尼克森微電子股份有限公司

資訊安全

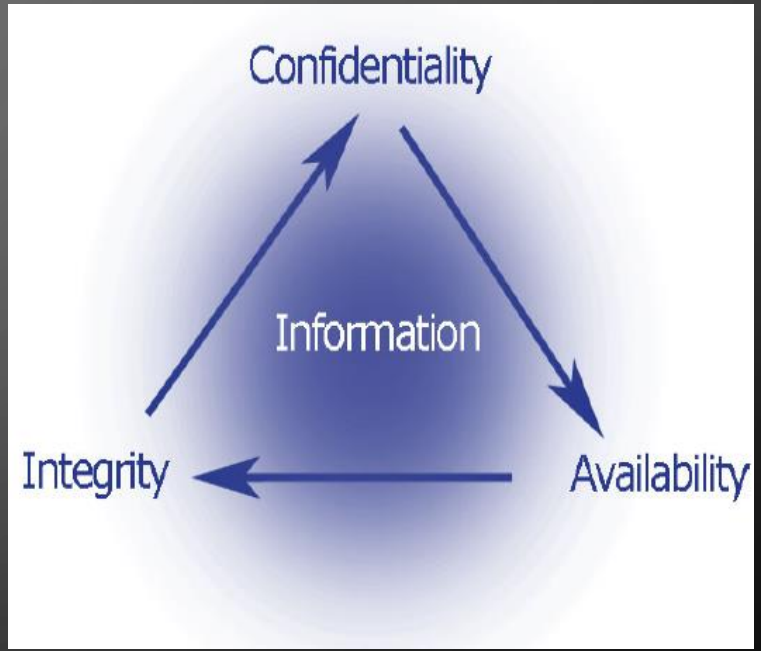
2022/10/03

何謂資訊安全

- “資訊對組織而言就是一種資產，和其它重要的營運資產一樣有價值，因此需要持續給予妥善保護。資訊安全可保護資訊不受各種威脅，確保持續營運，將營運損失降到最低，得到最豐厚的投資報酬率和商機。”
- — BS 7799：1995 / ISO 27001：2005資訊安全管理系統(Information Security Management System)標準定義

資訊安全三要素

- Confidentiality 機密性
  - ➢保護資訊不被非法存取或揭露
- Integrity完整性
  - ➢確保資訊在任何階段沒有不適當的修改或損毀
- Availability 可用性
  - ➢經授權的使用者能適時的存取所需資訊



常見資訊安全事件

設備故障/弱點

不當的使用
(人為疏失)

偷竊

病毒/惡意軟體

未經授權的存取

資訊安全的重要

- 資訊安全含括了網路安全、系統安全、資料庫安全、數位簽章、加/解密技術、電腦病毒和身份識別等不同層面的問題，隨著電腦技術之提昇及網路之發達，這些已經與我們的生活密不可分，才使資訊安全問題日漸引起重視與注意。
- 有些人誤解為電腦不連結網路或內部網路和外界網路不連結(實體隔離)就沒有資訊安全的問題；事實不然，從許多電腦犯罪的案例來看，人才是最大的關鍵。

資訊安全的威脅 (1/2)


安全威脅
人為因素
非人為因素
人員疏失
蓄意性威脅
員工操作失當
外來駭客
內部員工
水災，火災
地震，颱風
系統無法運作
需多種型態的偵測與防禦工具
管理制度的修正及持續的宣導

資訊安全的威脅 (2/2)

資訊安全威脅類型			可能發生事件	範例
非人為因素	天然災害		●火災、水災、地震、雷擊、冰雹等	納莉颱風
	基礎設施故障		●軟體程式、硬體、網路通訊障礙	硬碟壞軌
人為因素	人員疏失		●操作、維護及管理等疏失	電腦用畢未登出
	蓄意性威脅	資料破壞	●電腦系統破壞 ●資訊設備破壞 ●資料程式破壞 ●資料/程式竄改或毀損	病毒破壞
		資料濫用	●擅自使用電腦設備 ●不當使用資料或資訊服務 ●透過社交手法獲得使用權限或資訊	駭客入侵
		違反隱私權	●不當之資料收集、使用或公開	犯罪者竊取他人信用卡資訊

人為因素為最主要的威脅來源

網路帶來的安全威脅

線上活動	可能的安全威脅
• 電子郵件 • 即時通訊	➢ 電腦病毒 / 特洛伊木馬 / 網路蠕蟲 ➢ 網路釣魚 ➢ 垃圾郵件
• 線上購物 • 線上理財 • 下載音樂/影片/軟體 • 線上遊戲 • 在部落格發表文章 • 瀏覽網頁 • 網路相簿	➢ 電腦病毒 / 特洛伊木馬 / 網路蠕蟲 ➢ 間諜軟體 / 廣告軟體 ➢ 網路釣魚

名詞解釋-駭客(Hacker)

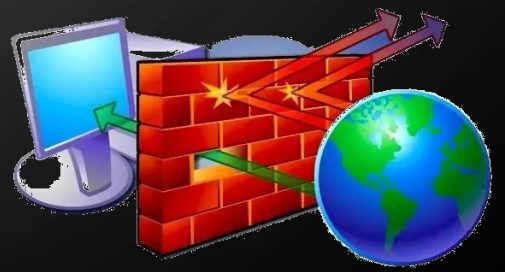
- 駭客(Hacker)
  - 技術高超的程式設計師
  - 白帽駭客（White Hat）、灰帽駭客（Grey Hat）、黑帽駭客（Black Hat），該名稱取自美國電影西部片中，正派往往戴白帽，反派往往戴黑帽。
- 劊客(Cracker)
  - 一個惡意（一般是非法地）試圖破解某個程式、系統或網路，進而竊盜、毀損或使其癱瘓的人。
- 腳本小子(Script Kiddie)
  - 腳本小子是利用他人所撰寫的程式發起攻擊的網路鬧事者。

名詞解釋-駭客(Hacker)

	白帽駭客	灰帽駭客	黑帽駭客（劊客）	腳本小子
技術	有			無
目的	改善	昭告	利慾	
屬性	狹義上的駭客（建設者）		電腦犯罪分子（破壞者）	

名詞解釋-防火牆(Firewall)

- 防火牆是能夠監控傳入和傳出網路流量的網路資安裝置，並依據一組已定義的資安規則來決定允許或封鎖特定流量。
  - 用戶端防火牆：用戶端防火牆是一種位於電腦上的軟體，可監控電腦上的所有網路流量。
  - 設備防火牆：設備防火牆是一種硬體裝置，連接網際網路與您的電腦。



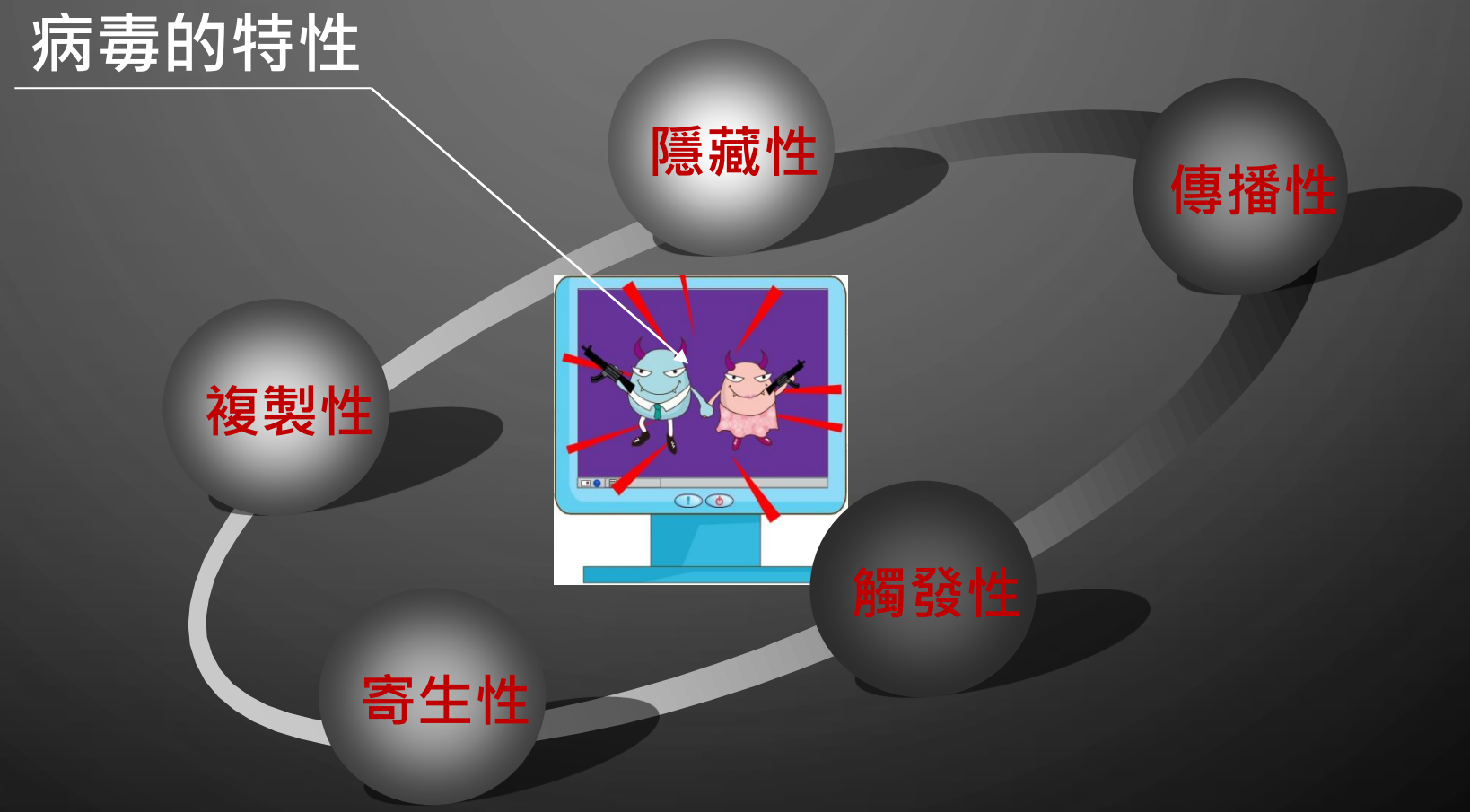
名詞解釋-防毒軟體(Antivirus Software)

- 使用於偵測、移除電腦病毒、電腦蠕蟲、和特洛伊木馬程式。防毒軟體通常含有即時程式監控辨識、惡意程式掃描和清除和自動更新病毒資料庫等功能，有的防毒軟體附加損害恢復等功能，是電腦防禦系統(包含防毒軟體，防火牆，特洛伊木馬程式和其他惡意軟體的防護及刪除程式，入侵防禦系統等)的重要組成。

認識電腦病毒(Virus)

- 電腦病毒是一種附掛在其他可執行程式的程式碼，在未經「正當」的允許下，進入電腦系統中，從事干擾電腦系統正常運作、在電腦螢幕上顯現訊息、或是損毀電腦系統中的電子資料等進行干擾性、破壞性、或惡作劇的行為，通常具備自我隱藏、複製與再生、變種等基本人工智慧。
- 在執行附加病毒的程式之後，病毒碼就會執行預設的動作，這些動作包含將自己散播到其他程式或磁碟之中；某些病毒更惡毒，不但會刪除檔案還可能造成電腦毀損。但某些病毒除了將自己散播到其他系統之外，並不會執行任何惡意的動作。

病毒的特性 (1/3)



病毒的特性 (2/3)

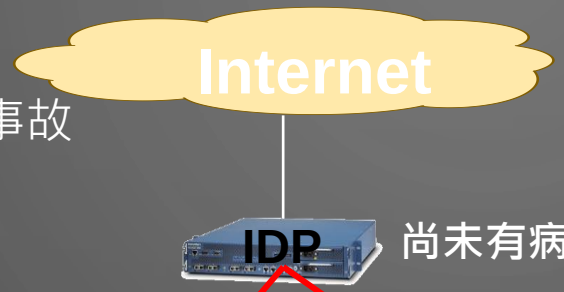
- 複製性
  - 當使用者存取到含有病毒的檔案時，病毒就會試圖將含有病毒的檔案，複製到電腦系統中。
- 傳播性
  - 病毒會透過各種管道(移動式儲存媒體、P2P、FTP、檔案分享等)來傳播，感染更多的電腦或系統。
- 隱藏性
  - 為了不讓使用者(防毒軟體)發現，以便順利傳播感染更多的電腦，因此會隱藏而不易察覺。

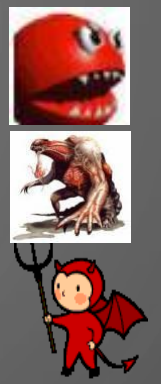
病毒的特性 (3/3)

- 寄生性
  - 病毒無法單獨存在，必須依附在其他檔案或程式中，當然也會跟著許多隨身裝置(USB、記憶卡等)到處亂竄。
- 觸發性
  - 有些病毒會依據某些特殊的狀況或是條件而啟動，像是特定的日期等。

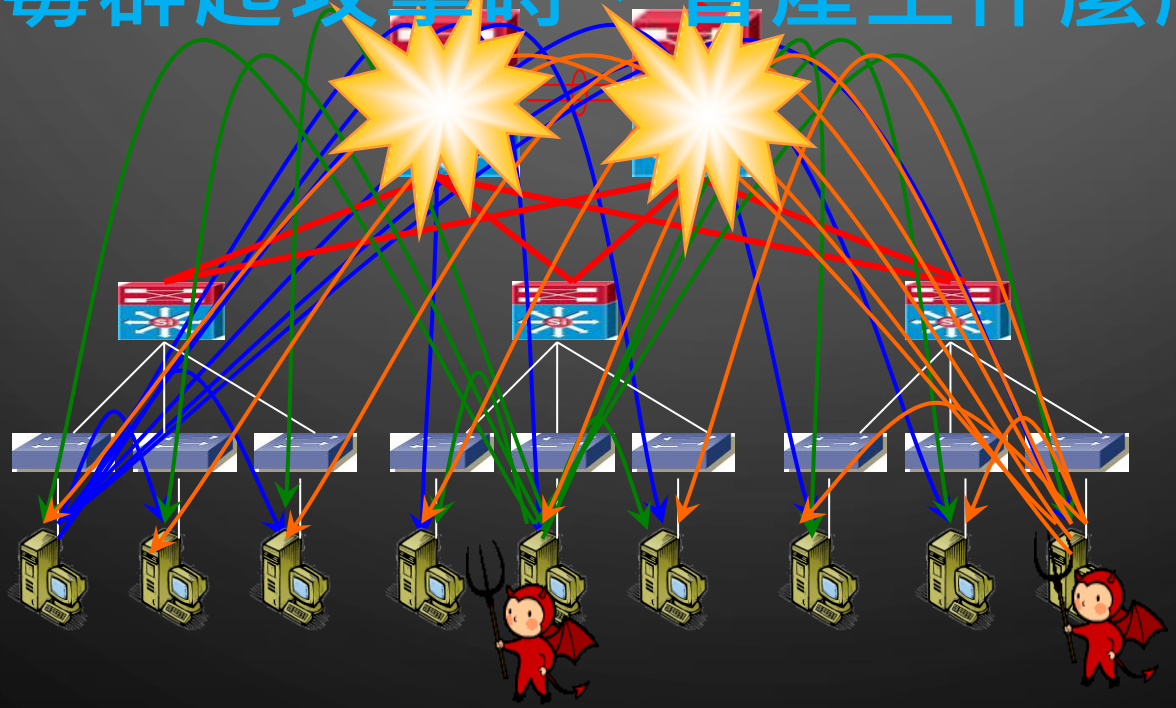
病毒擴散

70% 以上的網路資安事故
來自於內部的攻擊





當病毒群起攻擊時，會產生什麼狀況



名詞解釋-病毒碼(Virus Pattern)

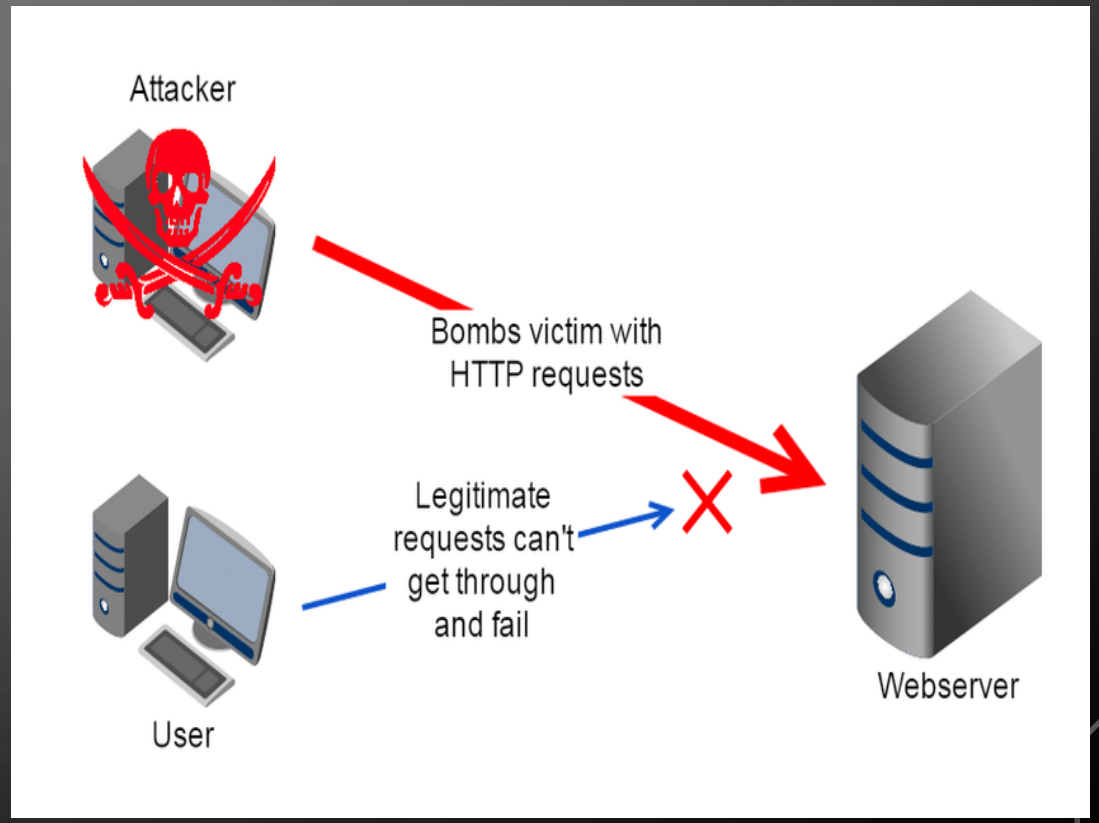
- 病毒碼像是犯人的指紋，當防毒軟體學校收集到一隻新的病毒時，他們會從這個病毒程式中截取一小段獨一無二的程式碼，就是所謂的「病毒碼」。防毒軟體就是靠掃描引擎，比對病毒碼，找出病毒，因為新病毒隨時都在產生，所以必須定時更新病毒碼，才能防範新病毒。

名詞解釋-弱點或漏洞

- 任何軟體或作業系統，在發表一段時間後，被發現設計上的瑕疵，這瑕疵容易被病毒入侵，讓攻擊者控制受害者的電腦，進行破壞任務。軟體設計者在發現瑕疵後，均會提出修護程式，讓使用者下載更新，這是要求Windows Update的理由。

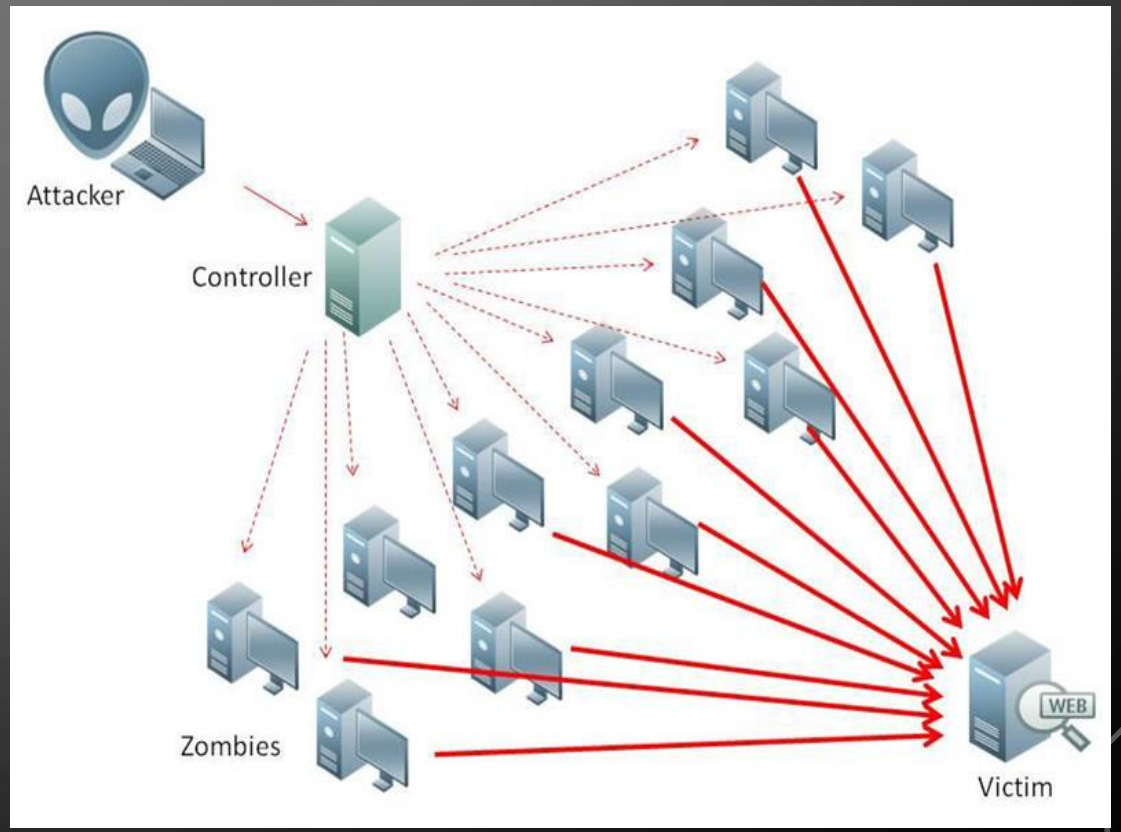
阻斷服務攻擊

- **阻斷服務攻擊**（英語：denial-of-service attack，簡稱**DoS攻擊**），是一種網路攻擊手法，其目的在於使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致其正常使用者無法存取。



阻斷服務攻擊

- 當駭客使用網路上兩個或以上被攻陷的電腦作為「殭屍」向特定的目標發動「阻斷服務」式攻擊時，稱為**分散式阻斷服務攻擊**（distributed denial-of-service attack，簡稱**DDoS攻擊**）亦稱**洪水攻擊**。



殭屍網路(BotNet)

- 殭屍網路（Botnet，亦譯為喪屍網路、機器人網路）是指駭客利用自己編寫的分散式阻斷服務攻擊程式將數萬個淪陷的機器，即駭客常說的傀儡機或「肉雞」（肉機），組織成一個個命令與控制節點，用來傳送偽造包或者是垃圾封包，使預定攻擊目標癱瘓並「阻斷服務」。通常蠕蟲病毒也可以被利用組成殭屍網路。殭屍網路可專門用來完成非法或惡意工作，包括傳送垃圾郵件、竊取資料、勒索軟體、以欺騙性手段點擊廣告或分散式阻斷服務 (DDoS) 攻擊。

阻斷服務攻擊分類

- 基礎設施層攻擊
  - Layer 3 和 4 的攻擊通常歸類為基礎設施層攻擊。這也是最常見的 DDoS 攻擊類型，包括同步 (SYN) 泛洪等攻擊途徑，以及使用者資料包封包 (UDP) 泛洪等其他反射攻擊。這些攻擊通常數量龐大，且旨在使網路或應用程式伺服器的容量超載。幸運的是，這類攻擊類型都具有清晰的簽章，因此很容易偵測。
- 應用程式層攻擊
  - Layer 6 和 7 的攻擊通常歸類為應用程式層攻擊。雖然這些攻擊較不常見，但卻更為複雜。這些攻擊與基礎設施層攻擊相比數量通常較少，但是傾向針對應用程式特定的重要部份進行攻擊，使實際使用者無法使用應用程式。例如，對登入頁面或重要搜尋 API 進行 HTTP 請求泛洪，或甚至是 Wordpress XML RPC 泛洪 (也稱為 Wordpress pingback 攻擊)。

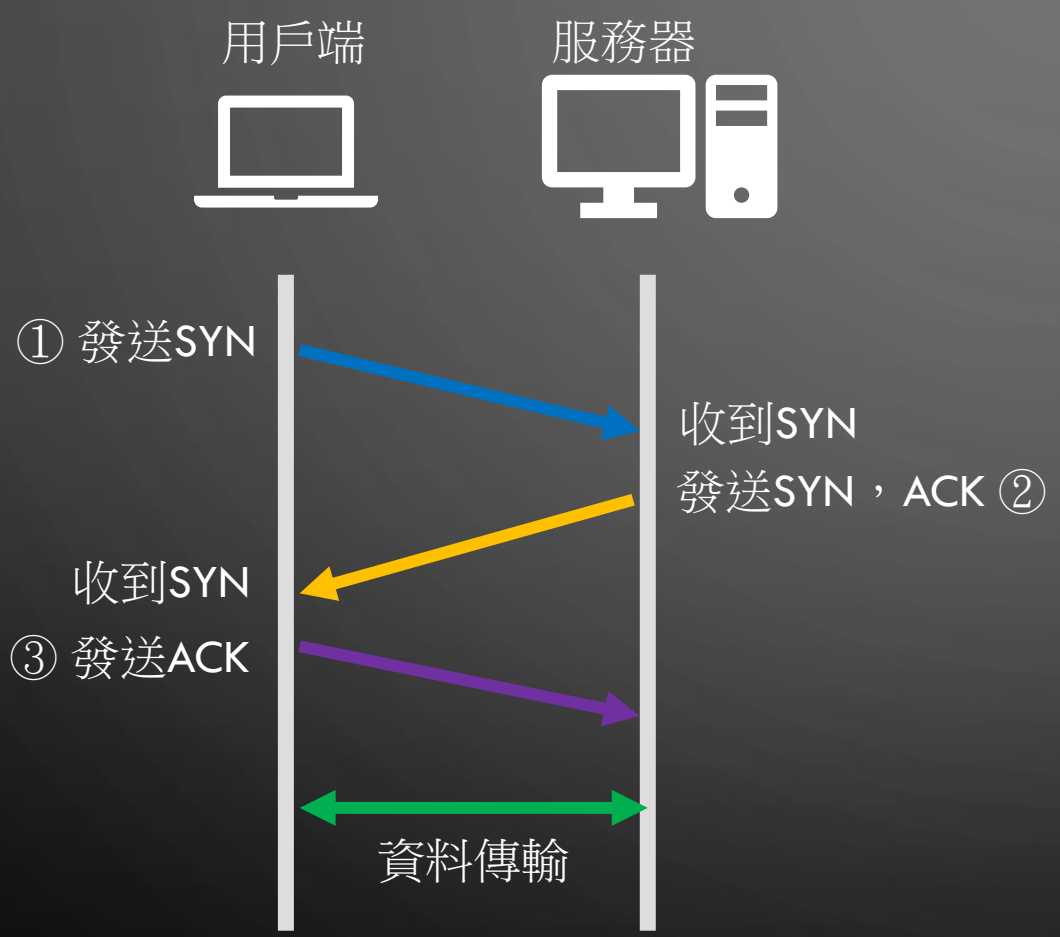
阻斷服務攻擊方式

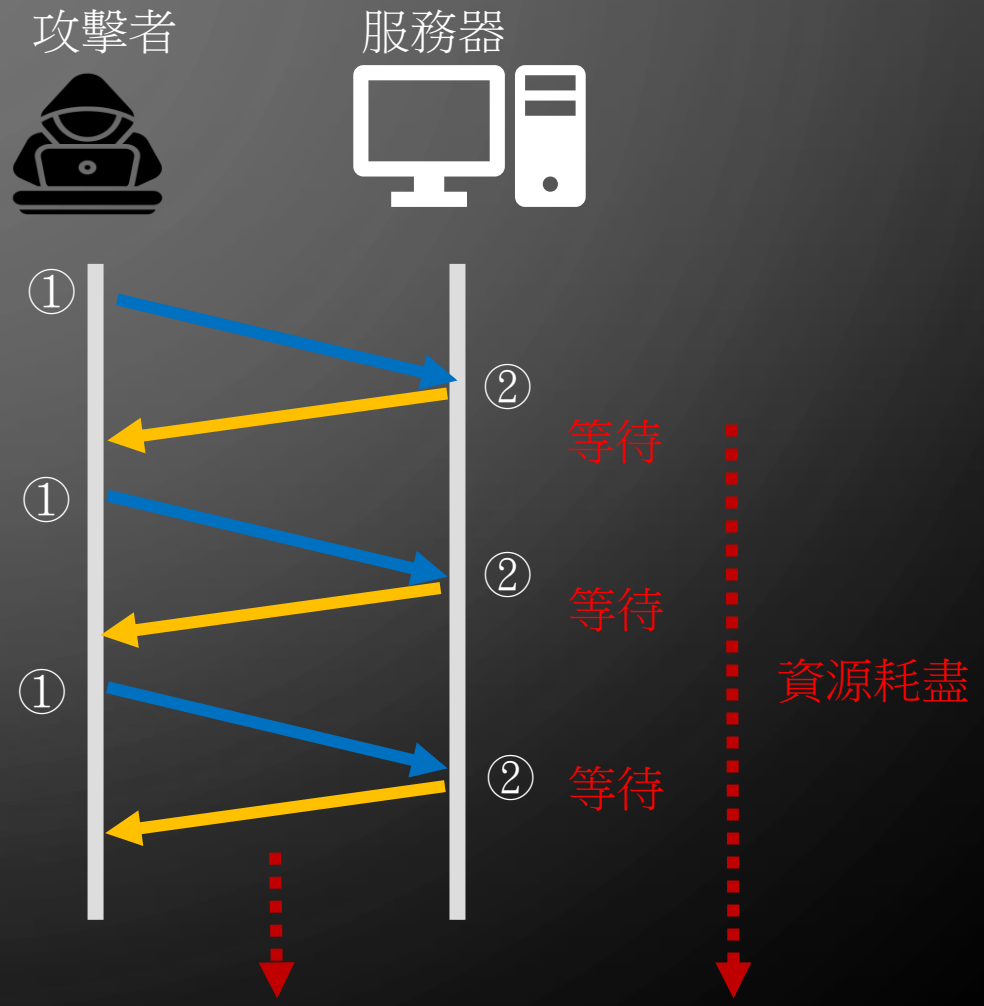
- 頻寬消耗型攻擊
  - UDP洪水攻擊（User Datagram Protocol floods，使用者資料報協定）
  - ICMP洪水攻擊（ICMP floods）
- 資源消耗型攻擊
  - 協定分析攻擊（SYN flood，SYN洪水）
  - LAND攻擊 (Local Area Network Denial attack，區域網路阻斷服務攻擊)
  - CC攻擊（Distributed HTTP flood，分散式HTTP洪水攻擊）
  - 殭屍網路攻擊
  - 應用程式級洪水攻擊（Application level floods）

阻斷服務攻擊方式

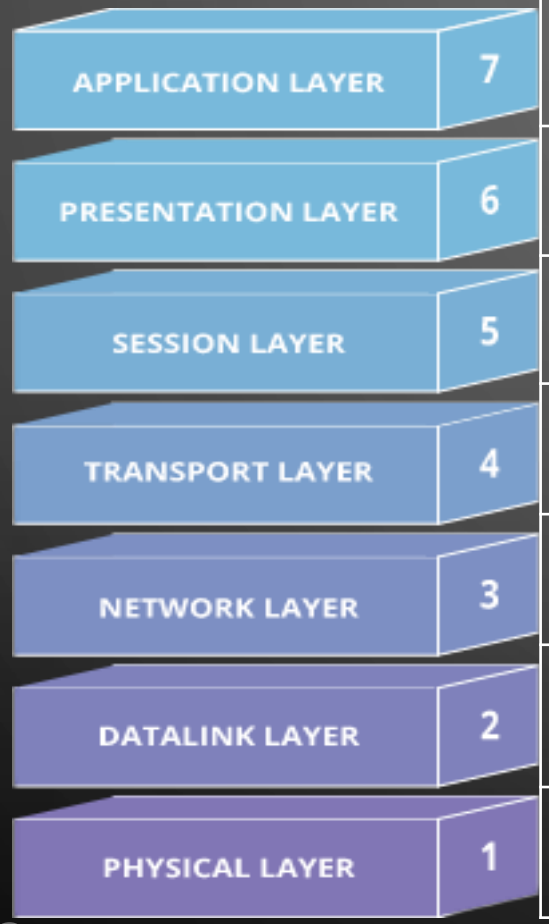
- 漏洞觸發型
  - 死亡之Ping（ping of death）
  - 淚滴攻擊

阻斷服務攻擊-SYN泛洪





受攻擊的開放系統互連 (OSI) 模型



層	應用程式	描述	向量範例
應用程式	資料	應用程式網路程序	HTTP 泛洪、DNS 查詢泛洪
展示	資料	資料展示和加密	SSL 濫用
工作階段	資料	中間主機通訊	不適用
傳輸	區段	端對端連線和可靠性	SYN 泛洪
網路	封包	路徑判定與邏輯定址	UDP 反射攻擊
資料連結	框架	實體定址	不適用
實體	位元	媒體、訊號和二進位傳輸	不適用

阻斷服務攻擊症狀

- 網路異常緩慢（打開檔案或存取網站）
- 特定網站無法存取
- 無法存取任何網站
- 垃圾郵件的數量急劇增加
- 無線或有線網路連接異常斷開
- 長時間嘗試存取網站或任何網際網路服務時被拒絕
- 伺服器容易斷線、卡頓、存取延遲

資安案例

- 新聞日期：2019/11/05
- 台股近日續創29年新高，但竟有歹徒趁券商熱絡交易，發動攻擊券商下單平台網站；金管會證期局今天表示，近日有6家券商向金管會通報，受到分散式阻斷服務攻擊（DDoS），但在導入流量清洗服務後，交易即恢復正常。

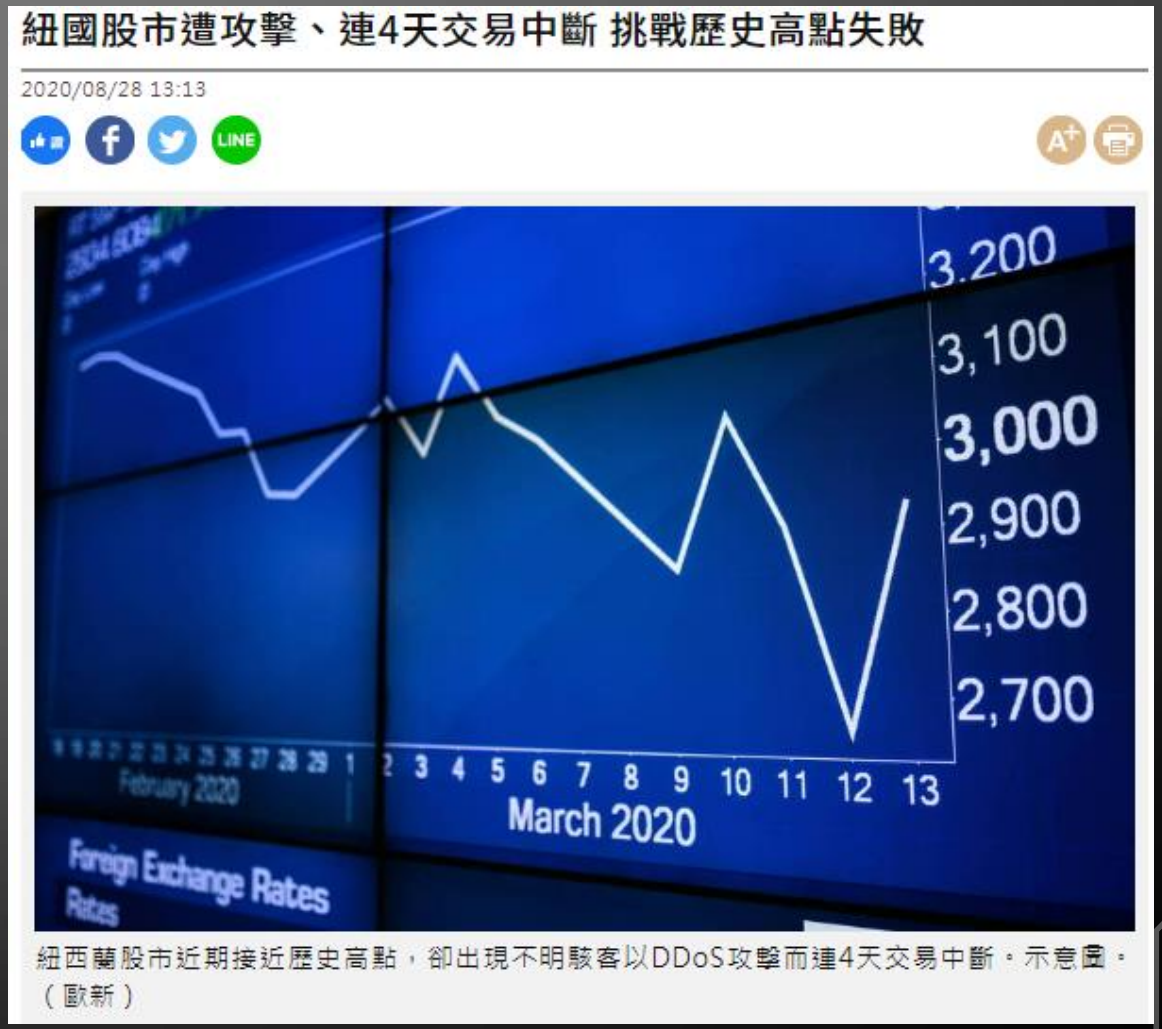
6家券商驚傳駭客攻擊 金管會祭9項強化措施

2019/11/05 22:20

金管會表示，近日有6家券商通報，受到分散式阻斷服務攻擊（DDoS），但在導入流量清洗服務後，交易即恢復正常。（記者王孟倫攝）

資安案例

- 新聞日期： 2020/08/28
- 市值2040億紐幣（約新台幣3.99兆元）的紐西蘭股市近期接近歷史高點，卻出現不明駭客以DDoS攻擊（分散式阻斷服務攻擊）攻擊該國證券交易所，已經連續4天出現交易中斷，當局目前只確定攻擊來自海外。



資安案例

- 新聞日期： 2021/10/25
- 綜合韓媒報導，當地時間25日上午11時20分左右，南韓電信公司「KT」所提供的有線及無線網路服務出現斷線、訊號不良的問題，不僅各地使用者無法上網，還有部分用戶無法撥打電話，使用KT電信網路的證券交易系統、數位支付系統也受到波及，災情持續約1小時。

資安案例

- 新聞日期： 2022/02/24
- 俄羅斯與烏克蘭間的戰火引爆，除了物理上的砲火攻擊，烏克蘭的許多網頁也遭到大規模分散式阻斷服務（DDoS）攻擊事件，烏克蘭政府昨（23）日公告，多個政府及金融機構遭到DDoS攻擊，另外，有數百部電腦被植入惡意資料刪除程式。

資安案例

- 新聞日期： 2022/07/19
- 在今年6月，Cloudflare揭露每秒達2,600萬次請求的HTTPS DDoS攻擊，經過一個月的追蹤，新的研究結果出爐。他們將發起這波攻擊的殭屍網路命名Mantis，並指出該殭屍網路仍持續橫行，已發動超過3,000次的DDoS攻擊。

資安案例

- 新聞日期： 2022/08/12
- 美國聯邦眾議院議長裴洛西（Nancy Pelosi）於8月2日至3日，率領美國眾議院國會訪問團來臺訪問，此行引發中國政府高度不滿，不只進行軍演，相關的網路攻擊更是從訪臺前就不斷出現，且前後持續了長達9天。這些攻擊手法大致可區分為分散式阻斷服務（DDoS）攻擊、內容置換（Deface），以及幾可亂真的假訊息等。

電腦病毒的防範之道

- 為了減少電腦中毒的機會，建議您多留意下列原則：
- 安裝防毒軟體並定期更新病毒碼
- 定期備份資料
- 勿使用來歷不明的軟碟或光碟開機
- 勿開啟或執行來歷不明的檔案、程式或電子郵件
- 沒有存取網路時要離線
- 多使用Web Based Mail（網頁式郵件）
- 拒絕來路不明的即時通訊，並慎選瀏覽的網站
- 定期更新Windows 作業系統和瀏覽器

容易常用密碼

- 密碼管理器NordPass公布了2021年全球最常用最常用密碼TOP200榜單，最常用的密碼前十名分別是以下：

1. 123456
2. 123456789
3. 12345
4. qwerty
5. password
6. 12345678
7. 111111
8. 123123
9. 1234567890
10. 1234567890

NordPass官網