下一場防守大戰　來勢洶洶的 APT 攻擊

量身訂做，高度客製化著稱　資安防護面臨更大挑戰

叡揚資訊 資訊安全事業處

> 今年 3 月 20 號，南韓多家電視台、廣播公司、銀行、保險公司等總計 32,000 台個人電腦感染，購物無法刷卡只能支付現金，ATM 卻無法提款，網路服務供應商中斷網路電信服務，南韓股市大跌，南韓國防部「情報作戰防禦態勢」（INFOCON）等級從 4 級調升到 3 級，整起事件不只是幾家企業受害，而是整個國家都陷入危機。
>
> 根據最近一份針對 ISACA（國際電腦稽核協會）會員的調查，有 21 % 的受訪者表示其企業曾經遭受 APT 攻擊，另有 63 % 的受訪者消極的認為其企業遭受攻擊是遲早的事。

近年全球接連發生多起天搖地動的資安攻擊事件，包括 2010 年初 Google 在極光行動（Operation Aurora）內部員工屢遭攻擊與發生程式碼外洩情事；以及伊朗周遭等國自 2010 年中迄今持續被棘手的超級資訊戰武器 Stuxnet、Duqu，與 Flame 等惡意程式攻擊成功，嚴重動搖核電廠等關鍵基礎建設的運轉與安全，當時更發現惡意程式使用到的數位簽章竟竊自台灣園區廠商；2011 年初動態密碼巨擘 RSA 被一封夾帶惡意程式的社交工程郵件入侵內部網路，並導致部分 SecurID 演算法與關鍵資料外洩。同年，日本三菱重工等三大國防工業廠商也相繼遭到社交工程郵件入侵成功，惡意程式感染數十台電腦；2012 年，台灣多個政府機關傳出大量機密資料遭竊取；2013 年 3 月南韓超過四萬台電腦遭受偽冒防毒軟體的惡意程式入侵破壞，導致多家金融機構業務停擺，歷經一週才全數復原；2013 年初漢光演習馬總統公開呼籲「網路世界是無聲戰爭，極短時間就能癱瘓戰力，對岸網軍 24 小時侵入我方網站，要做好防備工作。」

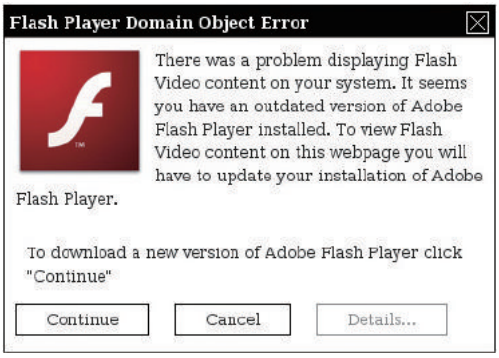
病毒不夠靈活可靠黑名單來防堵，人為操作的 APT 攻擊需靠「情資導向」防護

在過去 20 年，多數的電腦使用者是聞病毒色變，

2010 年 1 月 — Google：
在一起名為「極光行動」的事件中，Google 遭受 APT 攻擊。

當時一位 Google 員工點了即時通訊訊息中的一個連結，接著就連上了一個惡意網站，不知不覺下載了惡意程式，開啟了接下來一連串 APT 事件。

在此事件中，攻擊者成功滲透 Google 伺服器，竊取部分智慧財產以及重要人士帳戶資料。



圖說：「極光行動」常用像這樣的軟體更新下載程式作為誘餌

細數過去造成各地哀鴻遍野的病毒和蠕蟲攻擊包括 CIH 病毒（1998 年）、Melissa 病毒（1999 年）、iloveyou 病毒（2000 年）、Code Red 蠕蟲（2001 年）、Blaster 蠕蟲（2003 年）、Sasser 蠕蟲（2004 年）等等，時至今日黑名單技術已非常成熟，大部分的企業與個人都可相當程度地在網路層的封包和應用層的內容攔阻這些以病毒為主的舊時代資安威脅。

APT 的全名是 Advanced Persistent Threat (一般稱為進階持續性威脅)，此型態的攻擊行動以量身訂做，高度客製化著稱，不似從前的一般惡意程式攻擊缺乏嚴格掌控，APT 會花費較長的時間規劃、執行、偵查、蒐集資料及發掘目標的安全漏洞或弱點。面對這種攻勢，防守方應改變過去「黑名單導向」的資安防護，轉型為「情資導向」的資安防護。美國在 2012 年將網路攻擊納入第五個作戰空間，「武裝衝突法」（Laws of Armed Conflict）同樣適用於網路攻擊，至此資訊戰不再是一場沒有煙硝的戰爭。

南韓 APT 事件敲醒全球資安警鐘：真真假假、假假真真

2013 年 3 月 20 日下午 2 點，南韓陸續發生大量電腦遭強迫重新開機、硬碟嚴重損毀無法繼續運作，此波攻擊事件以 DarkSeoul 惡意程式為首，利用破解防毒軟體主機將偽冒的更新程式派送至大量的端點電腦，此 APT 攻擊事件有四大特色：

1. 玉石俱焚般的破壞行為，破壞重要開機磁區 MBR 覆寫成奇怪字串如 HASTATI，刪除硬碟資料。
2. 以假亂真的防毒更新，並刪除掉感染電腦上原始的合法防毒程式。
3. 定時炸彈設計，惡意程式的潛伏期長，不易觀察。
4. 攻擊方有備而來，感染電腦被植入多個駭客工具，如加密連線和加密傳輸。

面對驚天動地的 APT 攻勢，我們提出以下幾項觀察淺見，期單位更加重視 APT 防護：

1 看見威脅，量化風險，謀定後動 至少電子郵件應部署 APT 攔阻

今天的 APT 攻擊搭載在電子郵件作為主要入侵管道，電子郵件類型的攻擊有高度隱匿性的優點，目前不論是 SIEM 或 Log Management 設備均鮮少將 APT 活動納入監控資料來源，導致單位看不見 APT 風險。

2 了解問題，辨別手法，知彼知己 至少惡意檔案應進行 APT 分析

APT 時代來臨意味著難以保證利用沙箱（sandbox）、蜜罐（honeypot）誘捕惡意樣本，因為長時間下來攻擊方會察覺這些高互動的監控機制，進而加以反制。當然，現有的黑名單類型防護設備仍是必要的，但要贏得 APT 資安攻防的勝利是不足的，防守方務必要持續「隱匿地」收集與分析攻擊方攻勢，在不與之互動的前提下，知彼知己，百戰不殆。

3 掌握現況，定期巡邏，及時因應 至少端點電腦應落實 APT 鑑識

不論已有幾層縱深防禦，或已落實實體隔離，或已部署多套防毒軟體，單位內的所有電腦應視分類分級需求進行定期資安健診，透過定期巡邏掌握資安現況，以及早察覺是否有惡意入侵情事。有別於黑名單檢查 (如防毒軟體)，定期巡邏著重於電腦實際運作的程式行為與網路連線，透過數位鑑識技術發現惡意活動。