潔結構，有助快速理解系統實體互動，具體壓縮效果如**表 2**。

表 2 Graph Reduction 圖簡化效果

	Causality-Preserving Reduction	Transitive Reduction
APT Campaign	壓縮率	壓縮率
Higaisa	85.53%	90.36%
admin338	90.25%	93.77%
APT28	61.74%	77.53%
FIN7	48.57%	81.84%
CobaltGroup	90.09%	93.61%
Gamaredon	74.49%	83.49%
Patchwork	66.95%	74.12%
GorgonGroup	74.23%	89.42%

其次，在不同的分析情境下，為了避免因單一視角所產生的分析盲點。因此，Cloversmith 提供了版面控制 （Layout Control） 功能（如**圖 6（a）**區域所示)，基於 Cytoscape.js 函式庫，允許分析人員切換四種佈局。COLA[14]採用基於約束的力導向演算法，讓關聯緊密的節點能自然聚集。GRID[15]則將節點依照時間順序排列在網格中，特別適合用於快速概覽節點總數與種類，以及尋找攻擊的初始進入點。CIRCLE[15]將所有節點均勻分佈於圓周上，能清晰地展示所有節點間的依賴關係。最後 COSE[16] 提供另一種力導向演算法，能呈現較為緊湊且視覺平衡的效果。

再者，真實的 APT 攻擊，其行為持續時間橫跨數分鐘至數天不等。當時間跨度拉長，攻擊圖中節點與邊的數量會急遽增加且高度密集，使分析人員難以聚焦於特定時間點的具體行為。為解決此問題，Cloversmith 提供時間快照（Snapshot）功能（如**圖 6（c）** 所示)。此功能將完整的攻擊事件切分為多個連續的時間片段，分析人員可以像播放影片一樣，逐段觀察攻擊的演進過程，或直接跳轉至特定時間點，進行細粒度的行為分析。

此外，在大型攻擊場景中，尋找與特定 MITRE ATT&CK TTP 相關的事件，不僅耗時，也極易遺漏關鍵線索。因此，平台提供了 TTP 篩選按鈕 （TTP Filter Button） 功能。如**圖 6（d）** 區塊所示，系統會將日誌中偵測到的所有 TTP 彙整成一個列表，並將每個 TTP 項目都設計成一個互動式的篩選按鍵。分析師只需點擊感興趣的 TTP，分析介面便會立即篩選並顯示與該 TTP 相關的所有節點與事件，實現對特定攻擊手法的分析。

最後，APT 攻擊活動經常涉及橫向移動或與外部惡意 C2 伺服器進行通訊，這使得資安分析師必須在多個主機 IP 或網域之間來回進行探索與取證。為了使跨主機的行為追蹤更加明確與便捷，Cloversmith 在 TTP Attack Path Analysis 模式中提供了多主機視角 （Multi-host View） 功能。如**圖 6（b）** 區塊所示，此功能以頁籤的形式，將涉及的不同 IP 與網域分開呈現，使用者可以在不同主機的視圖之間切換，分析跨設備的攻擊流程。

4. 實驗

本研究實驗設計的目的為評估 Cloversmith，並針對以下研究問題進行驗證：

- RQ1：在真實 APT 攻擊案例中，使用者能否透過 Cloversmith 理解攻擊全貌並定位惡意事件？
- RQ2：Cloversmith 是否提高攻擊場景的解釋性？

為回答上述問題，我們邀請 10 位有上過資安相關課程的研究生，在 System Resource Analysis 模式與 TTP Attack Path Analysis 模式分別分析了兩個不同攻擊組織發起的 APT 攻擊案例。

4.1 資料集統計分析

表 3 SAGA 資料集中各 APT 攻擊活動的事件統計

APT Campaign	Total Events	Malicious Events	TTPs count
Higaisa	607,416	30	7
APT28	1,203,013	14,137	6
Gamaredon	442,729	59	9

本研究採用公開的 SAGA Dataset Version 2[17]，該資料集包含完整的攻擊標記，透過模擬真實進階持續性威脅（APT）攻擊，收集詳細的系統層級日誌，並提供精確的真實標籤（Ground Truth）。

為評估 Cloversmith 的實用性及真實攻擊案例分析的能力，我們自八個已知 APT 攻擊活動選取攻擊組織 Higaisa 與 Gamaredon 發起的案例於受試者評估系統；APT28 於案例分析。事件規模與惡意事件分佈如所示，三個攻擊活動的事件數量介於44萬（Gamaredon ）至 120萬（APT28）之間。

4.2 實作細節

本研究為受試者設計了兩份表單，用於評估 Cloversmith 的實用性。首先，請受試者在給定入侵節點以及指導語的情況下，使用 System Resource Analysis 與 TTP Attack Path Analysis 模式分析了兩個不同攻擊組織（Higaisa、Gamaredon）發起的 APT 攻擊案例，並填寫發現的可疑節點、可疑事件，以及攻擊描述。

4.3 實驗結果

表 4 受試者在 System Resource Analysis 以及 TTP Attack Path Analysis 進行攻擊調查的表現。

	System Resource Analysis				TTP Attack Path Analysis			
	Node-base		Event-base		Node-base		Event-base	
受試者	precision	recall	precision	recall	precision	recall	precision	recall
No.1	100.00%	33.33%	100.00%	10.00%	100.00%	39.13%	100.00%	11.86%
No.2	100.00%	25.00%	100.00%	6.67%	100.00%	21.74%	100.00%	6.78%
No.3	88.89%	66.67%	100.00%	20.00%	100.00%	82.61%	100.00%	74.58%
No.4	100.00%	58.33%	100.00%	16.67%	100.00%	82.61%	100.00%	28.81%
No.5	100.00%	91.67%	100.00%	33.33%	100.00%	39.13%	100.00%	23.73%
No.6	100.00%	66.67%	100.00%	20.00%	100.00%	100.00%	100.00%	35.59%
No.7	100.00%	25.00%	100.00%	3.33%	100.00%	8.70%	100.00%	1.69%
No.8	0.00%	0.00%	0.00%	0.00%	100.00%	17.39%	100.00%	17.24%
No.9	100.00%	66.67%	100.00%	23.33%	100.00%	52.17%	100.00%	15.25%
No.10	100.00%	41.67%	100.00%	13.33%	100.00%	17.39%	100.00%	5.08%
AVG	88.89%	47.50%	90.00%	14.67%	100.00%	46.09%	100.00%	22.06%

為了評估 Cloversmith 在不同分析模式下的有效性，我們依據表 4 的受試者表現回答 RQ1 與 RQ2。分析過程中使用四項指標來評估使用者任務的表現：TP 代表正確識別的攻擊節點或事件；TN 代表被正確識別的非攻擊項目；FP 代表使用者將非攻擊項誤判為攻擊；而 FN 代表未能找出攻擊。

首先，評估 System Resource Analysis 模式在 Higaisa 攻擊案例調查中的表現。結果顯示此模式可有效支援攻擊調查。多數受試者成功透過該平台找出可疑的攻擊節點與事件，且誤報率（FP）極低，代表使用者能精確辨識威脅，不易將正常行為誤判為惡意活動。然而召回率（Recall）仍有提升空間，使用者雖能精確鎖定部分威脅，但未能找出所有惡意活動（FN）。數據統計顯示，此模式在節點分析（Node-base）的平均精確度為 88.89%、召回率 47.50%；事件分析（Event-base），平均精確度則為 90.00%、召回率14.67%。

接著，分析 TTP Attack Path Analysis 模式的表現並與前者進行比較。由於此模式的設計僅呈現經 TTP 標記的攻擊事件，其精確度達到 100%屬於預期現象。關鍵差異在於事件召回率：此模式下以事件為基礎的召回率為 22.06%，顯著高於 System Resource Analysis 模式的 14.67%。綜合結果表明 TTP Attack Path Analysis 透過高層次的攻擊鏈敘事，增強使用者對攻擊事件層級的理解與發現能力；而 System Resource Analysis 則更適合深入的節點層級鑑識分析。最後如**圖 7**所示，受試者對系統滿足攻擊調查需求進行 Likert 量表評估。多數給予 4 或 5 分肯定，顯示 Cloversmith 已能有效支援攻擊調查。少部分受試者僅給予 3 分，反映該系統雖具備實務應用價值，仍存在進一步改進空間。

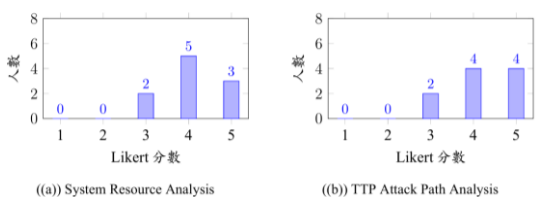

圖 7系統功能是否足以滿足攻擊調查需求

4.4 案例分析

本章節評估使用者是否能利用 Cloversmith 進行攻擊調查。本研究以 SAGA 資料集中的一筆模擬 APT28 攻擊案例進行分析。**圖 8**描述這起由 APT28 攻擊組織發起的攻擊[18]。攻擊者濫用 CVE-2023-3883 取得目標系統的初始立足點。

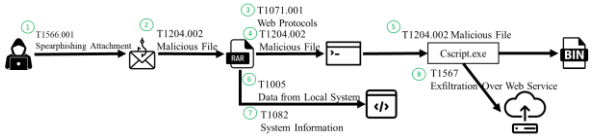

圖 8 APT28 攻擊流程

首先利用 Cloversmith 系統的 System Resource Analysis 功能，快速知道攻擊發生時與哪些 process 有關聯，並利用 System Resources Ranking 了解哪些系統資源是需要關注的，如**圖 9**所示。

為了能夠了解具體攻擊發生的流程以及運用了哪些攻擊手法，接續切換使用 TTP Attack Path 功能。如**圖 10**所示，首先點選紅色最先出現的 TTP(Phishing: Spearphishing Attachment），隨後點選 GRID 排版，讓節點依照時間由左至右由上至下排列。最終可以知道攻擊的起點發生在 firefox.exe，並且攻擊手法是 Spearphishing Attachment。

最後觀察 ATT&CK TTP T1567 Exfiltration Over Web Service，如**圖 11**所示，我們得知具體連接的 IP 以及被竊取的資料。這驗證了我們最初的攻擊場景描述，攻擊的最終目的是竊取資料。

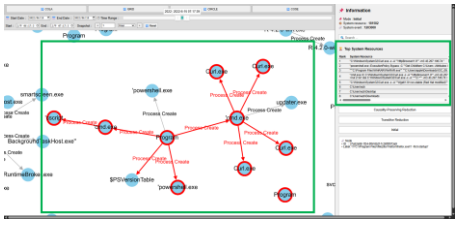

圖 9 System Resource Analysis 平台展示 APT28 攻擊相關結點

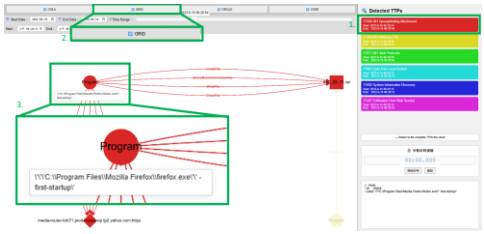

圖 10 利用 TTP Attack Path 平台尋找最終被竊取的資料以及流向

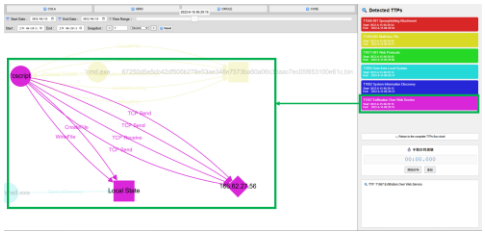

圖 11 利用 TTP Attack Path 平台尋找最終被竊取的資料以及流向

5. 結論與後續工作

本研究針對 APT 攻擊調查的困難，提出一套結合 MITRE ATT&CK 的可視化平台，協助資安分析師還原攻擊路徑與理解攻擊事件。

可視化平台除分析攻擊場景，也提供系統環境的日誌事件，並得以在不同拓樸關係視角檢視攻擊。而兩種模式交互使用可使資安分析師發現可能與攻擊相關的潛在威脅。Cloversmith 仰賴攻擊偵測的精確度，以避免冗餘的事件影響分析。

因成本考量，本研究未與現有工具如 ELK Stack、Splunk、Security Onion 等進行比較。此外，部分商用系統已結合大型語言模型，能將攻擊場景文字化描述，Cloversmith 尚未引入大型語言模型，無法產生文字描述攻擊發生的經過。

6. 致謝

本研究成果承蒙國科會計畫編號：112-2222-E-011-011-MY2 與 114-2634-F-001-001 -MBK 的支持。

參考文獻

[1] 周峻佑, “APT 攻擊者入侵東亞企業！駭客偽裝履歷、財務文件投放攻擊軟體.” Accessed: July 18, 2025. [Online]. Available: https://www.ithome.com.tw/news/169788

[2] A. Alsaheel *et al.*, “ATLAS: A Sequence-based Learning Approach for Attack Investigation,” in *30th USENIX Security Symposium (USENIX Security 21)*, USENIX Association, Aug. 2021, pp. 3005–3022. [Online]. Available: https://www.usenix.org/conference/usenixsecurity21/presentation/alsaheel

[3] H. Ding, J. Zhai, Y. Nan, and S. Ma, “AIRTAG: Towards Automated Attack Investigation by Unsupervised Learning with Log Texts,” in *32nd USENIX Security Symposium (USENIX Security 23)*, Anaheim, CA: USENIX Association, Aug. 2023, pp. 373–390. [Online]. Available: https://www.usenix.org/conference/usenixsecurity23/presentation/ding-hailun-airtag

[4] Q. Meng, N. Oo, Y. Jiang, H. W. Lim, and B. Sikdar, “Poster: M2ASK: A Correlation-Based Multi-Step Attack Scenario Detection Framework Using MITRE ATT&CK Mapping,” in *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, in CCS ’24. New York, NY, USA: Association for Computing Machinery, 2024, pp. 4979–4981. doi: 10.1145/3658644.3691392.

[5] MITRE, “MITRE ATT&CK® Framework.” 2015. [Online]. Available: https://attack.mitre.org/

[6] W. U. Hassan, A. Bates, and D. Marino, “Tactical Provenance Analysis for Endpoint Detection and Response Systems,” in *2020 IEEE Symposium on Security and Privacy (SP)*, 2020, pp. 1172–1189. doi: 10.1109/SP40000.2020.00096.

[7] S. M. Milajerdi, R. Gjomemo, B. Eshete, R. Sekar, and V. N. Venkatakrishnan, “HOLMES: Real-Time APT Detection through Correlation of Suspicious Information Flows,” in *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, pp. 1137–1152. doi: 10.1109/SP.2019.00026.

[8] J. Zeng, Z. L. Chua, Y. Chen, K. Ji, Z. Liang, and J. Mao, “WATSON: Abstracting Behaviors from Audit Logs via Aggregation of Contextual Semantics,” in *Network and Distributed System Security Symposium (NDSS)*, 2021. doi: 10.14722/ndss.2021.24549.

[9] M. B. Salem and S. J. Stolfo, “Leveraging Behavioral Traits for Insider Threat Detection,” in *Proceedings of the 2011 ACM Cloud Computing Security Workshop (CCSW ’11)*, New York, NY, USA: Association for Computing Machinery, 2011, pp. 79–84.

[10] A. R. Tuor, S. F. Kaplan, B. Hutchinson, N. A. Nichols, and S. T. M. H. End, “A Trait-Based Approach for Detecting Insider Threats,” in *2017 IEEE International Conference on Big Data (Big Data)*, Boston, MA, USA: IEEE, 2017, pp. 1162–1171.

[11] A. A. Hagberg, D. A. Schult, and P. J. Swart, “Exploring network structure, dynamics, and function using NetworkX,” *Proc. 7th Python Sci. Conf. SciPy*, vol. 2008, pp. 11–15, 2008.

[12] Z. Xu *et al.*, “High Fidelity Data Reduction for Big Data Security Dependency Analyses,” in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, in CCS ’16. New York, NY, USA: Association for Computing Machinery, 2016, pp. 504–516. doi: 10.1145/2976749.2978378.

[13] A. V. Aho, M. R. Garey, and J. D. Ullman, “The Transitive Reduction of a Directed Graph,” *SIAM J. Comput.*, vol. 1, no. 2, pp. 131–137, 1972.

[14] T. Dwyer, Y. Koren, and K. Marriott, “IPSep-CoLa: An Incremental Procedure for Separation Constraint Layout of Graphs,” *IEEE Trans. Vis. Comput. Graph.*, vol. 12, no. 5, pp. 821–828, 2006, doi: 10.1109/TVCG.2006.156.

[15] M. Franz, C. T. Lopes, G. Huck, Y. Dong, O. Sumer, and G. D. Bader, “Cytoscape.js: a graph theory library for visualisation and analysis.,” *Bioinforma. Oxf. Engl.*, vol. 32, no. 2, pp. 309–311, Jan. 2016, doi: 10.1093/bioinformatics/btv557.

[16] U. Dogrusoz, E. Giral, A. Cetintas, A. Civril, and E. Demir, “A layout algorithm for undirected compound graphs,” *Inf. Sci.*, vol. 179, no. 7, pp. 980–994, 2009, doi: https://doi.org/10.1016/j.ins.2008.11.017.

[17] “SAGA (Security Attack Graph Analysis) Dataset, Version 2.” Accessed: Aug. 21, 2025. [Online]. Available: https://saga-tw.github.io/dataset/v2

[18] DuskRise Threat Intelligence, “CVE-2023-38831 exploited by pro-Russia hacking groups in RU-UA conflict zone for credential harvesting operations.” [Online]. Available: https://www.duskrise.com/2023/10/12/cve-2023-38831-exploited-by-pro-russia-hacking-groups-in-ru-ua-conflict-zone-for-credential-harvesting-operations/