出國報告（出國類別：開會）

出席亞洲黑帽駭客大會（Black Hat Asia 2024）出國報告書

服務機關：數位發展部資通安全署
姓名職稱：方志祥分析師
洪誠澤分析師
派赴國家：新加坡
出國期間：113 年 4 月 15 日至 20 日
報告日期：113 年 07 月 19 日

摘　要

「黑帽駭客大會」是國際知名的資訊安全會議，每年都會吸引來自世界各地的資安專家、研究人員、駭客、企業和政府機構等各類人員參加，會議的目的是分享最新的安全研究成果發表及討論當前資訊安全問題和趨勢等，「黑帽駭客大會」也是世界著名的資安活動之一，每年會在亞洲、美國、歐洲、中東和非洲等地區舉辦。

「亞洲黑帽駭客大會（Black Hat Asia）」於今（2024）年 4 月 16 日至 19 日在新加坡舉行，共 4 天活動，活動包括簡報演講、為期 2 天的工作坊課程及 2 天超過 40 場演講，其中工作坊課程提供了一系列深入的技術實作，由資訊安全業界的頂尖師資和專業人士共同指導，旨在提升參與者的技能和知識，如機器學習、滲透測試、資安鑑識、紅隊演練及公開來源情報（OSINT）等課程；演講會則涵蓋現今最新的資訊安全風險、研究和趨勢，主題包括資安威脅情資、供應鏈安全、漏洞利用開發、逆向工程、APP 安全及物聯安全等。

目錄

壹、 目的

Black Hat Asia 是一個專注於資訊安全議題的全球性活動，會議是為了與資安領域的專家和同行交流，學習最新的研究成果和趨勢，透過參與工作坊課程，可以提升自己的技術能力，並獲得實際操作的經驗，學習最新的攻防技術。

Black Hat Asia 2024 於 4 月 16 日至 19 日在新加坡的舉行，我們參加的活動包括前 2 天深度技術實踐工作坊課程，後 2 天的資訊安全最新研究和漏洞揭露的演講，各講者會分享其最新的資安研究、風險及趨勢，讓參與者能夠更好地瞭解和管理潛在的威脅，也期望相關資安議題可作為本署制定資安防禦政策思考方向之一。

貳、 過程

一、 Black Hat Asia 大會介紹

Black Hat 是全球資訊安全最具影響力的會議之一，該會議始於 1997 年，在美國拉斯維加斯舉行，隨後擴展到歐洲和亞洲，而 Black Hat Asia 則是自 2000 年開始舉行，經常在新加坡濱海灣金沙會議展覽中心舉辦，今年亦是在此會議展覽中心舉行，該中心旁有捷運接駁，交通便利，腹地廣大。

圖 1、新加坡濱海灣金沙會議展覽中心，資料來源：自行拍攝。

圖 2、新加坡濱海灣金沙會議展覽中心景觀，資料來源：自行拍攝。

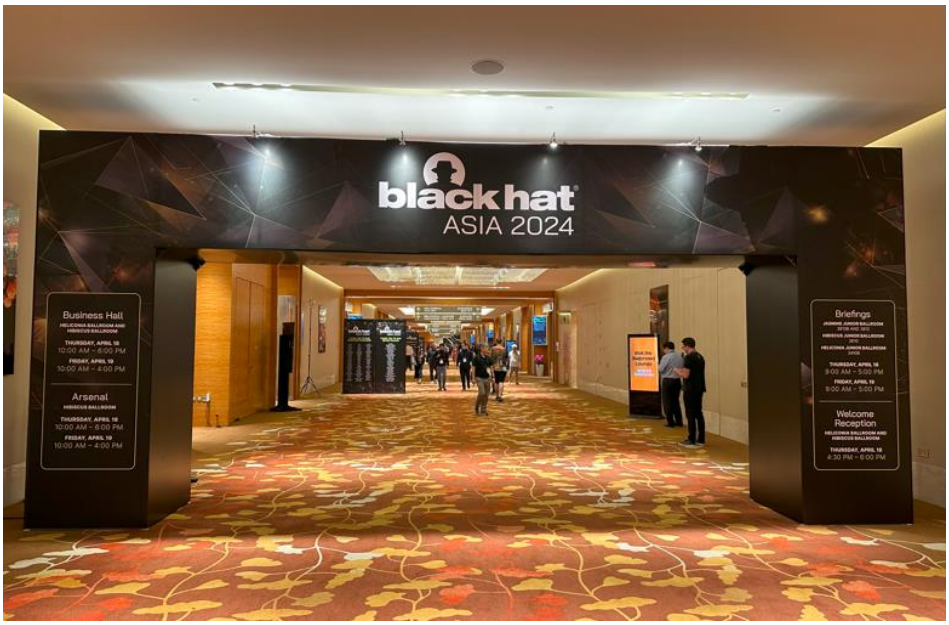


圖 3、Black Hat Asia 2024 會議入口，資料來源：自行拍攝。

二、 Black Hat Asia 2024 為期 4 天，自 113 年 4 月 16 日至 4 月 19 日止，參加場次如下：

日期	活動主題
4 月 16 日-17 日，2 人各參加 1 場工作坊	資料科學和機器學習在網路安全中的應用（Applied Data Science And Machine Learning For Cyber Security，講者：Summer Rankin）
	網路調查與人類智慧之基礎原理（Fundamentals of Cyber Investigations and Human Intelligence，講者：Christina Lekati 及 Samuel Lolagar）

4月18日，2人共同參與技術簡報	隱私偵探：發現安卓系統資料外洩（Privacy Detective：Sniffing Out Your Data Leaks for Android，講者：Meggie He 及 Abbie Zhou）
	從自帶驅動程式攻擊到零時差攻擊：揭開網路招聘詐騙中的高階漏洞（From BYOVD to a 0-day：Unveiling Advanced Exploits in Cyber Recruiting Scams，講者：Luigino Camastra 及 Igor Morgenstern）
	毒蘋果行動：追蹤信用卡資訊竊取到付款詐欺（Operation PoisonedApple：Tracing Credit Card Information Theft to Payment Fraud，講者：Gyuyeon Kim 及 Hyunho Cho）
4月19日，2人共同參與技術簡報	端點偵測與回應重裝上陣：遠端清除數據（EDR Reloaded: Erase Data Remotely，講者：Tomer Bar 及 Shmuel Cohenn)
	匯流排故障：新穎的匯流排故障攻擊方式破壞嵌入式系統中的可信執行環境（Faults in Our Bus: Novel Bus Fault Attack to Break Trusted Execution Environments in Embedded Systems，講者：Nimish Mishra）
	網路營運中心報告（Network Operations Center Report，講者：Neil Wyler 及 Bart Stump）

圖 4、電子看板，資料來源：自行拍攝。

圖 5、由新加坡網路安全局（CSA）首席執行官許大衛開幕演講，資料來源：自行拍攝。

參、 會議紀要

一、 資料科學和機器學習在網路安全中的應用（Applied Data Science And Machine Learning For Cyber Security，講者：Summer Rankin）

（一）資料科學與機器學習

1. 講者介紹

任職美國博思艾倫漢密爾頓控股公司首席資料科學家 Summer Rankin 為本次工作坊課程講者，為美國佛羅里達大西洋大學獲得了複雜系統和腦科學博士，主要向政府機構提供管理、技術以及安全服務，負責數據安全、國防、防禦間諜和獲取情報，同時也提供民間商業服務。

2. 資料科學及機器學習

在正式課程開始前，講者請每個學員用英文自我介紹，介紹自己的名字、年紀、國家、背景、為何想來學習這門課程等，除此之外，講師也鼓勵任何人都可跨領域來學習資料科學及機器學習，其本身也非本科系，但為了研究需要而跨領域學習資料科學及機器學習技術，建議學習這門技術前需要一些基本門檻，在「資料科學」中需要一些電腦科學及領域知識（Domain Knowledge）的專業能力（圖 6），如有程式撰寫能力來實現自動化工作，以減少人工作業，以及分析領域知識的數據，即具備該領域的專業知識；而「機器學習」則是以資料科學為基礎，依過去的數據並運用機器學習中的演算法建置模型，該模型可自我改善、回應且進行預測未來數據。

https://	protocol
www	subdomain
google.com	zone apex
google	domain
.com	top-level-domain (tld)
/search?q=URL...	path

圖 6、辨識惡意 URL 的領域知識，資料來源：講者簡報。

原則上，強調資料科學與機器學習是整體的概念，如要進入 AI 技術領域，要從數據科學、機器學習、深度學習、大型語言模型及生成式 AI 等逐步

深入。

首先要從異質性資料中分析想要哪些數據，需先整理好這些資料，需學習如何處理這些異質性資料，將這些亂無章法的資料，找出共同特徵並進行正規化，雖然這個過程不是困難的，但較繁鎖且需要花費大量時間，根據講者的經驗，整理資料會占專案中的 50%-90%工作量，也顯示出資料科學基本功的重要性。

3. 數據導入及清洗

數據導入及清洗是資料科學的精髓，也為後續的數據分析和模型建構提供了可靠的基礎。

本活動請參與者實作練習基本 python 語言熟悉字串操作、轉換檔案格式、刪除無效值、處理遺漏值、重複值和不一致性等，透過資料各種操作來瞭解數據導入和清洗，以利後續將資料進行預先訓練。

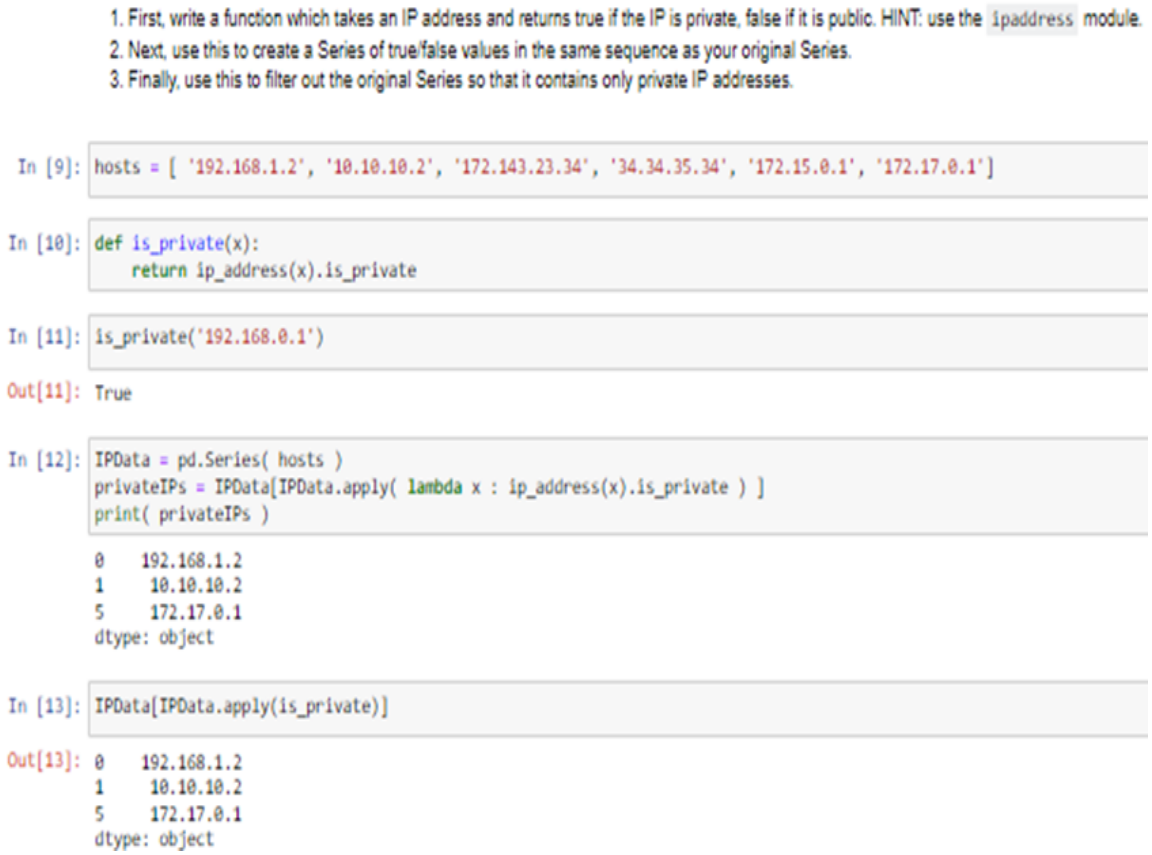


圖 7、判斷私有 IP，資料來源：自行截圖。

In this exercise, you will learn how to convert a PCAP file into JSON and do some basic summarization of the data. In the `data` directory, you will find a file called `http.pcap`. Our first step is to convert this to JSON. To do this we have installed a python module called `pcapview` (docs available here: https://pydigger.com/pypi/pcapview) which can convert the pcap file to JSON.

Once you've done that, your assignment is to answer the following questions:

1. What are the most frequent source IP addresses?
2. How many differnet source ports were accessed?

To do this you will have to load this data into a DataFrame. Using what we've learned in class, do the following:

1. Load the data into a DataFrame using the technique of your choice
2. Extract the requisite columns from the DataFrame, in this case, you want the source IP and source ports
3. Execute a `value_counts()` on those columns.

In [23]:
```
#Load the data
with open(DATA_HOME + 'http-pcap.json') as data_file:
    pcap_data = json.load(data_file)

#Normalize it and load it into a DataFrame
df = pd.DataFrame( pd.json_normalize(pcap_data) )

#View the results
df.head()
```

Out[23]:

	time	timestamp	IP.version	IP.ttl	IP.proto	IP.options	IP.len	IP.dst	IP.frag	IP.flags	...	DNS.opcode	DNS.rcode	DNS.ra	DNS.id
0	1.084443e+09	2004-05-13T10:17:07.311224	4	128	6	[]	48	65.208.228.223	0	2	...	NaN	NaN	NaN	NaN
1	1.084443e+09	2004-05-13T10:17:08.222534	4	47	6	[]	48	145.254.160.237	0	2	...	NaN	NaN	NaN	NaN
2	1.084443e+09	2004-05-13T10:17:08.222534	4	128	6	[]	40	65.208.228.223	0	2	...	NaN	NaN	NaN	NaN
3	1.084443e+09	2004-05-13T10:17:08.222534	4	128	6	[]	519	65.208.228.223	0	2	...	NaN	NaN	NaN	NaN
4	1.084443e+09	2004-05-13T10:17:08.783340	4	47	6	[]	40	145.254.160.237	0	2	...	NaN	NaN	NaN	NaN

5 rows × 61 columns

圖 8、網路封包流量.pcap 檔轉換成的 json 檔，資料來源：自行截圖。

(二)對應機器學習問題處理的方式

正規化後的資料，會視該資料的複雜程度，區分 4 種處理方式，即分類、迴歸、分群和降維，相關的演算法的內涵涉及微積分、機率論及線性代數等學科，所以講者儘量以淺顯易懂的方式說明：

1. **分類**（Classification）是利用離散的特徵值來預測未來的結果，這些特徵值通常是具體且有限的類別，例如將電子郵件分類為垃圾郵件或正常郵件，或者根據病人的症狀來預測是否患有某種疾病。分類技術在許多應用場景中都非常重要，因為可以協助做出快速而準確的決策。

2. **迴歸**（Regression）是利用連續型的特徵值來預測未來的結果。例如，可以利用迴歸分析來預測房價，根據房屋的面積、位置、年齡等連續變數來估算其市場價值，迴歸模型能夠提供精確的數值預測；對於金融市場預測、經濟數據分析等領域具有廣泛的應用。

3. **分群（Clustering）**技術主要用於識別資料集中的分組，目的是找出資料中相似的部分並將其聚集在一起，這種技術在市場行銷中廣泛的應用，可以幫助企業將客戶分成不同的群組，從而針對不同群組採取更有效的行銷策略。此外，分群還可以應用於影像處理、生物資訊學等領域，協助理解數據的內在結構關係。

4. **降維（Dimensionality Reduction）**是一種處理高維度數據的方法，在某些情況下，資料中可能包含大量的特徵，這會增加模型訓練的負擔和儲存空間的需求，透過降維技術，可以減少特徵數量，提取出最重要的變數，從而降低計算的複雜度。常見的降維方法包括主成分分析（Principal components analysis，PCA）和線性判別分析（Linear Discriminant Analysis，LDA），這些方法在影像處理、文本分析等領域中都有重要的應用。

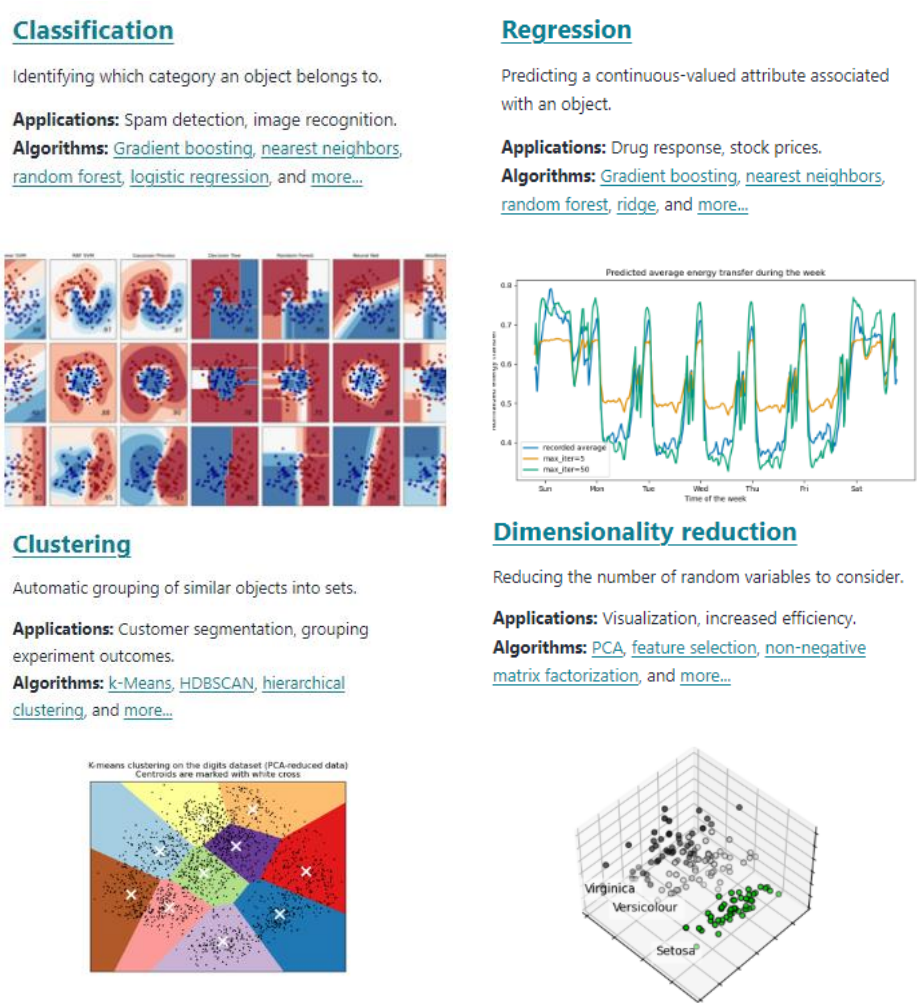


圖 9、分類、迴歸、分群和降維示意圖，資料來源：擷自 scikit-learn 官網。

有關分類、迴歸、分群和降維是資料科學和機器學習中的 4 種核心技術，每

一種技術都有其適用的情境和優勢，仍應視我們要應用在哪個領域及資料來源，從中再選擇適合的技術，可有效地處理和分析數據。

(三)監督學習與非監督學習

兩者不同是以準備進行預先訓練之資料是否已標籤化（Labeled）作為基準，已標籤化的資料進行訓練歸類成「監督學習」，反之，為「非監督學習」。

1. 監督學習（Supervised Learning）

「監督學習」是機器學習的一類，通過一組預先存在的已標籤化資料來訓練模型，進而達成分類及預測作用，其演算法包括線性迴歸、邏輯迴歸、決策樹和支援向量機（SVM）等方法，這些模型亦解釋了模型訓練和評估過程、特徵選擇以及避免過度擬合（Overfitting）的重要性。

(1) **線性迴歸**（Linear Regression）是一種基本且廣泛使用的預測模型，用於預測連續目標變數，通過找到輸入特徵與輸出目標之間的線性關係，從而進行預測，這種模型簡單且易於解釋，適用於很多實際問題，例如房價預測、銷售量預測等。

(2) **邏輯迴歸**（Logistic Regression）則是另一種常見的模型，主要用於分類任務，常使用在處理二元分類問題，例如除上述預測某封電子郵件是否為垃圾郵件，也可以擴展到多元分類問題，例如根據學生的成績預測其最終的學業表現；另外，邏輯迴歸也可利用邏輯函數（Logistic Function）將輸出轉化為機率進行分類。

(3) **決策樹**（Decision Tree）適用於分類和迴歸任務，決策樹通過學習決策規則將資料劃分成不同的子集，從根節點開始，根據特徵的取值進行分割，直到達到葉節點。每個葉節點代表一個預測結果。決策樹模型的優點是易於解釋和視覺化，但缺點是容易過度擬合，特別是在訓練資料較少的情況下。

(4) **支持向量機**（Support Vector Machine, SVM）適用於分類和迴歸的任務，支持向量機通過找到一個最佳的超平面，將資料點分開，從而進行分類。這個超平面使得不同類別之間的間隔最大化，從而提高模型的泛化能力。

SVM 可以處理線性和非線性問題，並且在高維度數據上表現良好

2. **非監督學習（或稱無監督學習，Unsupervised Learning）**

非監督學習是在沒有標籤回應的情況下可能無法分群，分群演算法應運而生，在資料中尋找可能的隱藏模型或內在關係結構，其演算法包括 K-means 分群法、階層式分群、DBSCAN 分群法及 PCA 分群法。

(1) **K-Means 分群法**（K-Means Clustering）是將資料點分成 k 個群，通過反覆疊代來最小化群內資料點之間的距離，使得每個群中的資料點彼此相似。K-Means 分群法簡單高效，適用於大量的資料集，且計算速度快，但需要預先設定 k 值，k 值即為分群的數量。

(2) **階層式分群法**（Hierarchical Clustering）是通過構建階層樹狀結構來表示資料的分層關係，這種方法不需要預先設定群的數量，而是通過將資料點逐步合併或分裂，形成一棵樹狀結構（或稱樹狀圖）。階層式分群法適合小型資料集，而且可以直接展示資料點之間的層次關係。

(3) **DBSCAN 分群法**（Density-Based Spatial Clustering of Applications with Noise Clustering）是基於密度的分群方法。與 K-Means 不同，DBSCAN 依據資料點的密度來進行分群，假設資料中高密度區域被視為一個群組，DBSCAN 能夠自動識別出不同形狀的群組，並且能夠處理含有雜訊的資料集，所以這方法很適合處理複雜和非均勻分佈的資料。

(4) **PCA 分群法**（Principal Component Analysis Clustering）是基於主成分分析的分群方法，PCA 用於減少資料的維度，同時盡可能保持資料的變異數；透過 PCA，可以將高維度資料減少至低維度空間，從而減少計算複雜度並保留主要的資訊結構。在降維後，可再應用其他分群方法（如 K-Means）來進行分群，例如金融數據分析人臉辨識、基因序列分析及蛋白質結構研究等。

(四)案例分析

講者提供一個實戰案例，當場展示如何利用資料科學及機器學習進行威脅蒐捕：

1. **使用信標（Beaconing）檢測**：惡意軟體感染後常通過信標回應指揮和控制伺服器，展示如何使用 Python 工具（如 Flare 和 RITA）檢測信標（如 IP 位址、網路埠號、網路協定及時間戳記等）。

2. **使用功能變數名稱生成演算法（Domain Generation Algorithm，DGA）檢測**：攻擊者使用這演算法生成各種不同的網功能變數名稱，進而逃避一般防毒軟體及 EDR 的檢測，常使用在殭屍網路（Botnet）中的伺服器（Command and Control servers）上，導致難以追蹤；此實作展示如何從大量 DNS 資料中檢測哪些是以 DGA 生成的網功能變數名稱，進而排除。

3. **實例**：圖 10 為篩選子網址後，運用 flare 開源工具，以字典集、自然語言模型（n-grams）及 DGA 網址名稱等進行訓練，預測 DNS 位址是否為合法。

Next we need to train extract the top level domains (remove subdomains) using flare so we can feed it to our classifier

```
In [44]: a_records_unique['domain_tld'] = a_records_unique.dns_rrname.apply(domain_tld_extract)
```

```
In [45]: a_records_unique.head()
```

Out[45]:

	dns_rrname	domain_tld
0	api.wunderground.com	wunderground.com
1	stork79.dropbox.com	dropbox.com
2	hpca-tier2.office.aol.com.ad.aol.aoltw.net	aoltw.net
3	safebrowsing.clients.google.com.home	com.home
4	fxfeeds.mozilla.com	mozilla.com

Train DGA Classifier with dictionary words, n-grams and DGA Domains

```
In [46]: dga_predictor = dga_classifier()
```

```
[*] Initializing... training classifier - Please wait.
[+] Classifier Ready
```

```
In [47]: a_records_unique['dga_predict'] = a_records_unique.domain_tld.apply(lambda x: dga_predictor.predict(x))
```

A quick sampling of the data shows our prediction has labelled our data.

```
In [48]: a_records_unique.sample(10)
```

Out[48]:

	dns_rrname	domain_tld	dga_predict
107	mirror.hmc.edu	hmc.edu	legit
76	download.windowsupdate.com	windowsupdate.com	legit
93	mirror.its.uidaho.edu	uidaho.edu	legit
106	mirrors.kernel.org	kernel.org	legit
176	client-software.real.com	real.com	legit
129	cloud.xmarks.com	xmarks.com	legit
126	FL	FL	legit
91	google.com	google.com	legit
83	api.facebook.com	facebook.com	legit
82	www.malwarecity.com	malwarecity.com	legit

圖 10、預測 DNS 位址是否為合法，資料來源：自行截圖。

二、網路調查與人類智慧之基礎原理（Fundamentals of Cyber Investigations and Human Intelligence，講者：Christina Lekati 及 Samuel Lolagar）

(一)講者介紹及課程簡介

講者 Christina Lekati 是一位心理學家和社會工程學專家，另一位為 Samuel Lolagar 曾經擔任過警官和偵探，擁有多年的刑事調查經驗，而現今從事網路安全工作。

本課程介紹網路調查技術和人類智能協助調查人員進行網路犯罪和數位取證工作之方式，此領域涉及公開來源情報(OSINT)、社群媒體情報(SOCMINT)及人類情報(HUMINT)，期待能讓學員能更有效地應對不斷變化的網路犯罪與數位威脅，協助保護組織與個人不受這些威脅的影響。

(二)公開來源情報(Open Source Intelligence，OSINT)

在網路安全領域中，利用公開來源情報（OSINT）在外國是被認為是重要的資安策略，主要作業是蒐集外部資安情資來增強組織的安全防護措施。OSINT 是指從各種公開資源中收集和分析資訊的技術，這些資源包括網站、社交媒體、新聞等，透過 OSINT 組織能夠及早識別潛在的威脅，追蹤攻擊者的活動，並有效應對各種安全挑戰。

首先，OSINT 可以幫助組織監測和分析駭客和攻擊者的動態，上網研究駭客社群、暗網市場和網路討論，可以提前瞭解新興的攻擊技術和漏洞利用方式，使安全專家能夠及時調整安全性原則，加強有關系統漏洞防禦，從而降低被攻擊的風險。

其次，OSINT 對於評估社交工程和網路釣魚攻擊的潛在風險也是重要的，主要是分析個人和組織在社交媒體上的活動和資訊公開度，可以識別哪些人可能成為攻擊對象，並對所有員工進行資安訓練，以提升資安意識。

此外，OSINT 亦可使用於實時監控和分析安全事件。通過檢視社交媒體平臺、新聞報導和其他公開資源，可以及時發現與組織相關的威脅和事件。有助於迅速啟動應急反應計畫，採取必要的措施來應對安全威脅，繼而最大程度地減少損失和風險。

OSINT 在網路安全中扮演著關鍵角色，從監測威脅情報到防範社交工程攻擊，再到應對安全事件，都可透過 OSINT 工具和技術的運用，讓組織提升資安防護的效果，確保關鍵資訊和資產免受各種威脅的侵害。

講師介紹 OSINT Framework（如圖 11）時特別強調，若是從事滲透測試人員或是參與過 CEH（Certified Ethical Hacker）課程肯定接觸過此工具。OSINT Framework 是一個彙集各種工具的網站，可於不同系統和知識庫中查詢公開情報資訊。

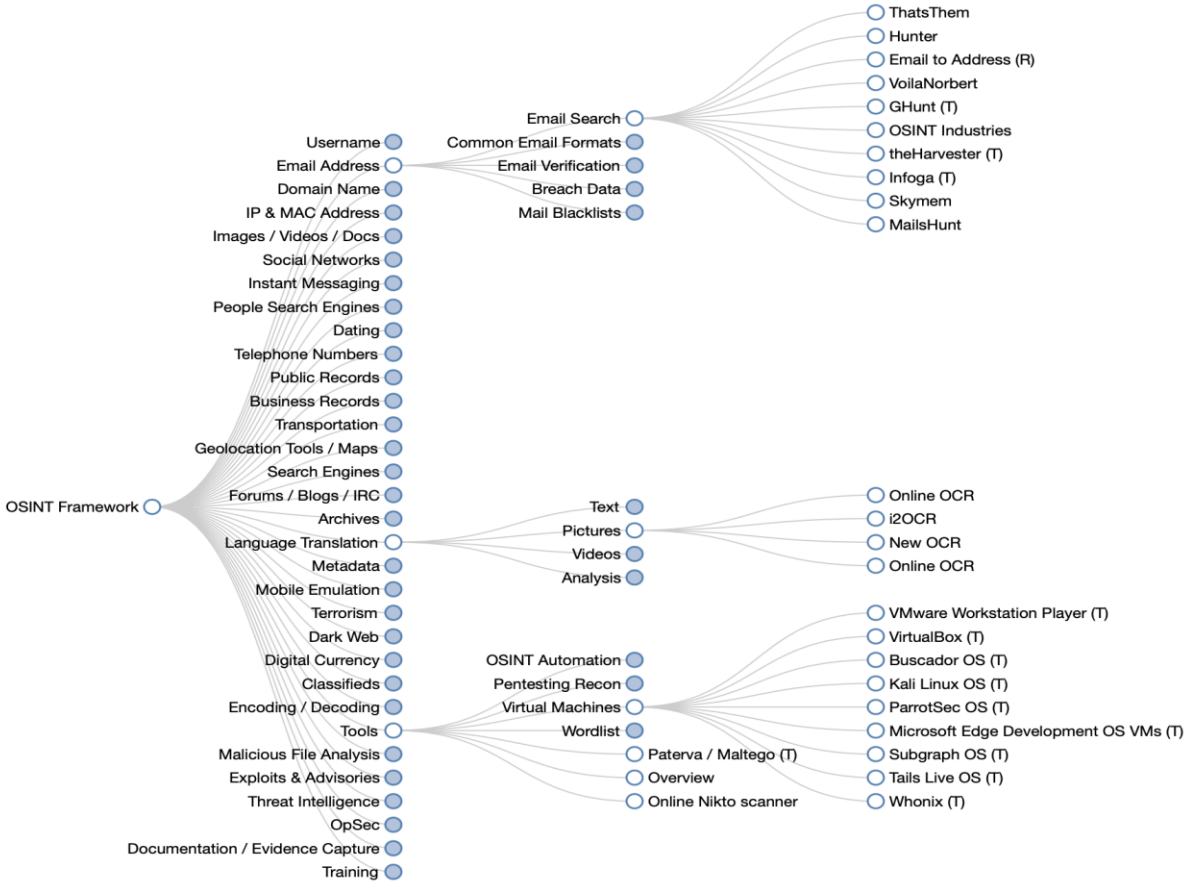


圖 11、OSINT Framework 網站，資料來源：自行截圖。

若想要尋找電子郵件相關工具，會選擇圖中的「Email Address」項目，點選後會延伸出眾多項目，再點選「Email Search」時，即可看到 Email Search 類型的工具或網站，如「Hunter」、「ThatsThem」等。當學員點選「Hunter」後，則會自動彈跳該工具的頁面，如圖 12 所示。Hunter 是個可以查詢專業人士的 Email，如 Google 員工、splunk 等企業 Email 資訊網站，更可能被利用作為尋找社交工程目標對象之一。

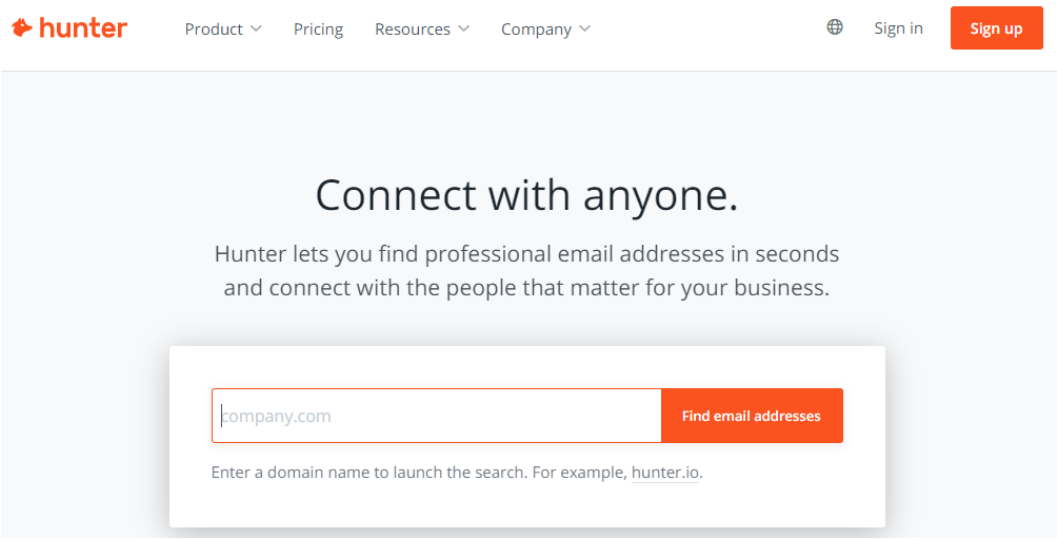


圖 12、E-Mail Hunter 網站，資料來源：自行截圖。

1. Wayback Machine(網站時光機)

為數位檔案館，用於管理、捕捉和歸檔網站在一段時間內的快照，可查看已關閉的舊網站，甚至下載以前網站的舊檔案。

例如 2024 年 5 月 13 日歐洲刑警組織 Europol 網站有遭駭客入侵情形，在 Wayback Machine 搜尋列輸入該網址後，會顯示該網站歷年異動情形，當然也可指定當日網站遭駭情形，此作法可運用在事後調查網站遭駭情形，並可推測可能遭駭時間點。

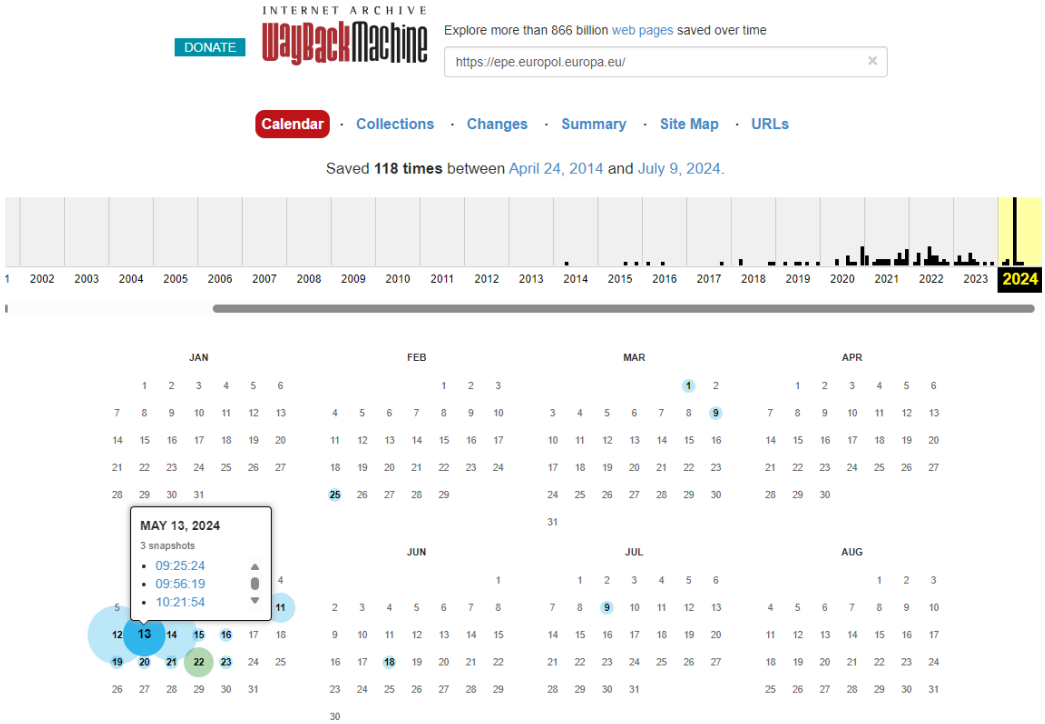


圖 13、Wayback Machine 搜尋結果，資料來源：自行截圖。

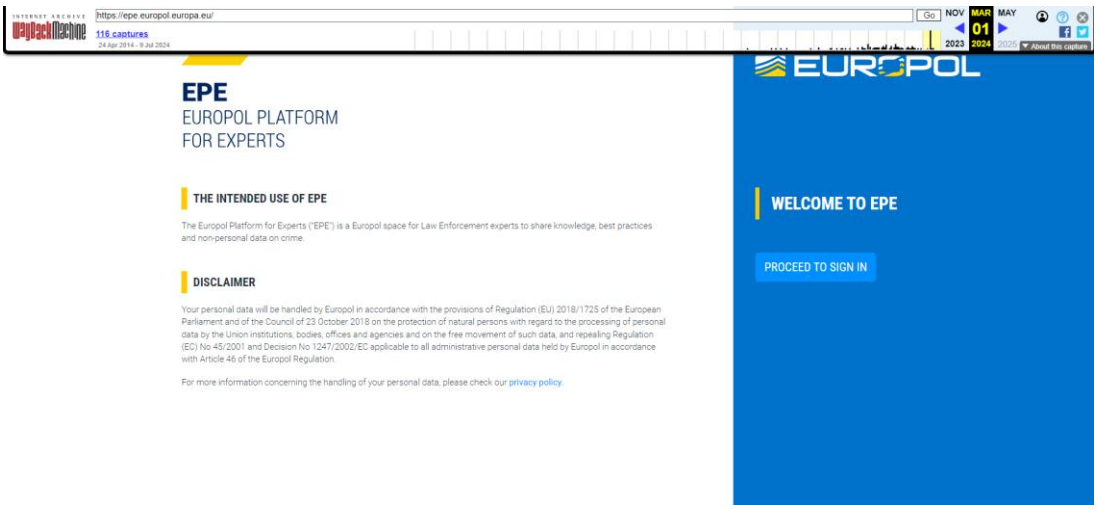


圖 14、刑警組織 Europol 網站 2024 年 3 月 1 日被駭前正常情形，資料來源：自行截圖。

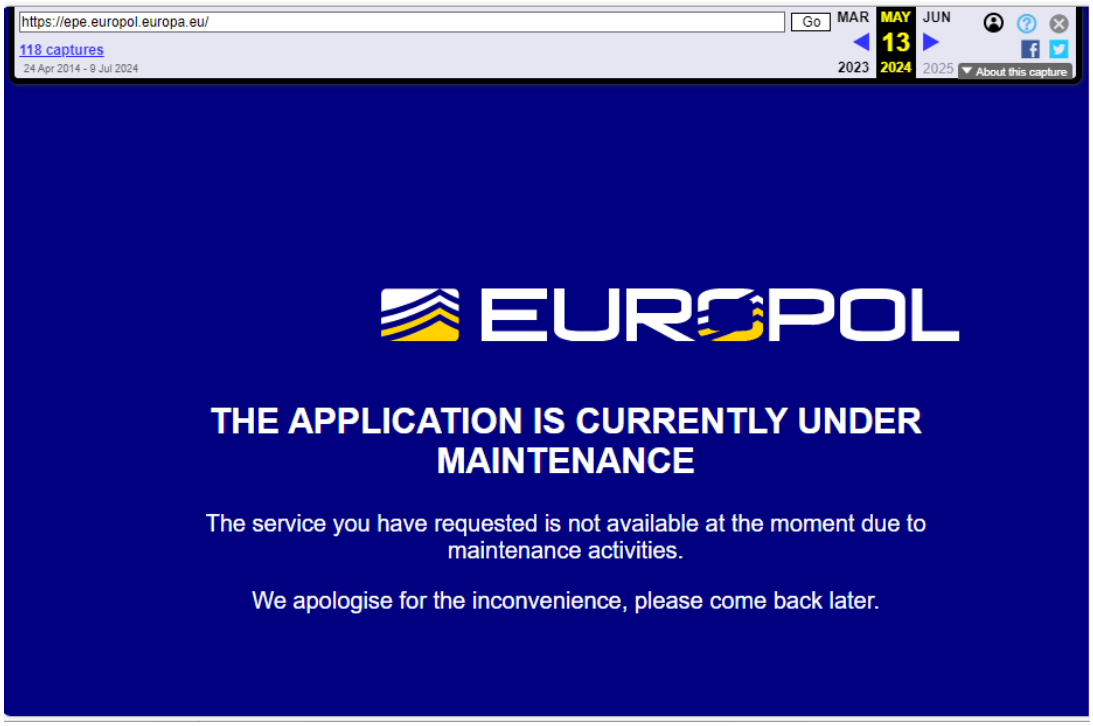


圖 15、刑警組織 Europol 網站 2024 年 5 月 13 日遭駭客入侵後情形，資料來源：自行截圖。

2. Maltego

可透過公開情報技術查詢 DNS 記錄、whois 記錄、搜尋引擎、社交網路等方式，發現資訊之間的關聯，以協助發現隱藏資料的關係和模式，屬於滲透測試人員的重要工具之一。

圖 16、以 DNS 追查可疑設備及 IP，資料來源：自行截圖。

3. Numverify

用於電話號碼驗證和地理定位的簡單 API，提供營運商和位置資訊，支援 232 個國家，包含台灣。

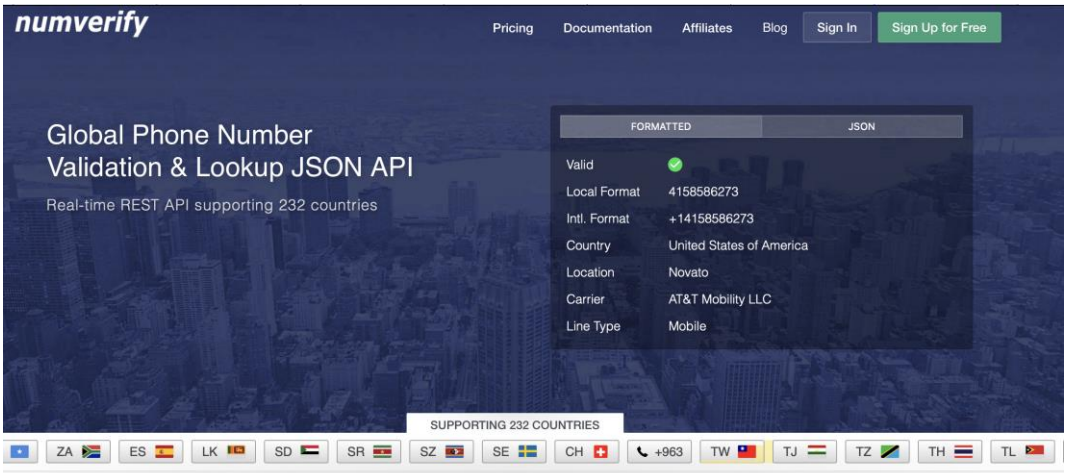


圖 17、Numverify 網站，資料來源：自行截圖。

綜上，在網路安全領域，OSINT 被視為評估安全風險和識別資訊科技系統漏洞的重要工具。許多組織運用 OSINT 來評估安全風險並找出漏洞，除了協助組織識別外在威脅外，OSINT 亦能用來評估內部風險，例如員工的線上行為可能引致的安全問題。而對於滲透測試或情蒐人員而言，透過 OSINT 取得目標網域資料、相關系統憑證資訊、目標使用者電子信箱、使用者名稱、密碼、API 資訊、機敏

性業務資料、基礎架構相關資訊等資訊，讓情蒐人員可進一步規劃或嘗試挖掘更多資訊。

OSINT 是一項強大的工具，能協助組織和個人從公開資訊中提取有價值的情報。然而，它也帶來隱私和安全的挑戰，因為駭客和其他威脅行為者也可能利用這些資訊進行惡意活動。因此，瞭解 OSINT 的運作原理和應用對於保護個人和組織安全至關重要。

(三)社群媒體情報(Social Media Intelligence，SOCMINT)

第三個主題是網路調查技術為社群媒體情報(SOCMINT)，SOCMINT 是指從社交媒體平臺收集和分析數據的過程，目的在於獲得有價值的資訊，進而做出妥適的商業決策並改進行銷策略。SOCMINT 是公開情報（OSINT）的一個子領域，主要聚焦在社交媒體網站上的資訊。

執行 SOCMINT 主要透過使用工具來收集和分析社交媒體數據來達成，一些常見的 SOCMINT 工具包括：

1. Who posted what

本工具係針對 Facebook 訊息，提供搜尋特定日期及關鍵字的貼文。

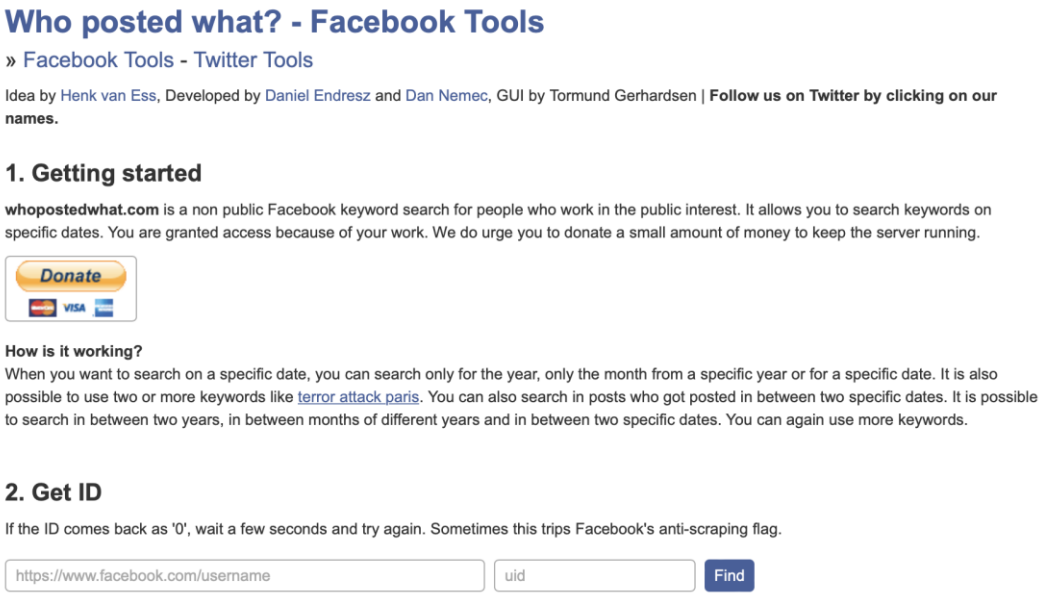


圖 18、Who posted what 網站，資料來源：自行截圖。

2. X Pro

原來稱 TweetDeck，是一款由推特(Twitter)提供的付費多功能社交媒體管理應用程式，用於幫助用戶更有效地管理和監控推特上的資訊流和互動。

透過搜尋功能，可隨時追蹤關鍵字新貼文。

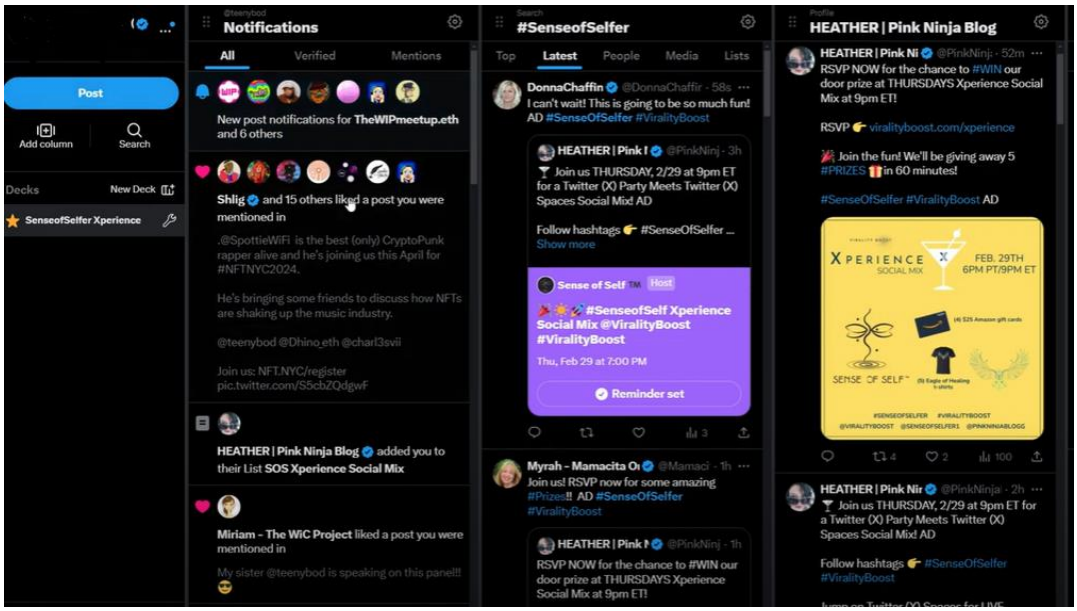


圖 19、X Pro 介面，資料來源：自行截圖。

3. Gramhir

是一個免費的 Instagram 帳戶分析與檢視工具，使用者不用登入並可匿名瀏覽，輸入 IG 帳號進行搜尋就能查看統計資料，有貼文、追蹤者、追蹤中數量，以及經由演算法產生的受歡迎程度。

最後提到隨著社群媒體的不斷發展和數據分析技術的進步，SOCMINT 將繼續成為情報收集和分析的重要工具。可預見它會協助組織更容易掌握公眾意見，預測市場趨勢，進而應對安全威脅。然而，隨著這些技術的發展，也需要政府或企業更多的監管和倫理考量，以確保個人隱私和數據安全。

社群媒體情報是一個不斷發展演進的領域，對情報和安全工作、市場行銷策略及公共政策制定都具有重要的影響；瞭解與適當地使用 SOCMINT，可為組織帶來巨大的價值，同時亦會對社會和個人隱私帶來影響。

(四)人類情報(Human Intelligence，HUMINT)

最後介紹人類情報(HUMINT)，HUMINT 是一種「實地」收集資訊的方式，透過人際交流和人力資源來收集情報。其主要目標為收集有關對手及其活動的資訊，以瞭解更多關於網路攻擊背後的人員，包括其動機、目標和技術。

HUMINT 通常透過間諜活動、偵查、審訊或證人訪問等方式進行，北約將 HUMINT 定義為「源自人類收集和提供資訊的一類情報」。這種情報收集方式的歷

史可追溯至古代，當時的間諜和使者已在國家間傳遞資訊。

隨著科技進步和全球化發展，HUMINT 將持續為情報收集的重要手段，未來的 HUMINT 可能會更依賴先進技術，如人工智慧和大數據分析，來提高資訊收集的效率和準確性。

人類情報是情報工作的關鍵組成部分，涉及國家安全、軍事、執法和商業等多個領域，隨著時代發展，HUMINT 將不斷適應新挑戰和機遇，但同時也需關注其對個人隱私和法律倫理的影響。

(五)實作案例

講者請學員就現場展示的加油站照片（如圖 20），利用課程介紹之工具搜索出加油站確切地址；後來得知是來自德國 2021 年 9 月 18 日社會案件後，進一步再請學員搜索出嫌犯姓名、相關社群帳號名、生日、電話、公司名稱及寵物名字等嫌犯背景資料，最終確實可透過社群媒體情報資訊，輕易地對比出嫌犯的活動軌跡及背景線索，此類課程互動過程加深學員對 OSINT 情資重要性之瞭解。

圖 20、德國加油站，真實事件案發現場，資料來源：自行截圖。

三、 隱私偵探：發現安卓系統資料外洩（Privacy Detective：Sniffing Out Your Data Leaks for Android，講者：Meggie He 及 Abbie Zhou）

講者 Meggie He 及 Abbie Zhou 介紹一款名為 Privacy Detective 的工具，開發此工具之原因，是因為發現 Android 系統上多個熱門應用軟體(App)存在個人隱私資訊外洩問題，同時也為符合歐盟隱私法規要求。這款工具主要是用來截取 Android 平台裡 App 中的所有資訊，再進一步判斷是否有任何資料外洩或不當蒐集使用者隱私資訊等不法行為。

本講題中介紹Privacy Detective工具，主要有3個模組，分別是資料收集(Data Collection)、資料處理(Data Processing)和資料分析(Data Analysis)，並說明Privacy Detective工具與Android系統介接方式(如圖21)。

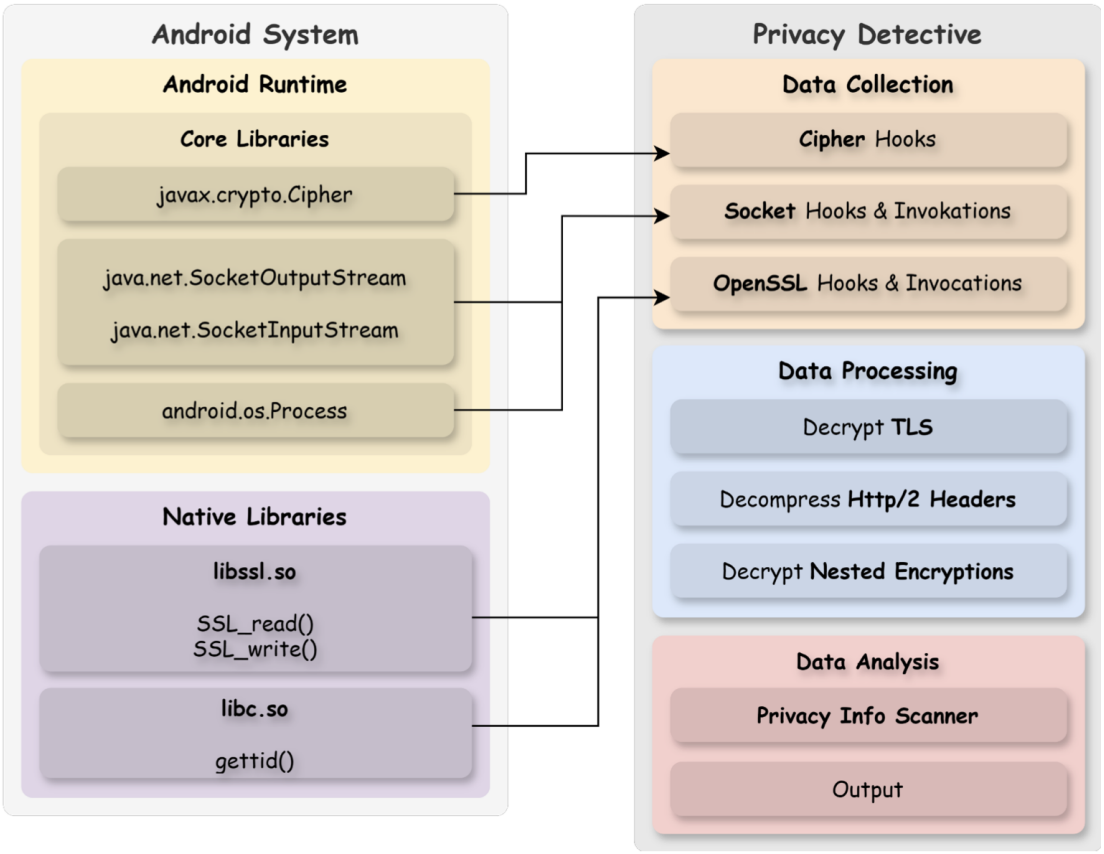


圖21、Privacy Detective工具與Android系統關聯，資料來源：講者簡報。

Privacy Detective工具運作方式是透過Android Frida框架，利用Hook方式進入Android平台的Java Runtime和Native Libraries，以攔截各種網路連線數據資料，包括TCP Socket、SSL連線、Cipher加解密等(如下)：

(一)在攔截到TCP Socket數據時，會記錄IP位址、連接埠號碼、執行緒ID等重要資訊。

(二)對於SSL連線是從Android的OpenSSL函式庫中取得SSL版本、Sequence Number等加密相關資料，另因Android沒有提供SSL連線的IP和Port資訊，因此必須改用執行緒ID來區分不同的TCP連線。

(三)Cipher加解密是讀取Java的Cipher類別、監控加解密運算，並蒐集加密區塊、演算法、金鑰等參數，藉此還原出原始的明文資料。

上述過程中，還特別額外處理因為攔截資訊而影響到 ByteBuffer 的 Position 問題，確保不會影響到原本的執行流程；針對 HTTP/2.0 連線，則是透過分拆 Client 和 Server 端的模擬方式，來解壓縮 HTTP Header 的內容。

最後獲得明文資料後，再使用自行開發的正規運算式掃描工具，查詢是否有任何個資、隱私權遭駭等違法行為，講師提及雖然部份 App 是合理地蒐集使用者位置資訊，無不法行為，惟仍要進一步分析才會得知其目的性。同時講者也提醒 Android 系統使用者應將軟體更新至最新版本，並刪減不需要的權限，來保護自己的隱私。

四、 從自帶驅動程式攻擊到零時差攻擊：揭開網路招聘詐騙中的高階漏洞（From BYOVD to a 0-day：Unveiling Advanced Exploits in Cyber Recruiting Scams，講者：Luigino Camastra 及 Igor Morgenstern）

本講題重點在於揭露北韓駭客組織Lazarus 利用Windows 系統的新零日漏洞(CVE-2024-21338)，散播一種名為 Kaolin RAT 的新型遠端訪問木馬(RAT)，成功獲取目標系統的 Kernel 最高權限，進而實現一系列惡意活動，例如檔案操作、命令執行以及與外部主機的連線等。

主要攻擊手法為以下步驟：(如圖 22)

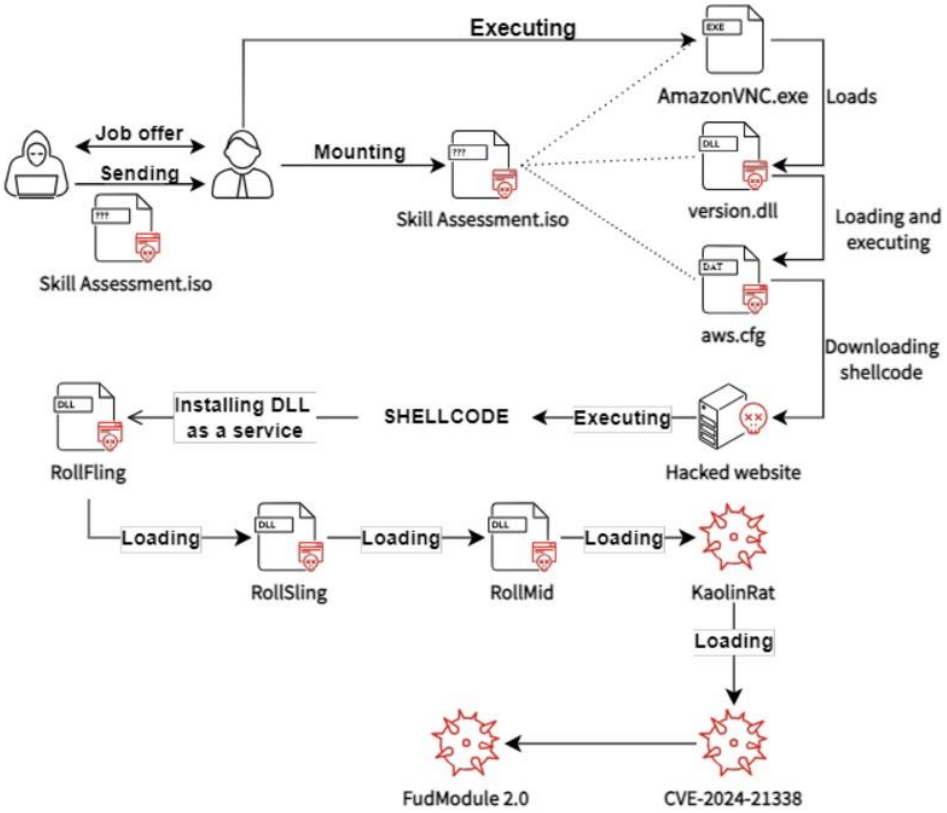


圖 22、駭客攻擊流程，資料來源：講者簡報。

(一)首先透過虛構的工作機會(LinkedIn、WhatsApp、電子郵件或其他平臺)傳送偽裝成 VNC 工具的惡意 ISO 檔案(此檔案包含 AmazonVNC.exe、version.dll 和 aws.cfg)，誘使受害者執行含有惡意程式 DLL 檔案，進而在受害者電腦中下載 shellcode。

(二)接著受害者電腦將主動執行 shellcode，自動安裝及執行一系列 DLL 檔案；第 1 個是 RollFling 檔案，此 DLL 檔案被視為服務程式，用於檢索和啟動名為 RollSling 下一階段惡意軟體。第 2 個是 RollSling 檔案，可直接在記憶體中執行，是為了逃避安全軟體的偵測。第 3 個為 RollMid 檔案，最主要功能是觸發 Kaolin RAT 的新型遠端訪問木馬(RAT)，一樣是在系統記憶體中執行。

(三)最後 Lazarus 組織開發了一個名為 FUD 的 rootkit 模組，能夠透過資料導向攻擊的方式，繞過多種主流的防毒和 EDR 等安全方案。FUD 模組實施了 9 種不同的 Kernel 物件操作技術，包括禁用回呼函數、過濾驅動程式、阻斷 ETW 記錄等，達到隱藏惡意活動的目的。

Lazarus 組織的動機可能是以獲利為主，透過感染個人電腦進而滲透企業網路，實現進一步的攻擊目標。Lazarus 組織投入大量資源，開發高階的 APT 攻擊手法，具有極高的隱蔽性，展現出攻擊能力水準。最後講者建議為應對類似 APT 攻擊，應加強培訓員工的安全意識，使他們能夠識別和應對釣魚郵件、惡意連結和可疑附件。

五、 毒蘋果行動：追蹤信用卡資訊竊取到付款詐欺（Operation PoisonedApple：Tracing Credit Card Information Theft to Payment Fraud，講者：Gyuyeon Kim 及 Hyunho Cho）

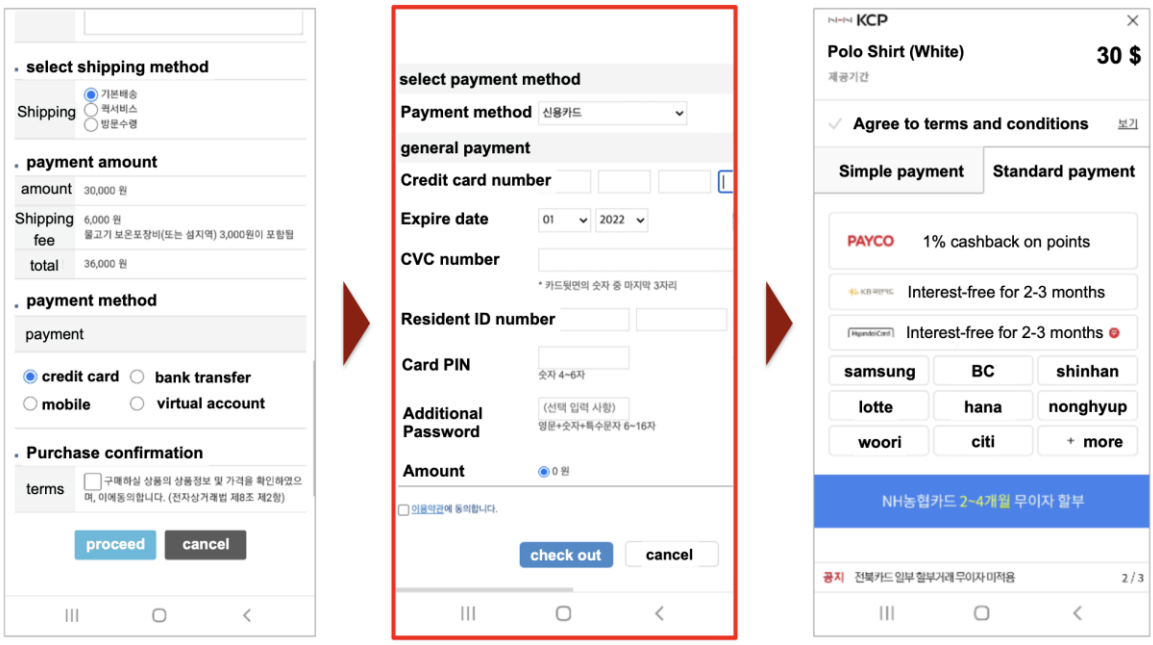
講者為韓國金融安全研究所(Korean Financial Security Institute)研究人員 Gyuyeon Kim 及 Hyunho Cho，他們分享在 2022 年 9 月發現了超過 50 家合法線上商店的一系列網路攻擊事件，並進一步察覺到當中有重大資料外洩事件。

駭客會設法操作這些線上商店的付款頁面，將信用卡、個人資料，以及合法資料傳輸到他們的伺服器中。為了不被發現，這些駭客組織利用多種漏洞與工具，採用各種規避策略來防止網站管理員與使用者偵測他們的網路釣魚頁面。此外，竊取信用卡資料只是這項計畫的一部分，研究顯示駭客獲利的主要方式之一是利用 Apple Store Online 的取貨政策漏洞，來進行犯罪。

首先對 5,000 多個功能變數名稱進行了檢測和分析，他們發現了 50 個被入侵的網站。駭客組織使用幾種方法來獲得對服務的初始連結行為，其中之一是 SQL 注入。

透由在易受攻擊的網站上成功注入 SQL，進而獲得了網站的管理員登入權限，隨著 Webshell 部署在伺服器上，駭客能夠持續連結伺服器，並透過 Webshell 在系統上執行命令。

當駭客可完全控制被入侵的網站時，他們使用網路釣魚工具程式在被入侵的伺服器上部署幾個網路釣魚頁面，這些網路釣魚頁面會嵌入在正常網站上蒐集付款資訊頁面（如圖 23）。



inserted the phishing payment page

圖 23、網路釣魚頁面，資料來源：講者簡報。

接著發現駭客使用與過往截然不同 3 種手法來獲取收益，有別於一般駭客通常使用暗網論壇上出售資訊，或是使用它們進行欺詐性交易：

(一)在二手交易平臺上欺詐性付款後退款：駭客使用被盜的信用卡資訊在二手交易平臺上購買物品。接著，駭客要求賣家退款，並要求他們收取少量費用，例如 20 美元取消。這筆退款金額被轉移到駭客集團擁有的另一個銀行帳戶，這使其成為某種洗錢技術。

(二)在公開二手交易平臺上銷售一些電子產品，感興趣的買家購買商品後，將錢轉入駭客的帳戶。隨後，駭客立即在其它公開市場以被盜的信用卡購買同一物品，並填入買方的送貨地址，如此買家誤認為他們用真實的錢從真正的賣家那裡購買產品。

(三)與案例 2 類似，駭客使用二手交易平臺來販售蘋果產品，再利用蘋果官網上購物及設定「其他人取貨」的選項(如圖 24)，讓買家可以前往蘋果直營店提取那些使用被盜信用卡購買的產品，而蘋果的隱私政策不允許披露買方的任何個人資訊，這使得執法當局更難追蹤這些駭客。

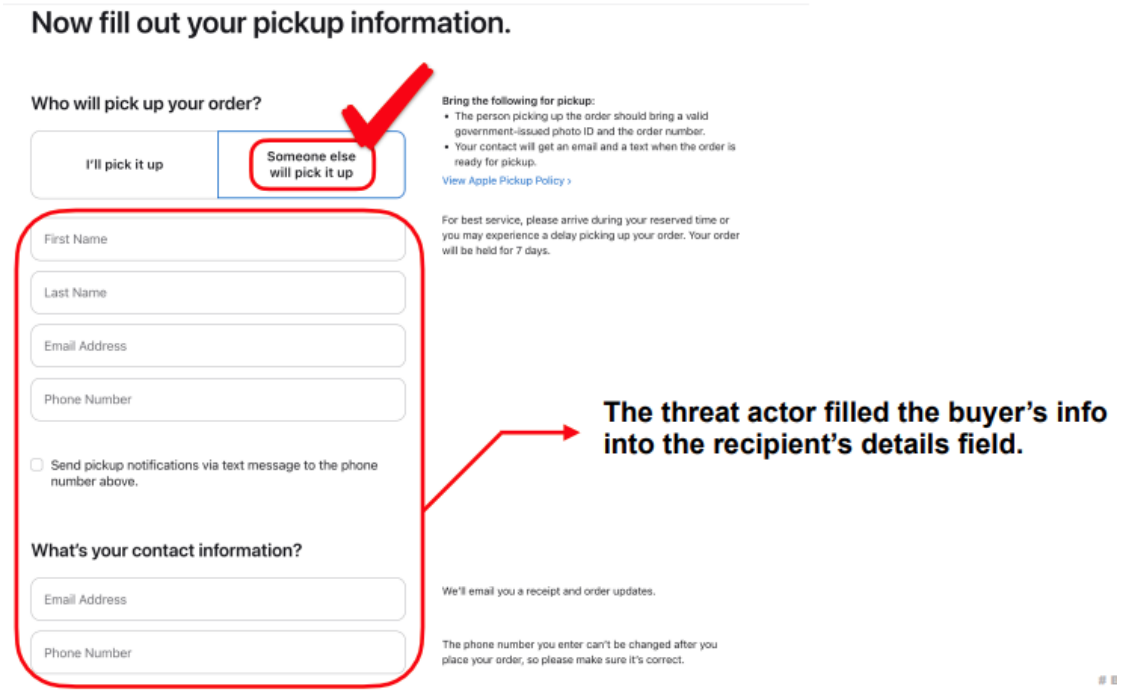


圖 24、蘋果官網「其他人取貨」頁面，資料來源：講者簡報。

進一步調查被盜網站的網路釣魚頁面時，發現了一個與駭客相關的特定電子郵件位址，接著追蹤並歸咎此攻擊活動來自一個名為"Evil Queen"的新駭客團體，該團體自 2009 年起就在亞洲國家進行網路攻擊活動，目前這項犯罪計畫的影響範圍為韓國與日本，駭客持續發展新的詐騙手法，未來可能會在其他國家出現現。

六、 端點偵測與回應重裝上陣：遠端清除數據（EDR Reloaded: Erase Data Remotely，講者：Tomer Bar 及 Shmuel Cohen)

SafeBreach 公司安全研究副總裁 Tomer Bar 及其安全研究員 Shmuel Cohen 在演講時指出，端點偵測及應變機制(Endpoint Detection and Response, 簡稱 EDR)是保護電腦系統免受各種惡意軟體威脅的最重要工具，通常包含多層檢測模組，亦包括位元組簽章偵測邏輯，通常被視為最可靠、誤報率最低。

然而網路攻擊者可以透過網路，從已完全修補的伺服器上遠端刪除關鍵數據，講者請學員思考，如果供應商釋出的更新檔仍可被利用時，怎麼辦？

首先介紹 CVE-2023-24860 之原始漏洞，該漏洞可未經身份驗證地遠端刪除整個生產資料庫等關鍵檔，目前測試過的三種知名端點安全產品，在預設設定下都存在該漏洞，並且完全無法偵測到，該漏洞可以在 Linux 和 Windows 上利用至少十種不同的攻擊向量，幾乎沒有任何限制。

講師解釋相關的根本原因，並實際在未修補的機器上展示多種攻擊向量，例如遠端刪除整個資料庫，在大多數情況下，資料庫服務和受影響的資料都無法輕易恢復（圖 25）。

Second report to Microsoft - CVE-2023-24860 patch analysis

Fixed Attack Vectors	unFixed Attack vectors
Remote deletion of Windows Event Log file	Remote deletion of IIS log file
Remote deletion of MySQL database	Remote deletion of Apache log file
Remote deletion of PostGRESQL database	Remote deletion of NGnix log file
Remote deletion of MongoDB database	Remote Deletion of Filezilla server log file
Remote deletion of MariaDB database	VMware deletion of VMX file
Unprivileged deletion of Windows Event Log file	Unprivileged deletion of Defender detections Log file
Local deletion of VMware VMDK files	

圖 25、安裝安全性更新檔後，部分 LOG 仍可被遠端刪除，資料來源：講者簡報。

最後展示電腦在已安裝 CVE-2023-36010 漏洞之安全性更新檔後，實作如何繞過微軟安全機制，仍然可以遠端執行刪除 MYSQL、MariaDB 資料庫和 VMware 設定、拒絕 MongoDB 服務、影響 PostgreSQL、遠端刪除 Web 伺服器日誌，Windows Defender 亦會刪除自己的偵測日誌，影響相當重大。

七、 匯流排故障：新穎的匯流排故障攻擊方式破壞嵌入式系統中的可信執行環境（Faults in Our Bus: Novel Bus Fault Attack to Break Trusted Execution Environments in Embedded Systems，講者：Nimish Mishra）

印度理工學院克勒格布爾校區學者 Nimish Mishra 指出，近期出現了像可信任執行環境（Trusted Execution Environment，TEE）之類的技術，除了可確保安全，甚至可在不受信任的作業系統上防禦攻擊者，因此 TEE 已是嵌入式系統核心中的重要機制。

在物聯網環境中，實體攻擊（如旁通道攻擊和故障攻擊）越來越重要，透過物理特性（如電磁遮罩）或軟體檢查（記憶體加密），TEE 可以防禦對處理器和記憶體晶片的實體攻擊。

這份研究顯現了不同攻擊層面，首先在晶片系統（SoC）匯流排上，可以挖掘「資料匯流排」和「位址匯流排」這 2 個匯流排的故障特徵，然後將一套可信任執行環境（Open Portable Trusted Execution Environment，OP-TEE）掛載到 Raspberry Pi3 嵌入式系統上，並針對該系統進行實體攻擊，進而發現 TEE 中（特別是 GlobalPlatform API 規格）是有漏洞，這方式有助於發現 Linux 函數定期回傳數值中可能的潛在漏洞。

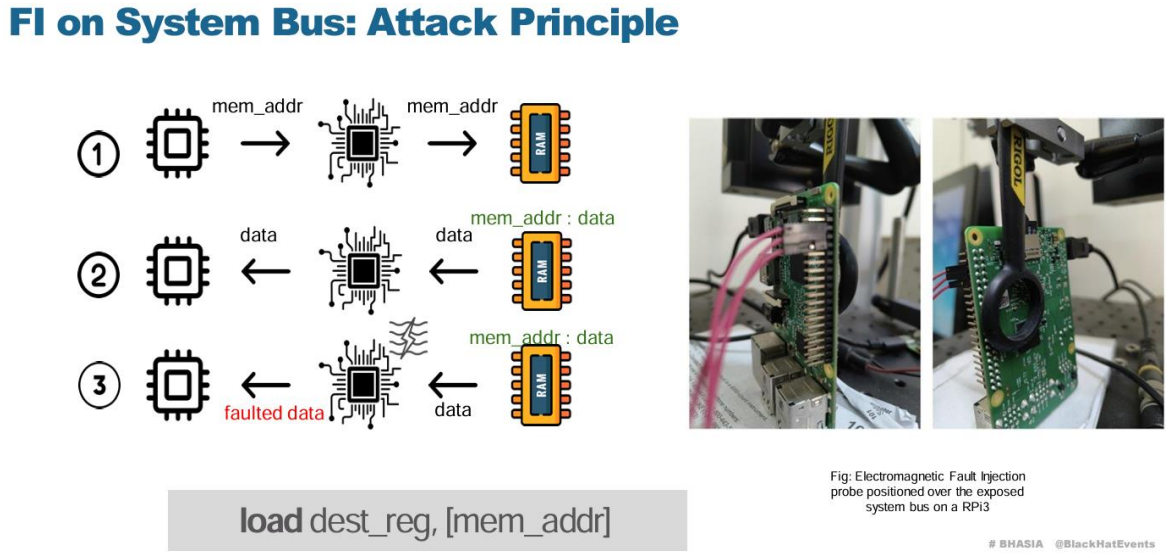


圖 26、實體故障注入攻擊情形，資料來源：講者簡報。

該研究提出了嵌入式系統領域需要重新審視嵌入式系統的 API 規範，以及 TEE 的軟體開發時，不僅記憶體會出現緩衝區溢位，還要另外注意系統匯流排，這項研究強調了抽象規範的軟體實作時，需要考慮實際執行環境的重要性。

八、 網路營運中心報告（Network Operations Center Report，講者：Neil Wyler 及 Bart Stump）

Black Hat 的網路營運中心(NOC)應該是在世界上最艱鉅的環境之一，因為全世界的黑帽駭客們為了展現他們超凡的資安技術，無所不用其極的攻擊這個網站，NOC 必須提供高安全性及可用性的網路環境。

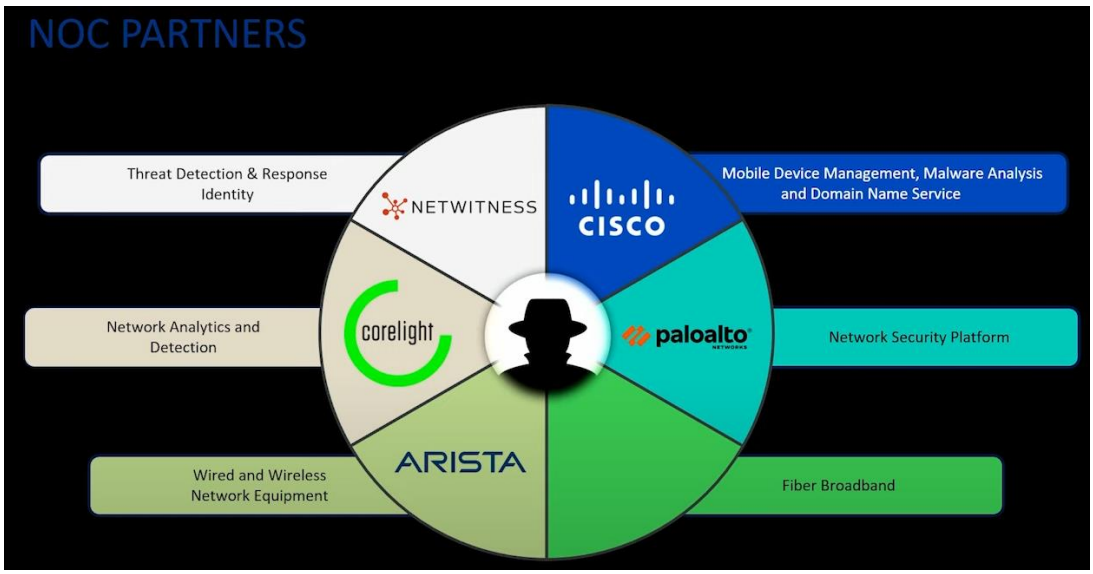


圖 27、Black Hat NOC 成員，資料來源：講者簡報。

這個團隊的成員並非都屬同一團體或公司，而是由許多公司中的精英們組成，在 Black Hat Asia 活動開幕的幾個月前，需就網管人員、網路設備、環境進行規劃及部署，必須提供並保證活動期間正常運作及其安全性、穩定性，且必須呈現實際網路狀況給所有人，最後的成果也讓人相當驚豔，活動期間均未有遭駭侵事件發生，直到閉幕都保持網路正常運作。

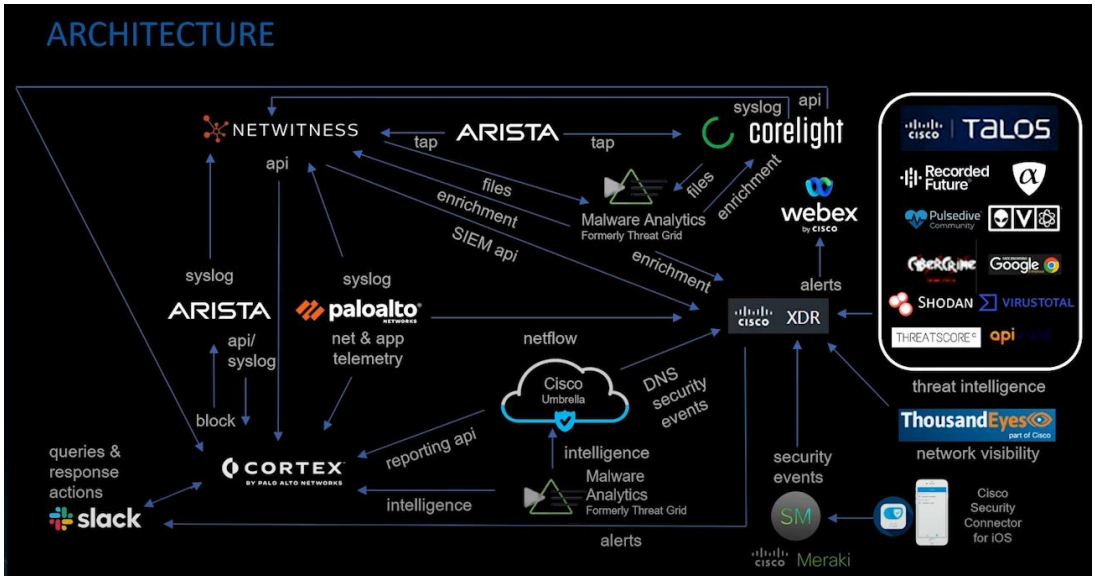


圖 28、BlackHatAsia 網路架構，資料來源：講者簡報。

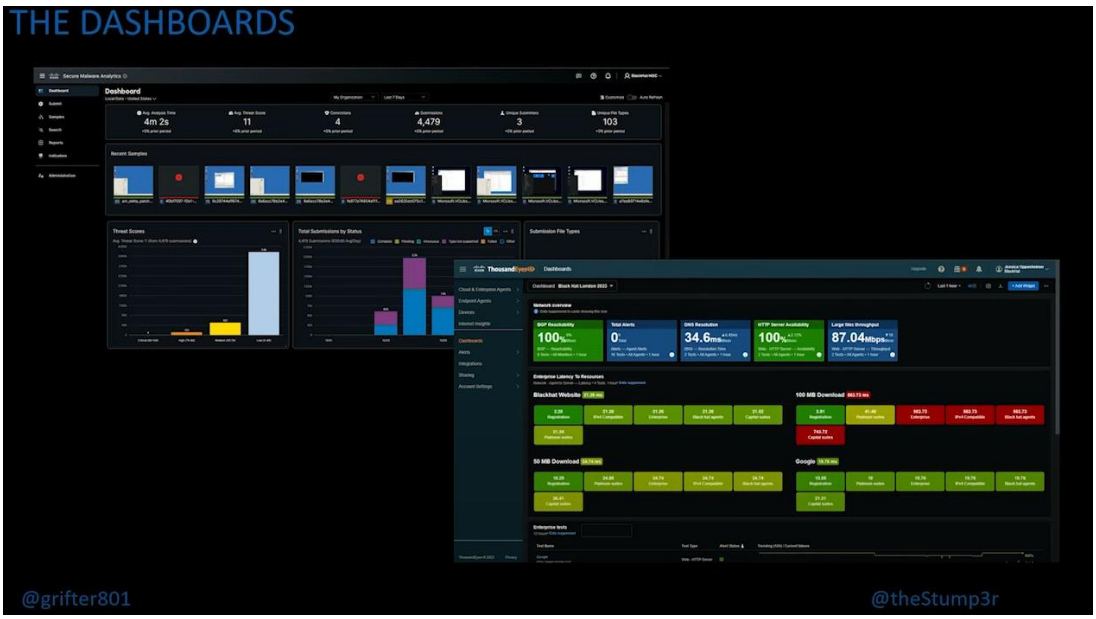


圖 29、NOC 儀表板，資料來源：講者簡報。

肆、 心得與建議事項

參加 Black Hat Asia 2024 是一次非常寶貴的經歷，給我們留下了深刻的印象，並對未來的職涯產生了正面且積極的影響，以下為此次參會的一些心得和收穫。

一、 主題演講（Keynote Sessions）

會議的主題演講是邀請了各面向的網路安全領域專家和學者與會，深入綜觀探討了當前網路安全的現狀、新興資安威脅以及未來的發展趨勢，特別是關於資料科學與機器學習在網路安全中的應用，以及如何利用各類資安技術來增強網路安全威脅檢測和應變的演講，分享了他們的研究成果和實際經驗，並強調了事前防範資安威脅及保持學習的重要性。

圖 30、各類會議資訊，資料來源：自行拍攝。

二、 工作坊課程（Workshops）

透過工作坊課程，以實際操作、參與者熱烈地討論，將理論知識運用在實際環境中，不僅有助提升資安技術水準，也拓展了不同面向的知識，深入解析某種攻擊技術的細節，並提供防禦方法，也更加深刻地認識到資訊安全及人工智慧跨領域的結合，對未來的重要性及前瞻性；亦提供了與專家直接交流的機會，通過實戰演練強化參與者的技能，更深入理解複雜的技術概念，提高實際操作能力，對我們未來的工作非常有幫助。

(一) 資料科學和機器學習在網路安全中的應用

從因地緣政治，我國屬全世界最容易遭受網路攻擊的地方之一，本署已有來自政府機關、關鍵基礎建設、私部門及國際合作之資安情資共用機制，而面對勢不可擋的 AI 技術，應嘗試將 AI 技術導入資安防禦技術中，爰建議未來可朝向：

1. **國家級資安威脅分析平台導入 AI 技術輔助機制**：綜整國家級資安監控中心（N-SOC）、國家級資安資訊分享與分析中心（N-ISAC）及國家級資安通報應變中心（N-CERT）之情資，加上台灣電腦網路危機處理暨協調中心（TWCERT/CC）、鑑識資料及國外資安情資，運用機器學習技術或深度學習演算法，進行各種威脅行為的交叉比對、分析及預測，找尋已知的 APT 駭客組織，更進一步挖掘並預測可能潛在的網路攻擊手法及 APT 駭客組織，以強化整體資安威脅防禦能力。

2. **政府領域骨幹流量辨識導入 AI 機制判別惡意行為**：運用機器學習技術分析 IoA 或 IoC 等資訊，自動化流程可減少人工辨識時間，有效並快速通報受駭機關，資通訊設備是否是否處於網路威脅中，以增加資安韌性。

而發展資安技術的同時，其資料隱私和安全問題也將變得更加重要，要注重倫理和法律框架的建立，以確保 AI 技術的安全和可控性。

(二) 網路調查與人類智能之基礎原理

OSINT、SOCMINT 和 HUMINT 是用於收集和分析公開資訊和資料，進行調查的情報收集方法，工具包括免費來源或是產品訂閱，如搜尋引擎、公開和商業線上工具及報紙訂閱期刊等，未來會更依賴先進技術，如人工智慧和大數據分析，來提高資訊收集的效率和準確性。

三、 技術簡報（Technical Briefings）

技術簡報多樣豐富且引人入勝，涵蓋了進階持續性威脅（APT）、惡意軟體逆向分析、漏洞研究、供應鏈安全和安全編碼等多方面的內容。其中，關於零日漏洞的簡報（從自帶驅動程式攻擊到零時差攻擊：揭開網路招聘詐騙中的高階漏洞）尤為突出，演講者通過展示真實世界的漏洞利用和討論緩解策略，深入剖析了網路攻擊的複雜性和防禦的必要性，這些簡報的技術深度令人印象深刻，滿足了不同專業水準與會者的需求，使大家滿載而歸。

四、 安全工具產品展示區（Arsenal）

主要為由網路安全社區開發的各種開源工具和專案展，提供許多實用的工具，證明他們增強網路安全能力；新工具在網路監控、事件回應和威脅情報方面的展示尤其令人印象深刻，展示區的協作精神突顯了新創業者對網路安全領域的貢獻，在推動資安技術領域上發揮了合作的重要性。

圖 31、安全工具產品展示區，資料來源：自行拍攝。

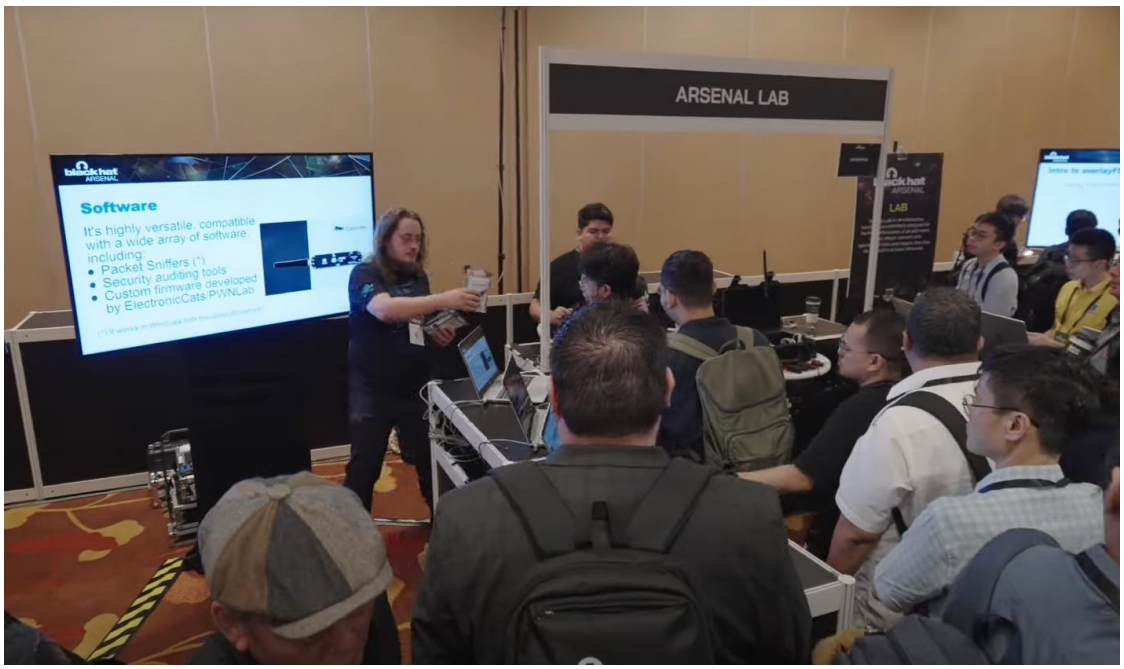


圖 32、安全工具產品展示區，資料來源：自行拍攝。

五、 總結

參與 Black Hat Asia 2024 會議，豐富了我們的資安專業知識及最新資安威脅，拓展我們的視野，為我們的職涯發展帶來了新的啟示和動力，特別是針對人工智慧、網路威脅情資分析、資安漏洞、滲透測試、紅隊攻擊、逆向工程及物聯網安全等議題，讓我們對目前資訊安全領域的發展有了更深入的瞭解及想像，這些內容都讓我們受益匪淺，並深信這些收穫將在未來的工作中發揮重要作用。