出國報告（出國類別：開會）

出席BotConf 2023會議出國報告書

服務機關：數位發展部資通安全署

姓名職稱：陳慧敏分析師

派赴國家：法國

出國期間：112 年4月11日至14日

報告日期：112 年 7 月

摘 要

此次出國任務係出席 2023 殭屍網路威脅情資會議(BotConf, The botnet & malware fighting conference)，研討會於 2023 年 4 月 11 日至 14 日於法國聖特拉斯堡舉行，主辦單位 AILB-IBFA (Alliance internationale de lutte contre les botnets, 暫譯為國際機器人/殭屍網路打擊聯盟)為法國非營利組織，每年舉行會議分享相關網路威脅情資，致力提升網路安全性。

本次研討會來自全球 30 個國家 400 多名參與人員，匯集學術界、工業界、執法部門和獨立研究人員，研究對抗殭屍網路的相關議題，研討會主題包含殭屍網路的運作、散佈殭屍網路相關惡意軟體的方法、參與殭屍網路開發或管理的團體組織等。為瞭解網路資通訊安全議題及網路威脅情資新知、協力共創安全的網路環境，資安署派員參與本次研討會，以掌握最新殭屍網路樣態及因應之道。

目 次

壹、目的

BotConf(The botnet & malware fighting conference)是一個國際科學會議，每年約聚集 400 名以上來自世界各地的執法人員、學術界、電腦資安事件應變小組（Computer Security Incident Response Team，CSIRT）、威脅分析團隊及防毒開發人員，致力於對抗惡意軟體及殭屍網路組織。藉由參與實體研討會，獲得最近駭客攻擊手法、與會者對各議題之想法，將有助於與會者瞭解最近關鍵議題及因應對策。

貳、會議經過

一、**會議日期：**2023 年 4 月 11 日(星期二)至 14 日(星期五)

二、**會議地點：**法國聖特拉斯堡(Strasbourg, France)

三、**與會人員：**來自全球 30 個國家約 400 名學術界、執法部門和獨立研究機構人員。

四、**參與場次表：**研討會第 1 天(4 月 11 日)是小型研討會，主要會議在 4 月 12 日至 14 日舉行。

日期	重點參加場次
4 月 11 日	One SMALI step for man, one giant step for researchers
4 月 12 日	Security Implications of QUIC
	RAT as a Ransomware - An Hybrid Approach
	Cyber Swachhta Bharat - India's answer to botnet and malware ecosystems?
	The Fodcha Botnets We Watched
4 月 13 日	Yara Studies: A Deep Dive into Scanning Performance
	MCRIT: The MinHash-based Code Relationship & Investigation Toolkit
4 月 14 日	When a botnet cries: detecting botnets infection chains
	The Plague of Advanced Bad Bots : Deconstructing the Malicious Bot Problem

五、會議重點摘要

本次 BotConf 會議由歐洲理事會資訊社會部負責人(Head of Information Society Department, Council of Europe) Patrick Penninckx 先生代表致歡迎詞後開始。

圖 1：Patrick Penninckx 先生致詞

(一) One SMALI step for man, one giant step for researchers

1.講者：Gabriel Cirlig, White Ops

2.重點摘要：

(1)講者針對 Android 逆向工程進行簡單介紹，帶領與會者從零開始，在虛擬機上逐步安裝工具軟體；課程內容涵蓋 Android 基礎知識、APK 結構、DEX 文件內部結構以及如何利用這些知識來反組譯惡意軟體。

(2) Android 套件(APK)：Android 套件是以 apk 為副檔名於 Android 作業系統或許多其他以 Android 為基礎的作業系統，用於發布和安裝 APP 及中介軟體，APK 檔案格式接受以 JAVA 或 Kotlin 語言為原始碼撰寫的檔案，並使用 Android App Bundles 產生該種格式的檔案。一個 APK 檔案套件包含.DEX 檔案、清單檔案(manifest file)、資源檔案(resources)、簽名摘要資訊等。在 linux 環境中可使用內建的指令(unzip)將 apk 拆開，拆開後大致

會有以下幾個資料夾，如圖 2。

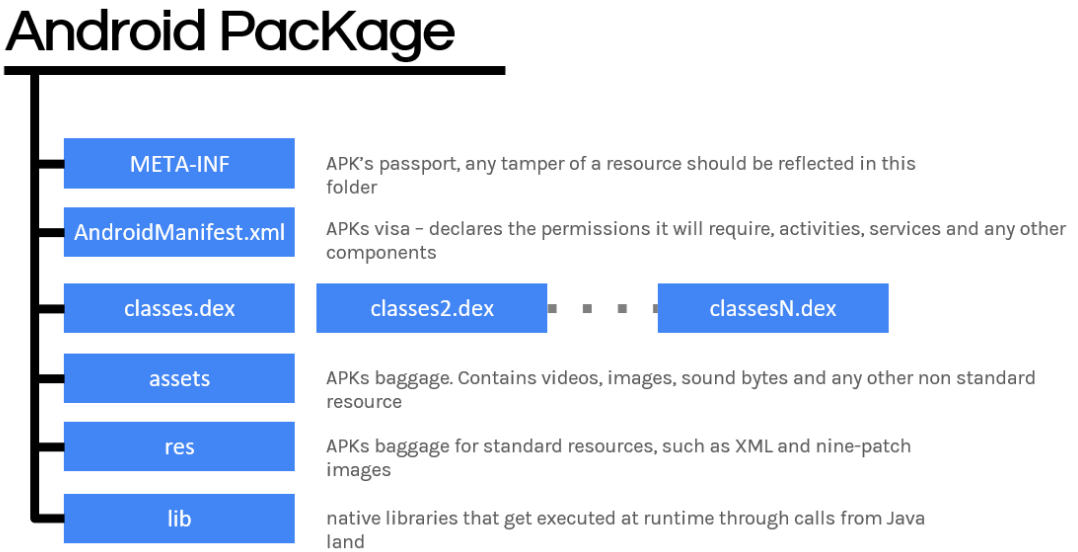

圖 2：APK 檔案組成(資料來源：研討會簡報資料)

(3)重組 apk 工具(Apktool)可以將 apk 重新打包組裝成.apk 檔，指令為 apktool b 解壓縮後的資料夾名稱 –o 新的 apk 名稱。Apktool 也有提供反編譯的功能，指令為 apktool d apk 資料夾路徑。使用 apktool 反編譯後，會出現 smali 資料夾，是 app 程式碼的 byte code(高階語言經過編譯的中間碼)，使用 jadx 工具可以將 byte code 還原出 Java 原始碼。

(4)在虛擬主機反編譯及打包 apk 檔需要先建置 Android 開發環境，因此必須安裝 Java 的軟體開發套件 JDK(Java Development Kit)，再安裝 Android Studio(Android 平台開發程式整合開發環境)， Android Studio 依模組顯示專案檔案及即時編輯功能，提升 Android 應用程式建構效率。

(二) Security Implications of QUIC(主題演講)

1.講者：Paul Vixie 博士, AWS Security

2.重點摘要：

(1)Internet 長期以來是 Web 的通訊基礎，使用 TCP/IP 協定傳輸明文訊息。2013 年著名的愛德華·史諾登 (Edward Snowden) 披露了一些美國國家安全監聽資料並飛往香港，從那之後，Web 社群重新考慮是否繼續明文傳輸以及傳輸協定由作業系統核心(kernel)啟動的機制。考量的結果是採用

QUIC(Quick UDP Internet Connections)，一個完全的加密傳輸協定，實作於應用層。

(2) QUIC 是由 Google 提出的傳輸層協定，因 TCP 協定有一些發展之初未考慮到的缺陷，於是 QUIC 將整個協定建構在 UDP 之上，QUIC 協定除了改善 TCP 從系統核心啟動的缺陷(核心中不再有 connect()及 accept()系統呼叫)，主要的目的是在預設情況下完整的端點至端點的通訊保密，並且可以更快的建立連線，更快的開始傳送資料，降低延遲時間。

(3)講者試著探討網路端點的安全變得沒有效率之原因

(a)無限的複雜性，大多數人知道得很少，很少人知道得很多，沒有人知道全貌。

(b)供應商、軟韌體版本、修補程式、人員、政策的頻繁異動。

(c)備份作業、日誌記錄、驗證機制等，所有這些做到「夠好」都需要付出昂貴的成本。

(d)不對稱的獎勵，攻擊可以賺取利潤，然而防守卻要付出具大成本。

(4)2013 年愛德華·史諾登 (Edward Snowden)前往香港，並且披露了一些重要的內容，在那之後，IETF(Internet Engineering Task Force, 網際網路工程任務組)邀請愛德華·史諾登發表全體演講，並且做出「普遍監控是一種攻擊」及「網際網路使用者的福祉應該被優先考量」的結論。

(三) RAT as a Ransomware - An Hybrid Approach

1.講者：Nirmal Singh 博士和 Avinash Kumar 先生, zscaler ThreatLabZ

2.重點摘要：

(1)在過去的幾年裡，講者看到惡意軟體即服務 (Malware-as-a-Service, MaaS)市場的大幅增長，這種收入模式為惡意軟體開發人員帶來了高收益，也讓技術較低的惡意威脅者更容易上手，透過攻擊大型企業和政府機構賺取數百萬美元。MaaS 團體銷售具有各種功能和訂價的複雜模組化遠端存取木馬程式(Remote Access Trojan, RAT)，這種遠端存取木馬程式最顯著的

模組是勒索軟體模組，手法是將資料加密並要求支付贖金才能解密，這些特徵使講者相信，所涉及的惡意威脅者正試圖透過使用勒索軟體來提高他們的經濟收益。

(2) Win32.Backdoor.RemcosRat 是 ZScaler Cloud 位居榜首的 RAT 威脅，佔所有威脅手法的 35%，不同的 RAT 威脅也有不同的功擊目標，例如 Gh0stRAT 攻擊的目標鎖定科技業、製造業及政府機構；RemcosRAT 鎖定能源、航空領域；QuasarRAT 鎖定外交和政府機構等。

(3)講者團隊發現一個新的 RAT(Anarchy Panel RAT v4.4)使用勒索軟體模組，雖然未發現惡意活動使用這個新的 RAT，但在可預見的未來，它會被使用於惡意活動，因為 Anarchy Panel RAT v4.4 在今(112)年 1 月在論壇上被發布，且在 Github 帳戶也發布它的攻擊特徵，例如：勒索軟體及感染主開機紀錄(MBR)、隱藏的遠端共享桌面軟體木馬等。

(4)頂級的 RAT 視其他應用程序提供的新功能可以隨時改變，惡意軟體組織使用來自不同惡意軟體家族的代碼版本，重新利用程式碼模組，組合成新版的惡意軟體。講者認為在未來這類型的惡意軟體將有更多功能，並且與其他類型惡意軟體組合，以達到惡意軟體組織增加收益的目的。

(四) Cyber Swachhta Bharat - India's answer to botnet and malware ecosystems?

1.講者：Pratiksha Ashok 博士, Uclouvain

2.重點摘要：

(1)2014 年，印度政府啟動了 2 階段的 Swachh Bharat Abhiyan(清潔印度運動)，用於清潔街道以促進公共衛生，任務除了清潔道路、衛生運動和垃圾分類，還包括安全的數位印度。2017 年，印度政府成立殭屍網路清理和惡意軟體分析中心(Cyber Swachhta Kendra)，該中心根據印度的「國家網路安全政策」目標設立，政策預計在印度創建一個安全的網路生態系統，並與 ISP 業者、防毒軟體公司密切協調與合作，為用戶提供資安警訊和工具以保護他們的系統/設備，當用戶的系統/設備存在惡意軟體攻擊

事件時，可以使用這些工具來刪除用戶設備上的殭屍網路或惡意軟體，而且工具由政府免費提供。除了提供用戶使用，亦鼓勵金融機構使用這些工具。

(2)講者試著探討政府是否應該提供有關惡意軟體和殭屍網路的解決方案及工具，以及提供此類工具的成效，目前印度政府以共同參與開發研究與投資的作法提供解決方案及工具。講者試著以從經濟、技術和法律的角度來探討優缺點，如：由政府提供目前惡意威脅軟體清單的可行性，優點是可以讓全部用戶避免使用正在傳播的惡意威脅軟體；缺點是政府無法即時提供所有的惡意威脅軟體清單，且惡意威脅軟體發展非常迅速，也會造成政府開發解決方案工具速度跟不上的困境。如果由政府免費提供可行的解決方案，對政府的財政將是沈重的負擔，致力於提供惡意程式解決方案的私人企業將會倒閉。

(3)是否由政府提供威脅軟體解決方案議題，講者以一個律師的角度探討，認為必須取決於國家的政權及主權目標。就印度而言，印度仍然是一個國民年收入較低的國家，人種非常多元，網際網路對普羅大眾而言是奢侈品，在一般大眾無法取得網路資源情況下，印度政府考量提供人民安全的數位環境、保護隱私及避免用戶個人資料的濫用，仍由政府提供威脅軟體解決方案，其他國家政府則不一定適合採取這種策略。以印度國情，目前仍然適合採取這種策略。

(五) The Fodcha Botnets We Watched

1.講者：Lingming Tu, Network Security Research Lab, Qihoo 360 Technology Co. Ltd.

2.重點摘要：

(1) Fodcha 是一個針對 Linux 物聯網(IoT)設備的新殭屍網路家族，在開發過程中，Fodcha 吸收許多 Mirai 殭屍網路的特點。自 2022 年 1 月首次被

偵測後，已在超過 140 個 C&C 網域(command-and-control domain)中找出分屬到 4 個 Fodcha 變種的 250 多個樣本，大多數 C&C 伺服器已被講者的追蹤系統成功發現，並檢測到超過 39,000 個受害者接收到 11,400 萬個攻擊命令，依講者統計，在 2022 年 3 月 20 日到 4 月 10 日之間，每日約 1 萬台 IoT 設備遭到感染。

(2)Fodcha 殭屍網路感染和攻擊的目標遍佈世界各地，沒有針定特定國家或行業發動攻擊，主要尋找曝露在網路上且存在漏洞的設備，包括路由器、監控主機(DVR)、GitLab 伺服器、Android ADB 除錯伺服器等，再使用 Crazyfia 工具暴力破解主機帳號密碼，部署殭屍網路病毒。

(3)摘述 2022 至 2023 年 Fodcha 殭屍網路惡意活動：

(a) 2022 年 6 月，Fodcha 對中國大陸某一省的健康碼組織發動 DDoS 攻擊。

(b)2022 年 9 月，其團隊在協助執法部門修復某公司語音業務遭受 DDoS 攻擊的證據過程中，發現 Fodcha 是幕後黑手。

(c)2022 年 9 月，某知名雲端服務商向 Qihoo 360 Technology Co.諮詢一個流量超過 1Tbps 的攻擊事件，經過數據交叉比對，確定攻擊者為 Fodcha。

(d)2023 年 1 月，Navicat 中文官網遭受 DDoS 攻擊，使用戶無法連到官網，官網持續癱瘓了 2 至 3 天。發動攻擊的殭屍網路屬於 Mirai 家族(亦包含 Fodcha)，在攻擊最高峰的 3 小時內，攻擊者共發動了 45 條攻擊指令，平均每波攻擊持續 450 秒。

(4)這場報告內容包括殭屍網路規模、操作漏洞和攻擊方法，講者從蒐集到的數據中，針對 C&C 通訊、攻擊手法和受害者方面進行詳細研究，攻擊者除了管理他們的殭屍網路，也將他們的攻擊服務出售給他人，講者認為其團隊所做的分析將有助於在未來提供更準確的檢測及緩解類似威脅。

(六) Yara Studies: A Deep Dive into Scanning Performance

1.講者：Dominika Regéciová, Gen Digital Inc.

2.重點摘要：

(1)Yara 規則透過查找特定特徵的規則來辨識電腦與網路環境的惡意軟體或文件，並且使用者可以針對所在的環境自行定義規則以識別針對性的攻擊與安全威脅。Yara 提供正規表示式、文本(text)或二進制模式(pattern)的惡意軟體描述，其規則由字串集合和布林表示式組成。

(2)Yara 規則由規則(rule)名稱、字串(strings)及條件(condition)等組成，圖 3 的規則會在整個搜尋範圍中尋找$h00 字串，若符合條件(檔案小於 1KB 且字串位置在檔案中的第 0 個位置)，則傳回規則的結果為「真」。

```
rule test_01{
    strings:
        $h00= {42 ?? ?? 00 00 61
    62 }
    condition:
        filesize < 1KB and
        $h00 at 0
```

圖 3：Yara 規則

(3)講者分享一些不恰當的 Yara 規則撰寫方式

(a)在字串中插入^符號：如果在定義搜尋字串中插入^符號($re=/p\^?o\^?w\^?e\^?r\^?s\^?h\^?e\^?l\^?l/)，Yara 在搜尋過程中可能漏失該字串的某些字元，造成不準確的搜尋結果。

(b)過短的搜尋字串：短的字串會降低 Yara 搜尋效率，建議定義字串長度在 3 至 4 個位元組。

(c)太過一般的規則：字串中有前綴符號「.*」會大大降低搜尋速度，並且會產生匹配結果過多的警告。例如宣告字串$re = /.*\.exe/可以改良為$re =".exe"。

(d)增加 IPv6 搜尋的準確度：部分分析人員會將搜尋 IPv6 字串的規則撰寫為$ipv6=/([a-f0-9:]+:+)+[a-f0-9]+/，但上述寫法可能造成無法準確搜尋到 IPv6 位址。如果在字串前加上 2001，可以縮小搜尋到僅以 2001 開頭的全球單一位址，建議修改為$ipv6=/2001:([a-f0-9]{0,4}:){1,6}[a-f0-9]{0,4}/。

(4)講者的研究認為 Yara 規則很容易撰寫，但是撰寫「夠好的」(高的準確度及高效能)Yara 規則是很困難的，藉由分享常見的 Yara 規則，提供更精確的檢測模式以及更快速的查找速度。

(七) MCRIT: The MinHash-based Code Relationship & Investigation Toolkit

1.講者：Daniel Plohmann 博士, Fraunhofer FKIE & University of Bonn.

2.重點摘要：

(1) 講者從 2017 年 BotConf 會議發表 Malpedia 專案以來，其團隊不斷的維護和擴展社群主導的資料集，目標在有效利用資料集分析程式碼和第三方函式庫，以研析防禦惡意軟體的新方法，實現有效率的 1 對多程式碼相似性分析。經過 4 年的研究，講者分享初版 MCRIT 研究成果，分享解析相似性程式碼源碼，及惡意軟體中的第三方函式庫。

(2)MCRIT 係為簡化 MinHash 演算法應用於程式碼相似性而創建的框架，可以快速實作反組譯(disassemble)函數的屬性進行編碼，然後透過 MinHash 演算法評估相似性。

MCRIT 運作方式如圖 4，首先將要比對的文件/程式碼進行拆解為較小的流程或功能，執行索引搜尋，並將部分資料用萬用字元取代，使用 PicHash 演算法比對後放入資料庫中；拆解的另一部分用 MinHash 演算法(可快速評估集合的相似度，搜尋速度為 O(log n)，過去常用在文本的索引或相似性分析)比對後放入資料庫。

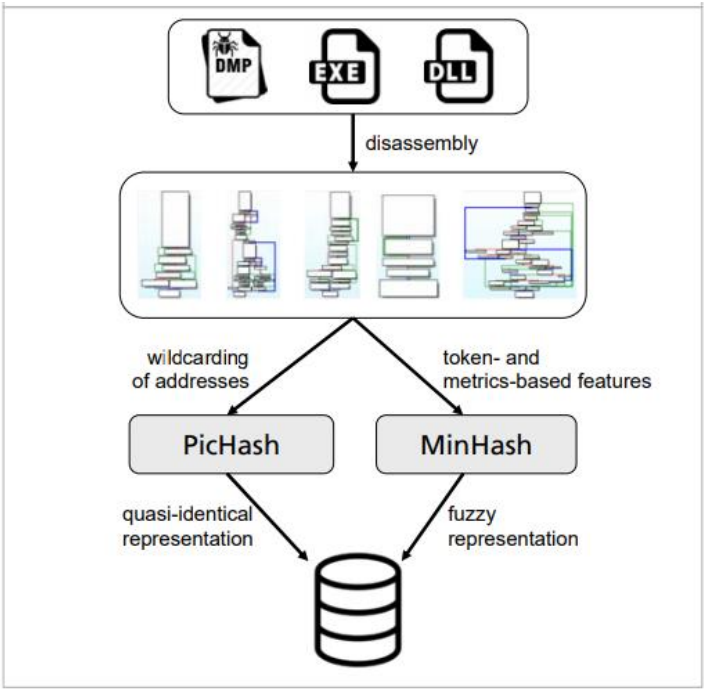

圖 4：MCRIT 簡要架構(資料來源：研討會簡報資料)

(3)MCRIT 系統部署資料庫(mongoDB)、執行索引的伺服器(mcgrid：restAPI server)、Web UI(使用 Python 和 Flask 程式語言撰寫)、HTTP 反向代理伺服器，使用 Docker 組合部署，詳如圖 5。

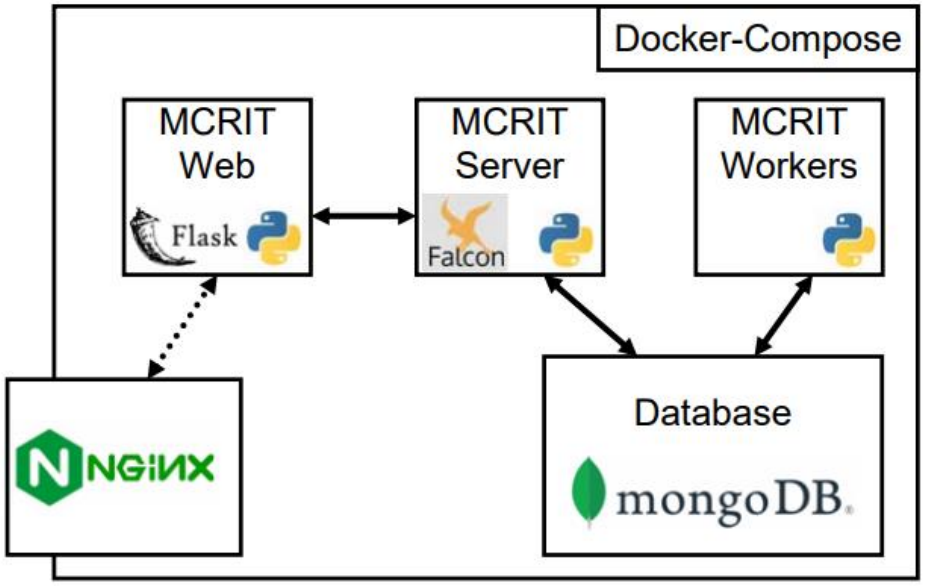

圖 5：MCRIT 系統部署(資料來源：研討會簡報資料)

(4) MCRIT 實作：講者最後展示程式碼相似性的比對結果視圖(如圖 6)，將兩個函數進行相似性比對，並以顏色表示相似程度。藍色表示完全匹配、

綠色表示至少指令序列相同、紅色表示兩個函數差異性過大。

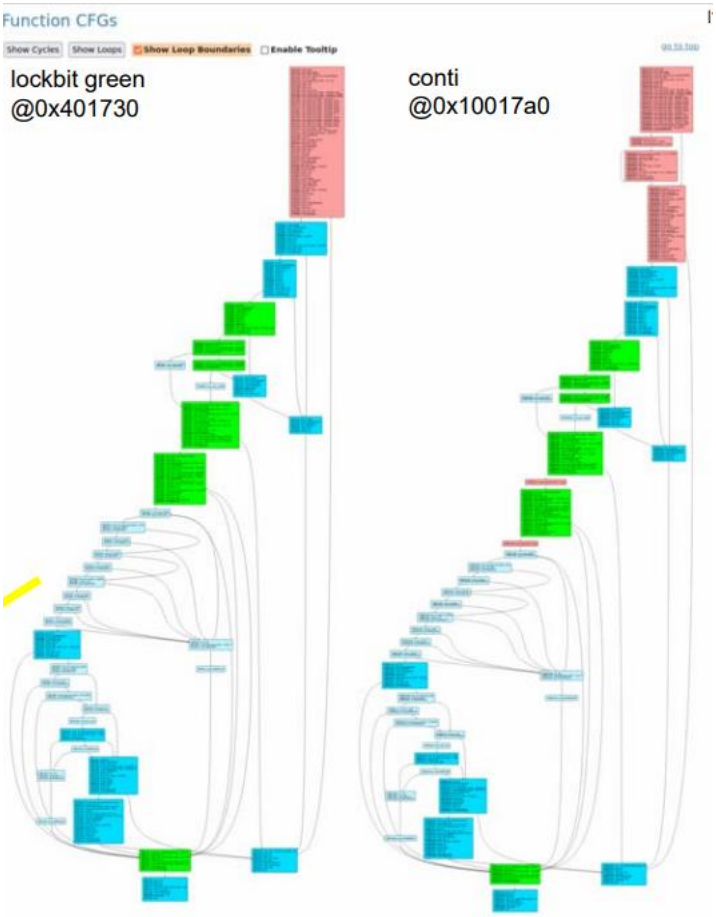

圖 6：MCRIT 程式碼相似性的比對結果視圖(資料來源：研討會簡報資料)

(八) When a botnet cries: detecting botnets infection chains

1.講者：Erwan Chevalier & Guillaume Couchard, Threat & Detection Research team at Sekoia.io

2.重點摘要：

(1)商業惡意軟體使用的感染鏈不斷發展，並使用各種技巧來繞過安全措施及使用者警覺意識，如 BumbleBee、QNAPWorm、IcedID 和 Qakbot 等經常作為第一階段的惡意軟體。講者分享數個知名的惡意軟體感染鏈以及感染鏈上的通用檢測規則，以幫助對抗殭屍網路。

(2)Qakbot：是一種模組化的殭屍網路，透過電子郵件傳播，使用非常規的加密功能隱藏通訊內容，當使用者下載點擊電子郵件夾帶的惡意 Excel

試算表或 zip 檔案連結即觸發感染鏈。使用者成為殭屍網路感染的新目標後，殭屍網路從遭感染的電腦蒐集各種設定資訊(如：使用者帳戶和權限、已安裝軟體清單、正在運作的服務等)，隨後會以動態連結程式庫(DLL)的形式下載一系列的惡意模組，以增強核心殭屍網路的功能。據 PRODAFT 統計，在 2022 年 2 月至 2023 年 2 月期間，至少已偵測到 100 萬個遭感染的受害者。講者以圖 7 說明使用 Qakbot 的團體或工具、透過何種工具下載惡意軟體、以及下載的惡意軟體。

圖 7：Qakbot 感染鏈(資料來源：研討會簡報資料)

(3)IcedID：亦稱為 Bokbot，是一種模組化的銀行業惡意軟體，目的在竊取使用者的財務資訊，它使用瀏覽器中間人攻擊來竊取財務訊息，包括銀行線上連線的登錄憑證。一旦成功完成初步攻擊，會使用竊取的資訊接管銀行帳戶並自動進行偽冒交易。IcedID 使用多種注入攻擊方法來規避防毒軟體和其他惡意軟體檢測方法，例如將自身駐在作業系統(OS)記憶體和常規程序，IcedID 開發者不斷更新 IcedID 模組， 以增加惡意軟體的持續性並逃避新的檢測作業，據 PRODAFT 統計，在 2022 年 8 月至 2023 年 12 月期間，至少已偵測到 2 萬個遭感染的受害者。講者以圖 8 說明使用 IcedID 攻擊的團體或工具、透過何種工具下載惡意軟體、以及下載的惡意軟體。

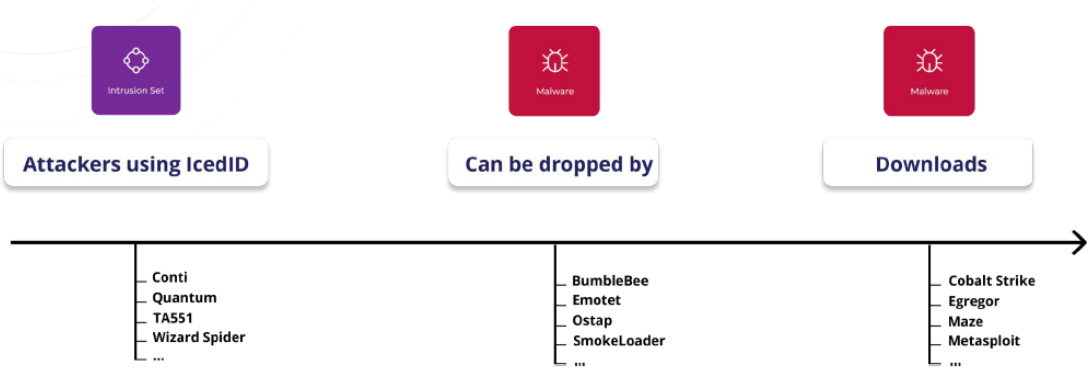

圖 8：IcedID 感染鏈(資料來源：研討會簡報資料)

(4) HTML Smuggling(HTML 挾帶)：HTML 挾帶是一種新的攻擊手法，該技術利用 HTML5 和 JavaScript 幫助攻擊者嵌入獨特製作的 HTML 附件，並傳送含有 URL 或附檔的釣魚信件。當受害者打開 HTML 附件或點擊連結時，將被重導到一個 HTML 網頁，並從該網頁解碼腳本(Script)，從網站下載惡意程式，在使用者裝置上組合成惡意檔案(如木馬或勒索軟體)。HTML 挾帶攻擊需要使用者點擊 URL 或郵件附檔，若要防止這類惡意攻擊，最根本方法是使用者提高警覺，不要隨意開啟陌生或不受信賴來源的電子郵件。講者以圖 9 說明使用 HTML Smuggling 攻擊的關聯規則，步驟順序如下：

(a)產製 HTML 檔

(b)可疑的瀏覽器程序

(c)產製可疑的檔案，上述動作通常發生在 5 分鐘之內，按主機名稱及使用者名分組。

(d)可疑的系統程序，通常在會發生(a)(b)(c)動作後的 2 分鐘內。

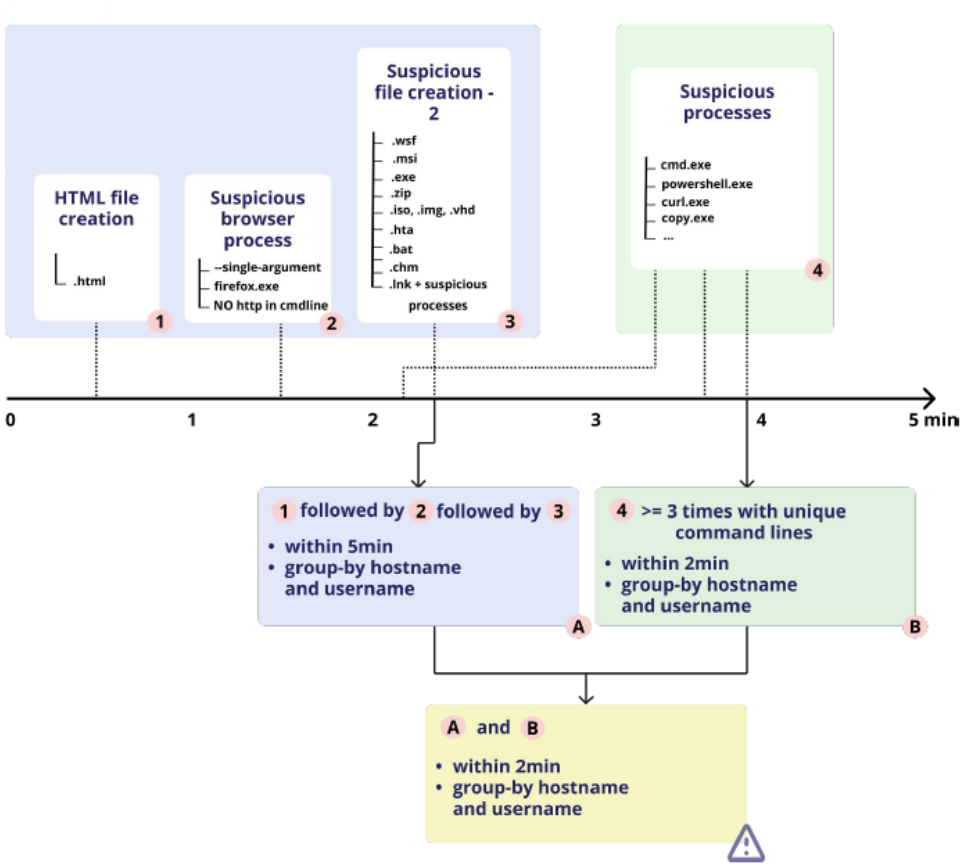

圖 9：HTML Smuggling 感染鏈(資料來源：研討會簡報資料)

(5)講者將入侵者造成受害者的威脅痛苦指數進行分級-痛苦金字塔，最低的是最容易防範電子郵件社交工程演練，其次是可疑的系統指令，痛苦指數最高的是 TTPs(戰術、技術與程序，Tactics, Techniques, and Procedures)攻擊。痛苦金字塔為企業網路防禦者提供了有用的參考，如果防禦者專注於檢測或阻止攻擊者行為，那麼將會讓攻擊者付出更大的代價並更加痛苦。

(九) The Plague of Advanced Bad Bots : Deconstructing the Malicious Bot Problem

1.講者：Yohann Sillam, Imperva

2.重點摘要：

(1)先進的惡意機器人已成為網際網路上的瘟疫，其威脅情況非常多樣化且目標廣泛，從影響州選舉的大規模建立帳戶到分散式阻斷服務(DDoS)攻擊機器人，高級機器人是模仿人類行為以程式方式通過驗證碼的軟體。

例如：它模擬類似人類的滑鼠動作，像人類一樣跟隨網頁滑動。講者討論自動惡意行為（如撞庫、盜刷等）的具體實例，以及分析惡意的機器人。

(2)機器人的生態系統：

(a) 2021 年網站流量中，其中 27.7%被惡意的機器人使用、14.6%被正當的機器人使用、57.7%由真正的人類使用。

(b)網路爬蟲(Web Scraping)社群：一些知名的網路抓取社群，分享豐富的抓取工具與經驗，幫助使用機器人或網絡爬蟲實現自動化流程，獲取所需要的資料，如：r/webscraping、Scraping Enthusiasts、Scraping in Prod、Scrapy Discord。

(c)機器人販售/租賃市場：一些最受使用者歡迎的機器人市場，並且將特定類型的機器人分類販售/租賃，如：TIDAL、BOTMART、easyrentals、CopSupply。

(3)機器人的共通結構：講者調查約 40 個高階機器人，似乎大多數的機器人都存在一些關鍵組成。首先是自動化的架構(用來遠端控制瀏覽器並執行操作)，如：Selenium、WEBDRIVER I/O、essentialobjects(.NET 元件)；使用代理伺服器也是機器人的必要工具，知名的有 GSA proxy scraper、chef proxies、oxylabs。此外，第三方反驗證碼工具也是必需，知名的有：2Captcha、CapMonster、DeathByCaptcha。

(4)Vinted 平台發生的攻擊事件：2023 年 Vinted 二手銷售平台用戶的帳戶遭到攻擊，駭客通過簡訊或電話要求會員更改其聯絡資料，並自動更改了與會員帳戶相關的銀行詳細訊息(操作不需要通過電子郵件或簡訊進行任何驗證)。駭客除了攻擊法國 Vinted 大量用戶之外，還攻擊西班牙和義大利的用戶，致使受害者損失錢或者其銀行的通知詳細訊息。雖然 Vinted 平台解釋，駭客利用的使用者資訊(帳號、密碼)是從該平台的外部取得，

與 Vinted 無關，但 6500 萬用戶希望 Vinted 平台採取額外措施，加強帳戶資訊的安全性，同時，使用者需要保持警覺，建議不要與第三方或可疑連結分享登入資訊。

(5)OpenBullet：OpenBullet 是一個受歡迎的開源軟體，用於抓取和解析數據、網路應用程式安全測試和滲透測試，惡意機器人開發人員使用它來自動執行各種 Web 攻擊，如：暴力破解、撞庫攻擊和帳戶接管等，近來 OpenBullet 已在 Github 上釋出第二個版本。

安裝和使用 OpenBullet 不需要程式撰寫背景知識，並且可以在網路上找到幾種不同的配置版本(在網站上執行活動的操作順序)，視窗化介面讓開發人員可以透過簡單的 UI 進行調整。因此，OpenBullet 常被缺乏撰寫程式碼背景的機器人開發人員廣泛使用，不僅如此，OpenBullet 還提供了一種高階程式語言，用來微調一些操作。

當 OpenBullet 在網站上自動執行操作程序時，網站所使用的框架和函式庫決定執行的動作，大致可區分為瀏覽器、網頁頁面及網頁屬性的操作。

OpenBullet 也經常被安全研究人員和滲透測試人員用來識別和修復網路應用程式中的安全缺陷，以免被惡意行為者利用。

參、心得與建議事項

一、網路安全防護的困境：

Paul Vixie 博士在主題演講中提到 2013 年愛德華．史諾登披露了美國國家安全監聽資料，向媒體透露美國政府大規模監控全球網路資訊，摧毀隱私及網際網路自由。自此之後，資(通)訊安全成為顯學之一，加密傳輸協定也更受到重視。隨著網路普及，各種行動應用程式取得容易，惡意軟體也偽裝為正常應用程式來竊取或破壞用戶的資料，且加密貨幣流通讓惡意軟體開發者取得贖金更為容易。網路安全防護的獎勵與駭客的獲得的利益已無法相比，近年來，不肖分子頻頻竊取民眾個資至暗網販賣以獲取非法利益，因法規規

範及人員管控的寬鬆，僅有極少數的不肖分子被繩之以法，因此建議加強可存取機敏資料人員的管控及提高相關刑/罰則，應可收到嚇阻犯罪的效果。

二、政府扮演資安產業發展領頭羊的角色

雖然 Pratiksha Ashok 博士提到印度政府的數位安全政策係由政府提供免費的資通訊安全解決方案，然而在多數的民主國家，仍然由自由市場經濟決定各種解決方案與工具的定價。在我國，政府政策扶植對於產業發展方向有舉足輕重的影響，如早期半導體投資、記憶體及面板產業，都帶動台灣電子相關產業鏈發展。台灣與以色列皆為小國、面臨地緣政治風險，但以國政府大力扶植資安產業，近年來已成為資安新創產業大國，以國政府透過與民間協力出資，與國際創投公司合作，挹注資金投入資安新創公司，促進以色列發展資安獨角獸，相關政策及金融舉措值得我們參考。

三、Yara 規則優化對惡意軟體識別日益重要

Dominika Regéciová 女士在 Yara Studies 場次介紹 Yara 規則結構，介紹提升 Yara 規則執行效率的撰寫方式，並提出字串搜尋實測結果，優化後的 Yara 規則，最短只需優化前不到十分之一的搜尋時間。Yara 規則撰寫須符合演算法的基本特性：輸入(可有零或多個輸入資料)、輸出(執行完畢後至少有一個輸出結果)、明確性(每個執行步驟必須是明確的指令)、有限性(演算法必須在有限個步驟內結束)、有效性(演算法中的每個步驟必須可執行且有效)，因此 Yara 規則必須在有限的時間內，在龐大的文本(text)資料中完成字串(pattern)搜尋，並輸出至少 1 個結果。

Dominika Regéciová 女士在 BotConf 2022 年會議介紹 Yara 規則，並接續於 2023 年會議提出增進 Yara 規則執行效率的建議，目前 Yara 搜尋引擎廣泛應用於惡意軟體識別工具，關注其後續發展有助於了解惡意軟體搜尋引擎之趨勢。