趨勢科技 APT Solution 縱深防禦

黃文亮

進階持續性滲透威脅（Advanced Persistent Threat ；APT）是指一種新型態的威脅攻擊，此攻擊行為代表著背後擁有高組織及豐富的應用資源，現階段傳統的安全防禦技術以及次世代防火牆等，把 APT 攻擊當成一般病毒事件處理，單依靠自動化的惡意程式清除工具，只能看到攻擊的冰山一角。所以過度依賴這類工具，只會讓 APT 攻擊行為惡性循環，還是必需要去強化對 APT 的主動監控及縱深防禦，去拉高背景感知能力，且能自動回饋分析並加上事件調查才能有效解決。

一、以多層式縱深防禦架構迎戰 APT

全球接連發生重大資料洩漏事件，揭開了 2014 年的序幕，從美國的零售業者到南韓的信用卡個資，大規模的資料外洩或許肇因於不同禍根，但其中最棘手且可能造成最大損害的首惡，就是有目標針對性的「進階持續性滲透威脅（APT）」。

在趨勢科技發佈的「2013 年台灣 APT 白皮書」裡，就顯示有超過 80% 的受駭組織，不知道自己遭受到 APT 攻擊，從政府單位、高科技產業、金融業和中小企業都包括在內。此外，更有高達 77% 的受駭組織，在發現時已經被駭客取得完全的掌控。但相對的調查指出，僅有 50% 的受害電腦會被找出惡意程式，顯見傳統的資安策略或一般的資安解決方案已經無法依賴。

二、認清敵人：什麼是 APT；

我們所熟知的惡意程式如傳統病毒，會經由大規模散佈及感染來毀損系統，導致電腦無法正常使用，傳統病毒多來自業餘駭客，但因使用者有感且容易取得樣本，風險反而比較低。

另一個常見的惡意程式則是殭屍病毒，源自著眼於控制權的利益導向型駭客，透過控制主機以伺機對外攻擊，由於具備大幅度擴散特性，同樣較容易取得樣本，不過由於會影響組織網路與電腦運作，造成效能的明顯低落，因而風險較高。

相較於惡意程式，APT 更像是一套精心規劃、量身打造的網路攻擊活動，發動者幾乎都是組織型駭客，他們伺機控制主機並竊取帳密，直到取得最高權限後帶走所需資料。由於絕大多數的攻擊都有針對性與持續性，而且是透過正常文件檔案與零時差攻