

形兵之極，至于無形
善用匿蹤技術之虛實優勢

層出不窮的攻擊事件

最近國內某大型電子業遭駭客入侵，偷走大客戶產品設計藍圖等重要商業機密資料，並要求大額加密貨幣的贖金，若沒收到贖金，駭客將公開其取得的機密資料。當然，這次事件對該電子業者而言，除了影響代工新產品開發及電子業者之信譽受損外，電子業者可能會因未善盡營業秘密保護責任，而遭到客戶求償，甚至調整訂單而影響未來營收。

面對處心積慮探測網路最薄弱環節之「看不見的敵人」，維護資訊的完整性，有效的保護管理重要數據和資訊已成當務之急。

尤其是應用程式和伺服器中可能含有未修補的漏洞，極容易成為駭客的入侵點，將勒索病毒植入系統。如Exchange Server、Database Server等，一旦發現漏洞或公布漏洞，就等同跟時間賽跑，未迅速修補漏洞的伺服器，便高度暴露於駭客入侵的風險之中。

不論企業網路建置多少安全防護，久未更新的軟體等於是為駭客敞開大門。無論使用何種防護工具，最終目的都是要保護企業或政府機構的重要數據和資訊，面對「看不見的敵人」——駭客，敵暗我明的態勢，除了內部宣導資安智能、建立早期預警系統、即時回報可疑攻擊外，該如何運用有利戰術，達成實質防護之效呢？

借鏡孫子兵法虛實篇

說到戰術，所聯想到的是實質作戰的策略及技術，隨著各國軍事競賽的白熱化，研發出「匿蹤技術」運用在軍事用途上，指以特殊設計、表面材質或裝置，直接運用於戰車、戰機、艦船等，降低其被偵測到的機會或縮短其可被偵測距離的科技。透過這個技術提高戰略或戰術目標的達成率，及戰場存活率。

在此引用孫子兵法虛實篇，其中一段「故形兵之極，至於無形；無形，則深間不能窺，智者不能謀。」。深意的解釋：善於進攻者，能做到使敵方不知道在哪防守，不知道怎樣防守。而善於防守者，使敵人不知道從哪進攻，不知怎樣進攻。見不到一點形跡，不漏出一點消息，所以能成為敵人命運的主宰。

將這個理論套用在現今資安防禦技術上，有異曲同工之妙。無論企業或政府機構都希望在資安戰場上，擁有最新最高端的防護，以保障重要的數據或資料的隱密性及安全性。所以，資安上的「匿蹤技術」。簡言之，將保護的數據或資料設定為「保護區」，讓「看不見的敵人」——駭客，「看不到」、「隱形」重要東西的位置，延緩勒索軟體引爆的時間，爭取更多時間找到阻斷攻擊的方法，希望能使損害控制至最低風險。

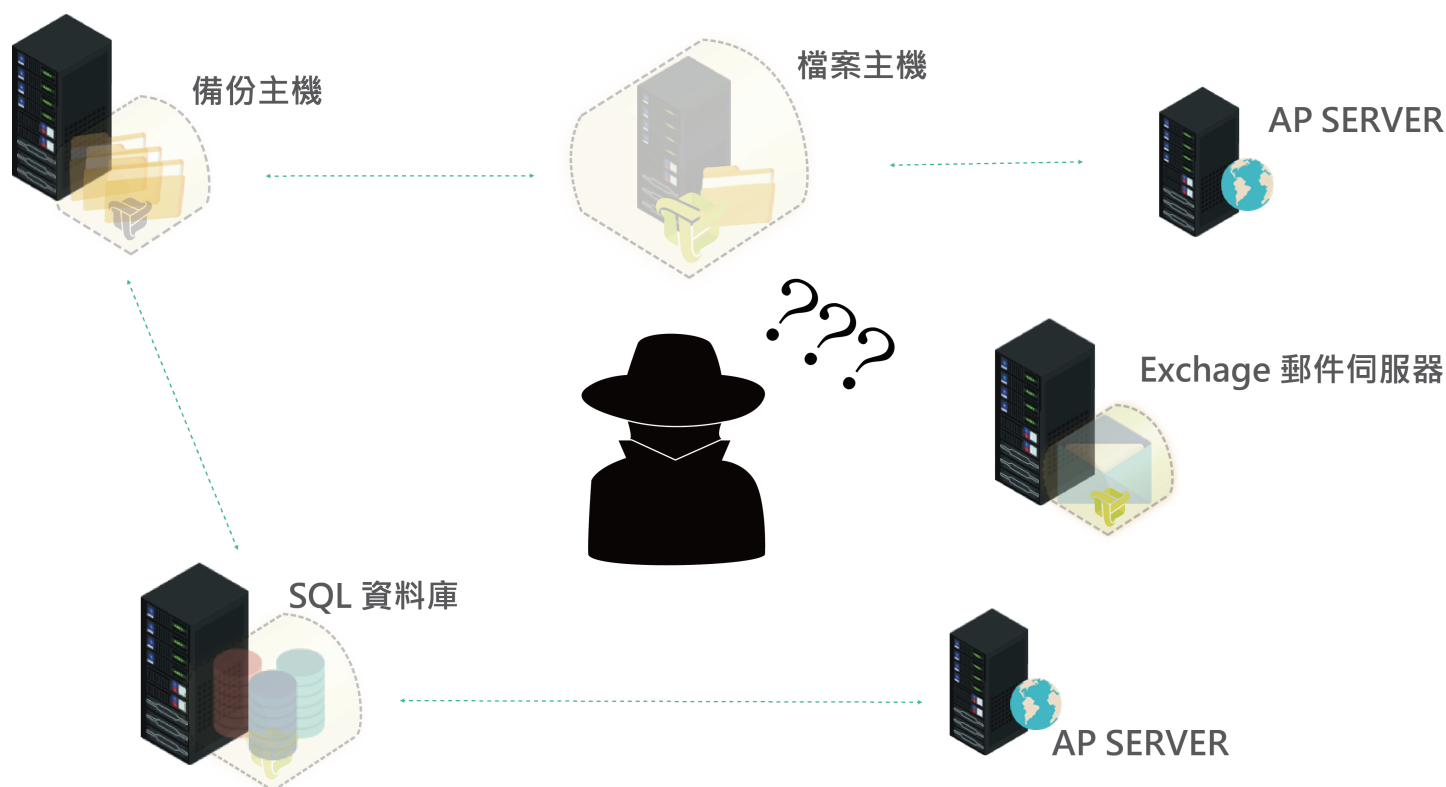
在技術上，可以視為存取管理（ACL）的進階版，除了身分認證與權限之外，匿蹤防禦更增加了程序、網路存取、可見與隱匿等控制。

綜上，重點有三：

1. 以主動的方式製造出「彼虛我實」的態勢，而不是以等對方出錯的應對之法，須懂得製造出利於取勝的態勢。
2. 「制人不制於人」，使敵人照著我們想要他行動的方式而行動，並間接削弱敵人在對戰間實力使其虛弱，才能真正取得勝利。
3. 敵人雖了解我方可能使用的招式和作為，但無法正確揣摩我方的心思和想法，也就無法得知我方真正的目的，只能被動的應付。

攻守易位—轉化優勢

套用虛實篇的重點，做為「匿蹤技術」之戰術理論。將企業或政府機構所要保護的重要數據和資訊的所在之處，隱匿無蹤，使網路犯罪者「看不到、隱形」檔案或路徑，以主動的防衛將原本駭客潛藏入侵的優勢易位，轉化為我方隱藏區域的優勢；萬一勒索病毒成功侵入並發生破壞行為時，已設定為「匿蹤保護區」的資料，亦可避免遭受攻擊具自我防護功能，勒索駭客無法直接寫入或刪除，「制人不制於人」，使其知難而退。



企業或政府機構的重要數據，不外乎以下幾類：

- 檔案伺服器
- 郵件伺服器
- 資料庫
- 網站應用系統

若這些重要數據多加運用「匿蹤技術」使勒索駭客無法於短時間內取得重要的數據或資訊，延緩勒索軟體引爆的時間，便能爭取到充足的應變時間，掌握主控權並降低損失。