5大駭客埋伏 台灣資安法規落

圖：詹千儀、文：詹千儀

駭客可大略分成五種，分別是「強盜、無賴、騙子、間諜和偏激分子」

首先是「強盜」， 現今駭客坐在冷氣房裡搶銀行、盜領ATM，就是典型的強盜手法， 今年二月初，多家券商網路被駭，在劉先覺看來是「無賴」行為。

劉先覺說，券商遭「分散式阻斷服務攻擊（DDOS）」後，對外網頁將被「頻寬滿載」，民眾登入網頁下單時，速度就會變很慢，但劉先覺說，「對方只派兩個人來而已，就把你頻寬占滿了，又不是派五百個人來」，被這種無賴手法攻擊，網頁就掛了，該檢討的其實是自己。

第三是騙子，劉先覺說，跟強盜駭客相反，騙子駭客會「假裝」成你的銀行、保險或信用卡公司，誘騙當事人帳號密碼等資訊，盜領你的資金。

至於「間諜」， 透過駭客竊取對方商業機密，或各國政府利用網軍攻陷敵營都算是 ；最後就是偏激分子，劉先覺舉例，曾有駭客對菸、酒商不滿，攻擊大型菸、酒商的網站，這類偏激分子專找麻煩，但不見得會勒索要錢。

劉先覺曾任全球人壽董事長，近年專攻「金融科技」尤其是保險科技領域。劉先覺說，資安風險是全球金融保險業公認的前五大風險之一，但台灣針對資訊安全法規相對落後、不嚴謹，且規範行業不夠多，各產業也不見得對做好資訊安全有基本認知。

劉先覺以美國為例，若有企業被網攻後，不通報，也不告知客戶，美國檢察官可起訴該企業負責人，因為這很可能會讓客戶處於資訊被曝光或利用的風險，形同違反社會企業責任，還要負法律責任。

圖：http://www.cw.com.tw/article/article.action?id=5082560 文：https://udn.com/news/story/7238/2475210

工業網路安全 6 大漏洞　Moxa 告訴你

Moxa（四零四科技）根據長年深耕工業網路通訊及自動化相關技術及解決方案的觀察，建議廠商在導入物聯網（Internet of Things）轉型至智慧自動化系統建置的過程中，除了關注連網設備功能、效率，及所導入的各項應用整合外，在網路犯罪日益猖獗之際，更要注意網路連網安全。除了雲端防火防禦設定外，也應同時注意系統基礎架構的每一個連接點是否有安全防護機制，建置天羅地網的全面性防護，才能在享受物聯網及自動化所帶來的產製革新之際，降低遭受網路攻擊或威脅的損失。

圖/文:李孟珊

根據 ICS-CERT（國際產業控制系統網路危機應對小組）在 2015 年底公佈的數據指出，網路安全已經高居物聯網趨勢中最大的顧忌。2015 年，全球在製造業有高達 97.33% 的比例通報網路安全事件，幾乎是 2014 年的 2 倍，造成製造業極大的恐慌。

Moxa 也歸納出六大網路安全防禦漏洞，提供系統管理者及專業人員，作為日常網路安全防護的監測依據。

1. 在系統控制中心，忽略有效的監控機制
2. 連網授權設定不完整
3. 重要資料加密疏失
4. 忽略完整記錄所有發生的安全事件
5. 多由人為一一設定與操作，不僅耗時且容易造成失誤機率
6. 不清楚或忽略應該依據資料內容的重要性，設定不同安全等級的防護機制

圖/文提供:http://www.appledaily.com.tw/realtimenews/article/new/20170307/1070821/

惡性軟體

電腦病毒

所謂的電腦病毒是會將本身複製到其他乾淨的檔案或開機區的惡性程式，當電腦使用者在不自覺的情形執行到已受病毒感染的檔案或磁片開機時，這個惡性程式就以相同的方式繼續散播出去，至於電腦病毒是不是都會在某特定日期發作且破壞電腦資料?這就和病毒的寫作者如何設計程式有關，並不屬於電腦病毒的特性。

圖/文:詹千儀/李孟珊

特洛伊木馬程式

特洛伊木馬程式就不像電腦病毒一樣會感染其他檔案，特洛伊木馬程式通常都會以一些特殊管道進入使用者的電腦系統中，然後伺機執行其惡意行為（如格式化磁碟、刪除檔案、竊取密碼等），Back Orifice 特洛伊木馬程式便是一個案例，透過該程式電腦駭客便有機會入侵主機竊取機密資料。

電腦蠕蟲

電腦蠕蟲也不會像特洛伊木馬程式一樣感染其他檔案，但『本尊』會複制出很多『分身』，就像西遊記中的孫悟空一樣，拔幾根毛就可以複制出幾個分身，然後像蠕蟲般在電腦網路中爬行，從一台電腦爬到另外一台電腦，最常用的方法是透過區域網路（LAN）、網際網路（Internet）或是 E-mail 來散佈自己。著名的電腦蠕蟲『VBS_LOVELETTER』就是一個例子。

惡性程式

『電腦病毒』單純指的是『Virus』，而『惡性程式』（Malicious Code）則泛指所有不懷好意的程式碼，包括電腦病毒、特洛伊木馬程式、電腦蠕蟲。

圖:http://www.linjiamm.com/detail/41767/ 文:http://computer.kuas.edu.tw/files/15-1006-