網軍滲入政府部門 工友電腦也不放過

Google 今年一月遭受到來自中國駭客所發動的「極光行動」攻擊，此類經過長時間的持續監控因而被滲透的目標式攻擊模式，國外稱之為 Advanced Persistent Threat (APT)。在台灣，這類的 APT 攻擊早已不是新鮮事。

在行政院研考會的要求下，各政府機關固定必須每年辦理電子郵件社交工程演練，以提高使用者的警覺。過去，最常遭受到社交工程威脅的是業務單位承辦人，駭客可以針對目標對象的業務承辦性質，精心設計相關內容的郵件，誘騙使用者點擊，然而這個態勢近來已有改變。近期發現就連非重要職務的使用者如技工、工友都成為攻擊目標對象。

由於電子化政府 e 化程度高，所有行政公告都必須透過電子郵件，因此所有職員幾乎都擁有郵件帳號，也因此當一般業務承辦人資安意識漸漸提昇時，駭客便轉向更不被注意到的使用族群身上。值得注意的是，這些端點設備被植入惡意程式可以一直潛伏在 PC 中，直到遠端駭客需要搜集特定情報，才下達指令讓惡意程式運作，系統管理者非常難察覺。目前政府機關資安 A、B 級單位有較多的資安防護資源，可以進行社交工程演練及訓練，然而 C、D 級單位卻相差甚遠，但 C、D 級單位中重要主管所擁有的資料敏感性並不見得比較低。一旦這些受害者攜帶中毒的筆電回中央單位開會，惡意程式就容易被夾帶回去。

為了促進民眾對於政府公共事務的了解，因此推行政府資訊公開，然而站在資訊安全的角度，在看不見的世界裡有一群人有組織地分配、監控單位裡所有人的工作執掌。究竟資訊要公開到什麼程度，值得有關單位深思。

（資料來源：資安人科技網）

臺灣屏東監獄
資訊安全執行小組