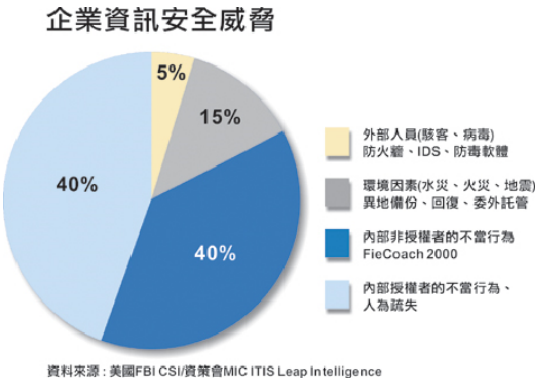
漫談內網資安管理（一）

天下武功，無堅不摧，唯快不破

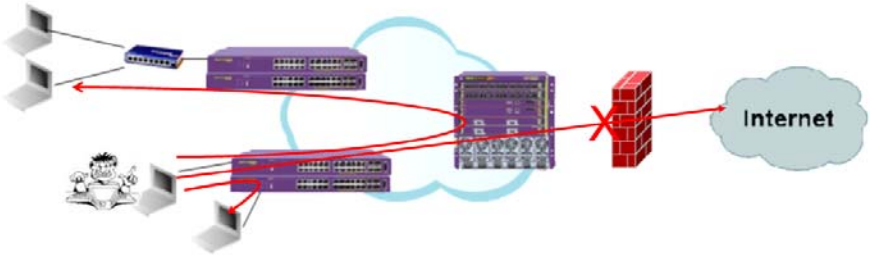
<文字取自電影[功夫]對白>

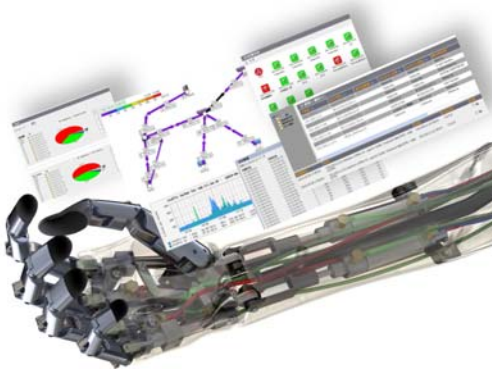
作者：葉華裔
任職：捷宇網安股份有限公司
E-Mail：santayeh@netaxle.com.tw

隨著網路應用的發達與普及，企業 e 化的環境與應用也更加的廣泛與成熟，網路已是各企業最重要的基礎建設與營運溝通命脈。 在複雜的網路環境中，大多數企業已建置防火牆等相關網路安全系統，其重點爲防禦外部使用者的攻擊，然而對於內部使用者的行爲則較少著墨。但是傳統的資安思維在近幾年中已有所改變， 因爲依據統計調查資料，企業資安事件只有 5%是來自外面的攻擊，而有 80%是由內部產生(註一)，因此新型網安系統的行銷重點慢慢趨向於如何防禦與監控內部使用者的上網行爲，並從而了解是否有攻擊或非法行爲隱藏其中。(註一：另外 15%資安事件是由天然災害等事由產生。)



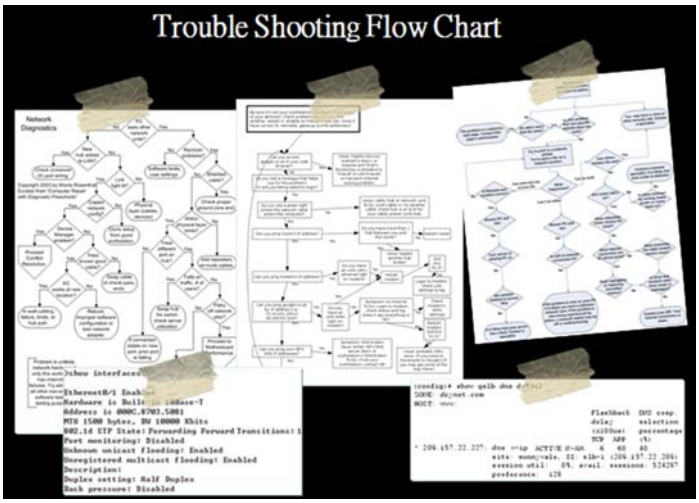
若企業憂慮的只是內部使用者是否上了不該上的網站，倒還有部份解決辦法，透過如 Palo Alto、M86，Blue Coat 等設備，即可做到很好的管理(註二)。然而若內部使用者的異常行爲不是存取 Internet 上的資源，而是攻擊企業內部的設備或其他內部使用者，現階段幾乎所有的網路佈建方式都無法阻擋，此時網路管理人員唯一能做的就是持續觀察網路相關設備與線路，收集不同的網路事件與告警，視其是否異常來判別是否可能有問題發生，例如觀察主機、路由器、交換器的 CPU 與記憶體的使用率與線路流量，察看 IPS、IDS、



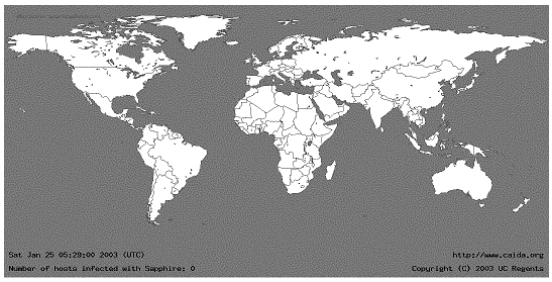


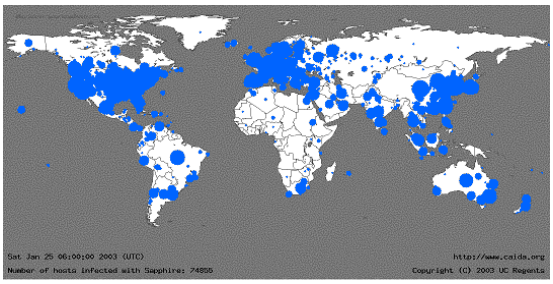
Firewall、VirusWall、Secure Gateway 等設備的告警事件。然而在開放的網路架構下，企業內部充斥著許多不同廠牌與不同類型的網路設備，使得網管人員每天需要操作各種的網管與監控軟體、審視數萬封各種的告警。然而即便網管人員努力地堅守崗位，還是常常在接到使用者反應後才知道問題發生了，因爲太多未經關聯整理過的資訊等於沒有資訊，網管人員也不可能全天候都坐在電腦前持續操作監看各種網管與監控軟體，所以網路管理人員若想確實做好網路安全的管理工作並不容易！(註二：但是現今 3G 上網普及，可能因此產生控管漏洞)

當問題發生時才是網管人員的挑戰開始。每種設備的告警訊息格式不相同，操作指令也各不相同，因此如何從網管軟體或告警訊息中找出有問題的“點”就考驗網管人員的功力了，尤其在解決問題的時間壓力下，容易使人亂了手腳；最常看到的情況是一網管人員桌前都有一堆流程或小抄，將每種可能的問題 SOP 寫下，若遇到較複雜的問題可能就需要同時整合 4~5 種流程來研判問題並加以解決。

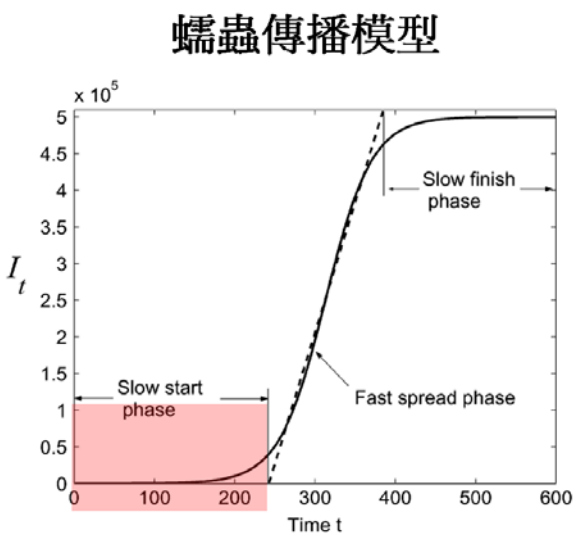


然而解決問題的時間壓力有時不僅僅是來自於公司或上級長官而是問題本身。我們以 Slammer 蠕蟲爲例，其在短短 30 分鐘內在全世界感染了 74855 台電腦，因此若類似狀況在企業內部發生，假設某種攻擊或感染的擴散情形是每 10 分鐘會由一個人擴散至十個人，那 30 分鐘後，受感染的人數將達 10 ^ 3 = 1000 人！到此狀況下對許多的管理人員而言，大概也不用太心急的去處理問題了，先將整個網路停擺以避免持續惡化擴大，再慢慢將正常與修復好的節點連回網路可能是較好的做法。





既然攻擊或蠕蟲傳播等的擴散速度如此之快，是否就真的束手無策？是否有較好的防禦方式？答案當然是有的。其實大部份的攻擊都有一個特性，在攻擊準備期間由於需確定那些是攻擊目標，因此攻擊或蠕蟲會先做些掃瞄偵測的動作，此期間是不會攻擊感染其他使用者的，但當準備動作完成後，其攻擊感染的速度就非常驚人。我們以蠕蟲傳播模型爲例，在啓始準備階段其攻擊力爲零，這階段的期間到底多長依不同蠕蟲或攻擊而有所不同，大多在 150 到 300 秒之間，所以這 3 到 5 分鐘的時間就是決勝關鍵了。



周星馳的電影《功夫》中，火雲邪神曾說過“天下武功，無堅不摧，唯快不破。”同樣適用在網路攻防之中。攻擊或蠕蟲的傳播速度非常快，確實很難破解防禦，唯一能破解防禦的方式就是比攻擊或蠕蟲更快，若能在蠕蟲或攻擊 3 到 5 分鐘的啓始階段就將其偵測出來並進而將其排除隔離出網路，就能確保網路與設關設備安全無虞。

因此防禦的第一步就是建立早期的偵測預警機制，否則等到終端使用者打電話通知網路出現問題時，大都已到攻擊或蠕蟲第二階段末尾了。爲何早期的偵測預警機制能偵測到攻擊或蠕蟲？如之前所說，攻擊或蠕蟲需先掃瞄網路以確定攻擊或感染目標，因此這些特定的掃瞄封包有可能會散佈到各個網段之中，透由 IDS、IPS、Flow Analyzer、Secure Gateway 等就有可能偵測到，但就算偵測到又能怎麼辦？以 email 或 syslog 通知網管人員？網管人員會隨時待到電腦旁接收訊息？就算看到訊息，其通知格式可能只是告知某一 IP 可能有某種攻擊行爲，網管人員還要再依據此 IP 再找到所接相關設備再決定是否需要使用 ACL 阻隔或將交換器埠直接關閉？所以單純只是依靠人力是不可能達成 3 到 5 分鐘隔離攻擊者這個目標的。唯有依靠系統自動化功能，從收集訊息到關聯分析以確定攻擊來源(可能是一個 IP 或 MAC 地址)，並自動下指令將攻擊來源隔離，才有可能實現。

然而原理簡單，但實做上卻面臨許多困難。訊息數百種，如何做關聯分析以確定攻擊來源是第一個挑戰；知道攻擊來源，是否需將其隔離是第二個挑戰；就算要隔離，如何將其隔離是第三個挑戰；如何讓管理人員清楚了解相關狀況是第四個挑戰！

我們以隔離方式爲例，現行隔離機制可使用 IP ACL、MAC ACL、Switch Port Shutdown、Quarantine VLAN、ARP Spoofing、IP Spoofing 等，而攻擊方式百百種，不同的攻擊方式適用的隔離方式不同，因此系統支援那些隔離方式，如何判斷該使用何種隔離方式就非常重要。

NetAxle 公司推出的 JetFish2 系列中的 NetIRS 設備就是一款全功能型的資安管理設備，可收集 syslog 與 trap 做關聯分析，其隔離機制支援 IP ACL、MAC ACL、Switch Port Shutdown、Quarantine VLAN、ARP Spoofing、IP Spoofing 等並可自動判斷以對攻擊來源採取最佳隔離機制。(註三：相關隔離機制需相對應的設備也支援相關功能。)

網管人員其實更關心的是第四個挑戰，如何將無形的網路與資安相關狀況清楚呈現出來。傳統網管提供了部份功能，但只能針對網路設備。NetIRS 將此功能更進一步擴充，使用全圖形資訊化方式將所有關鍵資訊利用網頁方式呈現。很難想像，網路安全管理居然就是移移滑鼠，點點左右鍵就完成了。更特別的是，由於是全網頁式的管理平台，使用 iPhone、iPad 也可隨時隨地輕鬆控管！