多重因子誘捕情資可信度分析

許勝翔[1] 高偉碩[2] 蔡一郎[3] 楊嘉麗[4]

財團法人國家實驗研究院國家高速網路與計算中心

[1]E-mail:1603015@narlabs.org.tw、[2]E-mail: suokao@narlabs.org.tw、[3]E-mail: yilang@narlabs.org.tw、[4]E-mail: d00joy00@narlabs.org.tw

摘要

隨資訊安全威脅問題日益嚴重，瞭解駭客攻擊行成為組織進行資訊系統安全防護之必要條件。其中誘捕系統(HoneyPot)以誘捕的手法吸引駭客攻擊，藉此蒐集攻擊者的來源、手法、特徵及模式，提供早期攻擊預警及資安事件分析資料，為蒐集攻擊情資的重要方式。然而， 誘捕系統收集之情資數量龐大且混雜，組織內的資安人員如何在有限的時間和人力條件下，快速審視高風險等級之資安情資並進行資安事件管理（Security Information and Event Management, SIEM），為系統管理人員重大之挑戰。因此，本研究目的強化誘捕系統資料可信度，首先以既有學術網路的水坑(Sinkhole)網路整合誘捕系統，有效地蒐集惡意行為資訊，再透過 SIEM 平台對所蒐集的資料流進行威脅比對及進行評分，分析出惡意行為及程式對系統威脅之風險等級。透過本研究所開發的系統，可以將誘捕系統偵測情資進行風險分級，提供系統管理人員優先關注處理的有效參考。

關鍵詞：水坑(Sinkhole)、誘捕系統(HoneyPot)、安全性資訊與事件管理(Security Information and Event Management, SIEM)、情資可信度。

1、前言

資訊普及帶來資訊安全的威脅，當前資安防禦局勢嚴峻，許多企業或公部門不惜大量投資在各種資安防禦方案，建置安全性資訊與事件管理系統（Security Information and Event Management, SIEM）輔助判斷惡意活動。然而實務上，組織內面對資安威脅第一線的資安團隊，隨時面對大量且龐雜的威脅情報，在有限的時間和人力之下，只能以極低的比例進行惡意行為審視、以及事件分析，因此提升資安系統情資資料可信度，有效協助組織快速發掘重大資安威脅，並進一步進行因應，為當務之急。

由於目前商用市場上，對應惡意程式之資安防護軟體及硬體眾多，主要防護項目可包含入侵偵測(IDS)、入侵防護(IPS)、沙箱(Sandbox)等。IDS 系統主要依據預先設定的安全策略，進行網路流量、連線行為監測;而 IPS 則化被動為主動，針對網路異常封包或攻擊行為，同時進行主被動防禦，並立即採取必要的處置措施; 而 Sandbox 則主要進行惡意程式分析與網站檢測。不論是那種資安防護方式，都需要收集大量資訊安全情資。因此本研究以台灣學術網路(TANET)為標的，整合長期建置在台灣學術網路的誘捕系統所蒐集的資訊安全情資，搭配商用 IDS 及沙箱，分析所收集到的情資之惡意行為，再透過 SIEM 整合平台，對分析過後的資料進行整合及評分。透過本研究發展之評分機制，能讓組織資安團隊在有限資源下，快速掌握與處理高風險惡意程式，有效提升組織資安防禦能力。

2、文獻探討

2.1 誘捕系統(Honeypot)

Honeypot 為建置一個吸引攻擊者的目標，透過誘捕的手法，吸引駭客發動攻擊，藉此收集與紀錄所有攻擊動作與過程。此外，Honeypot 誘捕系統同時具有消耗攻擊時間、轉移攻擊目標等的功能，因此已經成為蒐集駭客資訊的重要方式之一。Honeypot 發展與國際上重要非營利組織 Honeynet Project[1]息息相關， Honeynet Project 成立於 2000 年，由一群對誘捕技術具有高度興趣之資訊專家所組成，隨著駭客攻擊情勢日益險峻，目前 Honeynet Project 已開發超過五十幾套相關功能的誘捕系統，可在不同的作業系統運行模擬成高互動 Honeypot 與低互動 Honeypot。由於 Honeypot 系統皆採取開源軟體(open source)方式開發，使用者可以免費使用、修改與散布，因此在產學界大量廣泛使用，成為各種組織研究駭客行為手法之重要方式。尤其在學術網路安全偵測與防禦應用上，學術網路除了透過商用的資安設備確保網路安全外，也長期運用 Honeypot 協助安全偵測，Honeypot 已經為學術網路安全帶來明顯之效果。以臺灣學術網路為例，Honeypot 成果如下，包括(1)已開立 15 萬張的事件預警單，若攻擊來源 IP 為國內單位，則通知來源單位並開立事件單，若攻擊來源 IP 為 TANET， 則由台灣電腦網路危機處理暨協調中心(TWcert) 追蹤各校處理狀況；(2)統計每周攻擊超過一萬次連線的國內外 IP 並提供清單，提供各大學做為黑名單的參考依據；(3)分析捕捉到的惡意程式，並分享在惡意程式知識庫平台。

為使誘捕系統不成為受害主機，現階段臺灣學術網路所執行的誘捕系統類型，以中低互動的 Honeypot 為主，包含 Windows、Linux、IOT、工業控制等系統環境，並模擬已知的系統服務弱點去提供運作，現有系統服務說明如表 1 所示。

表 1 現有系統服務

模擬服務類型	功能說明	行為資料
Windows OS	模擬各種常見服務，包含 Web、FTP、UFTP、SMBD、MSSQL、MYSQL、RPC、SIP 等服務。	1.連線資訊 2.檔案下載點 3.檔案下載
Linux OS	使用虛擬終端機的形式，可供使用者在本地主機執行遠端 Unix 系統 SSH 管理服務，並提供可操作的 shell 環境。	1.連線資訊 2.帳/密暴力破解 3.Command 語法 4.檔案下載
Telnet	使用虛擬終端機的形式，可供使用者在本地主機執行遠端主機上的工作。	1.連線資訊 2.帳/密暴力破解
Web	提供以 Head、Get、Post 網頁操作方式	連線資訊
工業控制	工業控制常見的 HTTP、SNMP 系統等服務。	1.連線資訊 2.MIB 值 3.SNMP 版本
IOT 裝置	模擬裝置常見之服務，包含 MQTT、PTPP、UPNP、Camera。	連線資訊
OS 偵測	偵測連線者使用的作業系統資訊	Client OS 偵測資訊

2.2評分機制

本研究主要目的在於提高一般使用者對情資的認識，因此評分機制為其中關鍵的要素。目前市場上提供評分機制，大致可分為惡意程式沙箱與威脅情報蒐集平台二種。惡意程式沙箱提供的功能，主要為惡意程式檢測及網址(URL)檢測，沙箱種類眾多，主要目的為強化惡意程式檢測及辨識度，目前沙箱主要有分為二種，第一種是透過虛擬化技術，將硬體資源切割成多個與主系統隔離的虛擬作業系統作為沙箱[2]，因此沙箱需要安裝惡意程式相對應的應用程式，舉例來說，.docx 對應 word、.rar 對應 WINRAR，如**圖 1** 所示，將惡意程式投入沙箱時，系統會觀察檔案執行時會觀察 CPU 指令集及記憶體存取資訊來判斷惡意行為並依照影響系統檔案重要性來給予評分。第二種是將沙箱建置在網路架構之中，透過 CPU 虛擬技術並主動於網路上蒐集情資進而建立資料庫，再將流經網路的檔案與資料庫做比對，依照相似程度進行評分[3]。

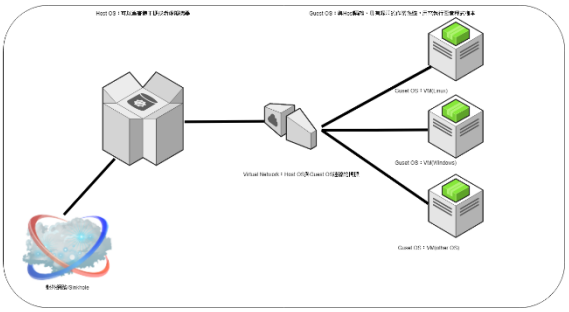

圖 1 虛擬化 Sandbox 架構[4]

威脅情報蒐集平台則是開發廠商經由與各國單位或同業進行合作，利用情資交換所蒐集的大量威脅情資進行分析及整理，將其中的 IP、連線及行為等具有指標性的項目標註，並給予風險等級評分，主要用途可以建置雲端威脅情資平台，提供客戶上傳檔案，或透過 md5、sha1 或 sha256 等雜湊碼查詢方式，檢查是否為已經收錄的惡意程式，再透過關聯式分析查看相關網路拓樸，進而提供使用者進行資安事件調查的方向。威脅情報蒐集平台將收集的情資整合，並作為資安設備的安全防護規則，提供硬體資安防護設備套用，可有效的在遭受入侵前即防賭惡意行為。

由上可知，目前市面上的資安防護軟體及硬體，為了更能夠說服使用者使用，惡意行為紀錄、網路拓樸及風險評分都是必要項目，因此要如何提高資料的可信度將會是未來一大課題。

3、研究方法

本研究的目的是強化誘捕資料流可信度，透過延伸 Sinkhole 架構，將攻擊流量分別導入至不同資安設備，如 IPS、Firewall、Sandbox、WAF 等，來進行威脅比對及風險評分，研究方法說明如下:

3.1 誘捕系統網路架構

本研究之誘捕系統，以 Sinkhole 的架構佈署在學術網路上，主要目在於精簡環境架構、降低人力建置成本，以及提升管理效率。誘捕系統判定是否為惡意程式的基本概念為「未提供真實服務，卻有人嘗試連線」，亦即針對誘捕系統的網路行為都屬於「惡意」。經由將 Sinkhole 架構中所有惡意流量，導向資安設備進行進一步的分析及偵測，如入侵偵測系統(Intrusion Detection System；IDS)、沙箱(SandBox)，再透過 SIEM 整合平台對所蒐集的資料流進行威脅比對及風險評分，藉此提升誘捕系統偵測情資的豐富程度，以維持組織對服務水平高可用性的期待。

Sinkhole 網路是透由 VXLAN(Virtual Extensible LAN)[5]技術又稱虛擬可擴展區域網路，個別於偵測點放置 VPN 設備，並與國家高速網路與計算中心(國網中心)建立 Tunnel 連線，使網路環境變成同屬於一個內網的 L2 架構，可將各偵測點的攻擊流量導回國網中心進行偵測[6]，如**圖 2** 所示。

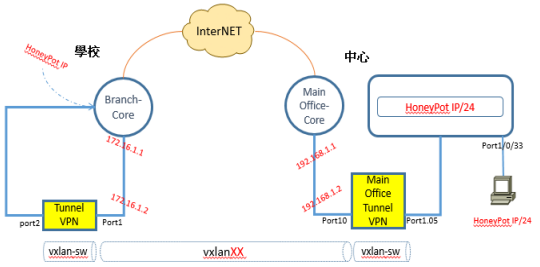

圖 2 Sinkhole 網路[7]

當誘捕偵測類型與範圍越廣，其所獲得資訊越加豐富，因此運用 Sinkhole 技術，除了可以容易擴充偵測佈署，並可以在彼此間攻擊流量不受干擾下，善用共用基礎設施資源，可進行單一主機就能服務所有網段誘捕之行為，如圖 所示。對於偵測到的資訊日誌也可集中放置於國網中心內部儲存。由於共用基礎設施集中於國網中心內部運作，對於設備維護困難度或資源不足時需平行式擴充，此架構在進行調整效果佳，如圖 所示。最為重要的是此誘捕網路 Sinkhole 架構，比傳統式的架構可省下約 60%的成本費用。

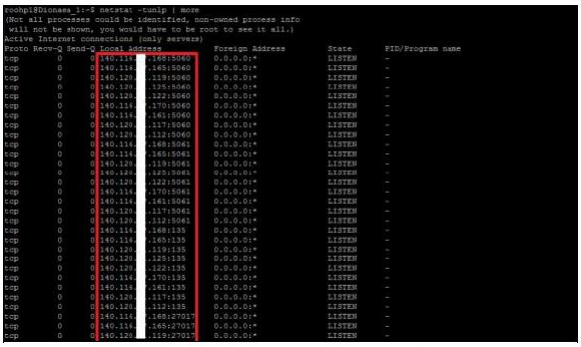

圖 3 資源共用

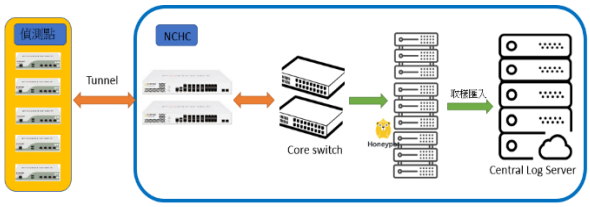

圖 4 誘捕網路 Sinkhole 架構

3.2 誘捕資料流單元

本研究透過 Sinkhole 技術，把屬於不同偵測點網段流量引導至國網中心集中，並利用 Virtual Switch 分別對應 VXLAN TAG 至誘捕偵測平台，來負責殭屍電腦行為資訊與惡意程式之收集，並將其記錄傳至日誌平台。

在原架構不變下，結合智慧型的流量複製器[8]，具備聚合、過濾、封包工程與流量分配之功能，能將誘捕流量錄製 PCAP 封包，以做為後續行為研究外，也能分別引導至不同資安設備進行偵測與分析，藉此提升誘捕系統偵測情資的豐富程度，如圖 所示。

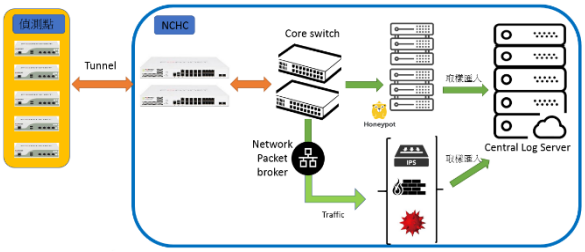

圖 5 誘捕資料流架構

3.3 風險評分單元

由於誘捕資料內只有連線者行為模式，無法顯示出每一筆資料的威脅等級，若能在每一筆依行為模式加以定義其分數，可使資安人員快速得知威脅訊息以做有效之措施。由於誘捕工具之類型不同，因此本研究先以 7 種不同工具與觸發之行為，做為一個基本評分判斷條件值，包含工具類型、嚴重等級、惡意樣本下載點、惡意檔本檔案、帳號與密碼、所下達指令資訊、網頁連線方式。另外提供 3 種加權條件值，包含近三個月共觸發幾個月來連線、有觸發到資安設備弱點特徵碼資訊、近三個月攻擊偵測點的目標數，來強化威脅程度之分數，如**表 1** 所示。

由於誘捕系統一開始設計概念即為運作中且無營運價值之系統，所以對於來進行訪問之訪問者都被視為可疑，當滿分為一百分時，這些連線即從50分開始計算，及透過相關專家一同進行量測表觸發之分數，以進行基本條件值分數與加值條件值分數，最後加總後成為威脅值。

表 2 威脅判斷條件值

條件式			Score_A(工具類型)							
			A1	A2	A3	A4	A5	A6	A7	A8
基本條件值	Score_B (嚴重等級)	B1	★	★	★	★	★	★	★	★
		B2	★	★	★	★				
		B3	★	★	★	★				
		B4	★	★	★	★				★
		B5	★							
		B6	★							
		B7	★							
		B8	★							
	Score_C (下載點)	C1	★	★	★					
		C2	★	★	★					

	Score_D (下載)	D1	★	★	★					
		D2	★	★	★					
	Score_E (帳號)	E1	★			★	★	★		
		E2	★			★	★	★		
	Score_F (密碼)	F1	★			★	★	★		
		F2	★			★	★	★		
	Score_G (指令)	G1				★	★			
		G2				★	★			
		G3				★	★			
	Score_H (url)	H1							★	★
		H2							★	★
		H3							★	★
加權條件值	Score_I (近三個月訪問蹤跡)	I1	★	★	★	★	★	★	★	★
		I2	★	★	★	★	★	★	★	★
		I3	★	★	★	★	★	★	★	★
	Score_J (弱點資訊)	J1	★	★	★	★	★	★	★	★
		J2	★	★	★	★	★	★	★	★
	Score_K (近三個月連線行為)	K1	★	★	★	★	★	★	★	★
		K2	★	★	★	★	★	★	★	★
		K3	★	★	★	★	★	★	★	★

3.4 資訊收集單元

目前佈署的誘捕系統，其攻擊資料已集中存放於 Splunk 平台內[9]，可透過搜尋指令與時間區間呈現資訊，未來資料流的日誌也導入至平台內，當資料越多樣化其威脅資訊會更加明確，並將威脅資訊建立一個可查閱的 Dashboard 介面，以便使用者能快速得知相關訊息。

4、系統實作結果

4.1 誘捕資料流合併

本研究經由 Network Packet Broker 機制，將誘捕流量導入資安設備進行偵測分析，並將偵測後之結果集中於日誌平台內，找尋誘捕系統日誌與資安設備日誌，做為關聯之條件，並把資安設備日誌截取威脅說明之欄位，結合至誘捕系統日誌內，能有效強化威脅資訊可信度，如**圖 7** 所示。

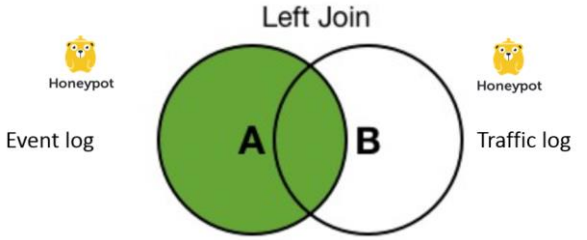

圖 6 誘捕資料流合併

圖 7 誘捕資料流資料合併

4.2 誘捕情資威脅評分結果

為了有效數值化誘捕威脅程度，本研究將所有碰觸到誘捕系統之訪問者都被視為可疑，將依工具名稱會對應到的行為共 176 種組合，分成為 28 條觸發條件對應到五個數值(50, 60, 70, 80, 90)，另結合額外 3 種加權觸發條件，加權條件一分對應到三個數值(0, 5, 10)；加權條件二分對應到二個數值(0, 5)；加權條件三分對應到八個數值(0, 1, 2, 3, 4, 5, 6, 7)，最終針對每一筆誘捕資料，將觸發到基本條件分數加上有觸發到加權條件，成為每一筆誘捕資料情資之風險分數，如**圖 8** 所示。

圖 8 誘捕情資威脅分數

現階段本研究使用日誌平台(Splunk Cluster)，將相關誘捕資料與資料流部份存儲，也額外集中放置學網之資安設備偵測到的攻擊行為，與外部情資[10][11]提供攻擊行為之資訊，利用 Splunk 具備索引功能與快速搜尋能力，來改善大量資料分析運算時效能不佳之問題。雖然資安專家或使用者可以透過 web 搜尋介面，進行查詢所需要之資訊，但在日誌呈現結果與使用所需語法將會是一大障礙，因此歸納使用者對資料呈現與習性，首先建立一個 SIEM(Security Information Event Management)查詢介面，依使用者常使用查看條件-依時間區間、受攻擊偵控點、攻擊者國別、攻擊來源是否為 TANET IP、資訊的威脅分數、可輸入查詢 IP 之欄位，做為判斷條件值；以及使用者會想知道資訊的報表-如誘捕日誌在前二週或前二個月遭受攻擊之趨勢、與外部情資比對的數量與資訊、與一週內放置學網資安設備比對數量與資訊、

攻擊者查詢來源 IP 數量與被攻擊端服務數量、Unique 惡意程式檔案與下載點、國內外及 TANET 的攻擊次數、攻擊者攻擊目標服務埠、資安設備偵測出的弱點資訊、攻擊端使用的作業系統、攻擊趨勢地圖、使用帳號密碼猜測名單、與前三個月攻擊 IP 比對，透過一個人性化的介面來呈現整體威脅趨勢，以使用者能在操作上更簡便，如**圖 9**、**圖 10** 表示。未來當使用者在使用上需要更多樣化資訊，也可參考使用者意見來進行 SIEM 介面的修訂。

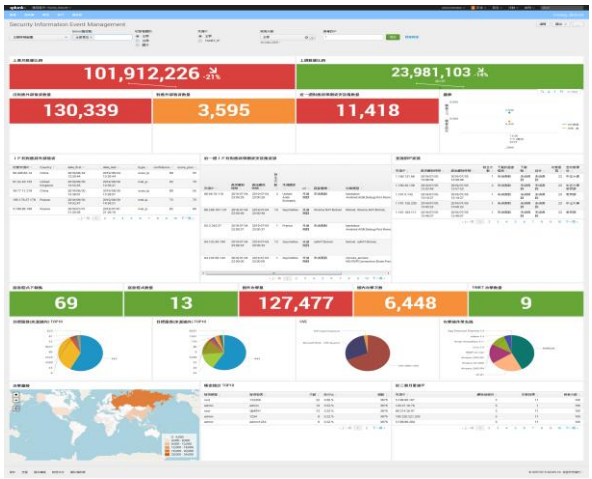

圖 9 SIEM 介面

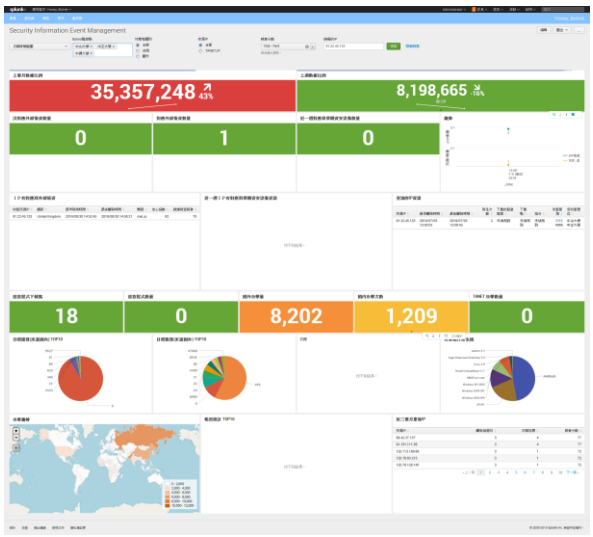

圖 10 人性化操作介面

5、結論與未來展望

5.1 結論

誘捕系統雖可所收集基本連線資訊、連線行為、攻擊手法之資訊，但透由資料流方式同時經由不同資安設備偵測與分析與交叉合併，更能強化誘捕日誌多樣性，再經由多項觸發條件值判斷，以分數來清楚定義出攻擊者對誘捕系統行為的威脅可信度。雖然攻擊者對於目標所進行之攻擊行為會不相同，經由本研究收集放置學網之資安設備對攻擊行為，與外部情資提供攻擊行為之資訊，來與誘捕系統所捕捉到的攻擊行為進行比對，對於誘捕系統所捕捉到的行為，與放置學網之資安設備資訊或外部情資資訊有比對到之攻擊者，可以很清楚此攻擊者的攻擊行為，若攻擊者在管轄範圍內即可進行資安事件單開立，反之若誘捕系統所捕捉到的行為，與放置學網之資安設備資訊或外部情資資訊沒有比對到，但因誘捕威脅分數達到一定分數上，可將這些資訊開立成預警單，以強化整體的資安防禦。

此外，本研究透過人性化的 SIEM 介面，除了將誘捕系統日誌與資料流日誌進行威脅可信度，並與既有偵測學術網路安全設備日誌與外部情資資訊進行交叉比對，能更清楚誘捕於網路安全協助偵測之可信度，來建立持續性威脅防護流程，形成一個資訊安全的生態系統(ECO System)。

5.2 未來展望

本研究誘捕情資可信度機制中，未來研究方向建議如下列三項。1.當資料流結合越多樣式設備進行偵測與分析，如加入不同產品的 IPS、IDS、Sandbox、WAF 等，可大大強化誘捕資料流之誘捕資訊可信度。2.在誘捕資料流之威脅評分機制，目前只透過相關專家一同進行量測表觸發之分數，若能透過更多計算方式來進行量測分數，如:平均法則、問卷調查統計法、Machine Learning 方式，以達到最佳化計算方法。2.當取得更多外部情資，更能獲得全盤的網路威脅，以便誘捕情資提供更明確的攻擊事件，與情報預警機制。

致謝

本論文感謝科技部計畫「MOST 108-2218-E-492-006 雲端攻防演練平台及惡意程式資料庫研製暨科學園區資訊分享與分析中心建置計畫(3/3)」提供經費支持本研究的進行，在此獻上最誠摯的謝意。

參考文獻

[1] The Honeynet Project http://www.honeynet.org/

[2] Seth H Pugsley, Zeshan Chishti, Chris Wilkerson, Peng-fei Chuang, Robert L Scott, Aamer Jaleel, Shih-Lien Lu, Kingsum Chow, and Rajeev Balasubramonian. Sandbox Prefetching: Safe run-time evaluation of aggressive prefetchers. IEEE, 19 June 2014.

[3] Huagang Xie, Xinran Wang, Jiangxia Liu. MALWARE ANALYSIS SYSTEM. United States Patent, May 24, 2011.

[4] http://docs.cuckoosandbox.org/en/latest/

[5] 許勝翔, 新世代誘捕系統, 台南市：國家高速網路與計算中心, 2018.

[6] https://fortiguard.com/encyclopedia/botnet/7630157/117-21-224-222-sinkhole-cncert-sinkhole-net

[7] https://resources.infosecinstitute.com/dns-sinkhole/

[8] https://www.garlandtechnology.com/blog/the-101-series-network-packet-brokers

[9] http://www.splunk.com

[10] Anomali 官網，威脅情報解決方案。檢自 https://www.anomali.com/ (August. 1, 2018)

[11] https://www.ithome.com.tw/review/109198