財團法人電信技術中心出國報告

出席 2019 年 The Honeynet Project Workshop 2019 報告

中心名稱：財團法人電信技術中心
單位名稱：資通安全組
姓名職稱：張助理工程師又仁
派赴國家：奧地利茵斯布魯克
出國期間：2019/06/29~2019/07/05
報告日期：2019/08/05

前言與摘要

The Honeynet Project Workshop 多年來致力於研究誘捕系統（Honeypot）、系統模擬欺騙技術，以及網路惡意情報蒐集。本次於奧地利舉辦研討會，與會者包含資訊安全從業人員與研究分析人員，共同討論電腦網路攻擊所涉及的工具、網路攻擊者的策略及動機，並分享自身的經驗。

The Honeynet Project 為國際非營利組織，其成立宗旨為掌握最新攻擊趨勢與開發誘捕工具，並向大眾發布網路攻擊資訊與系統模擬欺騙技術相關研究。近年來透過與 GSoC（Google Summer of Code）合作，吸引各式研究人員參與，同時亦開發多種開源工具協助研究網路攻擊事件，曾研發之軟體包含 Dionaea、Glastopf、Kippo、Honeyd 與 Glutton 等，皆為目前受到廣泛使用之主流誘捕系統，使用者可透過上述工具蒐集攻擊者資訊，例如攻擊指令、與惡意中繼站溝通的方式、攻擊系統時間，以及破壞系統後攻擊者採取的行為。The Honeynet Project 將資訊整合研析後，便透過 Know Your Enemy 系列論文及部落格向外界說明最新攻擊威脅，讓外界了解面對攻擊時可採取的基本措施與處理方式。

本次出席會議人員為：

財團法人電信技術中心 資通安全組 張助理工程師又仁

目錄

圖目錄

壹、目的

藉由參與 The Honeynet Project Workshop 國際研討會與各國交流誘捕系統研究狀況，反思我國誘捕架構革新之可能性，並透過講師與研究人員的分享，藉此獲得最新誘捕系統資訊、攻擊工具、分析方法等，加強自身不足之處，以提升 TTC 資安專業人員能量，強化通傳領域誘捕技術。

貳、行程

會議行程		
日期	**上午**	**下午**
7 月 1 日 星期一	• Introduction to the Workshop • Keynote: The Changing Landscape of Cybercrime • Keynote: Securing Civil Society • Can I be you, please? Deception with code attribution	• T-Pot, PEBA, Sicherheitstacho - Fighting evil forces by running a large scale honeypot installation • Tales from the CRYPT(3): Stories from the early Honeynet Project years
7 月 2 日 星期二	• Google Summer of Code at the Honeynet Project • SNARE/TANNER: The evolution of web application based honeypots	• Virtual Machine Introspection Based SSH Honeypot • Hiding in the Shadows: Empowering ARM for Stealthy Virtual Machine Introspection
7 月 3 日 星期三	• Honeypots and IDS 101	• Honeypots and IDS 101

參、議程活動

一、Introduction to the Workshop（介紹本次研討會）

圖 1：Introduction to the Workshop[1]

本次研討會開場由 The Honeynet Project 執行長 Faiz Shuja 主持，Faiz Shuja 表示希望藉由各國資安從業人員與研究分析人員的參與，分享誘捕系統經驗並進行技術討論，除此之外，Faiz Shuja 介紹研討會目的與重點，讓與會者了解會議內容與預期效益。

(1) 會議目的：交流誘捕系統相關工具與技術，並讓與會者進行經驗分享。

(2) 近年來 The Honeynet Project 主要研究方向：

- 蒐集攻擊者資料。
- 公開提供攻擊者使用之工具、技術及動機。
- 撰寫 Know Your Enemy White Papper 說明網路攻擊手法研究，此文件於 The Honeynet Project 的部落格公佈，簡稱為 KYE paper，目前最新一期為 2018 年 1 月 3 日發布之 KYE paper: Bots keep talking to us，主要探討網路中究竟充斥多少機器人（Bot）類型的掃描。為達成此項研究，研究員首先透過 AWS（Amazon Web Services）設置伺服器（Server），完成後關閉所有對他人有用之服務如 SSH（Port 22）、DNS(Port 53）與 HTTP(Port 80）

[1] 資料來源：The Honeynet Project 官方 twitter，https://twitter.com/projecthoneynet

等，並不把 IP 掛到任何域名（Domain）下，放置一段時間後，透過 wireshark 錄製封包，若發現仍有大量連線行為，將嘗試進行各種漏洞掃描。

(3) 本次會議將分享的知識：
- 現今網路最新威脅和漏洞的觀察。
- 宣傳 The Honeynet Project 經營之部落格與 Twitter。
- Know Your Enemy 相關文獻說明。
- 各式 Honeynet Workshop 教學。

(4) 本次會議與工具相關資訊：
- 開發誘捕系統與資安工具資訊。
- 釋出開源工具原始碼。
- GSoC（Google Summer of Code）相關成果。

(5) 開源誘捕系統資訊：Cuckoo、Dionaea、Glastopf、HoneyC、Conpot、Honeywall。

二、Keynote: The Changing Landscape of Cybercrime

圖 2：Keynote: The Changing Landscape of Cybercrime[2]

本場次主持人為 Ross Anderson，其研究領域為資訊安全工程，Ross 對於防範網路犯罪有許多開創性貢獻，如點對點網絡（peer-to-peer-networks）、硬體篡改防護方式和加密協議。

Ross 首先以學術研究角度提出網路犯罪常遇到的問題，包含以下幾點：

(1) 網路犯罪研究為近幾年流行之學科，卻沒有太多相關資料可以查詢。

(2) 常需要花一兩年以上時間蒐集網路犯罪研究資料，方可開始撰寫。

(3) 有些資料數據對其他人來說可能毫無價值，導致沒有資料可以參考，研究人員常需要從零開始進行研究。

2012 年起，網路科技逐漸發生變化，如大眾開始使用智慧型手機、

[2] 資料來源：The Honeynet Project 官方 twitter，https://twitter.com/projecthoneynet

雲端資料庫，以及社群網站，但即便使用型態有所改變，網路上依舊充斥著惡意程式與殭屍電腦。根據 Ross 的研究，近年來針對企業以及個人的詐騙行為尤其嚴重，其中詐騙手法從早期的電子郵件假傳帳單與釣魚信件等社交工程，轉變為勒索病毒 Ransomware (勒索軟體/綁架病毒)威脅，如透過比特幣的交易獲取暴利。

總結以上資訊，由於涉及隱私權，研究人員無法輕易取得遭受詐騙的使用者資訊進行分析，Ross 表示目前僅能藉由劍橋網路犯罪中心（Cambridge Cybercrime Center）蒐集的惡意郵件（Spam）、釣魚（Phish）、惡意軟體（Malware）等資料，分析網路犯罪攻擊手法，並採用誘捕系統進行誘捕，獲取攻擊者上傳之惡意郵件與惡意軟體資訊。Ross 亦經營個人網站（https://www.ross-anderson.com）刊載關於網路犯罪之研究。

三、Keynote: Securing Civil Society

圖 3：Keynote: Securing Civil Society[3]

本場次講者 Nex（Claudio Guarnieri）是義大利籍資安研究員兼軟體開發人員、多倫多大學公民實驗室顧問、The Honeynet Project 核心成員，隸屬於國際特赦組織（Amnesty International），常提供資安資訊予人權團體、記者與活動家。近年來 Nex 特別關注隱私權與系統監控，並在公民實驗室發表許多受害端系統監控之文章。

Nex 表示國際特赦組織主要與人權衛士（Human Rights Defenders,HRDs）合作，特赦組織分配研究人員至各分部進行資安威脅研究、網路安全顧問，以及資安指導，同時也開發工具、服務與回傳資安事件資訊等。Nex 分享幾件與該組織有關之資安事件，如下圖。

[3] 資料來源：The Honeynet Project 官方 twitter，https://twitter.com/projecthoneynet

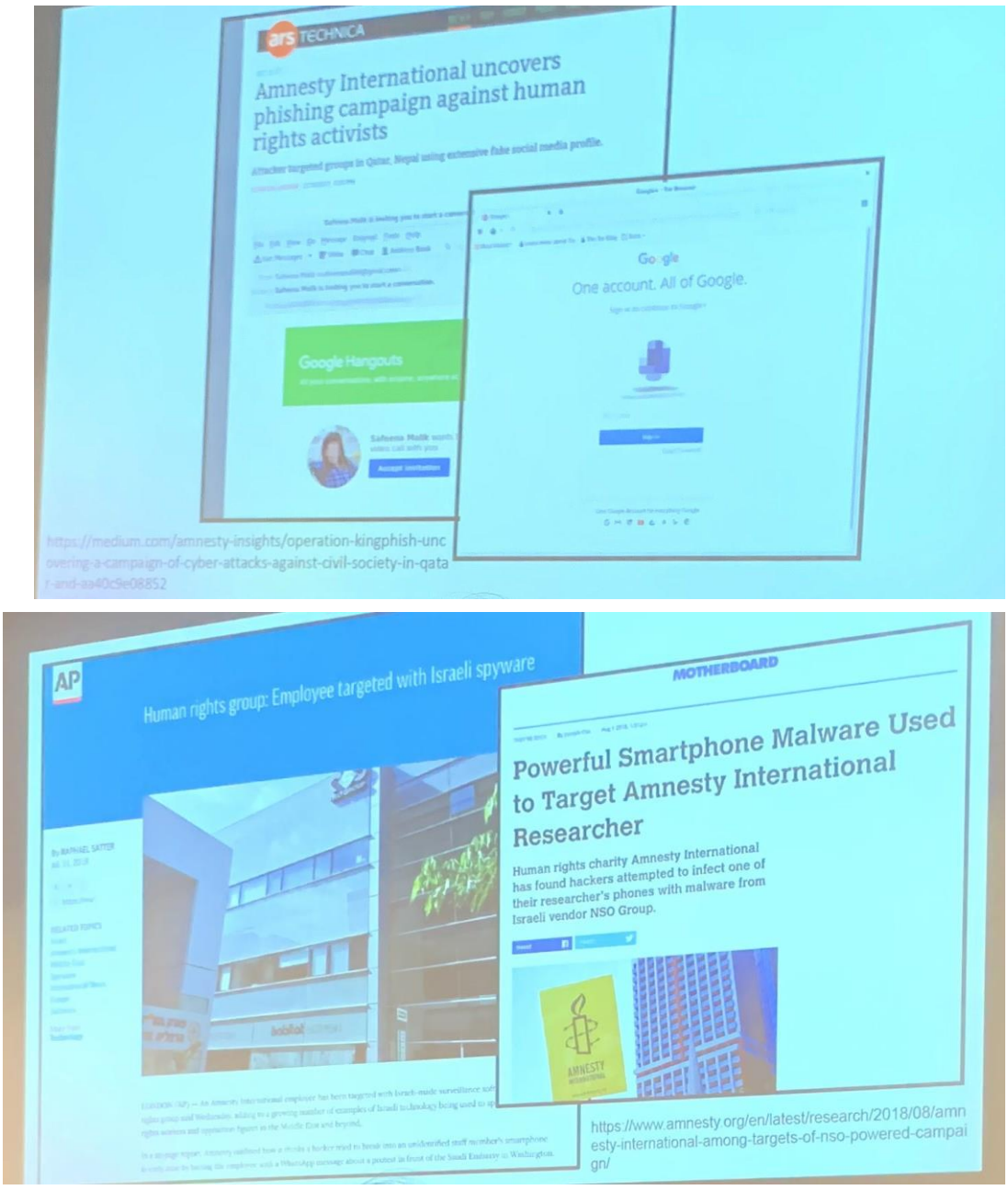

圖 4：國際特赦組織資安事件案例分享[4]

Nex 表示目前國際特赦組織統計之網路攻擊趨勢，最頻繁發生的攻擊類型為網路釣魚，現階段以雙重驗證（2FA）為常見之系統防護措施，在歐洲某些地區也發現針對安卓系統的惡意程式有逐漸上升之趨勢。除了上述攻擊範例與攻擊類型外，Nex 也說明國際特赦組織在網路攻擊中的角色特殊性，例如國際特赦組織、新聞從業人員與政治人物只有消費者等級（consumer-grade）資安防護能力，然而因其職務特殊性，卻得面對企業等級（enterprise-grade）的資安威脅，導致上述

[4] 資料來源：The Honeynet Workshop 拍攝之會議簡報

成員極需提升其資安防護能力。

消費者等級的資安產品通常專注於單純的系統防護，故需導入誘捕系統機制進行網路環境資安情報蒐集。以往誘捕系統主要功用在於紀錄惡意軟體樣本，引誘攻擊者進入並觀察其攻擊方式，近年來則用於檢查企業資安環境是否有漏洞，容易遭受駭客入侵。由於消費者等級的資安產品防禦力較弱且硬體資源稀短缺，難以抵擋網路惡意攻擊，因此，透過誘捕系統更可觀察是否有惡意程式之威脅。

四、Can I be you, please? Deception with code attribution

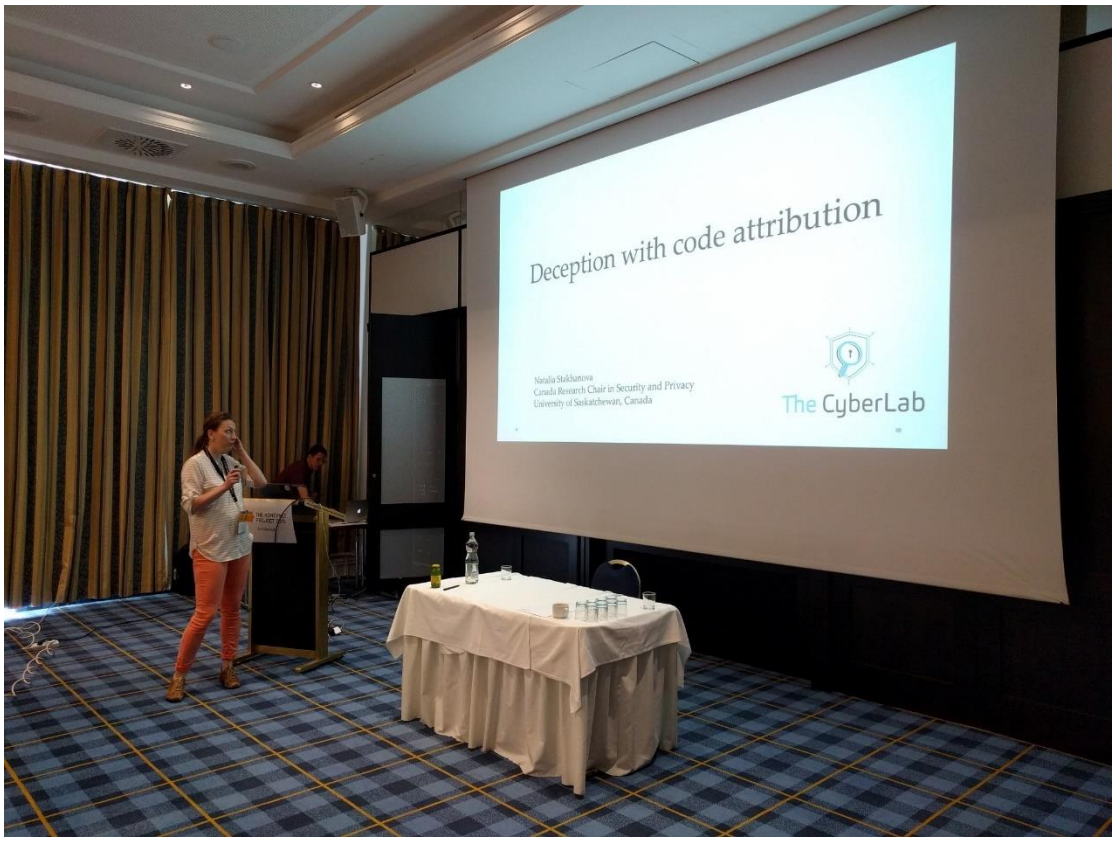

圖 5：Can I be you, please? Deception with code attribution[5]

Natalia 任職薩斯喀徹溫大學（University of Saskatchewan,UofS），加入薩斯喀徹溫大學前為新不倫瑞克大學（University of New Brunswick,NB）網路安全的 NB 創新研究主席（NB Innovation Research Chair）。Natalia 副教授主要工作為建立網路安全系統，並開發多項技術，曾在電腦資安領域獲得三項專利。

Natalia 表示所謂程式碼歸屬（code attribution）通常是開發人員在開發過程中，習慣使用一些代號或個人的程式風格，來識別程式碼由誰撰寫，本場次重點在於了解惡意程式如何偽造程式碼歸屬，以及保護自己的帳號。首先，Natalia 說明有很多種方法可取得應用程式的資訊，如藉由惡意程式偵測程式屬性、透過一些軟體盜竊程式（Software theft）偵測，以及使用數位鑑識方法確認數位簽章等資訊；同樣地，當我們要尋找工程師留在惡意程式碼中的軌跡也有很多種方法，舉凡確認原始碼撰寫架構、加殼方式、數位指紋，以及惡意程式感染方式（感染的協定、攻擊帶有何種特點/弱點之設備、安裝方式、感染手段）

[5] 資料來源：The Honeynet Project 官方 twitter，https://twitter.com/projecthoneynet

都屬於常見的手法，有了以上這些資料便可準確了解程式碼歸屬資訊。

Natalia 提出駭客常用的冒充流程三步驟：

(1) 蒐集受害者程式語法範本

(2) 了解受害者撰寫程式習慣

(3) 冒充受害者撰寫程式習慣

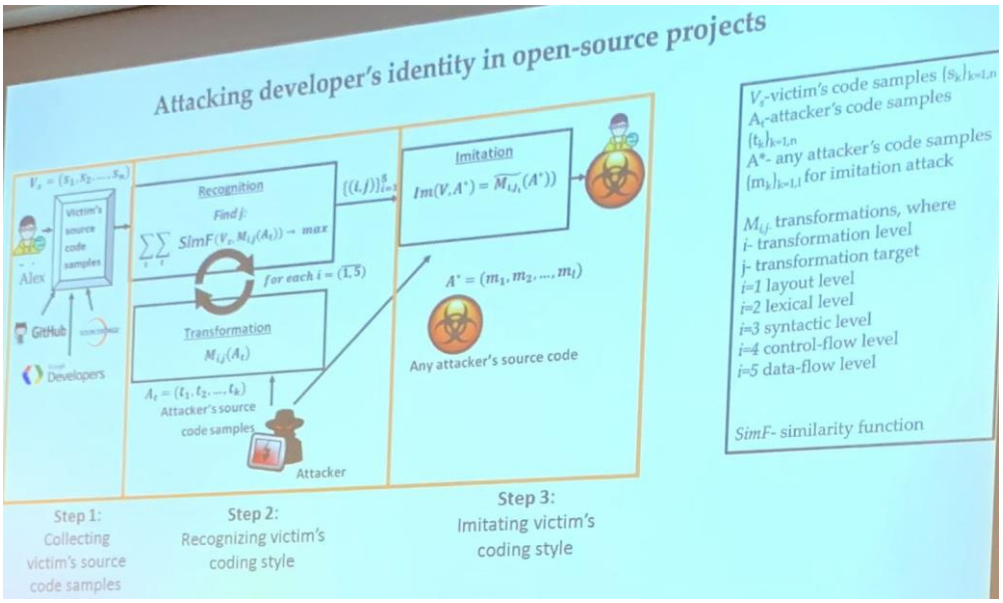

圖 6：駭客常用的冒充流程三步驟[6]

因此，為了保護帳號不受到攻擊者冒充，即需要針對檔案、習慣或上傳原始碼之帳號進行加密，Jeff Mitchell 曾在 HashiConf EU 2016 會議上提出「當你不注意所謂的加密，他便會在你不注意時暴露未經授權的進入點，提高你的風險。」，為了反制攻擊者冒充，有很多種方式進行驗證，首先是加密（Password）方式，包含對檔案使用密碼加密或透過演算法幫檔案加密（Salted）；憑證方式（Bearer Token）則是使用 API 驗證金鑰與 JSON 類型網頁憑證；私鑰方式（Private Keys）則為 SSH 私鑰、SSL/TLS 私鑰、DKIM 私鑰以及 HMAC 私鑰。

最後 Natalia 提出創建密碼的建議，密碼以 12 至 14 個長度的英文及數字隨機組合為佳，並避免在不同平台重複使用相同密碼、也不可使用傻瓜式密碼（123456789），以及不將密碼存在電腦或雲端中，建議民眾只要做好加密防護，便可保護自己的帳號與程式碼不被攻擊者利用。

[6] 資料來源：The Honeynet Workshop 拍攝之會議簡報

五、T-Pot, PEBA, Sicherheitstacho - Fighting evil forces by running a large scale honeypot installation

圖 7：T-Pot, PEBA, Sicherheitstacho - Fighting evil forces by running a large scale honeypot installation[7]

該場次講者為 André Vorbach 與 Marco Ochse 聯合發表，André 為電信安全領域的高級資安專家，主要研究滲透測試（Penetration Testing）及網路安全，André 曾在德國政府的緊急應變小組（Computer Emergency Response Team,CERT）工作，並在 2010 年加入德國電信股份公司（Deutsche Telekom,DT）後，開始建置德國電信的誘捕系統。Marco 則是德國通傳領域安全部門的高級資安專家，其專業為企業行動裝置（Enterprise Mobility）以及辦公室通信安全，Marco 也曾擔任金融領域安全顧問，2011 年加入德國電信股份公司便開始著手研究誘捕系統計畫。

兩位德國電信領域的專家介紹他們共同研發的專案 T-Pot，T-Pot 為德國電信的誘捕系統專案，該系統利用 Docker 容器技術集合眾多應用誘捕程式，目前 T-Pot 19.03 版內建多種誘捕系統（conpot、cowrie、dionaea、glutton…等），並透過 ELK stack 協助將各種誘捕系統蒐集到的資訊呈現在網頁上。

[7] 資料來源：The Honeynet Project 官方 twitter，https://twitter.com/projecthoneynet

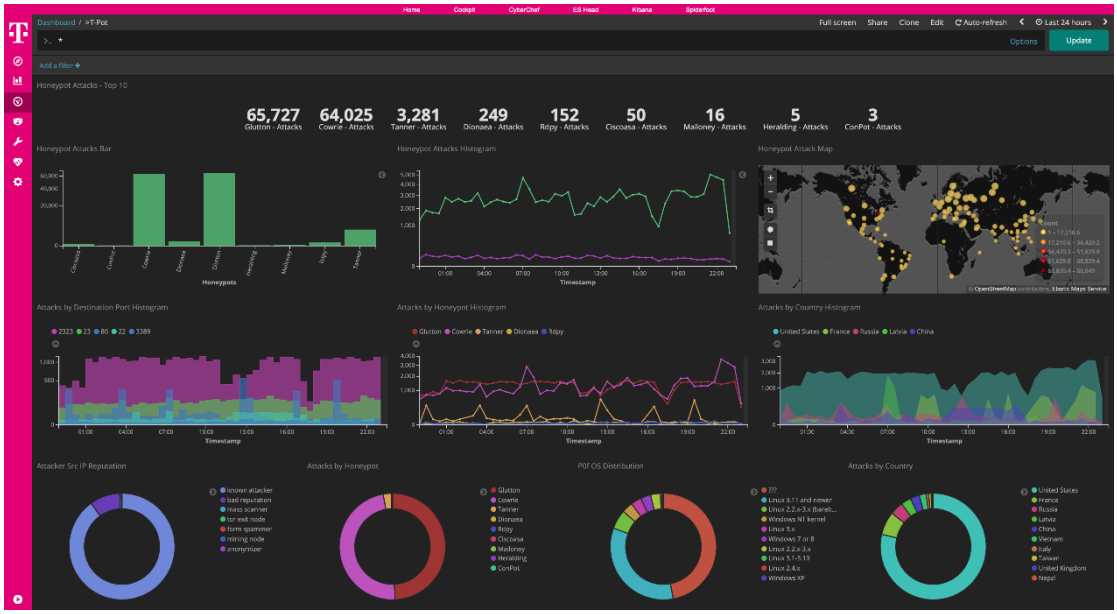

圖 8：T-Pot 介面範例[8]

我們可將 T-Pot 誘捕資訊應用於資安防護，藉由分析攻擊手法，定義其特徵，並協助使用者進行系統防護，T-Pot 能預設蒐集使用者的誘捕資料，並回傳至大數據資料庫進行分析，此回傳功能可於安裝後關閉。André 針對網際網路服務供應商（ISP）設計的殭屍網路處理三步驟流程如下：

(1) 偵測(Detect)：監控誘捕系統狀態，發生異常行為時立刻告警。

(2) 分析（Analyze）：透過沙盒（Sandbox）或其他工具追蹤攻擊手法，並關聯類似案件了解目前攻擊影響範圍。

(3) 回應（Respond）：透過網站公布入侵指標（Indicators of Compromise，IOC），並製作相關威脅報告予使用者參考。

會議最後提出 2018 年 9 月發生的 SATORI/MIRAI 案例，研究發現主要攻擊來源國為中國及美國，當時收到來自 68,361 個不同 IP 發起攻擊，攻擊者嘗試進入主機後下載 adbs 檔案，檔案放入 VirusTotal 後，發現過半數的防毒軟體判定為感染病毒，拆解執行檔確認內部指令與行為屬於 satori botnet，以上為 André 透過 T-pot 發現攻擊之流程範例。

[8] 資料來源：T-pot 官方網站，https://github.com/dtag-dev-sec/tpotce

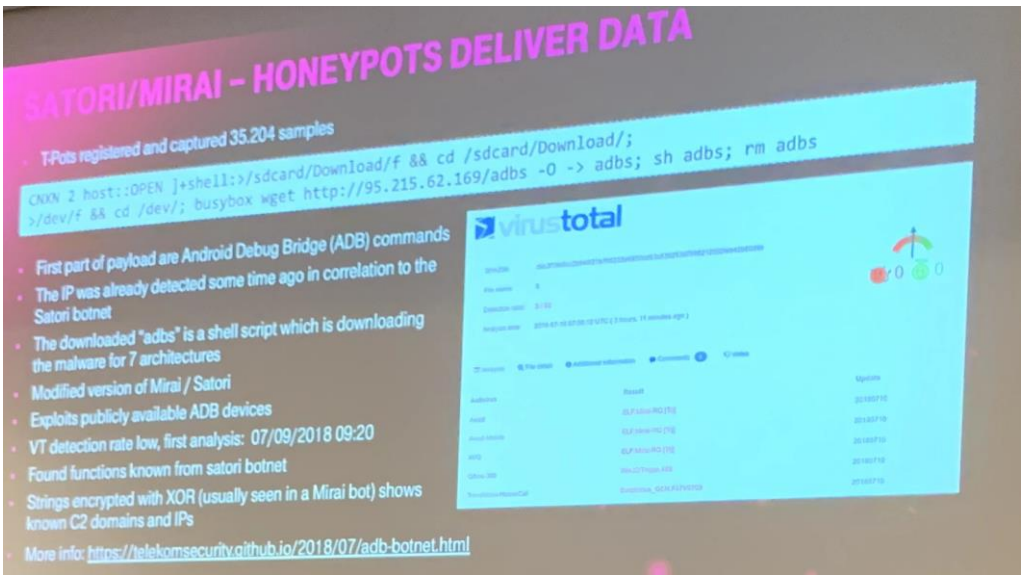

圖 9：satori botnet 攻擊範例[9]

[9] 資料來源：The Honeynet Workshop 拍攝之會議簡報

六、Tales from the CRYPT(3): Stories from the early Honeynet Project years

本次會議原定由 David Dittrich 主持，臨時改由 Brain 擔任主講人，議程主要介紹 Honeynet 的歷史，Brain 表示誘捕系統起初建置目的是讓 CS(Computer Science)學生了解實際發生在伺服器上的攻擊狀況，並增加網路連線設定經驗，再輔以實際案例進行說明，讓學生從做中學，在工作的過程裡培養自己的價值與專業，甚至產出極佳的分析文件，正因這個有趣的實際操作過程，誘捕系統逐漸在歐美學界流行起來。

Brain 表示現行誘捕系統環境大多在 Linux 系統上執行，並使用 Docker 的容器技術（Container），快速佈建大量誘捕系統進行資料蒐集。透過誘捕系統可蒐集現行網路較活躍的惡意程式，或遭受攻擊的資訊，並將受害範圍侷限於誘捕系統中，讓參與實作的學生感受實際環境，提升其學習興趣，也能更精進誘捕系統的發展。

七、Google Summer of Code at the Honeynet Project

圖 10：Google Summer of Code at the Honeynet Project[10]

本場次講者為 Maximilian Hils，Maximilian 為奧地利茵斯布魯克大學博士生，也是 mitmproxy（中間人監控封包程式）的主要開發人員之一，他積極參於各項開源專案，2012 加入 Honeynet GSoC（Google Summer of Code）後，現為 Honeynet GSoC 領域的負責人，並辦理本次會議。

GSoC 是一項全球計劃，致力讓更多學生參與開源軟體開發，學生在休學期間可選擇與一個開源組織合作（The Honeynet Project、API Client Tools at Google、Mozilla…等），進行為期 3 個月的編程項目，開源專案合作組織將指派一名有經驗的開發人員作為導師。

[10] 資料來源：The Honeynet Project 官方 twitter，https://twitter.com/projecthoneynet

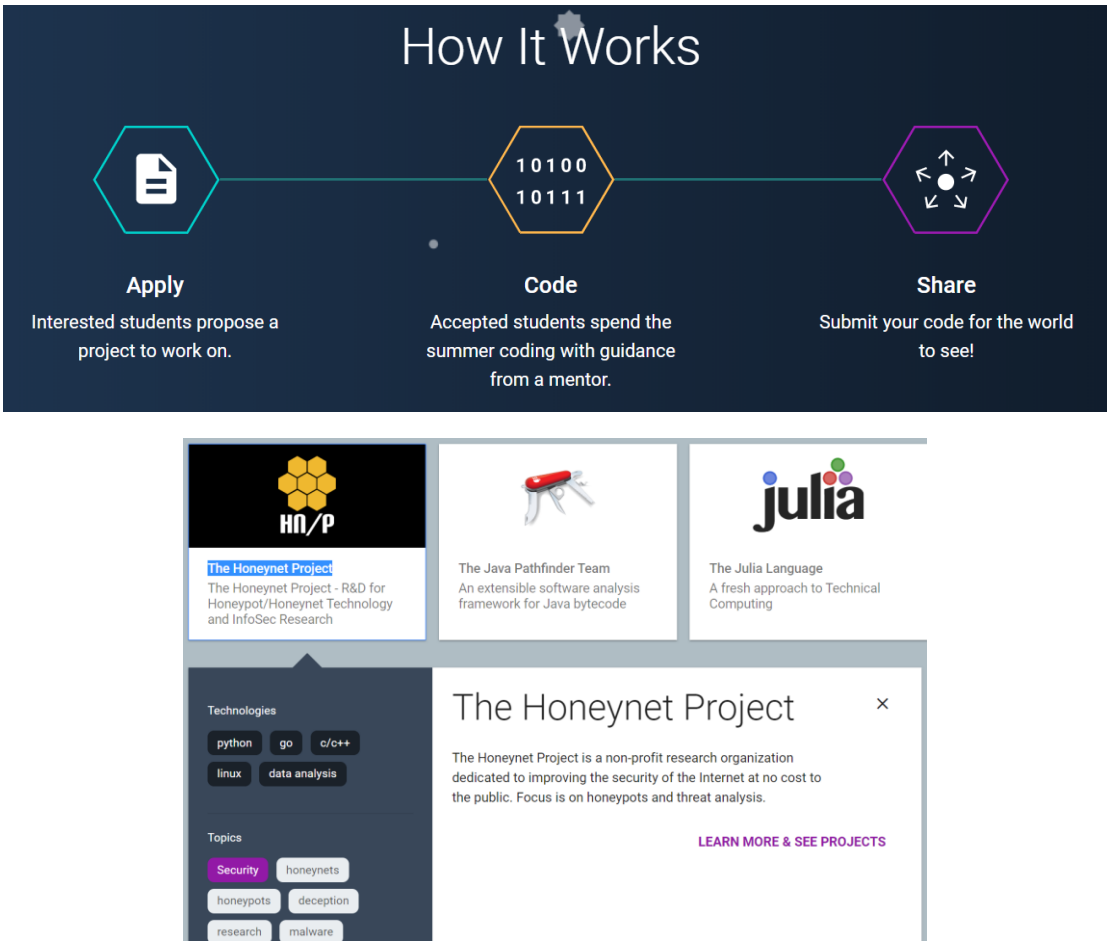

圖 11：GSOC 計畫說明[11]

CSoC 專案對合作組織、學生與 Google 三方各有好處，對合作組織來說，可招募新會員並開發新工具。對學生來說，加入 CSoC 專案對未來職涯有加分效果，也可實際操作真正發生在誘捕系統內的問題，更能從 Google 獲得一筆不錯的收入。對 Google 而言，則可提早網羅優秀人才進入 Google，如在網頁模擬誘捕系統領域中原本主流為 Glastopf，現在出現一個新的誘捕系統 SNARE /TANNER 逐漸取代 Glastopf，SNARE/TANNER 即是 GSoC 專案學生開發的產品。

[11] 資料來源：GSOC 官方網站，https://summerofcode.withgoogle.com/how-it-works/

八、SNARE/TANNER: The evolution of web application based honeypots

圖 12：SNARE/TANNER: The evolution of web application based honeypots[12]

本場次講師為 GSoC 成員 Evgeniia Tokarchuk，Evgeniia 為德國亞琛工業大學（RWTH Aachen University）碩士班二年級學生，主要研究領域為自動化系統資訊安全，2016 年 Evgeniia 在 GSoC 負責三個月 SNARE/TANNER 項目，2017 年與 2018 年成為 SNARE/TANNER 項目的導師。

何謂 SNARE/TANNER？簡單來說 SNARE 是網頁伺服器（Web Server），TANNER 則是遠端資料分析服務。SNARE 主要功能為網頁拷貝，可以模擬成實際存在的網頁以吸引駭客，由於無法複製資料庫中的機敏資料，也就沒有法律上的顧慮，目前 SNARE 遇到的最大難題就是如何讓假網頁看起來更逼真，以吸引駭客入侵系統。

[12] 資料來源：The Honeynet Project 官方 twitter，https://twitter.com/projecthoneynet

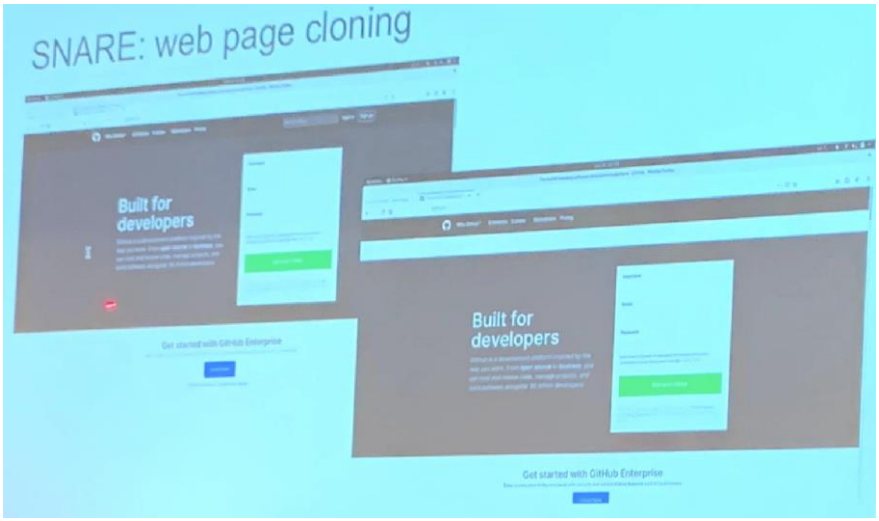

圖 13：SNARE 模擬介面[13]

接下來介紹 TANNER 運作流程，當 SNARE 收到外部的請求（Request）時，將 Request 導入 TANNER 中建立會話（Session）並進行管理，TANNER 亦會模擬各種訊息回覆（Response）給攻擊者。

我們可針對 Session 內容進行分析，但分析 Session 時要特別注意在進入內部系統前，應利用其特徵判斷有問題的攻擊者。

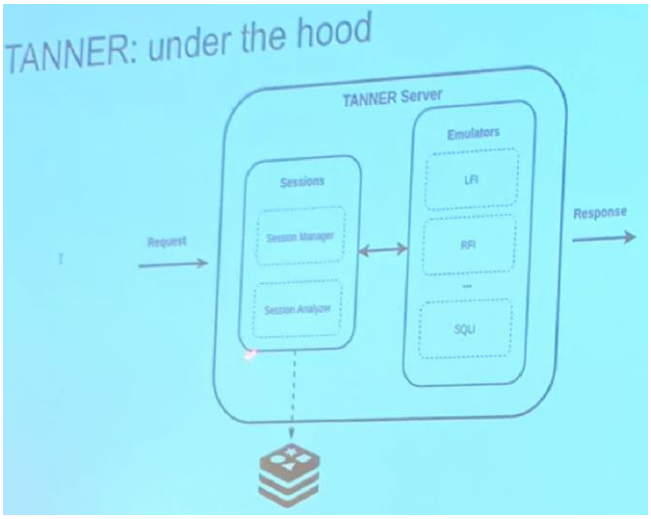

圖 14：TANNER 架構圖[14]

[13] 資料來源：The Honeynet Workshop 拍攝之會議簡報
[14] 資料來源：The Honeynet Workshop 拍攝之會議簡報

九、Virtual Machine Introspection Based SSH honeypot

圖 15：Virtual Machine Introspection Based SSH honeypot[15]

本場次由 GSoC 學員 Stewart Sentanoe 發表，Stewart 為德國帕紹大學（University of Passau）博士生，2018 年加入 Honeynet 的 GSoC 計劃，Stewart 目前主要開發項目為高互動 SSH 誘捕系統 Sarracenia，透過追蹤 VMI（Virtual Machine Introspection）提高監控隱密性，VMI 為一種偵測虛擬機系統運行狀態的監視系統，此功能通常用於系統調適或取證。

Stewart 開發 Sarracenia 的主因是有太多資安設備（如 IoT 裝置與部分老舊 Server）受到攻擊，因此想藉由分析誘捕系統，了解更多攻擊手法。Stewart 表示誘捕系統的偽裝技術分低、中、高互動三種，低/中互動之偽裝較容易被發現，且多數只能蒐集到掃描類或工具(Tool)類的資訊，相較之下高互動偽裝技術較難開發，且不容易被發現，同時可獲得更真實的網路環境攻擊資訊。

[15] 資料來源：The Honeynet Project 官方 twitter，https://twitter.com/projecthoneynet

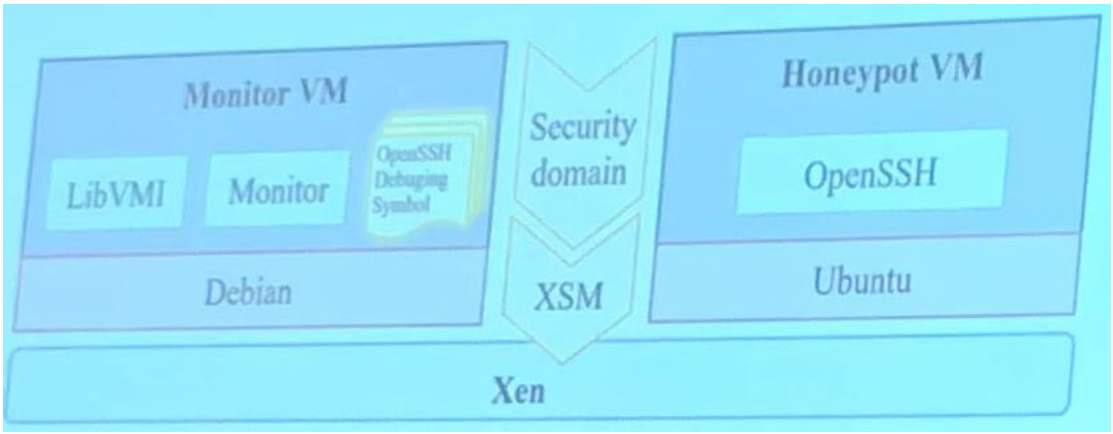

圖 16：Sarracenia 架構[16]

目前最流行之 SSH 類誘捕系統為 Cowrie，比較 Cowrie 與 Sarracenia 有很大的不同，Cowrie 採用模擬 SSH 回應的方式，預先設定好攻擊者輸入的指令時的回應訊息，設定完畢後，Cowrie 可以偽裝成真正的 Server，缺點則是當攻擊者送出的指令沒有設定回應的情況下，容易被發現為誘捕系統。Sarracenia 採用的則是直接開放有 OpenSSH 服務的虛擬機在網路上供人連線，由於本身為真實環境，因此不需要進行系統設置上的偽裝，頂多需要放置一些攻擊者可能會感興趣的檔案即可，最後透過 VMI 的技術，監控虛擬機系統運作狀況，以達到互動之效益。

下圖為 Stewart 提出之系統範例，A 為 Sarracenia 之系統範例，當攻擊者連線成功後，紅框部分顯示可以成功地修改密碼，藍框部分則在嘗試刪除使用者時系統回應不存在此使用者，綠框則是故意打錯指令，系統回覆找不到指令。B 為 Cowrie 之系統範例，紅框部分同樣顯示可以成功地修改密碼，但此回應為 Cowrie 模擬之回應，實際上虛擬機的密碼並未被修改，藍框部分由於 Cowrie 並未在腳本寫入該指令的回應，因此即便這是有效的指令，Cowrie 一樣表示查無此指令，同時輸入指令檢查使用者狀態也發現正常來說 IDLE（閒置時間）、JCPU（所有的程式在本次連線中使用 CPU 的時間）與 PCPU（當前的程序使用 CPU 的時間）應不會是零才對，但 Cowrie 卻回應皆為零，正常系統不可能會發生這些狀況，因此容易讓人判斷其為誘捕系統。

[16] 資料來源：The Honeynet Workshop 拍攝之會議簡報

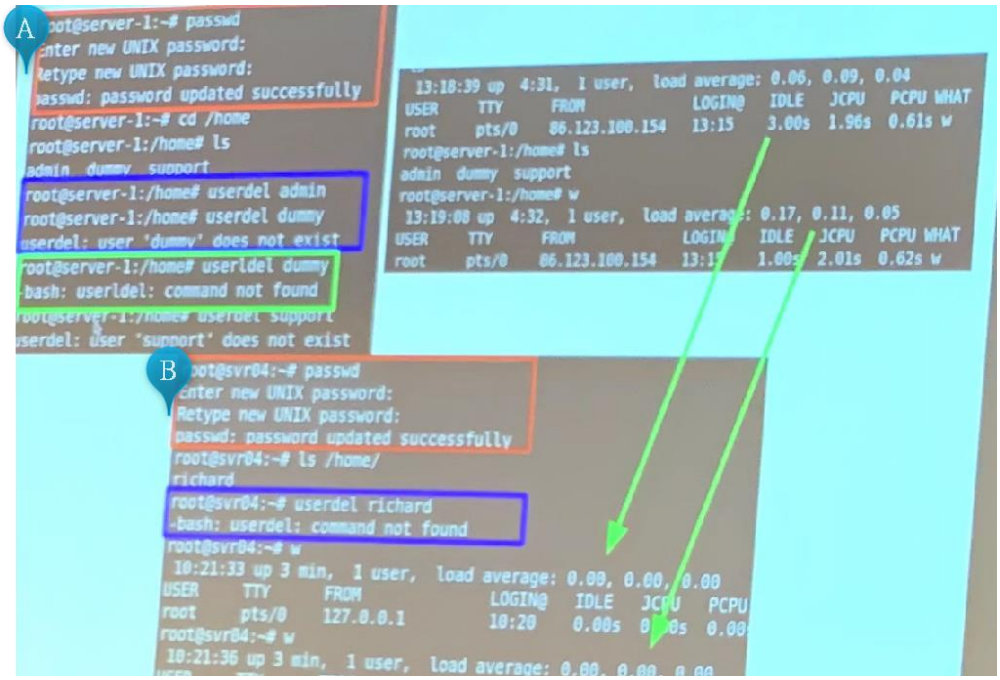

圖 17：SSH 誘捕系統畫面比對[17]

比較兩者間的誘捕狀態，Sarracenia 被登入的成功率較低、次數也較少，但被執行的指令卻高過 Cowrie 許多，代表攻擊者願意花更多時間在 Sarracenia 下指令攻擊，而非單純的利用工具。

雖然高互動誘捕系統 Sarracenia 優點突出，但講者同時也提醒大家：「高互動伴隨的就是高風險」，講者表示他就曾因為測試燒掉了兩台交換器（Burn up two core switch），雖然有點難以置信，但似乎的確帶來高風險。

[17] 資料來源：The Honeynet Workshop 拍攝之會議簡報，並自行整理

十、Hiding in the Shadows: Empowering ARM for Stealthy Virtual Machine Introspection

圖 18：Hiding in the Shadows: Empowering ARM for Stealthy Virtual Machine Introspection[18]

本場次由 Sergej Proskurin 與 Ulrich Fourier 共同發表，Sergej Proskurin 為慕尼黑技術大學（The Technical University of Munich）博士候選人，主要研究方向為 IT 資訊安全相關領域，特別專注透過 VMI 進行動態惡意軟體分析，同時也研究如何對客戶端虛擬機進行隱密分析的方法。Ulrich Fourier 則為慕尼黑技術大學訊息科學的碩士生，論文主要研究動態惡意軟體分析，2018 年夏天 Ulrich 加入 GSoC 的 Honeynet DRAKVUF 項目，DRAKVUF 是讓一種基於虛擬技術的二進制（Binary）檔案分析系統，可以對任意二進制檔案或操作系統進行深入追蹤，無需在分析的虛擬機上安裝其他軟體。

VMI 的架構與上一場會議 Stewart 提出的意見大致相同，透過 VMI 監控虛擬機（Guest VM）將結果顯示在 VMM 上（Virtual Machine Monitor）。本場次兩位講者也提出一個建立在 Xen 系統上的監控機制，Xen 是一種開源的虛擬機監視器，同時可以在單台伺服器上運行大量作業系統，接著在 Xen 上分別建立 VMI 監控以及用戶虛擬機，VMI 監控主機可透過 LibVMI 與 DRAKVUF 進行介接，LibVMI 主要專注於虛擬機（VM）讀取和寫入記憶體，並可支援 Xen 或 KVM 中運行

[18] 資料來源：The Honeynet Project 官方 twitter，https://twitter.com/projecthoneynet

的虛擬機，最後通過安裝插件（Plugins）的方式讓 DRAKVUF 可以對應不同的虛擬機資料。

最後 Ulrich Fourier 總結表示，要在一個硬體設備能力不足的情況下進行隱形的動態分析是相當困難的，需要透過虛擬化技術克服硬體限制才可進行原始碼檢測。

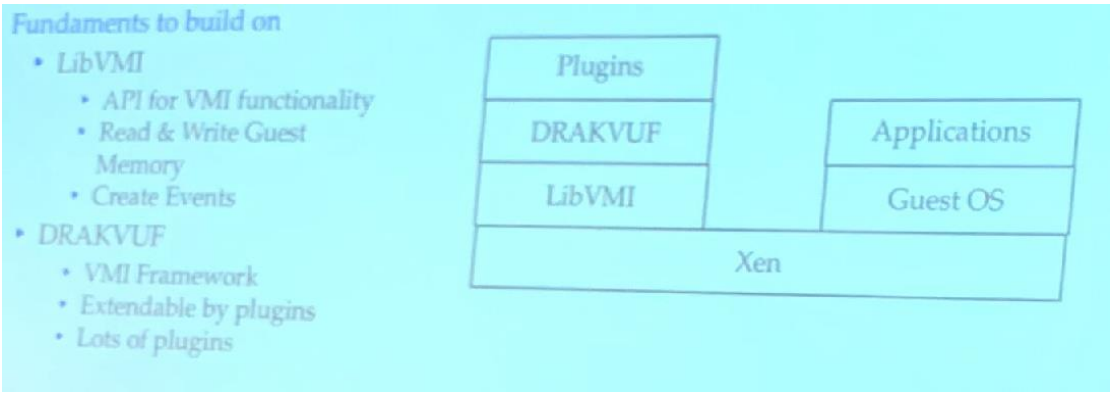

圖 19：VMI 與 DRAKVUF 合併架構[19]

[19] 資料來源：The Honeynet Project 官方 twitter，https://twitter.com/projecthoneynet

十一、Honeypots and IDS 101

本場次講者為 Miguel Bautista，Miguel 是 UNAM-CERT（Universidad Nacional Autónoma de México）的一員，該 CERT 由墨西哥最大的大學組成，Miguel 負責處理影響學網的資安事件。2017 年 Miguel 進入 Talos 團隊，開始與 Snort 密切合作，協助這項開源 IDS（入侵檢測系統）開發規則。

本場次屬於介紹型會議，主要讓與會者了解誘捕系統與 IDS 等技術，並利用佈署它們來檢測潛在威脅，保護網路設施避免遭受攻擊。講者首先說明低、中、高互動誘捕系統的差別，該場次內容在先前有稍微提及，詳細說明如下：

- 低互動誘捕系統
  - 模擬系統的服務，內部系統承受的風險較低。
  - 與入侵者互動程度低。
  - 主要目的監控特定服務是否遭到攻擊。
- 中互動誘捕系統
  - 根據資安人員的誘捕目的與誘捕系統設定，決定與入侵者的互動程度。
  - 容許入侵者或惡意程式執行系統中的部分程序。
- 高互動誘捕系統
  - 不使用模擬環境而是使用真實系統。
  - 入侵者可以使用任何資源，甚至操控系統。
  - 此類系統會記錄入侵者所有行為，能蒐集完整攻擊行為。
  - 承擔風險高。

	Low Interaction	Medium Interaction	High Interaction
Installation	Easy	Involved	Difficult
Maintenance	Easy	Involved	Difficult
Level of risk	Low	Medium	High
Requires control?	No	Variable	Yes
Information gathering	Limited	Variable	Extensive
Type of interaction	Emulated services	As required	Total control

圖 20：互動等級比較[20]

[20] 資料來源：The Honeynet Workshop 之會議簡報

上述提到的低、中、高互動誘捕系統為 Sever 類型的誘捕系統，該類型包含幾個特點：

- 誘捕系統將模擬成有特定漏洞的服務主機。
- 目的是讓入侵者進行偵測、攻擊。
- 屬於被動式等待入侵者攻擊。
- 由於沒有對外公開，因此所有進入服務主機內的連線都應視為可疑。

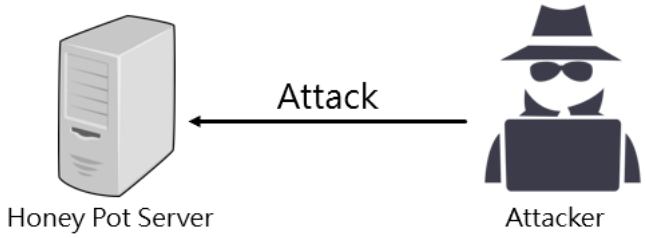

圖 21：Sever 類型誘捕系統[21]

另外還有一種 Client 式的誘捕系統，特點為：

- 模擬為客戶端應用程式
- 主動與外部疑似惡意主機互動

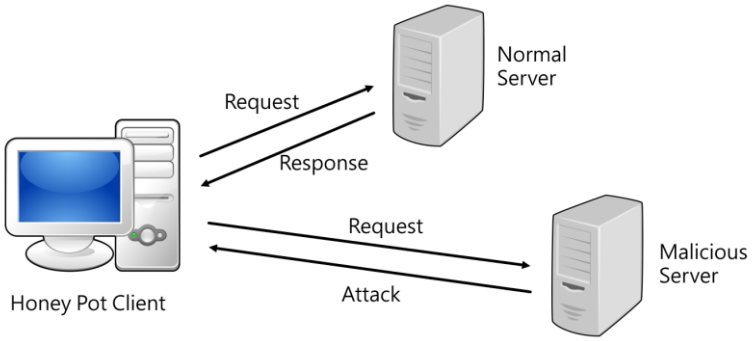

圖 22：Client 類型誘捕系統[22]

接著針對現在常用的誘捕系統 Dionaea、Cowrie 與 Glastopf 進行說明，Dionaea 是一種低互動誘捕系統，可以模擬一些常見的 Windows 網路服務，Glastopf 也是一種互動誘捕系統，可以模擬很多漏洞的 HTTP 網頁，Cowrie 則是一種中互動的誘捕系統，用來模擬 SSH 的服務，讓攻擊者連線進入後紀錄其輸入的指令。

---

[21] 資料來源：自行整理

[22] 資料來源：自行整理

名稱	特性
Dionaea	模擬各種微軟常見的服務，以誘捕微軟系統弱點
Cowrie	針對SSH/Telnet設計，可誘捕嘗試登入之帳號密碼與暴力攻擊模式
Glastopf	模擬大量web漏洞，針對攻擊的不同攻擊手段來回應攻擊者，誘捕網頁攻擊

圖 23：誘捕系統類型[23]

入侵偵測系統（IDS）是一種專門捕獲分析網路流量而設計的系統，透過 IDS 偵測網路封包，可以找出來自外部的異常連線行為，後續再由分析師確定是否為資安事件，IDS 主要偵測方式為特徵偵測（SIGNATURE-BASED DETECTION）分析師會先將惡意程式的特徵或一些惡意的 IP 設定進 IDS 中，當偵測到流量有符合條件之封包時，便標註為惡意流量，但 IDS 並不會進行流量阻擋。

現今開源 IDS 最常被使用的即為 Snort，其官方網站提供 Snort 安裝指南，Snort 主要有三種模式，第一種為嗅探（Sniffer）模式，嗅探模式僅從網絡中讀取封包，並顯示在控制台上而不對流量進行任何動作，第二種為封包紀錄（Packet Logger）模式會將封包儲存到硬碟中供分析人員確認，第三種模式為最常被使用的網路入侵偵測系統（Network Intrusion Detection System ,NIDS）可即時檢測分析現行網路流量，以上三種模式為 Snort 三大功能。當天下午的議程主要說明如何安裝誘捕系統及 Snort 相關指令，便不多加贅述。

[23] 資料來源：自行整理

肆、檢討與建議

參與本次會議可深入了解誘捕系統翹楚 The Honeynet Project 最新技術，以及討論多年的 T-Pot，顯示目前 The Honeynet Project 正朝高互動誘捕系統進行研究，雖然今年提出兩款高互動誘捕系統（SNARE 與 Sarracenia），但開發人員表示仍在研發中，相對於過去的誘捕系統風險也高出許多，並不適合大量佈建，佈建高互動誘捕系統需要注意的事項如下：

1. 頻繁的確認誘捕系統狀態並定期重置
2. 將其設置於實驗室環境中，讓網路無法連接到其他內部設備。
3. 配置專人進行監控，提高監控頻率並隨時了解系統狀態，當發生異常時便可立即重置。若有足夠的人力建置高互動誘捕系統，便可獲得更加真實的攻擊資訊，提高團隊資安分析能量。

本次 The Honeynet Project Workshop 偏向學術探討，沒有詳加說明誘捕技術該如何應用於企業環境中，但透過各國優秀資安專家之分享與討論，學習最新誘捕技術及架構，期許未來能應用於本中心誘捕系統，建構安全的網路環境。

伍、相關照片與附件

已隨附相關照片與附件於報告內文中。