資安事件分析與惡意封包分析

課程目標：

· 訓練IT技術人員，分析惡意程式網路活動。

講師

劉得民

中華民國網路封包分析協會
理事長

時間

114.05.28

09:30-17:30

時間	主題(大綱)	內容
09:00-09:30	報到	
09:30-10:20	現階段惡意程式通訊探討	瞭解目前資安事件、駭客攻擊與惡意程式的來龍去脈，同時說明截至目前(2025年)最常發生的惡意程式網路通訊特徵，與網路封包分析重點。
10:20-10:30	中場休息	
10:30-11:30	網路封包分析的基本技巧	針對目前惡意程式的網路通訊，探討如何顯示(過濾) 網路異常通訊的過濾條件(以Wireshark為例)，並發展歸納出實際可應用的實戰分析技巧(NSPA Skills)。
11:30-12:30	網路封包分析的實際練習	透過實際惡意程式與正常流量的PCAP檔案，讓學員們應用網路異常通訊的過濾條件，並實際練習分析網路封包內容。
12:30-13:30	午餐及交流時間	
13:30-14:20	惡意程式的家族探討	惡意程式的發展，已經不是單純使用防毒軟體或端點防護工具的情況。惡意程式已經發展許多重要派別(家族)並且個自有其程式語言與APT攻擊特徵　　。
14:20-14:30	中場休息	
14:30-16:30	加密勒索攻擊的探討	加密勒索攻擊是目前最嚴重、也是最具破壞性的網路攻擊之一。不論是系統漏洞或是社交工程，攻擊者只要進入企業組織的內部網路，就容易發展出加密勒索。瞭解目前加密勒索攻擊，是所有資安人員的必備專業知識之一。
16:30-17:30	模擬案例的封包範例	針對實際資安案例，在課堂最後使用模擬情境產生的PCAP網路封包檔案，讓學員瞭解更多實戰分析技巧(NSPA Skills)。
17:30-	結束/賦歸	

ACW SOUTH
數位產業署沙崙資安服務基地

數位發展部數位產業署
Administration for Digital Industries, moda