社交工程攻擊與擺渡攻擊

社交工程攻擊

社交工程(Social Engineering)是一種攻擊行為，即攻擊者利用人際關係間的互動特性，所進行的攻擊法。社交工程攻擊是以影響力或說服力來欺騙他人，藉以獲得有利入侵的資訊，這是近來造成企業或個人極大威脅和損失的駭客攻擊手法。駭客利用社交工程假冒為同事、新進員工、廠商、客戶、政府單位等寄發E-mail，再將病毒與惡意程式隱藏在E-mail中，有系統地實施針對性精準攻擊。當受攻擊目標開啓駭客寄來之E-mail或點選E-mail中的超連結，就可能下載病毒或惡意程式；通常駭客利用電子郵件的社交工程攻擊成功率約80%。

擺渡攻擊（隨身碟攻擊）

目前政府機關防範駭客入侵的主要方法即是採用實體隔離，這種機制是將內部工作網與網際網路隔離，嚴防機密資料外洩；當內、外網電腦間有資料需交換時，再以行動碟(或拇指碟)為媒介傳遞資料。然而目前駭客已運用擺渡攻擊，破解實體隔離的防護機制。駭客擺渡攻擊的方法，是由連結網路的電腦將autorun.inf與ghost.pif(惡魔程式)等擺渡木馬程式植入行動碟中，待行動碟與內部工作網進行資料交換時，擺渡木馬程式立刻感染內網電腦，再將欲竊取的資料下載至行動碟中。完成上述擺渡程序後，只要使用者再將行動碟連接網際網路電腦，被竊取的資料就會自動傳送給駭客。