◎資通安全宣導

追蹤網路攻擊一直是資安人員最大的難處，特別是在技術上仍難以突破，因此資安人員開始藉由受害者的類型來做出簡單的區分，期望藉此強化資訊安全。

～網路攻擊的基本分類～

網路間諜（Cyber Espionage, CE）當前資安界大多將涉及國家安全的網路竊盜事件，皆以網路間諜（CE）為分類的代號。對國家級網軍而言，利益並不是其關注的目標，其可以不惜任何成本代價只為了得到具有戰略價值的情報。而其選取的目標也不會是具有商業價值的銀行或是一般公司企業，而是會以政府單位、關鍵基礎設施、軍火公司、重要智庫研究單位為攻擊目標。當然這些單位理論上都會有一定的資訊安全防護措施。因此對網軍而言，會為了竊取情報長期潛伏在上述單位之中，等待適當機會進行網路攻擊。甚至從組織外圍（外包商）進行滲透，只為了最終能夠得到情報。

如 2011 年，美國航太公司洛克希德馬丁（Lockheed Martin）所研製的 F-35 戰機數據資料遭網軍竊取。其攻擊的流程，便是先以洛馬所採用的動態密碼供應商 RSA 為目標，將惡意程式偽裝成 Excel 檔並以人員應徵的名義寄送至 RSA 員工信箱，取得帳號密碼竊取動態密碼的演算法相關資料，攻破最後目標（洛馬）的資安防線，竊取重要的戰機資料。類似的攻擊手法也出現在許多國安相關產業中，如能源產業、航太公司、甚至國防安全的相關學術機構等也都是網路間諜覬覦的目標。網路戰（Cyber-Warfare, CW）有別於國家網軍所發動的間諜行為，國家級網軍從單純的竊取情資，升級成主動對政府或是媒體、企業進行大規模網路攻擊，期望藉此干擾該單位的網路系統。類似的案例並不是首次出現，早從 2007 年俄羅斯對愛沙尼亞發動網路攻擊開始，類似的案例便層出不窮，早期可能只是單純置換官網首頁、更換領導人照片等騷擾行為，其宣示意義大於實際破壞。但隨著人類對於科技的依賴加深，網路攻擊開始透過所謂的分散式阻斷服務攻擊（Distributed Denial of Service attack，以下簡稱 DDoS）攻擊癱瘓目標的網路伺服器，使其失去作用。類似的攻擊手法經常出現於針對某國家政府單位的攻擊，以及一些立場相異的媒體。如 2014 年，對中國態度一向較不友善的蘋果日報，就遭到了國家級網軍有系統的攻擊，並且利用 DNS 反射與散布在各地的殭屍網路，同時發起大量的訊號，嘗試癱瘓該媒體的網路功能。此外，隨著關鍵基礎設施防護觀念的興起，人們對於許多重要設施的依賴程度日益上升，而這些系統也多半利用資訊化管理，因此若是有心人士透過資訊滲透的方式，進入關鍵基礎設施資訊系統中，適當的時機發出錯誤的訊息，或是藉機破壞資訊系統，使其失去效能，其所衍生出來的國安問題不亞於戰爭。如美國與以色列聯手開發的震網病毒（Stuxnet），便是針對伊朗核電廠的電腦系統所特別量身打造的惡意程式。先入侵工程師的家用電腦，再透過可攜帶式電腦裝置，進入機密的電腦系統，藉由干擾控制器的方式，讓核子離心機的轉速過快出現故障，成功地拖延伊朗在核子武器上的研發速度，日後的火焰病毒也有類似的模式。從上述案例中，我們都可以發現國家級網軍的行為，已超脫

過去單純的竊取資訊，其造成的影響已經從虛擬走向現實，透過網路攻擊是可以直接對國家安全造成直接的影響。這也是美國開始將網路攻擊視為戰爭行為的主要原因。

網路犯罪（Cyber Crime, CE）相對於國家級網軍造成的損害，網路犯罪集團雖然不會將關鍵基礎設施列為攻擊目標，但其所衍生的國安問題以及造成的經濟損失，亦隨著資訊科技的進步而日益擴大。對這些網路犯罪集團來說，如何獲取最大的利益會是關鍵，因此在目標選擇上，會以保存大量個資以及金融交易紀錄的組織單位為主，如銀行、戶政事務單位、保險公司、或是經由第三方支付的線上交易平台，都是犯罪機團所覬覦的目標。如美國知名連鎖零售商 Target 便在 2013 年遭到黑帽駭客入侵其 POS 刷卡終端系統，竊取顧客資料、信用卡簽帳卡號碼、到期日與驗證碼，影響一億多名客戶權益，也導致其公司執行長引咎辭職，其公司的商譽也受到嚴重的影響。雖然在各國政府的強力要求之下，許多金融單位都開始使用雙認證或是其他保護措施來加強對消費者的資安保障，但道高一尺、魔高一丈，網路犯罪的技術仍然持續精進，並利用人性的弱點以社交工程做為掩護，令有關單位防不勝防。而近年又出現勒索軟體（Ransomware）將資料加密要求使用者透過線上比特幣支付。近年受害者增加許多，讓勒索軟體都有中文版或是支付教學的說明，甚至出現所謂的早鳥票可以打折，這都代表其所帶來的暴利相當可觀。

網路激進主義（Hacktivism）有別於網路犯罪以及國家組織的網軍，近年來在網路世界中也出現了一群特殊的駭客團體，其所做出的滲透和攻擊與利益並無關係，甚至會為了理念而去對特定政府組織網站進行攻擊，但他們並無受到任何政府的授意，完全是自發性的採取行動。著名的網路駭客激進團體：匿名者（Anonymous）便擁有相當高知名度，其為網路上的一個虛擬組織，只要認同其理念歡迎任何人參與其行動。雖然其最終目的標榜是為了維護網際網路自由，但隨著其名氣與實力增長，其對抗的目標除了權威政府之外（北韓、中國），也在維護正義的名目之下對參與戀童與人口販運有關的網站展開攻擊，甚至直接對 ISIS 恐怖組織宣戰，這都是其近期知名活動。雖然上述行為可能都有違法的嫌疑，匿名者團體認為身為駭客，自然要為其所做的事負責，這些行為雖可能觸法，但絕對經得起道德的考驗。經由以上的探討，可以瞭解雖然使用網路進行的惡意攻擊手法有相同之處，但是背後動機以及組織的型態有相當大的差異。經過追蹤以及攻擊特性的分析之後，經常可以發現，許多的網路攻擊與網軍的關係並不大，反而是企業自身的資安防護的疏失，而讓資訊犯罪者有機可乘。因此，對於名詞的使用與精確的定義是有其必要，且越瞭解自身的威脅才有助增進風險分析並擬定正確的資安策略。

臺中榮民總醫院關心您也提醒您！