惡意程式檢測分析

課程簡介

惡意程式 (Malware) 是指一種被設計來對計算機系統、網絡或用戶造成損害、進行非法活動或竊取敏感信息的軟體。惡意程式的目標可能包括但不限於數據竊取、系統破壞、勒索、廣告欺詐、間諜活動等。這些軟體通常是由惡意攻擊者或駭客開發的，以在未經授權的情況下操縱受害者的系統或數據。為了對抗惡意程式，資訊安全專業人員需進行惡意程式**靜態分析**(檔案結構、代碼檢查)和**動態分析**(在運行時觀察行為)，以深入了解其功能、行為和傳播方式。

本課程將介紹惡意程式威脅及惡意程式分析，搭配 MITRE ATT&CK Matrix 框架作為惡意程式分析的基底，讓學員可以從中了解業界撰寫惡意程式分析報告所需符合的架構，以及介紹 x86 組合語言和 Windows 可執行檔、惡意程式分析工具、常見惡意程式行為，並藉由靜態惡意程式分析以及動態惡意程式分析實作練習，使學員熟悉惡意程式分析工具和技術，並能夠有效地應對不斷演變的惡意程式威脅。

***數位發展部於 108 年實施「資通安全管理法」，規範「公務機關」和特定的「非公務機關」之資通安全專職(責)人員、資訊人員訓練要求，本課程完訓後可申請時數認證，惟實際申請仍以國家資通安全研究院查核結果為準，敬請學員踴躍報名。**

課程目標

本課程旨在使學員將深入了解惡意程式的威脅和分析方法，藉由介紹 x86 組合語言和 Windows 可執行檔、惡意程式分析工具、以及靜態和動態惡意程式分析，藉由實作練習使學員將能夠識別和分析

各種惡意程式，理解其行為模式，並掌握應對這些威脅的方法。透過課程使學員能夠熟練運用惡意程式分析工具和技術，提高對惡意程式的辨識和應對能力，以保護系統和數據免受潛在的威脅。

課程大綱

[Note] 每個章節預計有 2~4 個實作

日期	主題	內容
5/ 10(五)	1. 惡意程式威脅及惡意程式分析 Introduction to Malware Threat & Malware Analysis	透過介紹不同的惡意程式樣態以及對應的惡意行為並搭配 MITRE ATT&CK Matrix 框架作為惡意程式分析的基底，讓學員可以從中了解業界撰寫惡意程式分析報告所需符合的架構。
	2. x86 組合語言和可執行檔介紹 Introduction to Disassembling & Portable Executable	了更進一步分析惡意程式，透過介紹 x86 組合語言和 Windows 可執行檔 (Portable Executable) 的構造，學員們可以具備進行深度解析樣本的背景知識。
	3. 惡意程式分析工具介紹 Introduction to Debugging Tools	透過介紹不同的惡意程式中常用的分析工具，可以在不同的情境下，使用最適當的分析技巧，達到事半功倍的效果。
	4. 常見惡意程式行為及惡意程式分析 Common Malware	綜合上述內容，進行完整的惡意程式樣本分析

	Behaviors & Malware Analysis	

課程實作電腦環境配置:

* 硬體： x86 cpu, 8 GB RAM, 500 GB ROM
* 軟體： VMware Workstation or VMware Player

課程對象

1. 程式開發、資訊安全、網路安全、系統管理相關從業人員。
2. 資通安全管理法規範之資通安全專職(責)人員、資訊人員。

講師簡介

陳 講師

現職：社團法人台灣 E 化資安分析管理協會 專任講座

專長：惡意程式分析、逆向工程、滲透測試、漏洞挖掘及利用

課程資訊

1. 課程地點：工研院光復院區 1 館，實際地點以上課通知單為主
2. 課程日期：113 年 5 月 10 日 (五)
3. 課程時間：9:30-16:30 (6 小時)
4. 報名方式：線上報名
5. 聯絡資訊：黃小姐 03-5732961

課程費用

原價：每人**$5,400 元**整

早鳥優惠價：開課前 14 天報名 每人**$ 4,800 元**整

團體報名價：同單位 2 人(含以上) 每人 **$ 4,500 元**整

繳費方式

繳費方式為信用卡、ATM 轉帳，無法受理現場報名和繳費。

ATM 轉帳（線上報名）:

繳費方式選擇「ATM 轉帳」者，系統將給您一組虛擬帳號「銀行代號、轉帳帳號」，此帳號只提供本次課程轉帳使用，各別學員轉帳請使用不同轉帳帳號。轉帳後，寫上您的「公司全銜、課程名稱、姓名、聯絡電話」與「收據」傳真或 E-mail 給黃小姐。

信用卡（線上報名）:

繳費方式選「信用卡」，直到顯示「您已完成報名手續」為止，才確實完成繳費。

銀行匯款(公司或個人電匯付款)：

主辦單位將於確認開班後通知您相關匯款帳號，匯款後，寫上您的「公司全銜、課程名稱、姓名、聯絡電話」與「收據」傳真或 E-mail 黃小姐。

注意事項

1. 為確保您的上課權益，報名後若未收到任何回覆，請來電洽詢方完成報名。
2. 若報名者不克參加者，可指派其他人參加，並於開課前 3 日通知。
3. 因課前教材、講義及餐點之準備，若您不克前來須取消報名，請於開課前 3 日以 E-mail 或電話通知主辦單位聯絡人確認申請退費事宜，學員於開訓前退訓者，將依其申請退還所繳上課費用 90%，另於培訓期間若因個人因素無法繼續參與課程，將依上課未逾總時數 1/3，退還所繳上課費用之 50%，上課逾總時數 1/3，恕不退費。
4. 為尊重講師之智慧財產權益，無法提供課程講義電子檔。

5. 為配合講師時間或臨時突發事件，主辦單位有調整日期或更換講師之權利。
6. 因應中央疫情防疫規定，本場次課程將以「實體舉辦」為主，後續將視中央疫情規定保留調整為「線上辦理」之權利，實際上課資訊請依上課通知為準。