視覺化系統事件日誌攻擊調查

作者: 楊明翊、 黃意婷
國立臺灣科技大學 電機工程所
報告日期: 2025/10/22

2025 臺灣網際網路研討會暨全國計算機會議

研究動機

攻擊場景重建的高耗時與高人力成本。

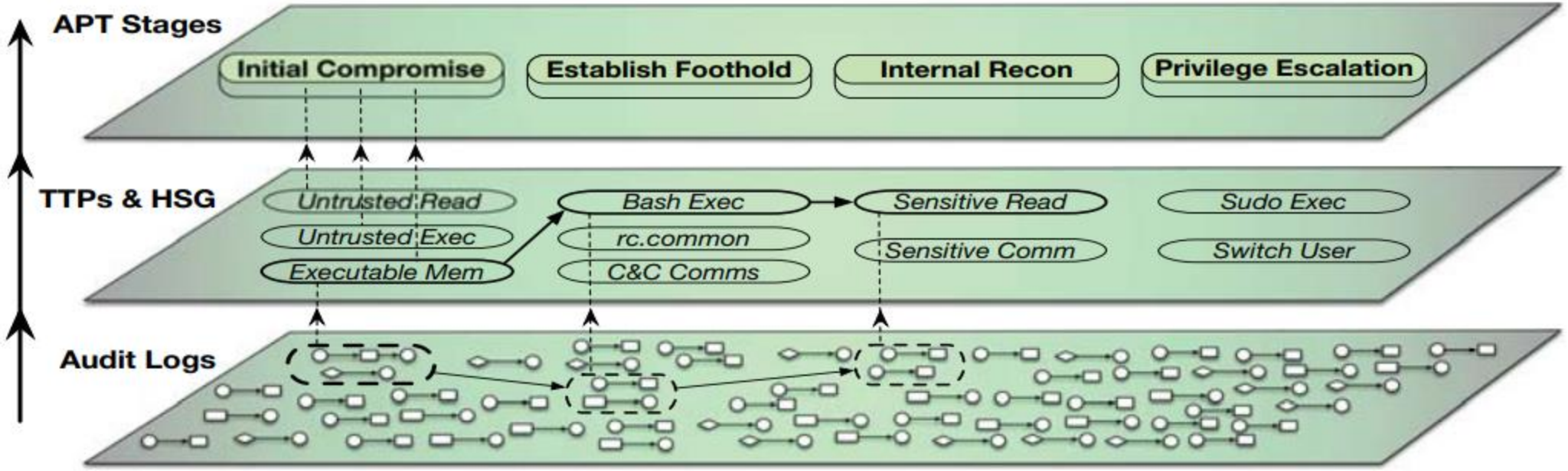
- 當攻擊警報發生時，資安專家必須針對大量的警報做關聯後，嘗試還原整個攻擊情境，並分析攻擊發生的來龍去脈。

- 當我們利用現有的工具，例如 NetworkX[11] 、 Graphviz 建立溯源圖時，容易面臨依賴性爆炸，以及沒有任何操作性。

- M²ASK[4] 提到現今有些攻擊調查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），這會導致攻擊描述過於籠統，缺乏對攻擊具體細節的描述。

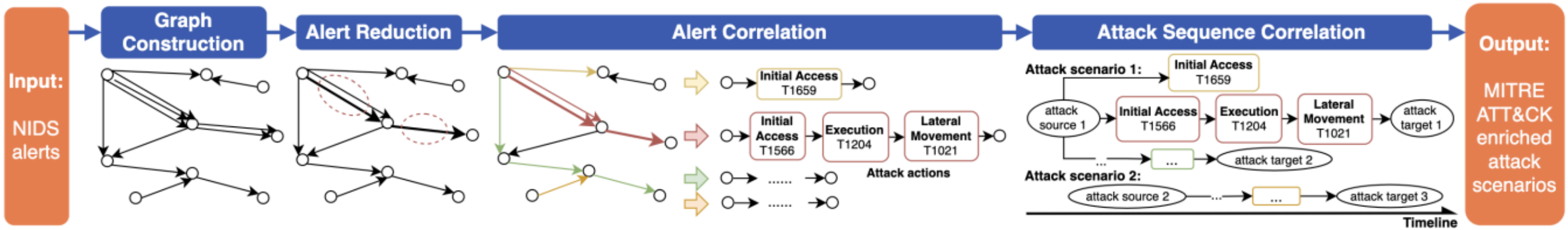
文獻探討

相關文獻	摘要	與本研究的關係	限制與缺點
HOLMES[7]	將稽核日誌建立溯源圖，再抽象成 High-level Scenario Graph (HSG)	從高層次視角分析，應對依賴爆炸的問題。	攻擊偵測依賴規則，導致攻擊調查的效果有限。



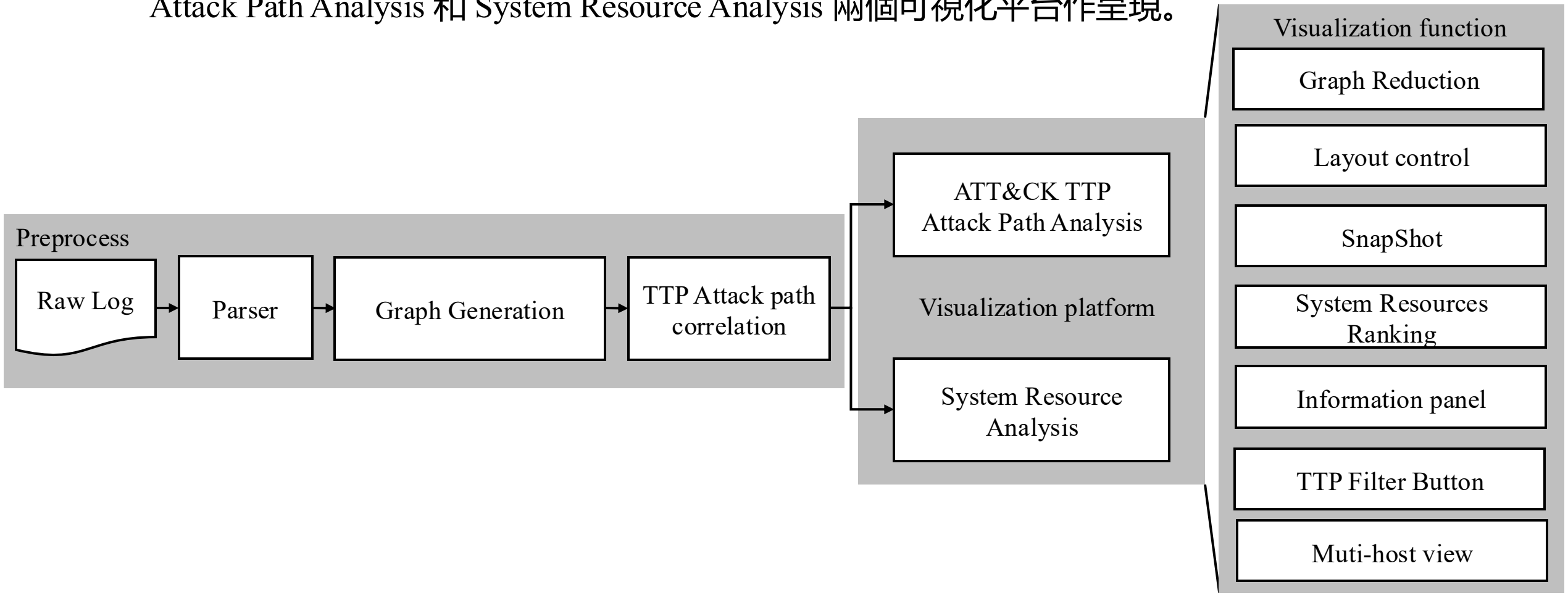
文獻探討

相關文獻	摘要	與本研究的關係	限制與缺點
M²ASK[4]	將 NIDS警報關聯後，透過 MITRE ATT&CK 框架串聯成攻擊情境圖。	多步驟的攻擊關聯，與本研究希望串連多個孤立攻擊路徑的目標相似。	對 NIDS 警報的依賴。

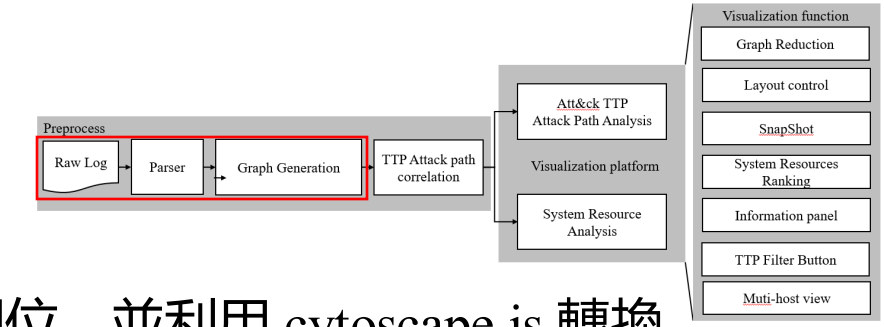


Cloversmith

- 本研究開發了 Cloversmith 攻擊可視化平台，將稽核日至經由前處理後，經由 ATT&CK TTP Attack Path Analysis 和 System Resource Analysis 兩個可視化平台作呈現。

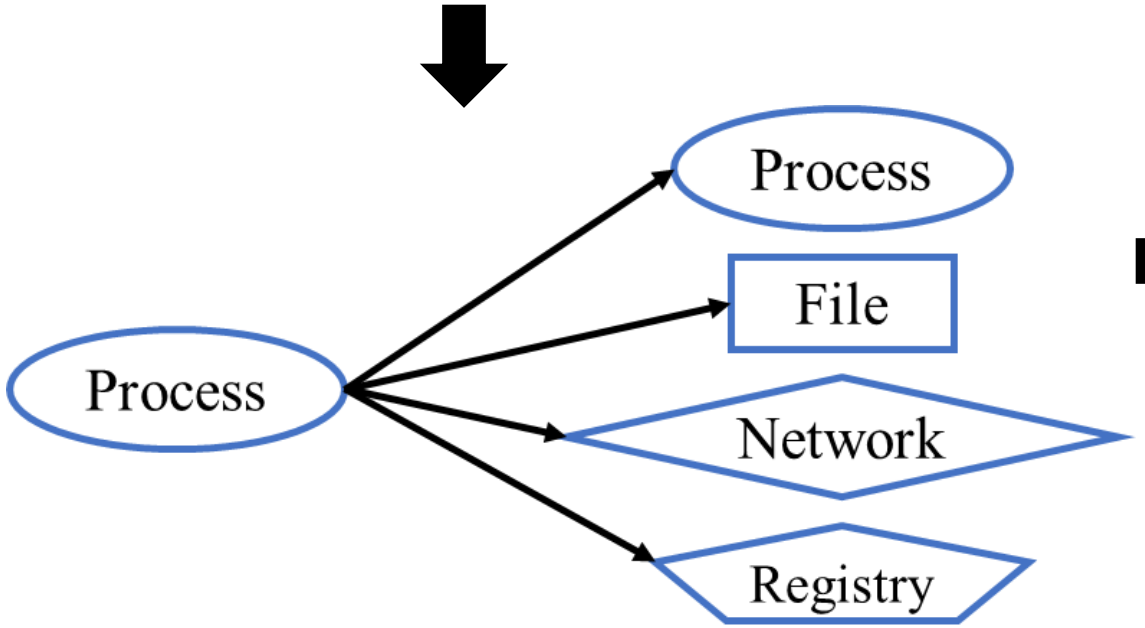


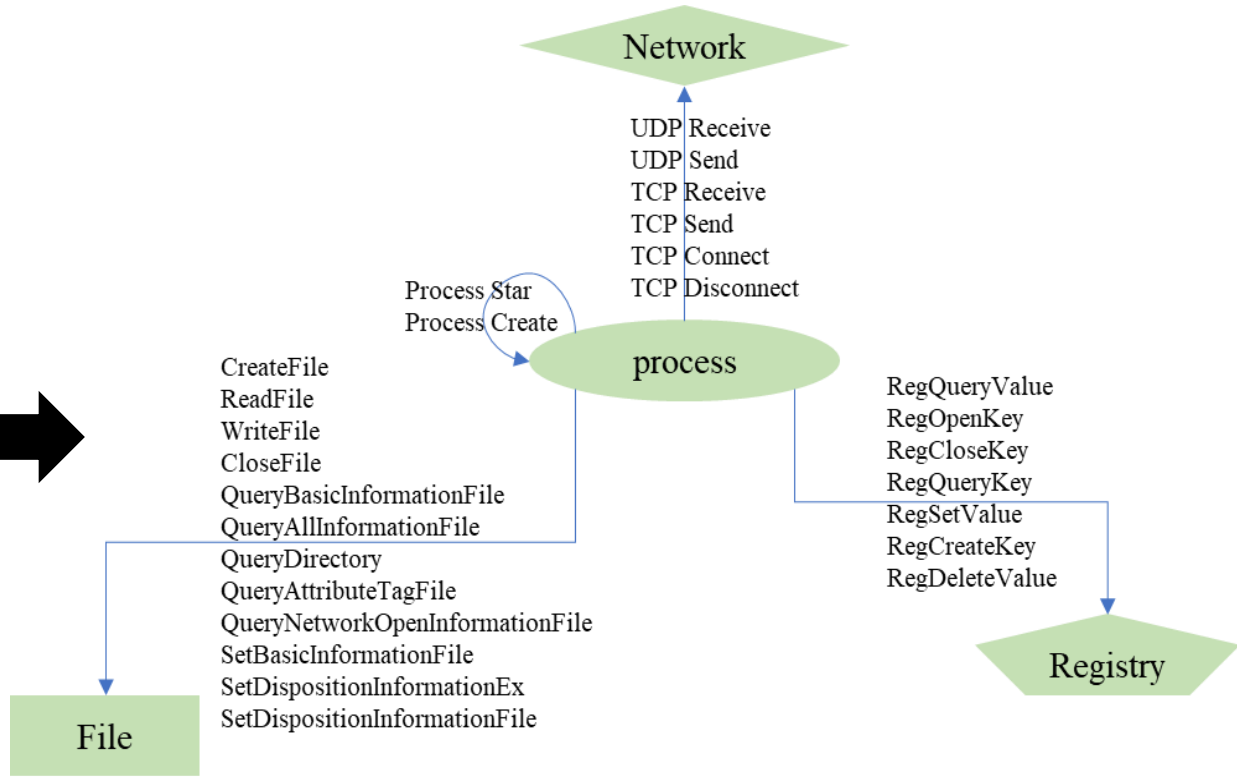
前處理-Preprocess



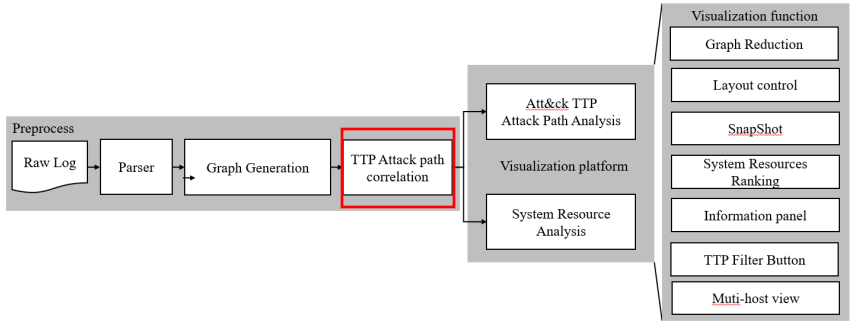
- 首先，從稽核日誌中提取 Process、File、Network、Registry 欄位，並利用 cytoscape.js 轉換為溯源圖。

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
下午 02...	Discord.exe	8672	RegEnumKey	HKCU\Software\Valve\Steam\Apps
下午 02...	Discord.exe	8672	RegQueryKey	HKCU\Software\Valve\Steam\Apps

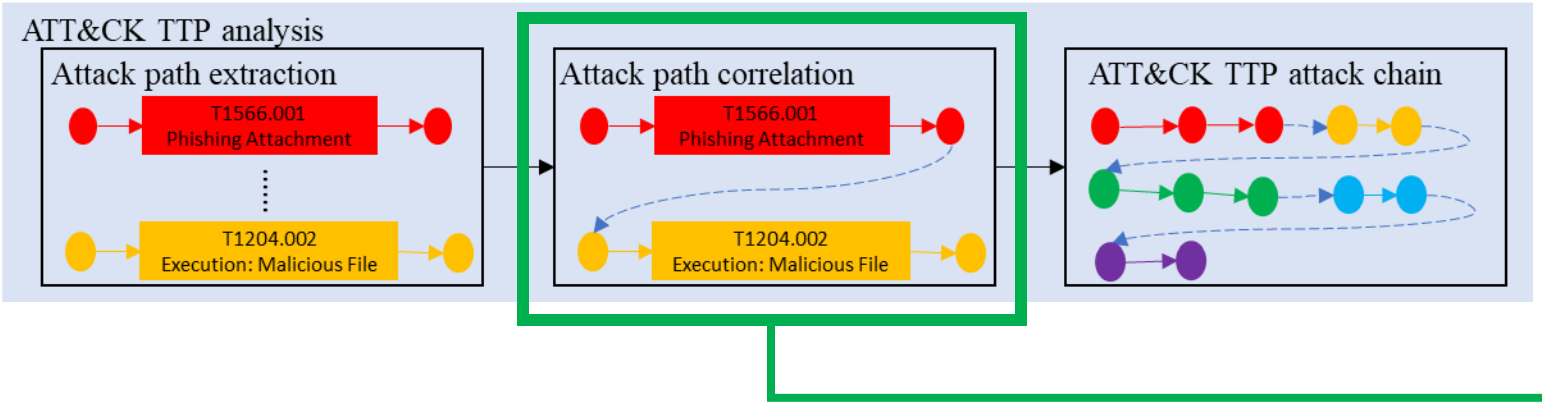


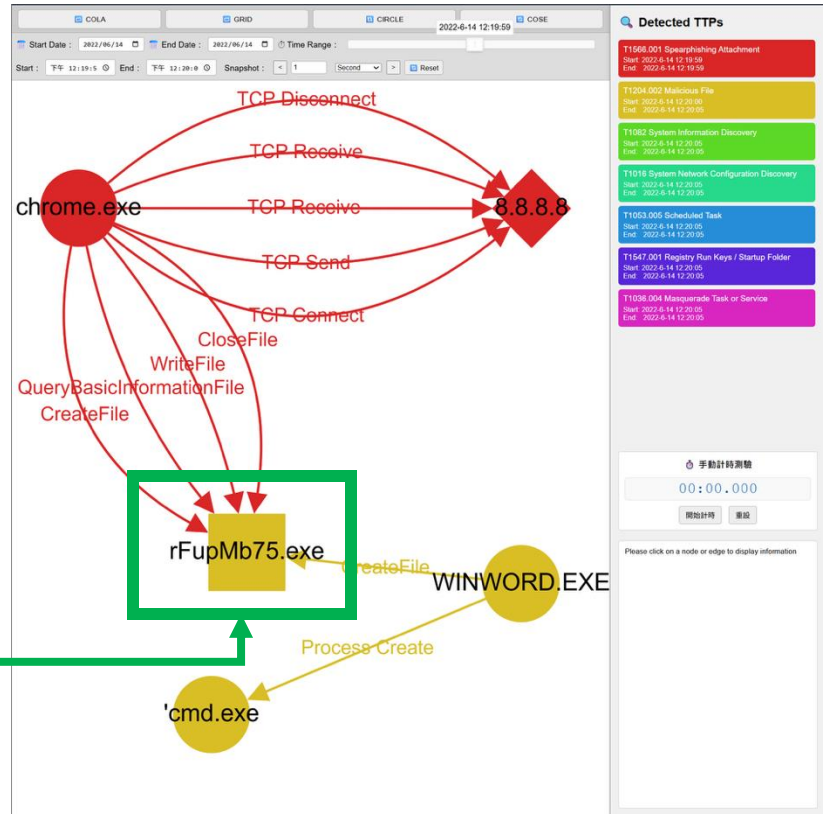


TTP Attack path correlation

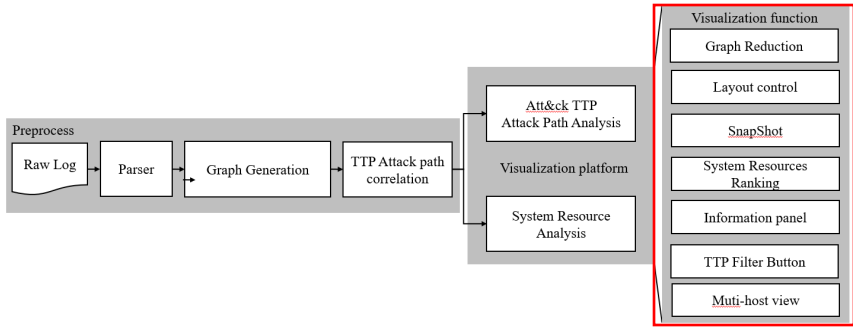


- 此功能是 TTP Attack Path Analysis 模式產生攻擊路徑的方法
  1. 攻擊路徑萃取 (Attack path extraction) 系統首先會從完整的溯源圖中，萃取出所有與 ATT&CK TTP 直接相關的事件與系統實體，形成多個獨立的攻擊片段。
  2. 攻擊關聯 (Attack path correlation) 我們的關聯邏輯是去尋找共享同一個系統實體的攻擊事件。





Visualization function - 攻擊可視化工具

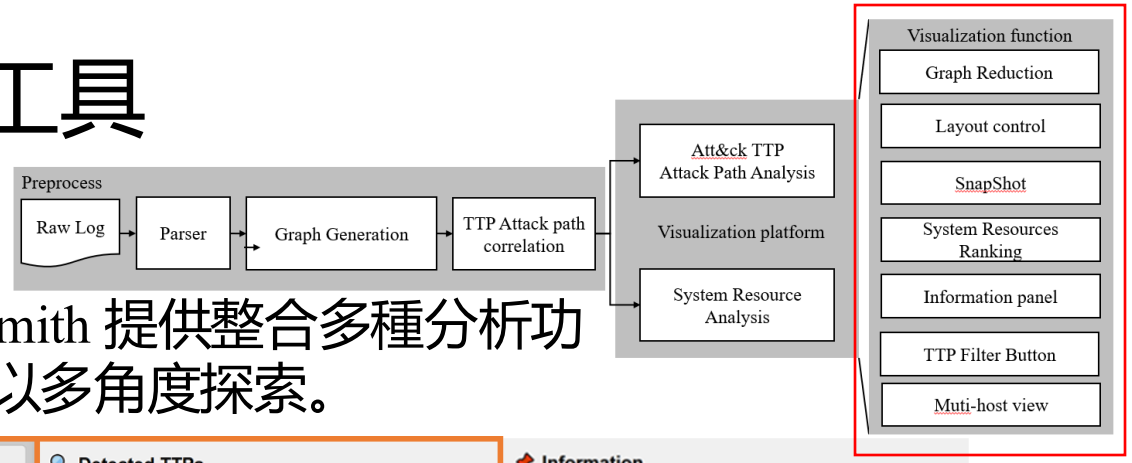


Cloversmith 以日誌事件作為輸入，分析人員可依需求選擇不同模式進行視覺化探索。

- TTP Attack Path Analysis 模式聚焦於 MITRE ATT&CK TTP 的關聯與攻擊路徑追蹤。
- 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。

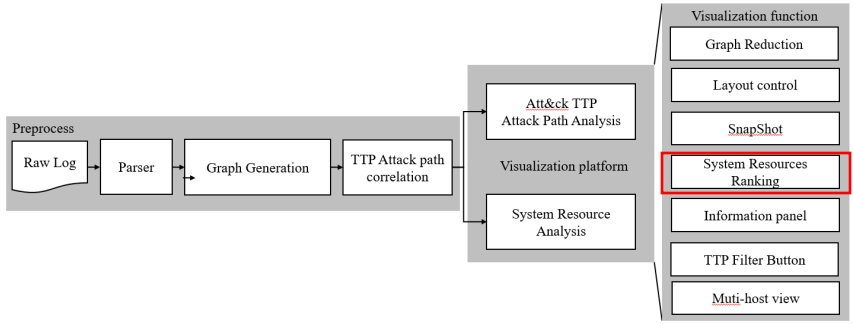
功能模組	TTP Attack Path Analysis	System Resource Analysis
Graph Reduction	✗	✓
Layout Control	✓	✓
Snapshot	✓	✓
System Resources Ranking	✗	✓
Information Panel	✓	✓
TTP Filter Button	✓	✗
Multi-host View	✓	✗

Visualization function -攻擊可視化工具



- 為了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。透過一系列輔助功能，分析師得以多角度探索。

System Resources Ranking



- 為了快速定位到最關鍵的系統實體， System Resource Analysis 平台設計了一套系統資源排序功能。計算圖中每一個節點的流量分數，並依分數產生一個「Top System Resources」列表。

1. **基礎分數 (Base Score):** 我們使用 Degree Centrality 作為節點的基礎分數 S_{base}。對於任一節點 n，分數為入邊數量（in-degree）與出邊數量（out-degree）的總和。這代表了該節點在系統中的活躍程度。

$$S_{base}(n) = \deg_{in}(n) + \deg_{out}(n)$$

2. **攻擊節點判斷:** 一個節點 n 被定義為攻擊相關節點（is_attack_node(n)），且任何一條與其相連的邊 e 帶有 TTP 標籤。

$$\text{is\_attack\_node}(n) = \exists e \in E_{adj}(n) : \text{label}(e) \neq \text{'benign'}$$

3. **最終分數 (Final Score):**我們首先將所有節點的基礎分數正規化到 [0, 1] 區間。接著，給所有被判斷為攻擊相關的節點一個獎勵分數（+1）。

$$S_{final}(n) = \frac{S_{base}(n)}{\max_{v \in V} S_{base}(v)} + \mathbb{I}(\text{is\_attack\_node}(n))$$

System Resources Ranking

- 在 Higaisa APT 攻擊場景中，可以看到經由排名後的結果，名次靠前的都是與攻擊直接相關的系統資源。

Retrive4075693065230196915.vbs

Search ...

Top System Resources

Rank	System Resource
1	C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE /n /dde
2	"cscript //E:Jscript ""Retrive4075693065230196915.vbs"""
3	"cmd.exe /C echo var url = ""http://ocsp.digicert.com/MFYwVKADAgEAME0wSzBJMAkGBSsOAwIaBQAEFN+qEu WScript.CreateObject('MSXML2.ServerXMLHTTP'); request.open('GET', url, false); request.send(); if (request.statu else {WScript.Quit(1);}WScript.Quit(0); > Retrive4075693065230196915.vbs && cscript //E:Jscript Retrive407569
4	C:\Program Files\Google\Chrome\Application\chrome.exe
5	Retrive4075693065230196915.vbs
6	8.8.8.8

chrome.exe

Top System Resources

Rank	System Resource
1	C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE /n /dde
2	"cscript //E:Jscript ""Retrive4075693065230196915.vbs"""
3	"cmd.exe /C echo var url = ""http://ocsp.digicert.com/MFYwVKADAgEAME0wSzBJMAkGBSsOAwIaBQAEFN+qEu WScript.CreateObject('MSXML2.ServerXMLHTTP'); request.open('GET', url, false); request.send(); if (request.statu else {WScript.Quit(1);}WScript.Quit(0); > Retrive4075693065230196915.vbs && cscript //E:Jscript Retrive407569
4	C:\Program Files\Google\Chrome\Application\chrome.exe
5	Retrive4075693065230196915.vbs
6	8.8.8.8

研究問題

- 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？

資料集

- Datasets
  - 使用 SAGA[17] - Known APT Campaign，分別為 Higaisa、APT28、Gamaredon，並統計每個活動中所涉及的 ATT&CK 技術（TTP）。

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

ATT&CK TTP ID	ATT&CK TTP NAME	Higaisa	APT28	Gamaredon
T1005	Data from Local System		v	
T1007	System Service Discovery			
T1016	System Network Configuration Discovery	v		
T1021.001	Remote Services:Remote Desktop Protocol			
T1033	System Owner/User Discovery			
T1036.004	Masquerading:Masquerade Task or Service	v		
T1046	Network Service Discovery			
T1047	Windows Management Instrumentation			v
T1049	System Network Connections Discovery			
T1053.005	Scheduled Task/Job: Scheduled Task	v		v
T1055.002	Process Injection: Portable Executable Injection			
T1059.001	Command and Scripting Interpreter:PowerShell			
T1069.001	Permission Groups Discovery: Local Groups			
T1071.001	Application Layer Protocol: Web Protocols		v	v
T1082	System Information Discovery	v	v	v
T1083	File and Directory Discovery			
T1087.001	Account Discovery: Local Account			
T1105	Ingress Tool Transfer			
T1112	Modify Registry			v
T1204.002	User Execution: Malicious File	v	v	v
T1219	Remote Access Tools			
T1491	Defacement			v
T1518.001	Software Discovery: Security Software Discovery			
T1547.001	Boot or Logon Autostart Execution:Registry Run Keys / Startup Folder	v		v
T1547.009	Boot or Logon Autostart Execution: Shortcut Modification			
T1548.002	Abuse Elevation Control Mechanism:Bypass User Account Control			
T1562.001	Impair Defenses:Disable or Modify Tools			
T1564.003	Hide Artifacts:Hidden Window			
T1566.001	Phishing:Spearphishing Attachment	v	v	v
T1567	Exfiltration Over Web Service		v	

RQ1:能否透過 Cloversmith 理解攻擊全貌並定位惡意事件?

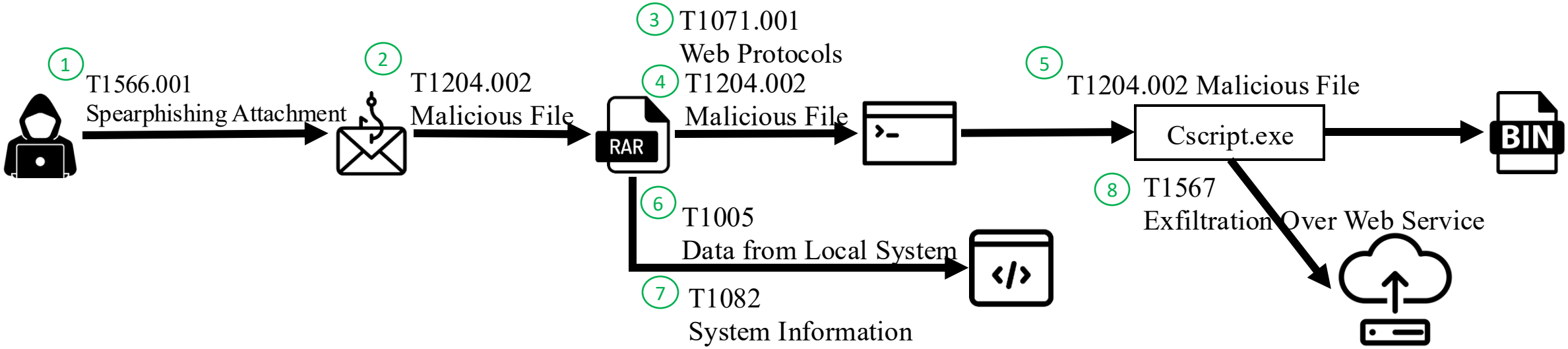
- 本研究為受試者設計了兩份表單，用於評估 Cloversmith 的實用性。
- 首先，請受試者在給定入侵節點以及指導語的情況下，使用 System Resource Analysis 與 TTP Attack Path Analysis 模式分析了兩個不同攻擊組織（Higaisa、 Gamaredon 發起的 APT 攻擊案例，並填寫發現的可疑節點、事件，以及攻擊描述

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%

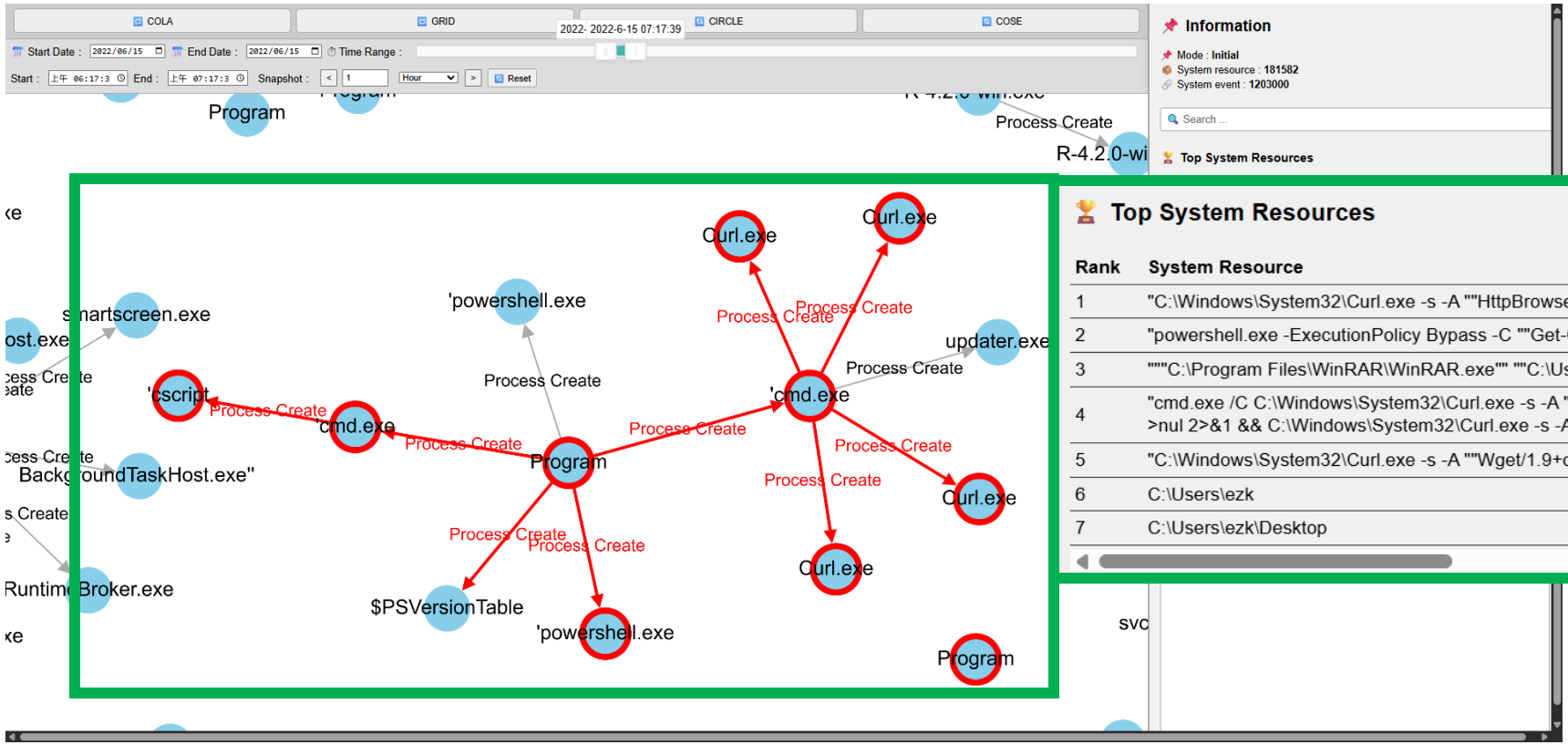
RQ2:案例分析

- **Background** : APT28[18] 是利用 WinRAR 的漏洞，在 WinRAR 6.23 版本以前攻擊者會製作惡意 RAR 檔案，內容包含正常檔案與存有惡意執行檔的同名資料夾，當受駭者遭誘騙開啟正常檔案時，同名資料夾內的惡意執行檔將會觸發執行。
- **Attack scenario** :



RQ2:案例分析

- 我們首先利用 **Cloversmith** 系統的 System Source Analysis 功能，快速知道攻擊發生時與哪些 process 有關聯，也可以利用 Top System Resources 了解哪些系統資源是我們需要關注的

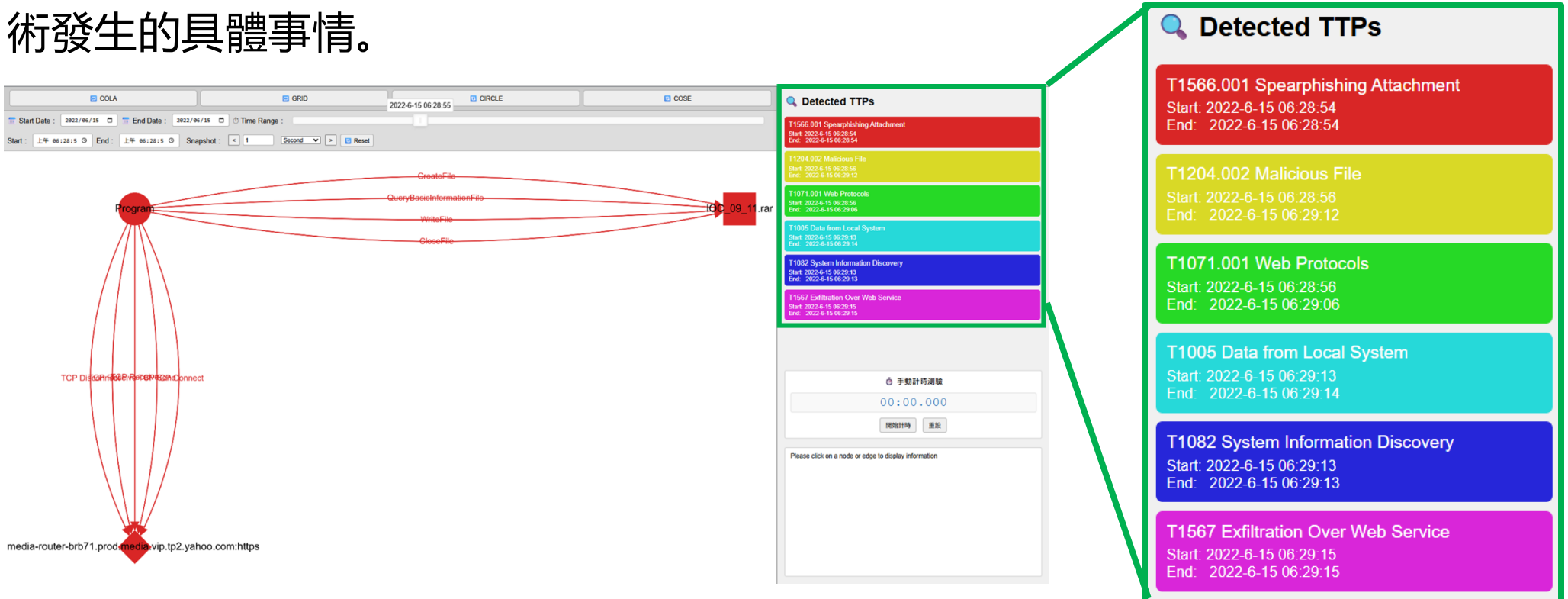


Top System Resources

Rank	System Resource
1	"C:\Windows\System32\Curl.exe -s -A ""HttpBrowser/1.0"" -m3 43.207.106.74 "
2	"powershell.exe -ExecutionPolicy Bypass -C ""Get-ChildItem C:\Users -Attributes Directory+Hidden -ErrorAction S
3	"""C:\Program Files\WinRAR\WinRAR.exe"" ""C:\Users\apple\Downloads\IOC_09_11.rar"""
4	"cmd.exe /C C:\Windows\System32\Curl.exe -s -A ""HttpBrowser/1.0"" -m3 43.207.106.74 >nul 2>&1 && C:\Windo >nul 2>&1 && C:\Windows\System32\Curl.exe -s -A ""*<|>*"" -m3 43.207.106.74 >nul 2>&1"
5	"C:\Windows\System32\Curl.exe -s -A ""Wget/1.9+cvs-stable (Red Hat modified)"" -m3 43.207.106.74 "
6	C:\Users\ezk
7	C:\Users\ezk\Desktop

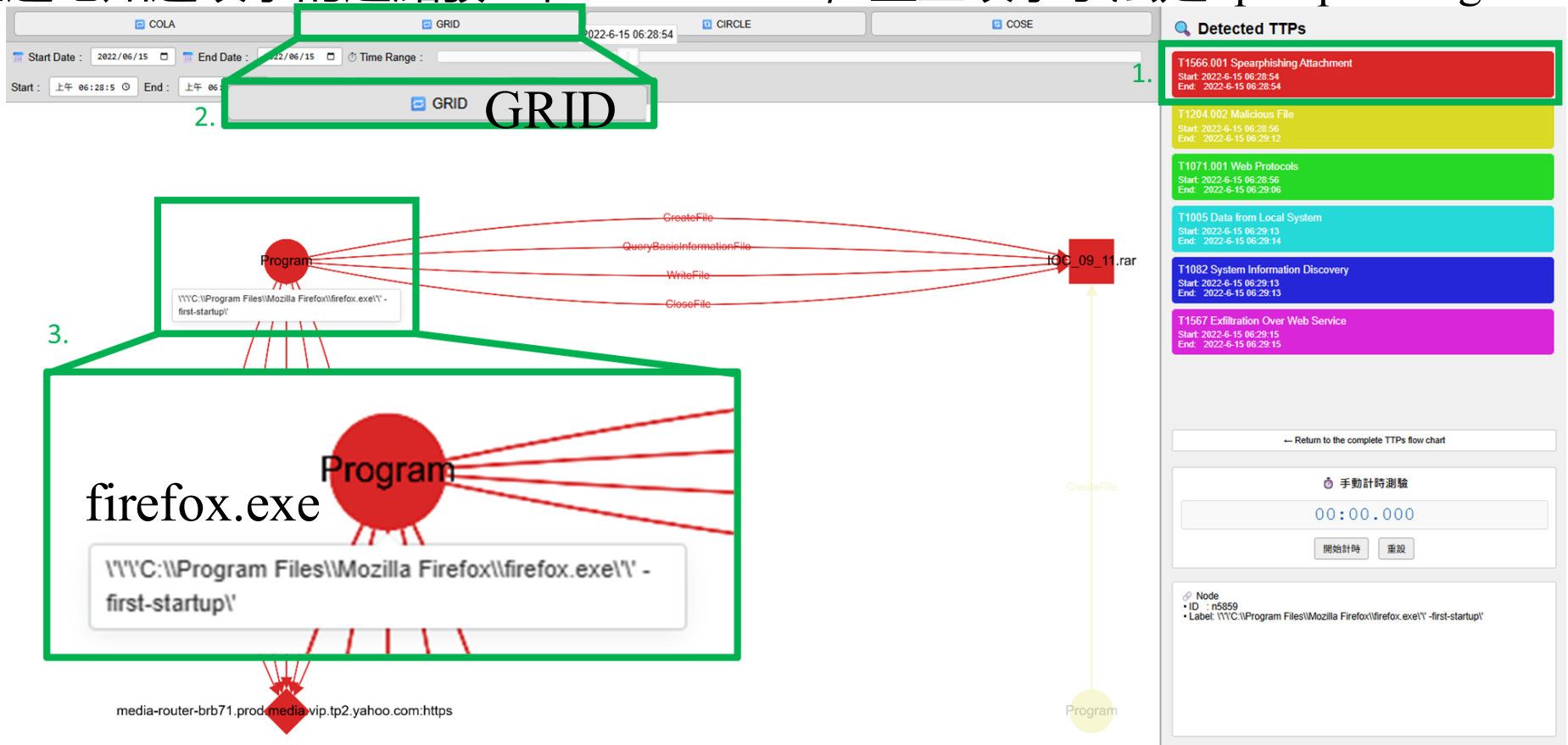
RQ2:案例分析

- 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，我們切換使用 TTP Attack Path 功能。
- 我們先看到介面右邊，這邊顯示的是此攻擊手法使用到的 ATT&CK TTP，並且該列表示依照出現的時間順序作排列，因此我們可以點擊每個 ATT&CK TTP 逐一了解每個攻擊技術發生的具體事情。



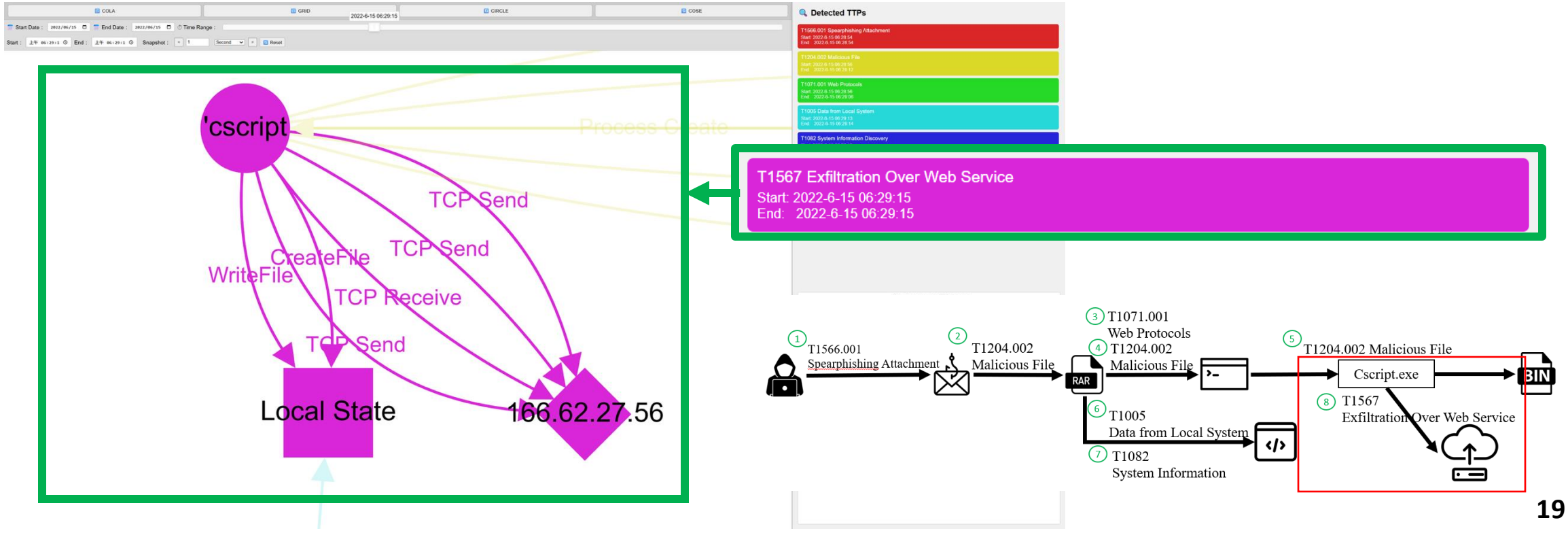
RQ2:案例分析

- 首先我們先點選紅色最先出現的 ATT&CK TTP， 該 TTP 為 Phishing: Spearphishing Attachment， 隨後我們點選 GRID 排版，讓節點依照時間由左至右由上至下排列。我們可以迅速地知道攻擊的起點發生在 firefox.exe， 並且攻擊手法是Spearphishing Attachment。



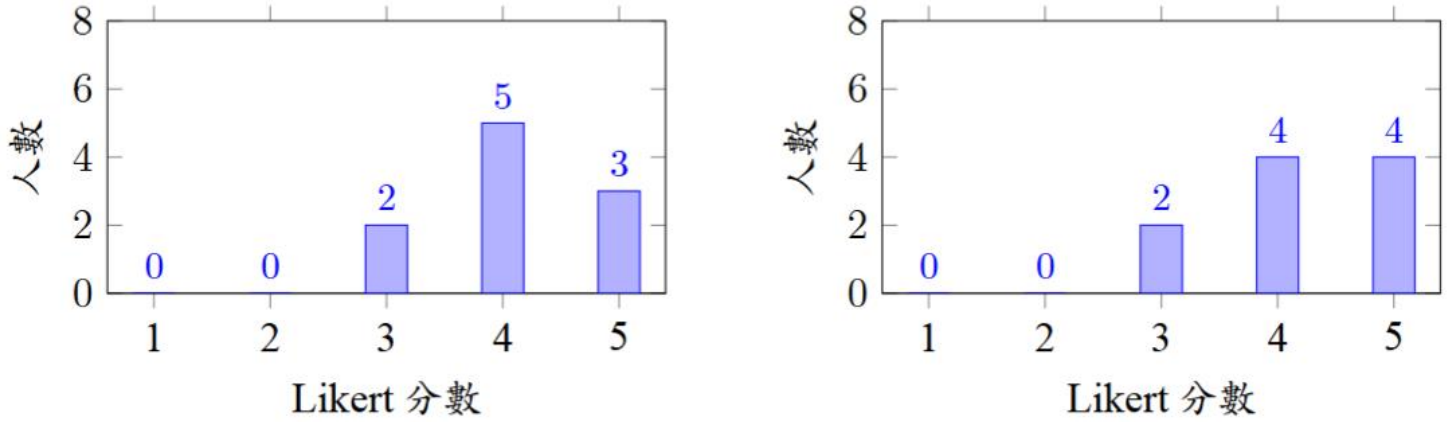
RQ2:案例分析

- 我們接續直到最後一個 ATT&CK TTP T1567 Exfiltration Over Web Service，我們得知具體連接到哪個 IP 以及具體是哪個資料被竊取。
- 這驗證了我們最初的攻擊場景的最後一步，攻擊的最終目的是竊取資料。透過點擊 T1567 Exfiltration OverWeb Service，Cloversmith 不僅證實了這一點，還揭露了具體的竊取細節。



滿意度調查

- 實驗中，我們統計受試者對系統是否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。



((a)) System Resource Analysis　　((b)) TTP Attack Path Analysis

圖 7 系統功能是否足以滿足攻擊調查需求

結論

主要貢獻:

- 建立了一個多層次的攻擊視覺化框架，允許資安分析師在高階的 MITRE ATT&CK 技術攻擊路徑，與詳細的底層系統資源互動兩種視圖間切換。

- 另外，與現有的攻擊溯源工具例如 NetworkX 與 graphviz 相比，我們的攻擊可視化工具除了提供詳細的日誌場景，也提供了高層次的攻擊場景，並以平台的方式呈現，提升可操作性。

未來的研究方向:

- 雖著 APT 攻擊時間跨度的增加，日誌的檔案大小會急遽攀升，在未來預計加上一些前處理來應對大型的稽核日誌。
- 希望在未來可以新增語言模型，提供對攻擊場景對初步的文字解釋，提高解釋性以及降低使用上的難度。

Thank you!