國立臺灣師範大學資訊工程學系

113 資訊專題研究（一）期中書面報告

PhishEye：基於審計日誌的釣魚郵件偵測

PhishEye: Leveraging Audit Logs for Phishing Email Detections

指導教授官振傑教授

學生李曜宇撰

中華民國 113 年 10 月

摘要

隨著電子郵件成為企業日常通信的主要工具之一，釣魚信件逐漸成為攻擊者發動網路攻擊的首選手段之一，尤其是在 APT（Advanced Persistent Threat，高階持續性威脅）攻擊中，釣魚信件是其常見的入侵起點。APT 攻擊者通過釣魚信件騙取受害者的信任，讓其打開惡意附件或點擊惡意鏈接，進而獲得進一步入侵系統的權限。本專題旨在通過分析 Audit Log（審計日誌）中的行為，開發一套有效的釣魚信件偵測方法，並實作一個 Proof of Concept（POC）系統，以展示該方法的可行性。本研究不僅專注於偵測釣魚信件，還試圖從日誌中提取潛在的惡意行為模式，為未來的網路攻擊防禦提供參考依據。

1 研究動機

近年來，APT 攻擊在全球範圍內日益猖獗，攻擊目標多為企業、政府機構及高價值組織。APT 攻擊的核心特點在於其長期滲透、隱秘操作與定向攻擊，通常目的是竊取敏感數據或破壞系統的正常運作。APT 攻擊者經常利用釣魚信件作為攻擊的第一步，通過精心設計的社交工程手段，使受害者誤信郵件中的惡意內容，從而無意間為攻擊者開啟了系統後門。

然而，現有的垃圾郵件過濾器和防毒軟體對於這類釣魚信件偵測存在不少局限，尤其是針對日益複雜的攻擊手段，傳統的防禦工具往往無法及時發現。Audit Log 是系統在運行過程中所記錄的詳細操作日誌，其中包括了用戶的登入登出行為、檔案操作、網路請求等多種行為記錄。這些資料為識別異常行為提供了豐富的數據支持。透過對日誌的深入分析，我們可以提前識別出潛在的威脅，並提取出攻擊者入侵後的惡意操作行為，從而有效預防釣魚攻擊的後續損害。

因此，我們的研究希望透過分析 Audit Log，設計一套基於異常行為模式的釣魚信件偵測系統，並實作一個 POC 來驗證該系統的實際效果。此外，透過分析日誌數據，我們期望能提取出攻擊者入侵系統後的惡意行為模式，為企業的網路安全防禦提供有力的支持。

2 研究問題

1. 如何利用 Audit Log 有效偵測釣魚信件，特別是在 APT 攻擊情境中？
    - APT 攻擊者通常在成功發送釣魚信件後進行後續的滲透和操作，如何通過 Audit Log 捕捉這些異常行為，並及時辨識其背後的惡意意圖？
    - 哪些特徵和行為模式可以作為識別釣魚攻擊及其後續操作的關鍵？例如，系統異常的登入行為、敏感資料的異常訪問或下載操作等。
    - 如何設計一套基於 Audit Log 的釣魚信件偵測模型並實作 POC？
2. 如何從 Audit Log 中提取具體的惡意行為？
    - 攻擊者在釣魚信件成功發送後，會進行哪些後續的惡意行為？這些行為可能包括非法的權限提升、敏感資料的未授權訪問、異常的網路請求以及嘗試在系統中安裝惡意程式等。我們如何從日誌中提取出這些行為模式，並通過分析來加強未來的安全防禦？
    - 提取出的惡意行為模式是否能夠轉化為防禦策略，並形成一套自動化的響應系統，以便在偵測到這些行為時迅速採取防禦措施？
3. 該偵測方法及 POC 系統的效能和準確度如何評估？
    - 如何設計實驗來模擬實際的 APT 攻擊情境，並通過真實數據測試 POC 系統的偵測能力？系統是否能夠應對複雜的攻擊行為，並且在真實運行中達到預期的效果？

- 我們應該使用哪些指標來評估該模型的效能？例如，準確率、召回率、F1 分數等評估指標能夠幫助我們理解模型在不同場景中的表現。

3 預期成果

通過本研究，我們期望能夠：

1. 開發一套基於 Audit Log 的釣魚信件偵測方法，並實作一個概念驗證（POC）系統來展示該方法的可行性和效能。
2. 通過分析 Audit Log 提取出具體的惡意行為模式，這些模式將有助於未來構建更加有效的自動化網路安全防禦系統。
3. 提供一套完善的評估方法，通過多次實驗來驗證該偵測模型的效能，並針對不同場景進行調整，以應對不斷變化的網路威脅。

我們的研究最終希望實證一項資訊安全防禦思路，通過分析系統日誌數據，讓我們可以更好地應對包括 APT 攻擊在內的複雜網路威脅，進一步提升針對釣魚攻擊和其他惡意行為的防禦能力。