資訊安全概念

成大計網中心
楊峻榮
2004/5/20

本校常見之資安事件

- 病毒或worm
- DoS or DDoS（阻絕服務）
- 入侵(被當跳板較多，成為目地較少)
- 匿名信件或廣告信
- 誹謗事件

* 依事件處理統計約有90%未裝設防毒軟體或未更新病毒碼及未修補Patch，10%為權限設定或管理不當。

資訊安全弱點

- 系統漏洞
- 人為疏失
- 因服務需要或過於注重便利性
- 無危機意識（事前預防）
- 無所謂（事發之處理及心態）
- 無專人負責之系統

Windows系統應用漏洞

- 未裝設防毒軟體或病毒碼未更新。
- 系統或應用程之漏洞未修補(Windows Update & office Update) 。
- 系統或應用軟體組態設定不良(ex: IE之安全性設定)。
- 瀏覽不當網頁及Download不當軟體。
- 帳號權限設定不良(未設密碼或不明之帳號與不當之權限) 。
- 檔案分享未設限。
- 接收不當之郵件。
- 上次遭入侵所建之後門未阻絕。

傳統病毒Life-cycle

- 管道：一切可接觸感染源的方式與途徑
- 感染：確定經由管道感染病毒
- 病發：待病發條件成立時，將形成破壞
- 擴散：向外擴散
- 防堵：阻絕再次感染之途徑
- 清除：清除已存在之病毒
- 偵測：持續偵測預防病毒再次感染

入侵Life_cycle

- 針對系統或人為漏洞入侵
- 植入後門程式
- 進行破壞(當跳板，竊取資料，服務阻斷)
- 修補漏洞
- 清除後門程式或病毒
- 持續監控

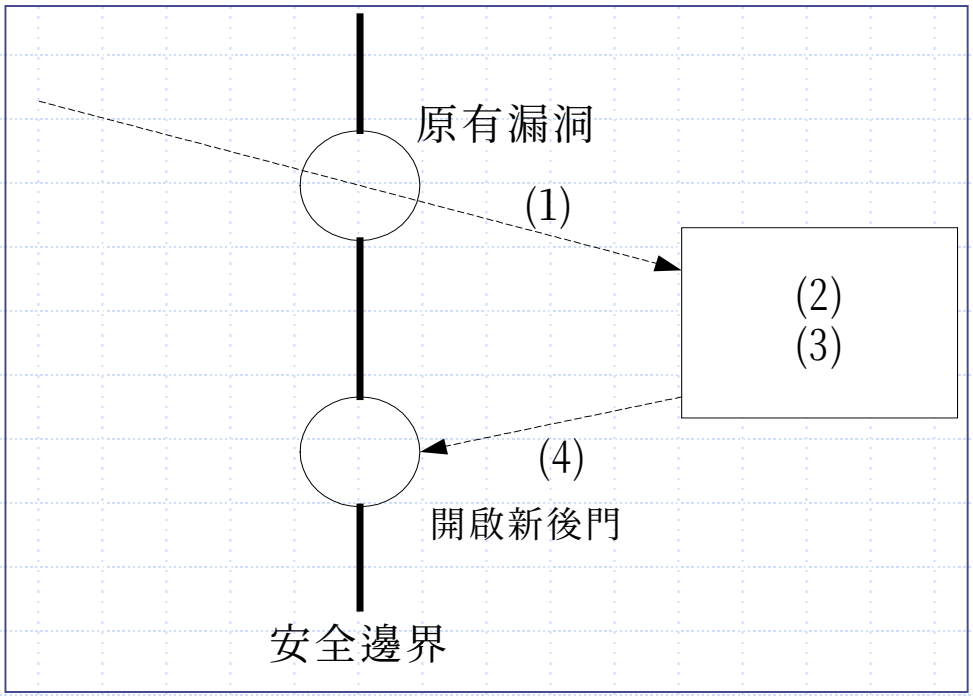
入侵之定義

- 凡舉非系統所有人所願之對於主機(PC)存取資料，植入程式或資料，程式與組態更改。
- 造成運作失常或系統失效，資料毀損或業務中斷或資料外洩資料之行為。
- 一般之存取或試探活動大都以網路從事，但以非網路活動之存取及試探活動也屬入侵行為（例如由主控台登入）。

入侵型態

- 固定模式：以病毒或worm方式，其入侵及破壞與所植入之檔案（檔名或擺放位置也許有異）皆是固定行為模式，故大部份可由防毒軟體偵測出來(已裝有該入侵行為之病毒碼)
- 人為模式：入侵之目的主要為非法行為，如資料竊取，破壞，或當成其他入侵之跳板，其入侵之模式不定，故較難偵測。入侵試探手法可能固定（ex 利用即有之系統漏洞），但入侵後所擺放之後門程式是可變的。

入侵或病毒之程序



(1)經由原有漏洞入侵或感染

(2)建立檔案或修改組態

(3)破壞及向外感染或攻擊

(4)開啟新漏洞或後門

- 病毒或入侵清除措施可解決(2),(3)及部份(4) 。
- 必須清除或阻絕原有漏洞。

疑似中毒或遭入侵之徵兆

- 系統反應速度變慢。
- 系統重新開機或不正常關機。
- 出現不正常之提示或視窗或網頁。
- 軟體或程式無傳輸資料卻有大量網路傳輸。
- 工作列有非預期之啟動圖示。

中毒怎麼辦?

- 更新病毒碼。
- 使其為離線狀態，如拔除網路線或將網卡Disable。
- 重新啟動電腦至安全模式或 VGA 模式。
- 掃描和刪除受感染檔案。
- 額外之手動程序，例如編輯登錄表。
- 裝上網路線，啟動防火牆，重新啟動電腦後執行 Windows Update(假設是因為系統漏洞感染)。或是在離線狀態以Patch光碟進行系統漏洞修補。
- 再次手動掃瞄病毒。
- 持續監視一段時間。

防毒軟體處理程序

- 偵測
  由pattern比對是否為Virus
  記錄檔案所在位置供處理階段參考
- 阻擋
  阻止病毒資料寫入磁碟機
- 處理
  依設定決定對於此檔案清除，刪除或隔離

防毒軟體即時掃瞄之訊息判斷

- 在處理階段偵測到病毒並知道它要寫入那個位置。
- 因被阻擋所以病毒並未寫入。
- 在處理階段防毒軟體要去刪該檔，因該檔被阻檔未寫入，故無法清除或刪除。
- 須確定該檔案確實不存在。
- 及若一直發生考慮阻擋該port或停止該service。
- 以上概念不適用手動掃瞄，也就是以手動掃瞄偵測到病毒，幾乎可斷定為中毒。

收到Mail Server發出之病毒訊息

- 由mail server發出偵測到您發出病毒信之訊息。
- 確定是否有發出該信件並再手動檢查是否已中毒。
- 目前病毒信會依PC內之通訊錄假造送件者或收件者之email_address 。
- 故第三者有您之email_address，若他已已中毒，您很有可能收到該病毒訊息。
- 若同時（一段時間內）收到同樣之訊息，很可能是已經中毒。

個人資訊安全概念總結(實務)

- 裝設防毒軟體，可能的話另裝設個人防火牆，連線監視及弱點評估軟體。
- 裝設防毒軟體並不代表不會中毒,裝設防火牆或入侵偵測系統也不代表就不可能被入侵。
- 將Windows update及病毒碼更新當成例行性工作。
- 重裝OS是高成本的解決方式，且並非最根本的解決方式，很可能會引發新的問題（忘記或不易補Patch)。
- 瀏覽器設中高安全性，瀏覽不當之網頁前請三思。
- 收信軟體取消〔信件預覽〕，來路不明之信件附件檔不予開啟。
- 設定不易破解之密碼，刪除不必要之帳號及權限。
- 重要資料須有備份機制 。
- 不要開啟無法確定的Service(範圍,程度)。
- 對於協力廠商，要有一套管制及因應措施。
- 對於系統必須有一套預防、事件處理及善後處理的措施。

個人資訊安全概念(觀念)

- 資訊安全，人人有責。使用者需付成本。
- 在網際網站之世界裡，除了保護自己的系統，也要不影響別人的系統。
- 看不見問題，並不代表沒有問題。
- 安全的措施愈多，其安全係數愈高，但應以合理成本及不增加系統負載為考量。
- 了解自己系統的安全邊界，並方施以充分的控制指施。
- 資訊安全是一個持續性的工作，而其防護措施也沒有極限。防護措施可能會因時間因素而失能，故須時常更新。
- 資訊安全領域不只是網路安全而已（駭客，病毒）。
- 安全措施及設備非萬能，也沒有100%安全的系統。
- 便利性和安全性總是相衝突的，實施的控制措施應該是在合理的平衡點。
- 充分了解安全機制之功能及其邊界。