Communications of the CCISA
Vol. 25 No. 4 Nov. 2019

資安日誌管理暨惡意程式分析平台系統建置－以學校系所為例

楊慶裕[1]、郭家祥[2]、吳信德[3*]
國立澎湖科技大學資訊工程系
[1] chingyu@gms.npu.edu.tw、[3]wuhsinte@gms.npu.edu.tw

摘要

隨著科技時代進步，網路也提供人們許多便利性，不僅讓眾多企業帶來商機，也導致被用於犯罪的工具，使得電腦網路犯罪問題逐年累增，例如：竊取公司機密、阻斷服務攻擊、被植入惡意程式等犯罪事件發生，因此現在公司需增加一套完善的系統在犯罪事件發生後立即有效處理電腦鑑識的流程，一但犯罪事件發生，需要有追蹤犯罪電腦之作業程序的能力及技術，可以在最短的時間有效及快速地找到公司內部來源端電腦及犯罪者。

本文提出的系統是由三種不同軟體所組成，先將犯罪者的電腦系統備份，並對備份完成的系統進行蒐集、分析 Log、索引查詢，簡化過去繁鎖且沒效率的調查工作，並透過 Cuckoo Sandbox 沙盒分析，了解程式執行動向進而產生文件報表。

關鍵詞：資訊安全、網路安全、惡意程式分析、Docker 平台、ELK 套件

Regular Paper

Communications of the CCISA
Vol. 25 No. 4 Nov. 2019

Building a Platform System for Information Security Log Management and Malware Analysis—an Example at the School Departments

Ching-Yu Yang [1], Jia-Siang Guo [2] , Hsin-Te Wu
Department of Computer Science and Information Engineering, National Penghu University of Science and Technology, Taiwan.
[1] chingyu@gms.npu.edu.tw、[3]wuhsinte@gms.npu.edu.tw

Abstract

With the advances in the technology era, the Internet has provided tremendous convenience. Apart from bringing business opportunities for enterprises, the Internet has also become a criminal tool for unscrupulous people, which has increased the problem of cybercrime year by year, such as stealing confidential information, denial-of-service (DoS) attacks, malware implantation, and relevant crimes. Therefore, enterprises are suggested to install a comprehensive system that could implement the process of digital forensics effectively and immediately right after encountering a cybercrime. Once a cybercrime happened, it requires a processing system with sufficient capability and techniques to track the computers that involve in the crime, which enables the company to find the source computer internally and the criminal efficiently and effectively in the shortest time.

The system this study offers consists of three different kinds of software, it back the computer system of the criminal up and conduct investigation processes of searching, analyzing logs, and index scanning; the system simplifies the old cumbersome and inefficient investigation process to understand the execution tendencies of the software and produce reports through Cuckoo Sandbox Analysis.

Keywords: Information Security, Network Security, Malware Analysis, Docker Platform, ELK Stack

壹、前言

隨著科技發展網路安全性更顯著重要，現今許多病毒或者駭客入侵造成企業經濟損失，全世界超過 54%的企業執行長認為企業隨時會遭受網路安全的攻擊，可見資安問題已是重要的企業危機[1]。現今個人資料保護也受到各界重視，許多企業雖然建置完善的電腦機房，但對於網路安全防護設備建置不完整，當網路安全設備不完整時就容易受到駭客惡意攻擊，為了能夠追朔相關攻擊事件是由內部或者外部攻擊，企業需要建立網路監控日誌系統，但目前監控日誌系統需要花費大量經費建置，因此對於中小型企業而言是一大負擔，因此需要利用免費監控軟體進行網路封包紀錄，並且需要過濾封包相關資訊，了解來源與目的端的 IP，因此監控日誌系統需要更快速方法可以解析封包，本文提出方法可以降低中小企業建置系統費用壓力，並且當駭客入侵或者遭到內部惡意攻擊時，監控日誌可以提供線索追蹤攻擊者的位置，目前個資法受到世界各國重視，當企業資料受到外洩或者竄改情況發生時，受害者提出相關告訴或法律問題時，企業需要進行舉證或者相關軟硬體數位鑑識結果，降低企業因駭客行為造成經濟損害，由於法律訴訟或者數位鑑識需要一段時間處理，並且需要更多日誌提供給鑑識人員確認入侵的方式，但由於當入侵案件發生時需要一段時間進行相關法律流程，因此日誌需要更大空間進行儲存，並且需要一些密碼學技術進行加密保護，以確保日誌的隱密性、來源性以及不可否認性，本文提出的方法可以有效儲存日誌，並且確保日誌的安全性。

本文提出的方法希望透過對於網路安全的認知，建立良好的正確觀念，本文研究期望達到底下幾項目標:1. 建立資安知識及技術的基礎，2. 建立 ELK 事件追蹤平台與 Cuckoo Sandbox 分析平台及 3. 加強平台、系統架構之穩定性，本文主要利用各種免費監控日誌軟體建構系統，並且利用各種軟體的特色依照各種資料來源進行分析，並且進一步解析封包，本文也建置報表系統可以讓管理者觀看目前網路安全品質，本文透過系所網路監控進行實驗，本文提出的系統可以有效儲存各種惡意攻擊日誌，並且透過系統可以監控網路攻擊情況，由實驗結果可以得知本文提出的方法是可行的。

貳、文獻探討

在文獻[5]中主要利用分散式入侵偵測系統避免整體網路遭到惡意攻擊，由於現今入侵測系統屬於集中式系統，容易遭到駭客攻擊因此癱瘓，本文獻主要利用分散式概念當單一節點遭到攻擊時，會有其他系統進行代理監控，本文獻雖然需要花費大量經費建構系統，但可以避免集中式遭到大量封包攻擊的風險。文獻[7]中提到入侵檢測系統定義了重要的網路全動態研究領域。入侵的作用安全體系結構內的檢測系統正在改進通過辨識所有惡意和可疑的安全級別在電腦或網路系統中可能觀察到的事件。與入侵檢測有關的更具體的研究領域是異常檢測。基於異常的入侵檢測網絡是指在網絡中發現非典型事件

的問題觀察到的網路流量不符合預期正常模式。假定一切非典型/異常可能很危險，並且與某些安全事件。為了檢測異常，許多安全系統實現分類或聚類算法。文獻[6]中提到監控系統的安全技術的產生避免惡意活動，入侵偵測系統需要達到即時性。在文獻[4]中提到協作式入侵檢測網絡（CIDN）提出一個入侵偵測系統來收集信息並從其他人那裡學習經驗入侵偵測系統節點。維護一組入侵偵測系統之間的交互節點，CIDN 有望在檢測方面更強大一些複雜的攻擊，例如拒絕服務（DoS），一個入侵偵測系統。在實際部署中，我們確定每個 IDS 在檢測不同的信號時可能具有不同的靈敏度入侵類型。因此，在本文中，我們定義了入侵的概念敏感性並研究使用它進行評估的可行性。

在文獻[8]中提到網絡入侵是任何未經授權的活動在計算機網絡上。因此，有必要開發一種有效的入侵檢測系統。在本文中，我們認識使用改進的遺傳 k 均值的入侵檢測系統用於檢測入侵類型的算法（IGKM）。本文也顯示了入侵檢測系統之間的比較，使用 k-means ++算法和入侵檢測系統使用 IGKM 算法，同時使用 kdd-具有數千個實例的 99 個數據集和 KDD-99 數據集。在文獻[2]中提到網絡入侵檢測系統（NIDS）具有防止網絡攻擊和未經授權的挑戰遠端控制。NIDS 通常遵循兩種不同的策略。第一個旨在檢測網路的禁止使用，第二個集中於發現非法行為。在文獻[3]中基於遺傳網路程式（GNP）的分類關聯規則探勘方法，提出了一種結合誤用檢測和異常檢測的網路入侵檢測方法。建議的方法是使用 GNP 的入侵檢測方法的擴展，因此它可以檢測和區分正常的，已知的入侵和未知入侵。實驗結果可以得知，與傳統入侵相比，檢測率有所提高。

參、技術介紹

3.1. Docker－虛擬化技術

Docker 主要為開放源碼，主要是為 2013 年初產生，一開始是 dotCloud 企業內使用的專案軟體，Docker 主要是 google 所推出的 Go 語言進行開發完成，軟體加入 Linux 開放源碼行列，依照 Apache2.0 協定，Docker 的願景為在不同的應用程式以及作業系統中都能運行，以期望達成無平台限制，簡單來說就是希望在實體端、虛擬端、雲端上都能順利的運行，以實踐 Docker 的願景，Docker 核心原理[9]，主要如下:1. 隔離性-以 LXC 為基礎，作業系統進行虛擬化作業為 Linux 作業系統容器功能中一個使用者空間介面。2.獨立環境[10]，利用 Cgroups 與 Namespace 功能，建立視覺化軟體為以作業系統為主的操作環境，不需要使用 Hypervisor 建構軟體層協定，由於容器主要是以輕量化為設計，所以有利提升建立虛擬機器的執行速度與效率，Docker 最初使用進階多層統一檔案系統（Advanced multi–layered Unification File System，AUFS）作為容器檔案系統層，目前仍作為 Docker 的儲存後端之一，Docker 三大核心[11]，Docker Image 類似於虛擬機的映像檔，建立 Docker 的容器基礎，主要利用版本管理及增量的檔案系統，Docker 建立一套

較為簡易機制進行建立並更新現有 Image，使用者可以利用網路進行下載已經製作無誤的映像檔，並利用指令操控 Container，相似於輕量沙盒，Docker 使用 Container 進行執行以及隔離應用軟體。Container 是從 Image 建立的實際案例，可以進行 Run、Start、Stop、del，而 Container 之間都是互相隔離。Docker 倉庫相似和程式碼倉庫是 Docker 共同存儲 image 的空間，依照存放的 image 進行分想與否，Docker 倉庫分為 public 倉庫以及 Private 倉庫兩種模式，現今，最大 public 倉庫是 Docker 交換器，儲存數量較大的 image 供使用者下載，Container 與 Virtual Machine 的比較，Container 相較於 Virtual Machine 硬體容量佔用空間小，執行速度更快[12]。

3.2. Cuckoo 沙盒介紹

Cuckoo 沙盒[13]提供相關惡意程式的資料庫，並會自動針對程式相關執行情況進行偵測，由相關分析中視覺化畫面以及分析報告，有利於相關惡意程式進行相關分析報告。

3.3. 惡意程式分析介紹

特洛伊木馬病毒（Trojan Horse）常被簡稱木馬病毒[14]，在資訊領域中主要稱為後門病毒，Hacker 主要是用來竊取使用者的個人隱私資訊。間諜病毒軟體[15]主要是未經使用者同意之下竊取電腦中的相關資訊。間諜病毒主要是在 1994 年所發現。廣告程式[16]主要以廣告需求為目的，例如:彈跳程式等。後門病毒[17]主要是指避過軟體安全性控制，利用隱秘的 channel 取得對程式或者系統存取的惡意竊取方法。在應用程式開發時,設定後門病毒可以方便修改程式以及測試程式中的缺點。但如果後門被其他人知道，或是在發布軟體之前沒有去除後門,那麼它就對電腦系統的安全造成威脅,如 NC(Netcat) 就是一個後門程式。Rootkit[18]主要說明的功能如下：1.隱藏惡意程式，主要為一個或一個以上的程式； Rootkit 主要視為一項主要技術，Rootkit 主要是利用驅動程式載入到作業系統中核心程式的惡意程式。

3.4. 數位鑑識

以現代的電腦科學技術來說，對數位證物[19]的蒐集和分析相當重要，當犯罪事件發生時，對電腦系統或設備尋找相關的犯罪性證物，電腦鑑識簡單來說，針對電腦硬體儲存媒體中，進行犯罪相關證物做修復、備份與分析，例如犯罪者的電腦硬碟損壞，可以嘗試更換磁頭或磁碟片來做修復，找出相關犯罪證據。

3.5. ELK Stack 與相關套件介紹

所謂 ELK Stack[20-22]是基於 Elasticsearch、Logstash、Kibana 三種套件的開頭單字縮寫而成。Elasticsearch 是基於 Lucene 的搜索引擎，能夠全面搜索與碰觸 HTTP Web 界面和無架構 JSON 文件，官方 API Client 有 Java、ASP.NET、PHP、Python、Apache、Groovy、Ruby。Logstash 主要用來管理日誌和相關事件的應用程式，可以利用他收集日誌、轉換日誌、分析日誌，並且可以利用這些資訊進行相關調換或交換的動作，例如：資訊搜尋、資訊儲存等。Kibana 主要是前端日誌的展現框架頁面，Kibana 可以仔細將各種日誌轉換為圖表來查看（創建條形圖、線條、散點圖、餅圖），為 Client 端提供強大的可視化數據。Winlogbeat 是輕量型的採集工具，即時將 Windows 裡事件日誌資料由 Logstash 轉換至 Elasticsearch 儲存。

肆、方法

本文利用 Digital Forensic 及 Docker Container 來建置監控日誌系統。數位鑑識方面以 ELK 系統來做建置，先將 Winlogbeat 安裝在每台測試機上來收集 Windows 系統相關的事件，再回傳到 Elasticsearch 做資料彙整，最後至 Kibana 上做可視化處理，如下圖所示。

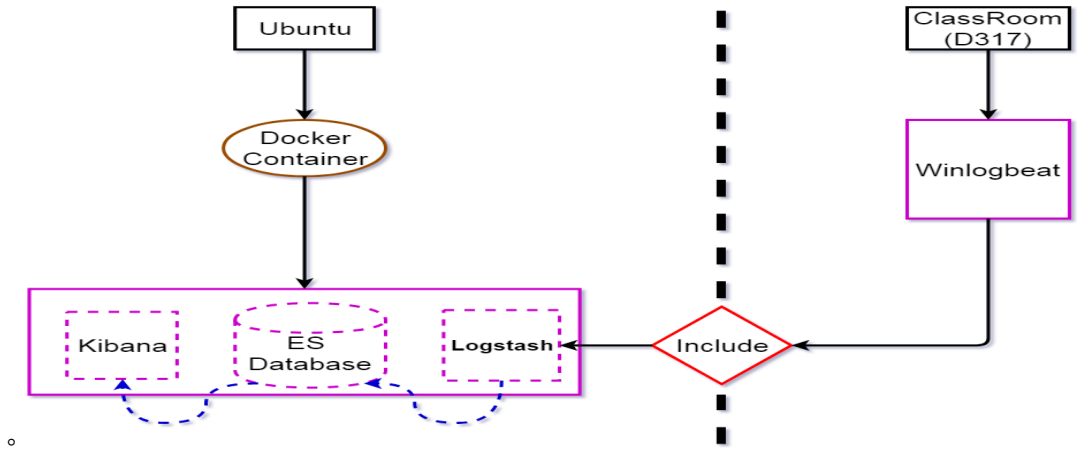

圖 1、ELK 數據採集關係

惡意程式分析方面分為兩項，靜態分析（Static Analysis）及動態分析（Dynamic Analysis），靜態分析方面以 Docker Container 來實做，動態分析分面以 Cuckoo Sandbox 來實做，如下圖所示。

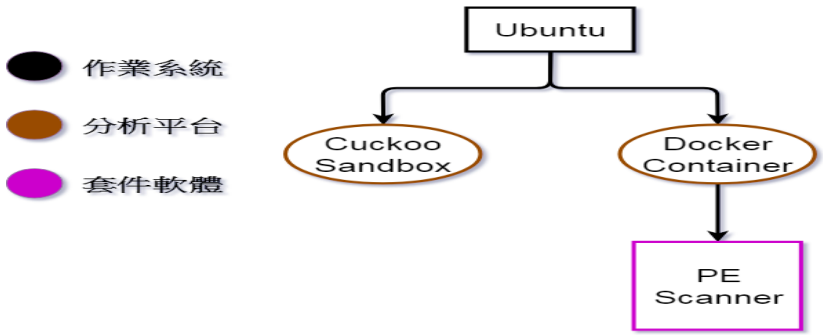

圖 2、惡意程式分析關係圖

環境建置方面我們分為鑑識端跟分析端，在鑑識端完成 ELK 事件追蹤平台的設置，以及 Wimlogbeat 採集端的設定，並在分析端架設 Cuckoo Sandbox 的動態分析沙盒環境及 Docker 容器下的 PEscanner 靜態分析環境。本文系統建置流程如下圖所示。

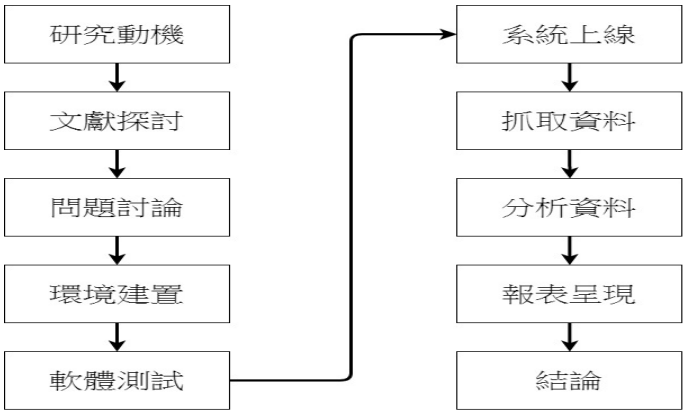

圖 3、流程圖

伍、實驗結果

5.1. 環境建置

Elasticsearch 配置[23-25]以及 Logstash 配置如圖 4 所示。

```
elasticsearch:
  build:
    context: elasticsearch/
    args:
      ELK_VERSION: $ELK_VERSION
  volumes:
    - ./elasticsearch/config/elasticsearch.yml:/usr/share/elasticsearch/config/elasticsearch.yml:ro
  ports:
    - "9200:9200"
    - "9300:9300"
  environment:
    ES_JAVA_OPTS: "-Xmx2g -Xms2g"
  networks:
    - elk
```

圖 4、Elasticsearch 與 Logstash 配置

在 Cuckoo Sandbox 裡的 Virtualbox.conf 檔，我們需要將 Interface 設成虛擬網卡的名稱 Vboxnet0，而 ResultServer_IP 要改成 IP：192.168.99.1。在 Cuckoo Sandbox 裡的 Cuckoo.conf 檔，我們需要將 Label 設成 Cuckoo1，IP 改成自己設定的 192.168.99.101，Snapshot 則是設置成 Snapshot1。

5.2 實驗結果

首先透過鑑識端建置的 ELK 系統與 Winlogbeat 發現可疑檔案，並使用 Cuckoo Sandbox 來分析可疑的檔案，並以報表呈現結果。透過 Kibana 的數據圖來觀察是否有與病毒相關的 Event_ID（事件編號）發生，如圖 5 中的 1116 編號事件即為病毒事件。最後再將報表給的 MD5 碼丟進 Virustotal 網站中來判別是否為病毒，如圖 6 所示。

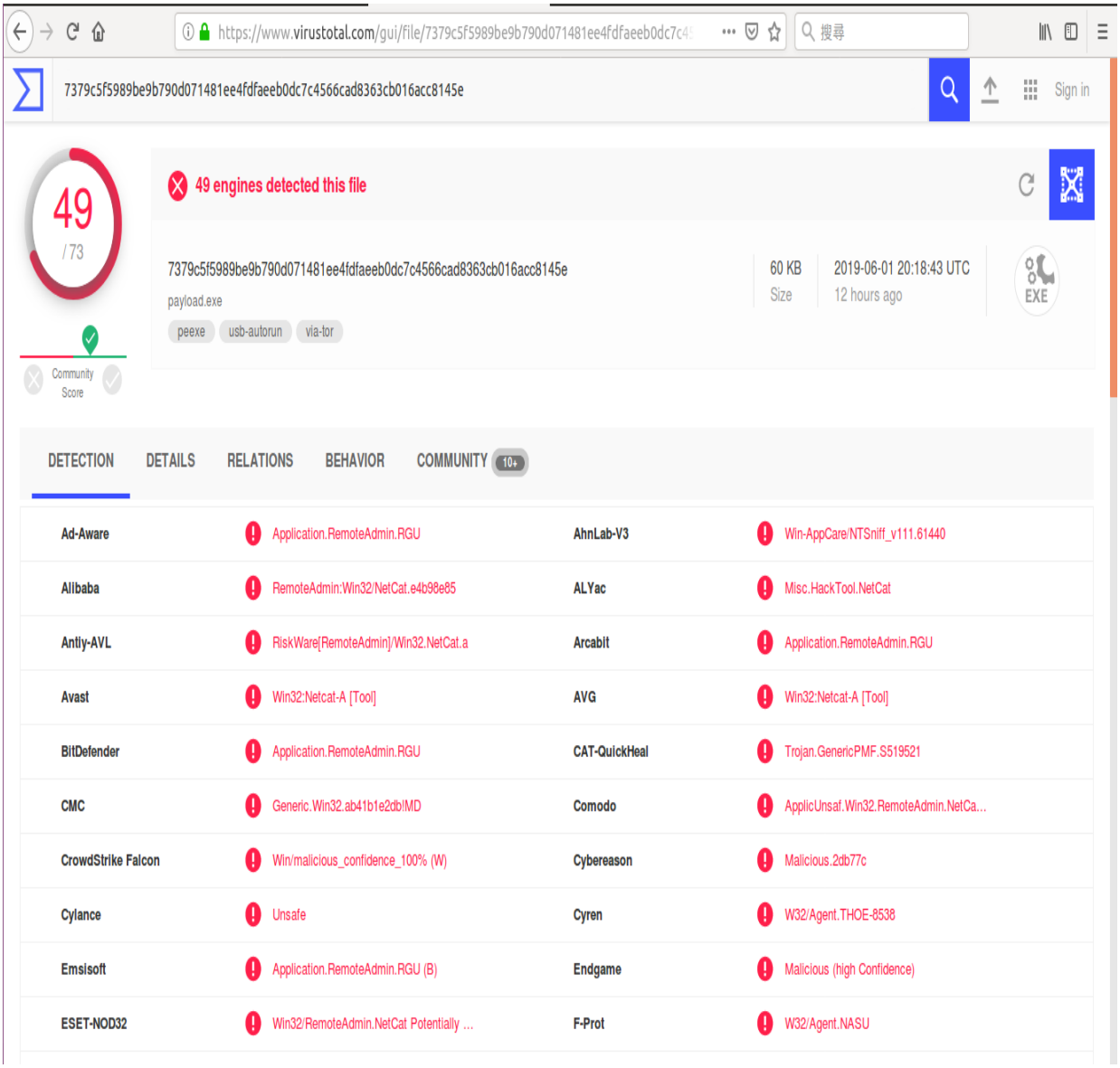

圖 5、Kibana 圖

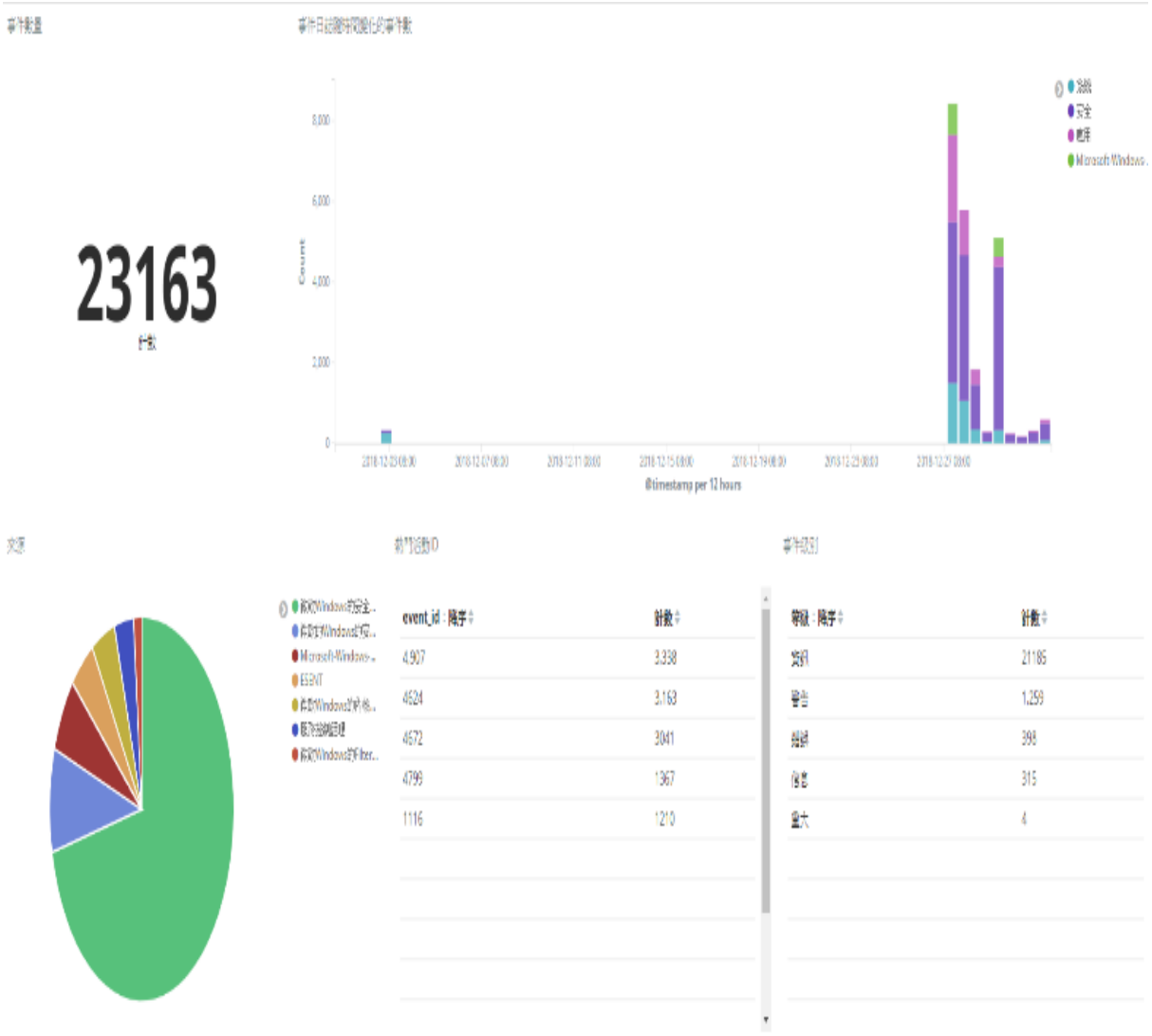

圖 6、動態分析

陸、結論

本文透過 ELK 日誌系統，於本校資工系上電腦監控，抓取惡意程式做分析，並使用 PEscanner 及 Cuckoo Sandbox 做動靜態分析。實作之前，系統資料抓取方式需在每台電腦裝上 Winlogbeat 作傳送，並以 PEscanner 來分析程式。分析過有少數幾個 32 位元檔案無法進行分析，Docker 目前只能在 64 位元電腦上分析，所以 PEscanner 無法分析 32 位元病毒檔，ELK 系統存取容量不足解決方式為，需改系統配置檔、定期手動清除暫存或寫自動化腳本來管理，以便達到整套系統之穩定性；由於 PEscanner 軟體是 Docker Container 支援，以至於用另類程式才能做靜態分析。在未來，因應網路世界的發達，不

管是手機、平板電腦、電腦等都會面臨可能被有心人士執入惡意程式的風險，這時如何抓取資料來做惡意程式分析顯得非常重要。

參考文獻

[1] Borkar, A. Donode and A. Kumari, "*A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS)*", 2017 International Conference on Inventive Computing and Informatics (ICICI), 2017.

[2] J. V. A. Sukumar, I. Pranav, M.M. Neetish and J. Narayanan, "*Network Intrusion Detection Using Improved Genetic k-means Algorithm*", 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2018.

[3] Y. Gong, S. Mabu, C. Chen, Y. Wang and K. Hirasawa, "*Intrusion detection system combining misuse detection and anomaly detection using Genetic Network Programming*", 2009 ICCAS-SICE, 2009.

[4] W. Li, Y. Meng, and L.-F. Kwok, "*Enhancing Trust Evaluation Using Intrusion Sensitivity in Collaborative Intrusion Detection Networks: Feasibility and Challenges*", 2013 Ninth International Conference on Computational Intelligence and Security, 2013.

[5] R. Lupu, R. Badea and I. C. Mihai, "*Agent-based IDMEF alerting infrastructure for distributed intrusion detection and prevention systems: Design and validation*", 2016 International Conference on Communications (COMM), 2016.

[6] Y. K. Penya and P. G. Bringas, "*Experiences on Designing an Integral Intrusion Detection System*", 19th International Conference on Database and Expert Systems Application, 2008.

[7] Warzyński and G. Kołaczek, "*Intrusion detection systems vulnerability on adversarial examples*", 2018 Innovations in Intelligent Systems and Applications (INISTA), 2018.

[8] Ryan Watson（2018 年），*Windows Events Sysmon and Elk...oh my！*（Part1），SilentBreakSecurity 網站，來源：https://silentbreaksecurity.com/windows-events-sysmon-elk/。

[9] Ryan Watson（2018 年），*Windows Events Sysmon and Elk...oh my！*（Part2），SilentBreakSecurity 網站，來源：https://silentbreaksecurity.com/windows-events-sysmon-elk-part-2/。

[10]（美）蘇庫拉・*塞哈特（2016 年），Learning ELK Stack*，電子工業出版社。

[11] *Docker 三大核心概念：鏡像、容器、倉庫*，http://www.aboutyun.com/blog-31226-2831.html。

[12] *Docker 快速入門之原理篇*，https://zhuanlan.zhihu.com/p/31654581。

[13] *James 的資訊安全實驗室--如何自行架設惡意程式分析沙盒（Cuckoo Sandbox）_介紹篇*，http://jameshclai.blogspot.com/2017/03/cuckoo-sandbox.html。

[14] *Rootkkit*，https://zh.wikipedia.org/wiki/Rootkit 。

[15] WarunikaAmali，*Cuckoo Sandbox 安裝指南*，2017 年 7 月 9 日，https://medium.com/@warunikaamali/cuckoo-sandbox-installation-guide-d7a09bd4ee1f。

[16] weiweiwesley（2017 年），*30 天 Docker、ELK Stack 系列*，iT 邦幫忙網站，來源：https://ithelp.ithome.com.tw/users/20103420/ironman/1046。

[17] *木馬（Trojan）*，https://zh.wikipedia.org/wiki/%E7%89%B9%E6%B4%9B%E4%BC%8A%E6%9C%A8%E9%A9%AC_(%E7%94%B5%E8%84%91) 。

[18] *有容雲-原理｜Docker 存儲驅動之 AUFS*， https://kknews.cc/other/nxlqn68.html。(2017-03-17)

[19] 何宗諭，*淺談輕量化的虛擬技術-Docker 容器*，臺灣大學計算機及資訊網路中心程式設計組幹事，http://www.cc.ntu.edu.tw/chinese/epaper/0036/20160321_3611.html。

[20] *後門（Backdoor）*，https://zh.wikipedia.org/wiki/%E8%BB%9F%E9%AB%94%E5%BE%8C%E9%96%80 。

[21] *間諜軟體（Spyware）*，https://zh.wikipedia.org/wiki/%E9%97%B4%E8%B0%8D%E8%BD%AF%E4%BB%B6。

[22] 資安科技研究所/技術研發中心/財團法人資訊工業策進會，*Docker 容器虛擬化資安最佳化實務與應用*，http://tprc.tanet.edu.tw/tpnet2017/training/10611.pdf。

[23] *廣告軟體*，https://zh.wikipedia.org/wiki/%E5%BB%A3%E5%91%8A%E8%BB%9F%E9%AB%94。

[24] 叢培侃（2005 年），*特定領域之整合式搜尋引擎分類系統設計與建置*，中央警察大學，資訊管理研究所碩士班。

[25] 饒琛琳（2017 年），*ELK Stack 權威指南*，電子工業出版社。