# 防駭尖兵-資料匿蹤的資安思維

網路犯罪組織將勒索軟體結合 APT 發展為新的犯罪模式，鎖定目標企業直接攻擊，致使許多知名企業相繼受害，犯罪組織除以加密檔案做為勒索條件外，更威脅公布所竊得之企業資料，以要求索取更高額贖金。

隨著雲端服務、 AI 技術、物聯網等新興科技的迅速發展，經專業機構統計，有 2 成左右的企業每年遭遇超過 50 次以上的資安事件，換算起來幾乎是每一周發生一次。意味著企業存在許多資安問題，讓犯罪組織駭客能夠入侵網路，並在企業網內遊走，找到企業的關鍵系統或資料進行勒索。因此企業主及資安工作者必須確實認知「**網路可能會遭受入侵**」的事實。

各種防駭、防盜措施，也無法百分百保證抵擋的住攻擊。如 2020 年 9 月發生某知名軟體公司之伺服器遭駭客攻擊刪除 6.5TB 用戶資料。其主要起因是一台未設置控制認證程序的設備，在遭受直接攻擊後，致使伺服器受到重大災害。

## 匿蹤防禦新思維

資安防禦技術及方法型態很多，各有各的優點和用途，大多是阻擋駭客的入侵，以及抓到惡意軟體為主要目的，但是仍然災害頻傳。換個角度，假設駭客已經入侵的情境下，一個新的防禦概念「匿蹤」，可以作為加強資料防禦的新技術。

在許多電影中，「隱形」是常用的經典梗，例如：電影「哈利波特」中的隱形斗篷，是最讓人驚豔的魔法聖物。而「隱形」，顧名思義就是「看不到」，這項科技現今主要是應用在軍事用途上，最知名的為隱形飛機（stealth aircraft），透過低可偵測性技術使飛機不被雷達所偵測，而具有此類技術幾乎屬軍事戰機，所以常被稱為「匿蹤戰機」。

根據「匿蹤戰機」的概念，資安的「匿蹤」技術，也可以用在抵禦駭客的攻擊。於驅動層做主要的控制，讓一般系統上的執行程序「看不到」受保護的

伺服器路徑及檔案，這些受保護的區域便稱為「匿蹤保護區」。使用者須透過信任程序的認證，例如：持有憑證簽章，以憑證的認證程序，確認是合法的及可信任的，使用者才能看到伺服器路徑及檔案。保護的效果等同於實體隔離的安全效果，卻不需要大費周章的做實體隔離，因此也稱為「虛擬隔離」。

本文的前段曾提醒企業主及資安工作者，確實認知「**網路一定會遭受入侵**」的事實。這就表示，無論安裝多少防毒軟體、做員工行為分析、防駭監控技術等，都不可能百分之百完全防範。更何況駭客犯罪集團的技術，翻新速度變快，願意為錢鋌而走險的網路駭客更不在少數。我們應該運用怎麼樣的方法，使災害降到最低？

「匿蹤」技術可運用於現今所面對的勒索駭客問題上，只要讓駭客「看不到」伺服器檔案或路徑，讓駭客誤以為已經全面加密資料，實際上重要資料仍然完好如初，讓企業快速恢復資料與設備；或者讓駭客一直找不到重要資料，花費更多時間，進而為企業內其它的防毒防駭工具爭取更多時間偵查，找到入侵來源，降低企業的損失。

## 保險箱的自我防護概念


再與大家分享保管的觀點，我們日常生活中，常有些重要文件或重要物件，卻沒有一個妥當的放置地點，例如：房屋地契、金銀首飾等，這些東西很重要但平常卻用不到，可是放在家裡可能發生需要時找不到，或被偷走直接奉送給小偷兒，免不了咒罵和覺得倒楣！

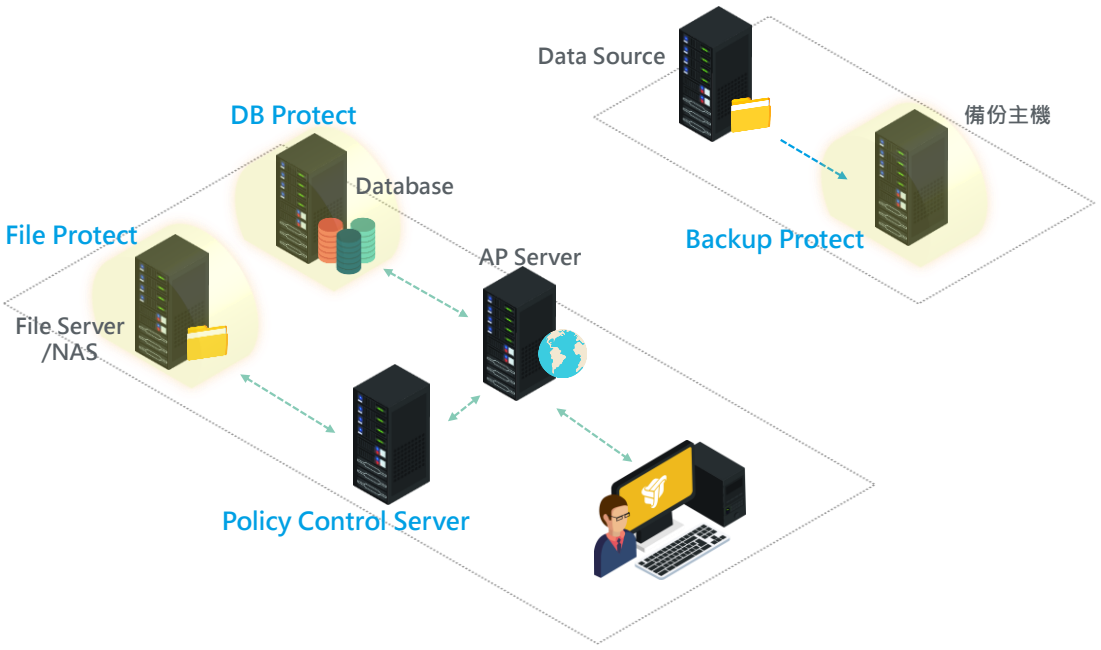
所以，銀行發展出「保管箱」的業務，提供人們具有安全性及保障性的放置地點。一般人到銀行，如未經身份認證是無法輕易進入保管箱的存放區域，而且要打開保管箱須由租用人及銀行端的 2 把鑰匙，同時開鎖才能打開，達到兼具保存、保管和安全的功能。

把「銀行保管箱」的概念套用到「匿蹤」技術中，將每台伺服器設定為一個保管箱，亦稱為「匿蹤保護區」。當伺服器被設定為「匿蹤保護區」的模式時，任何人在網域中都無法看到其蹤跡，也就降低被使用或被侵入的機會。在保障安全的考量下，惟有具權限的使用者，透過安全認證的程序，輸入「開箱的鑰匙」，經系統認證核實後，才能取得「看到」的權利。

當企業中任一個使用者設備，因瀏覽網站或執行惡意程式而中毒，在裝設「匿蹤保護區」後，所影響的層面也只是這台設備的檔案資料，不會損毀後端內部網路所存放重要資料，且資料也不會有外洩的風險。但事情不可能都是十拿九穩，萬一勒索病毒已成功侵入及進行破壞時，此時已設定為「匿蹤保護區」的資料起直接防護的作用，避免遭受攻擊，且具自我防護功能，防止程式及安裝的檔案被刪除，使勒索軟體及駭客無法直接寫入。

## 伺服器的應用情境

企業為保障及管理自家的資料，常會於內部部署許多的伺服器。包含如：公司資料庫、網站、郵件、備份硬碟、備份備援主機等。接下來，說明企業所部署伺服器的類型及潛在危機。



1. **資料庫伺服器：**

存放著企業許多營運系統資料庫，常透過像是防火牆之類的設定，來限制連線至資料庫，伺服器的來源位址做管制。

對犯罪組織的有心人士來說，可能因為一些系統錯誤資訊中曝露所在主機的連線位址、登入帳號、及密碼，而取得發動攻擊時十分有用的資訊，成為勒索軟體攻擊主要目標，一旦將資料庫檔案鎖定加密後，什麼系統也無法運作，且企業為了能盡快恢復功能及避免資料外洩，一定會妥協支付贖金。

只要將資料庫檔案設定為「匿蹤保護區」，上述情況發生，資料並未損毀，可以快速恢復資料庫伺服器的運作。

2. **檔案備份伺服器：**

企業擔心發生被勒索或系統損壞等情況，為了可以盡快恢復系統，又做了資料備份的動作，而有了備份伺服器。但只要在同一網域內，還是有可能成為勒索軟體的攻擊目標。所以，企業又要將檔案備份伺服器另外切割為另一網域，無形中加重許多作業程序及備份的風險而不自知。

另一個問題，通常只有在意外發生後，才開始與復原步驟進行第一次接觸，所遇到的問題是：回復原資料時間過久、復原程序過於繁瑣，且資料只能回復至備份時間開始的地方。對企業而言，復原複雜程序、資料重建和復原時間的壓力，都使工作更為困難，可能導致損失擴大的原因。

同樣地，將備份伺服器設定為「匿蹤保護區」，也可以避免上述的資料損毀與復原的複雜流程。

3. **網頁應用程式**

以往企業較專注於維護網路免受外界攻擊(如建置防火牆)，如今網頁應用程式安全已成為企業重視的核心議題。企業內部的主要營作業常仰賴程式開發人員開發提供，過程中如能投注部分心力，注意相關檢核事項，減少程

式本身的漏洞，再搭配入侵偵測系統及防火牆等所建構的防禦機制，可提高系統整體的安全性。 但資訊安全，除了知己知彼，瞭解攻擊者的意向，更應使用最有效的方法，建構強化型對應的防禦措施。

將應用程式存取的資料，無論是檔案存取或者資料庫存取，都可以「匿蹤」技術保護應用程式處理的重要資料。

## 結論

企業部署了重要的伺服器，主要就是為能存放重要的核心資料，所以，關於「匿蹤」技術的應用重點說明如下：

1. 「匿蹤」特性：主要是「看不到」，勒索軟體及 APT 攻擊無法找到被「匿蹤」的檔案。例如：竊賊知道這個家很有錢，想方設法要去偷盜，但實際卻只看到一些零頭，卻不知道貴重財務藏在那裡，那竊賊可能就拿走看到或放棄。
2. 隱形保管箱：將伺服器站台設定為「匿蹤保護區」，設定後就看不到的 除非有特殊鑰匙才會看到其中的資料庫、檔案存放位置即為隔離區。
3. 安全程序：只准許擁有通行權限的使用者，經過安全檢核程序後，才能存取檔案伺服器或 NAS 站台的資料。
4. 隔離防刪寫：已設定為「匿蹤保護區」的資料起直接防護的作用，除了避免遭受攻擊外，還具自我防護功能，防止程式及安裝的檔案被刪除。
5. 降低災害：使用「匿蹤」防護技術後，受到保護的伺服器及檔案未受到損失，縮短企業回復系統運作時間，降低災害損失。

總歸來說，企業不得不選擇各種防禦技術，否則等於是坐以待斃。必須假設沒有任何一個解決方法是百分之百完整保護，理想的策略是運用有利的技術為企業爭取反制時間，降低風險減少損失。