資安威脅趨勢與案例分享

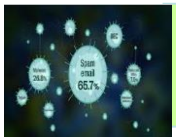
行政院國家資通安全會報技術服務中心

109年12月

大綱

- 資安威脅趨勢與案例
  - 全球資安威脅趨勢
  - 政府機關威脅情勢與通報案例
- 近期攻擊手法說明
- 結論與建議

全球資安威脅案例



疫情讓資安風險大增 社交工程事件頻傳

2020/8/31趨勢科技統計，半年攔截880萬次COVID-19攻擊

趨勢科技發表2020年上半年資安總評報告顯示6個月內即攔截880萬次新冠肺炎相關威脅，其中近92%是經由垃圾郵件散布

APT攻擊串聯網通設備漏洞發動攻擊

2020/09/14美國國土安全部公告，中國利用各大網路設備已知漏洞，對美國政府單位發動攻擊

美國國土安全部發現中國APT駭客組織利用Citrix、微軟Exchange Server、F5及Pulse VPN等多項產品漏洞，攻擊美國政府單位

供應鏈攻擊鎖定GitHub開源軟體專案

2020/5/29駭客將惡意程式注入開源專案中，透過GitHub平台上散布後門程式

GitHub發現名為Octopus Scanner惡意軟體，可進行主機遠端操控，GitHub團隊調查後發現，已有26個開源專案遭攻擊者借殼上架後門程式

物聯網設備資安弱點威脅升高

2020/6/10 IoT裝置驚爆漏洞，恐引發資料外洩與DDoS攻擊

通用隨插即用協定來發現其他裝置並與之互動的物聯網設備及區域網路裝置，存CallStranger安全漏洞，可藉此漏洞竊取資料、發動分散式阻斷服務攻擊

勒索軟體轉向目標式攻擊，資安威脅遽增

2020/10/27全球受勒索軟體攻擊次數近3個月暴增5成

資安業者Check Point研究指出，相較於2020上半年，過去3個月受勒索軟體攻擊的每日平均次數增加50%，7月底Garmin傳出疑似遇害而導致服務與網站一度中斷，5月初中油、台塑、力成先後遭駭客鎖定攻擊

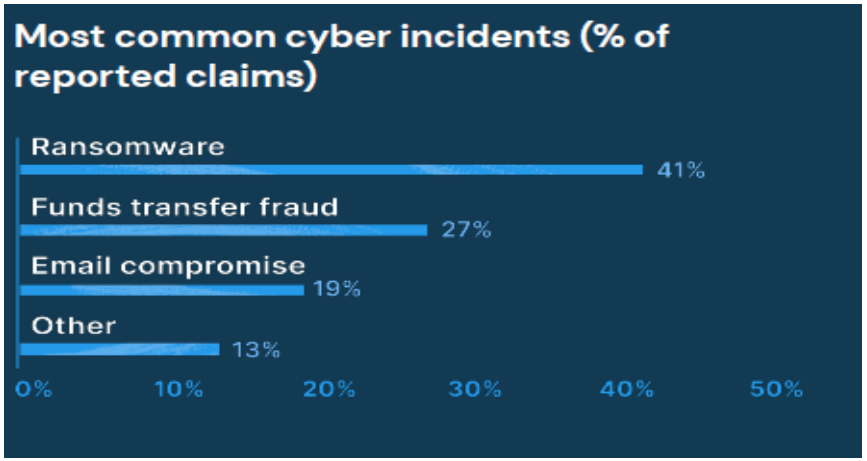
資料外洩，個資、商業機密全都露

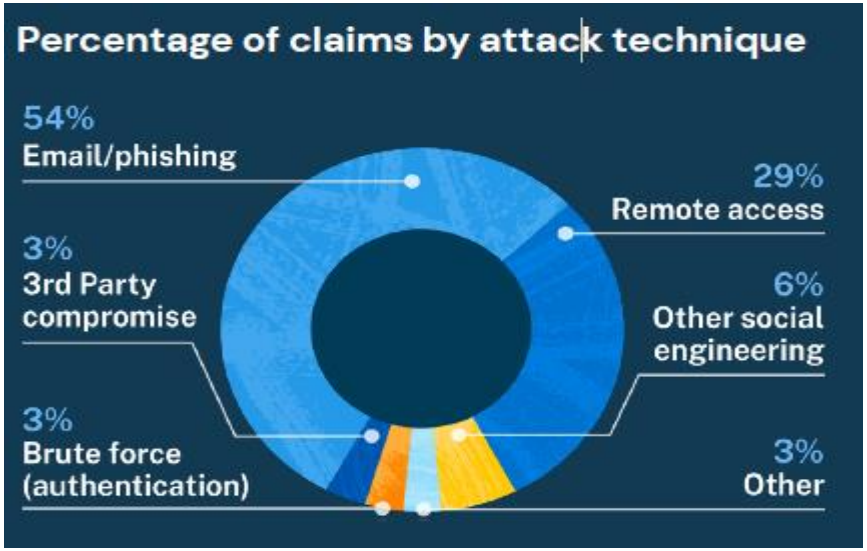
2020/11 Prestige Software雲端配置錯誤，造成Booking.com、Expedia與Agoda等客戶的房客資料外洩

提供架站服務的Website Planet近日揭露，Prestige Software雲端配置錯誤造成多家住房網房客資料外洩，約有10萬名房客的信用卡資訊，受害者遍及全球

資安威脅趨勢統計(1/2)

- 資安事件分類
  - 勒索軟體攻擊(41%)
  - 資金移轉詐騙(27%)
  - 電子郵件入侵(19%)
- 攻擊技術
  - 郵件釣魚(54%)
  - 遠端存取(29%)
  - 除郵件外社交工程(6%)
  - 第三方工具(3%)
  - 暴力破解(3%)

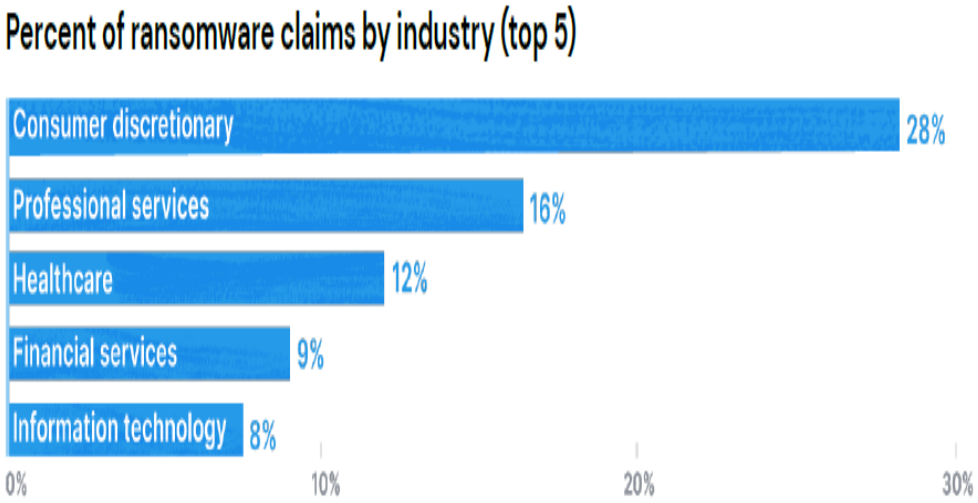




資料來源：2020網路與資訊安全保險業者Coalition上半年索賠報告

資安威脅趨勢統計(2/2)

- 被攻擊產業類別
  - 消費者領域(28%)
  - 專業服務(16%)
  - 健康照護(12%)
  - 金融服務(9%)
  - 資訊科技(8%)



大綱

- 資安威脅趨勢與案例
  - 全球資安威脅趨勢
  - 政府機關威脅情勢與通報案例
- 近期攻擊手法說明
- 結論與建議

政府機關資安威脅情勢

01

社交工程搭配時事議題做為攻擊主軸

攻擊啟動從釣魚郵件開始，駭客以近期受關注程度高的政經議題為由施行攻擊，例如肺炎疫情、總統520就職等，鎖定特定相關機關進行攻擊

02

APT類型攻擊轉而利用商用工具軟體與服務

駭客利用網路上現成的工具程式或商用軟體進行入侵攻擊，並滲透與掌控AD系統，利用政府導入政府共通組態基準(GCB)以合法的服務，透過GPO派送惡意程式進行橫向擴散

03

供應鏈攻擊活動加劇

入侵系統委外廠商後，以其做為跳板，滲透客戶組織
駭客藉由入侵特定軟/韌體開發公司或人員電腦，進行竄改程式或下載連結等行為，造成大範圍的感染與擴散

04

物聯網攻擊鎖定監視與網通設備

鎖定機關監視器與網通設備做為攻擊標的，以弱密碼/預設密碼配合已知弱點攻擊程式進行探測並入侵控制

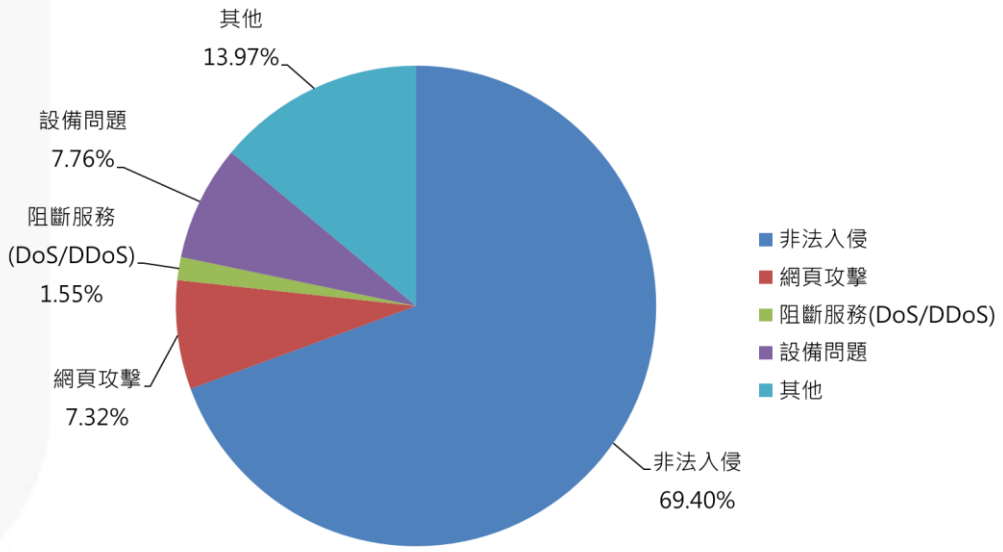
05

勒索軟體攻擊風險激增

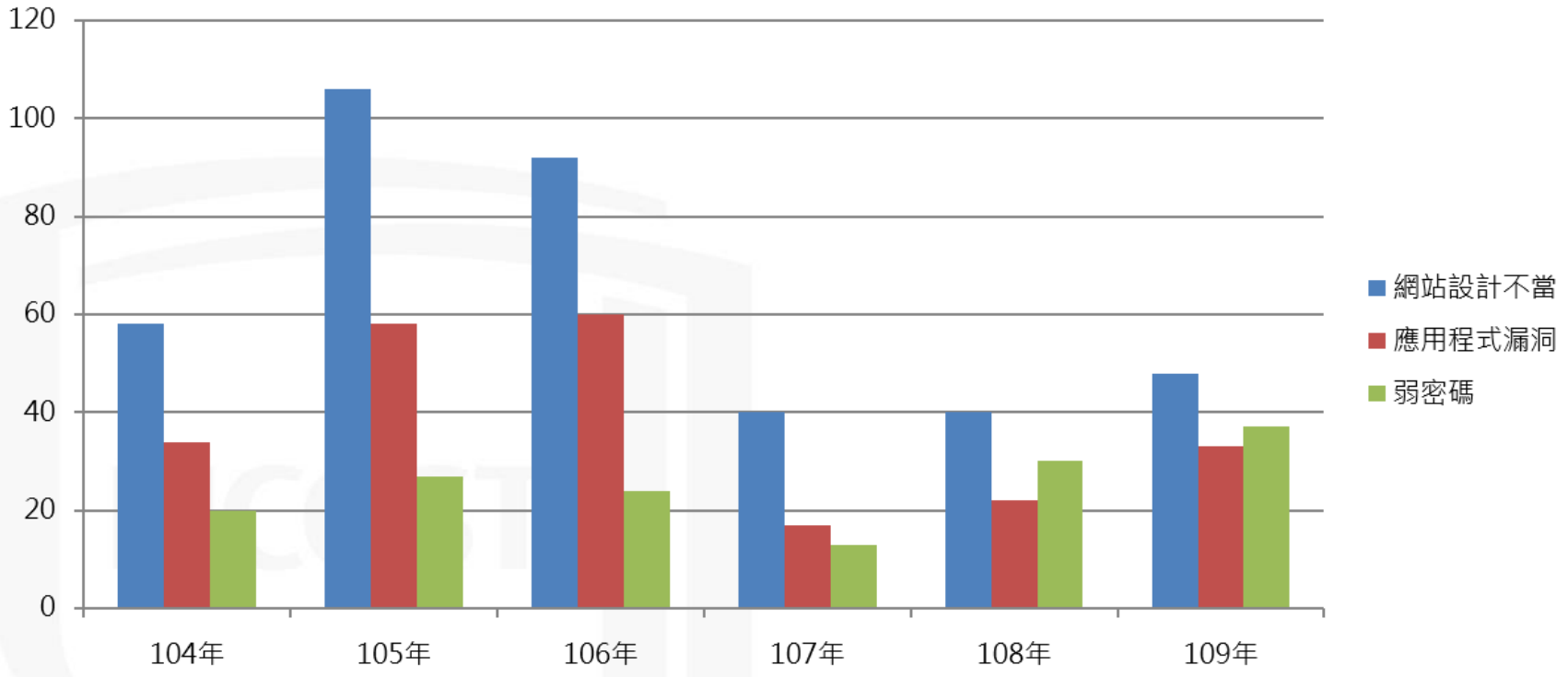
由亂槍打鳥轉向特定目標，遭鎖定對象包含委外廠商、機關人員、機關之公文系統資料庫主機、對外服務網站、環控系統、檔案分享系統等，藉以癱瘓系統運作，中斷服務提供

109年政府機關資安事件通報統計

- 109年1月1日至10月27日共接獲451件資安事件通報，其中57.2%(258件)為機關接獲技服中心警訊通告後所進行之通報
- 通報資安事件等級
  - 4級事件：0件
  - 3級事件：8件
  - 2級事件：51件
  - 1級事件：392件



政府機關資安事件主要發生原因

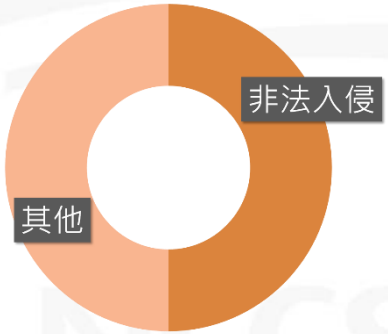


註：109年資料統計至10月27日

政府機關重大資安事件通報統計

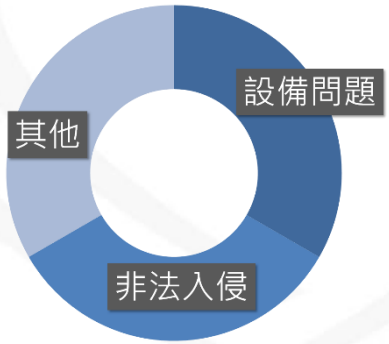
- 109年共接獲8件重大資安事件通報，5件為資料外洩，3件為核心業務中斷

資料外洩發生原因



- 網站設計不當，導致網站具漏洞可存取敏感資料
- 供民眾登記資料的表單權限設定錯誤，導致可被公開檢索與編輯
- 機關內部人員疏失，將含有敏感資料檔案夾帶於信件中寄出

核心業務中斷發生原因



- 機關遭非法入侵植入勒索軟體，因無法啟用備援機制，影響核心業務運作
- 設備故障，影響涉及關鍵基礎設施維運之核心資通系統運作

註：109年資料統計至10月27日

重大資安事件案例 – 資料外洩1、2

案情提要

- 機關A與B為辦理活動，採用**Google表單**供民眾登記資料，惟Google表單**權限設定錯誤**，導致可檢索其他登記民眾資料

【機關處置方式】

–即時關閉表單、調整Google表單權限

–依個資法規定，通知當事人個資外洩情形

防護建議

- 機關辦理活動供民眾填寫資料，應評估填寫內容含有個資之必要性，不得逾越特定目的之必要範圍
- 提供民眾填寫的表單若涉及個資，應確認表單檢視權限，以避免個資外洩疑慮

重大資安事件案例 – 資料外洩3

案情提要

- 機關新進人員寄信件通知活動相關人員時，誤將**含有機敏資料檔案**夾帶於信件中寄出

【機關處置方式】

–即時聯繫收件人，請其勿再將資料擴散

–依個資法規定，通知當事人個資外洩情形

防護建議

- 新進人員應加強資安防護意識，避免因人員疏失導致機敏資料外洩

重大資安事件案例－資料外洩4

案情提要

- 機關網站因存在**角色權限設置不當**漏洞，一般帳號可藉由修改URL網址，直接存取管理後台並匯出資料，約7萬筆個資遭下載

【機關處置方式】

－修補漏洞並刪除個人資料

－依個資法規定，以公告方式通知當事人個資外洩情形

防護建議

- 網站若提供管理後台，應落實存取權限控管，若非必要可限制開放外部IP存取
- 網站若提供個人資料資訊供檢視，可進行適度遮蔽，以避免個資外洩疑慮

重大資安事件案例－資料外洩5

案情提要

- 機關網站使用自然人憑證身分驗證機制，因驗證簽章儲存在使用設備上，導致後續無需使用自然人憑證，即可利用儲存在設備上之簽章下載該使用者資料

【機關處置方式】

- 立即將網站下線完成漏洞修補，確保驗證簽章僅供當次登入驗證使用
- 針對使用憑證之應用系統進行安全性檢查作業後，重新上線

防護建議

- 網站開發可依安全軟體發展流程(SSDLC)，評估各項防護措施是否符足資安要求

重大資安事件案例 – 核心業務中斷1

案情提要

- 機關因防火牆異常，影響多台伺服器無法對外連線

【機關處置方式】

–設備維運廠商修復並排除防火牆異常狀況後恢復正常運作

–後續評估防火牆設備效能以符合使用需求

防護建議

- 機關應定期檢視設備狀況，並評估設備效能以符合使用需求

重大資安事件案例 – 核心業務中斷2

案情提要

- 機關發現多個設備遭感染勒索病毒，影響機關日常作業，且核心資通系統無法於可容忍中斷時間內回復正常
- 經查為設備**維護廠商維運使用之帳號密碼遭外部暴力破解**，駭客利用該帳號登入維運設備後，再橫向擴散至其他設備

【機關處置方式】

–後續以白名單限制存取系統並鎖定來源IP、限制維護廠商帳號與管理者權限帳號專機專用，並重新設置維運使用之帳號密碼

防護建議

- 密碼設置應符合複雜性原則，並避免使用常見之排列組合如!qaz2wsx
- 廠商現場維護可降低資安風險，不建議機關設備開放遠端桌面登入維護

重大資安事件案例 – 核心業務中斷3

案情提要

- 機關提供民眾服務系統，因夜間無預警自動重啟失敗，顯示作業系統錯誤訊息，直至上班時間經內部同仁發現，通知廠商處理

【機關處置方式】

– 緊急將相關業務改由人工收件，以維護民眾權益
– 設備維護商先行以作業系統修復嘗試回復運作，並另設置啟用備援主機，後續因作業系統成功修復而恢復使用

防護建議

- 針對重要服務之資通系統，可評估設置監控機制，偵測系統異常時，可即時通知應處
- 針對重要服務之資通系統，應設置相關備援機制，確保事發期間可正常切換之備援系統

供應鏈攻擊案例

案情提要

- 機關發現設備夜間，來自**維護廠商IP，以VPN帳號連至跳板機**存取後，設備即遭植入惡意程式並連至中繼站
- 機關與廠商確認，當時並無人員進行設備遠端維護作業
- 惟廠商維護機關設備的電腦已重灌，導致無法進一步調查

【機關處置方式】

- 立即移除惡意程式，並修改所有系統密碼，後續為避免資安疑慮，關閉維護廠商遠端維護作業
- 將廠商維護設備與核心資通系統重灌，避免惡意程式殘留

防護建議

- 廠商現場維護可降低資安風險，不建議機關設備開放遠端登入維護
- 依資通安全管理法，監督委外廠商其資通安全維護情形

物聯網攻擊案例

案情提要

- 機關某廠牌監視器發現遭植入Mirai家族惡意程式，並至中繼站報到
- 經調查該監視器遭揭漏存在存在路徑走訪(Path Traversal)、緩衝區溢位(Buffer Overflow)及命令注入(Command Injection)漏洞等安全性漏洞

【機關處置方式】

–重置設備、變更監視器預設帳號密碼，並更新韌體版本至最新版本

防護建議

- 應評估設備供外部連線之必要性
- 設置新購資訊設備應立即變更預設帳號密碼
- 定期檢視並更新設備系統/韌體版本

大綱

- 資安威脅趨勢與案例
  - 全球資安威脅趨勢
  - 政府機關威脅情勢與通報案例
- 近期攻擊手法說明
- 結論與建議

入侵攻擊手法組合

- 根據風險諮詢公司德安華(Kroll)統計，被攻擊事件中，有47%開啟RDP、26%釣魚郵件、 17%漏洞利用、10%帳號接管，開放的RDP、網路釣魚、漏洞利用及帳戶接管，為攻擊的前兆
- 政府機關面臨相同之攻擊組合
  - 透過社交工程(釣魚郵件、惡意檔案)載入惡意程式
  - 利用商用工具軟體與服務(VPN連網設備+ RDP服務)，遠端控制機關內網主機
  - 運用已知軟體漏洞入侵， 隱匿或繞過身分驗證，取得特權帳號接管整個網域控制，並透過工作排程散播惡意程式

社交工程電子郵件案例
-COVID-19社交工程攻擊

COVID-19社交工程攻擊

- 彙整近期新型冠狀病毒(COVID-19)社交工程惡意電子郵件分析，可分為以下2類

1

釣魚郵件

內含健康調查與Coronavirus資訊之釣魚郵件，使用客製化頁面，誘騙使用者輸入個人帳密

2

惡意郵件(附檔)

以W.H.O、COVID-19、Coronavirus及Mask等關鍵字為主旨，並夾帶惡意程式之社交工程電子郵件

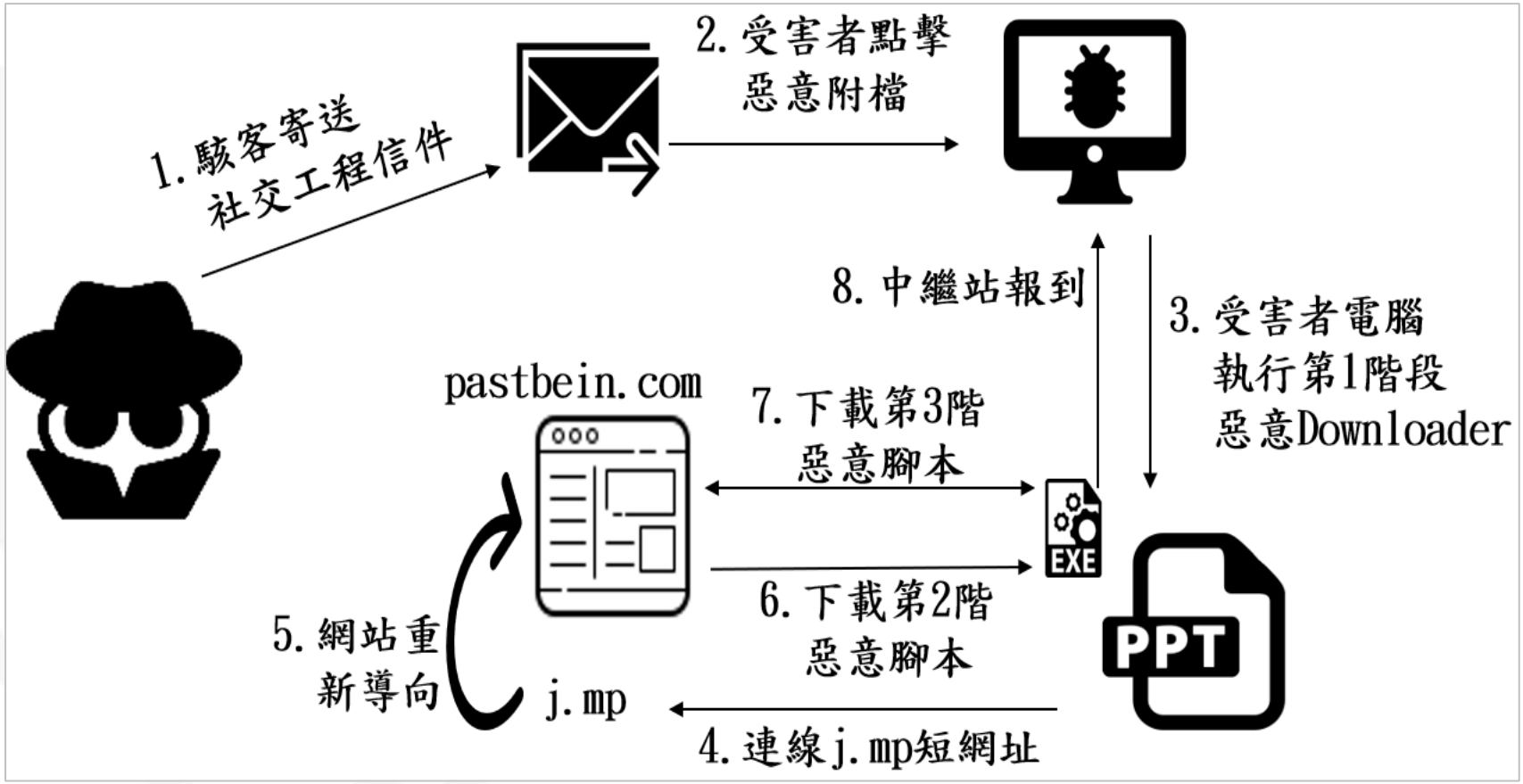
社交工程電子郵件案例
-利用短網址服務攻擊

利用短網址服務攻擊(1/2)

- 駭客偽冒國內大學信箱與冒用校徽圖示，大量寄送社交工程郵件給政府機關
  - 收件人開啟惡意郵件並點擊附件檔案後，受害電腦將植入第1階段惡意程式(Downloader)執行

利用短網址服務攻擊(2/2)

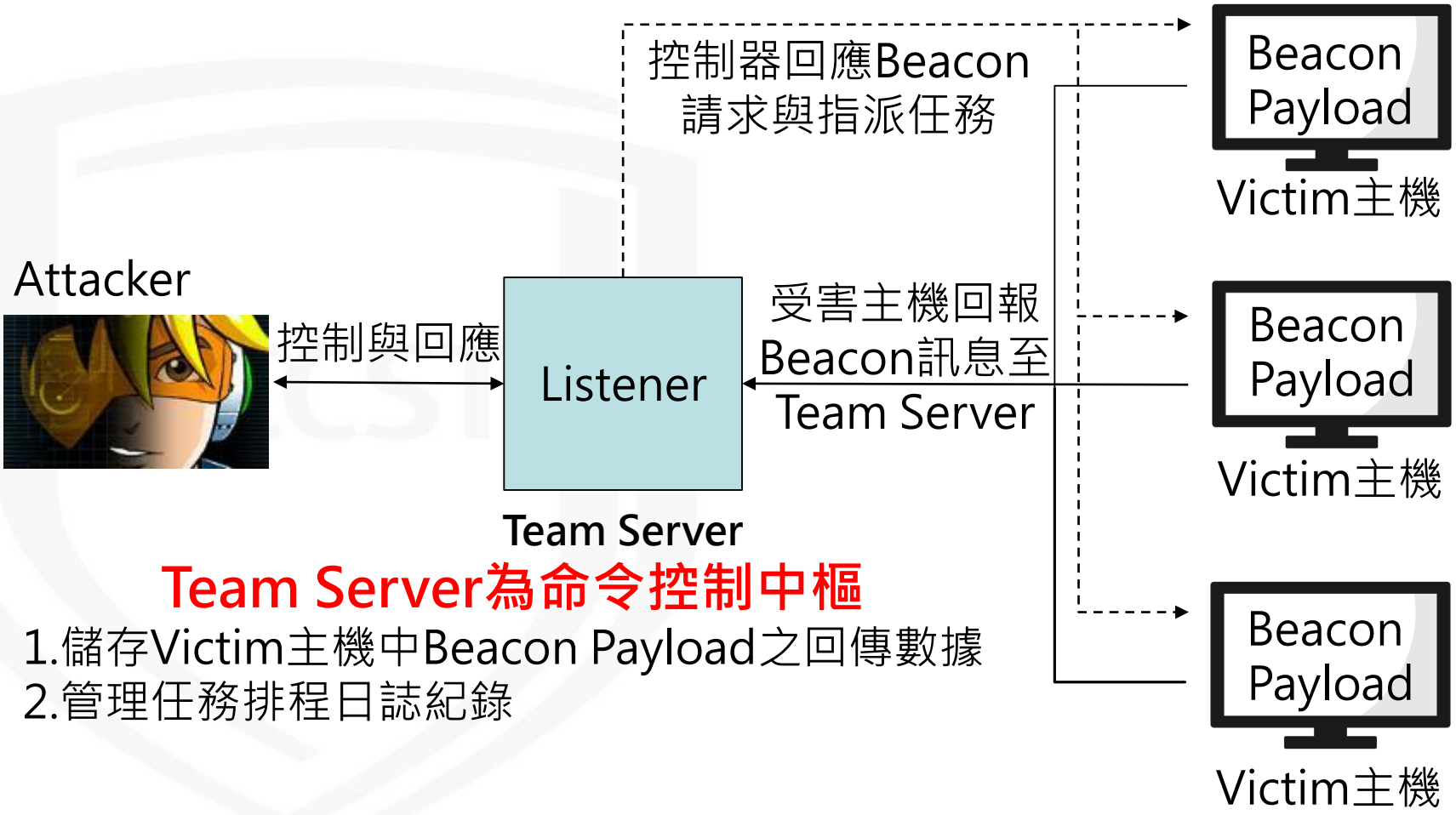
- 讓受害電腦連線至合法之短網址域名(j.mp)下載惡意程式，藉此規避中繼站黑名單阻擋機制



利用商用工具軟體與服務進行遠端控制
-以Cobalt Strike為例

Cobalt Strike Client Server架構

- Cobalt Strike為基於Java之滲透工具平台，用以進行偵察、魚叉式釣魚、瀏覽器代理等攻擊

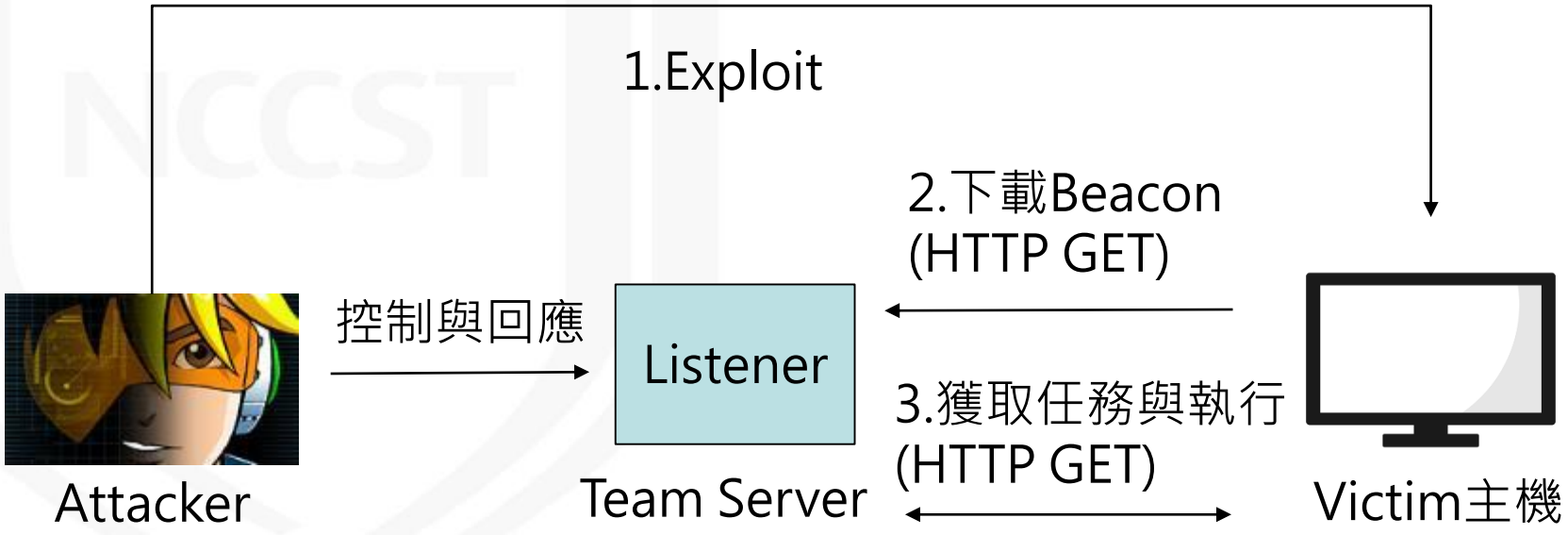


Team Server為命令控制中樞

1.儲存Victim主機中Beacon Payload之回傳數據
2.管理任務排程日誌紀錄

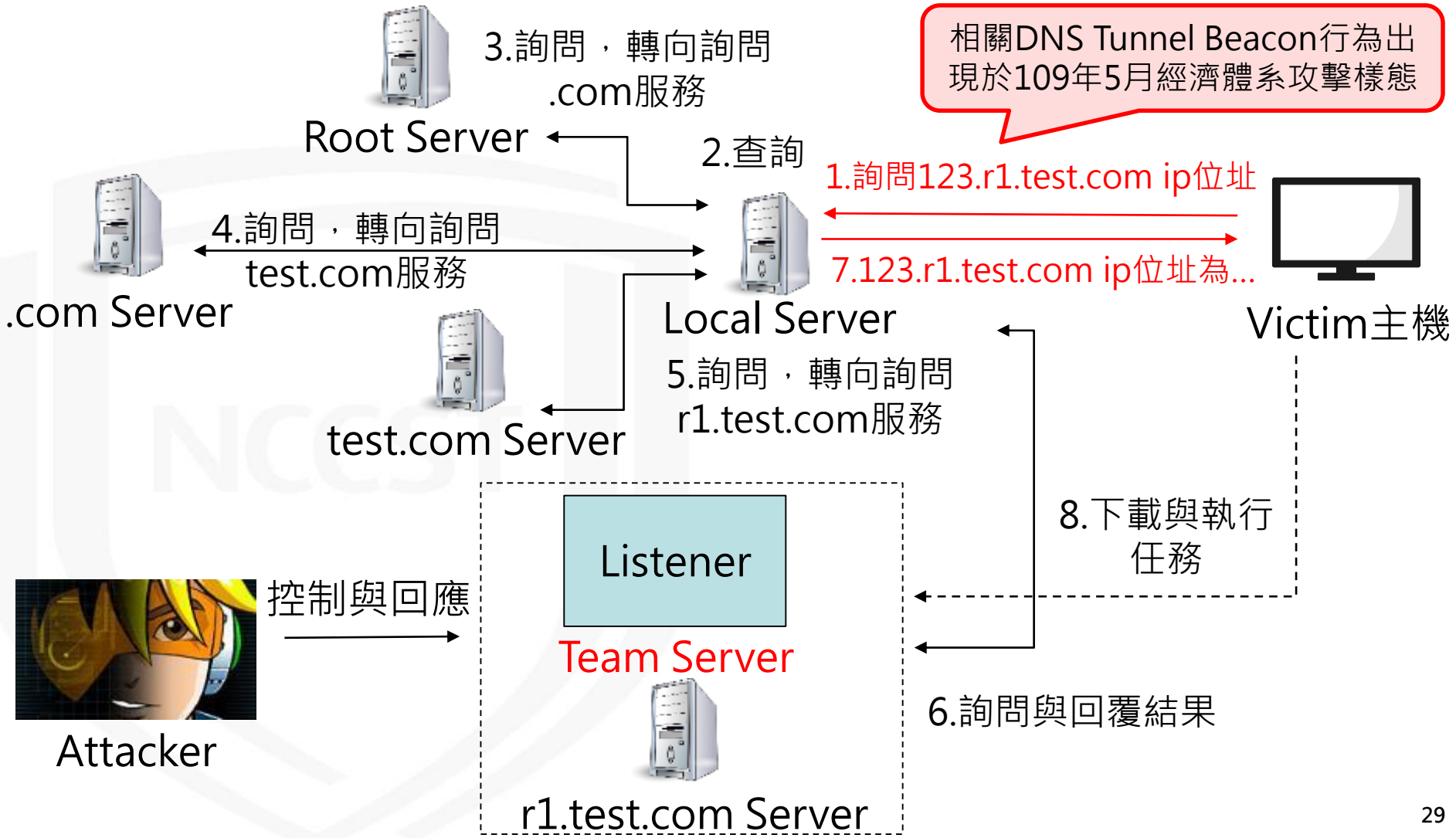
Cobalt Strike Beacon類型(1/3)

- 受害主機遭入侵後，Cobalt Strike透過Beacon進行命令與控制行為
  - 支援http (https)、 dns、 smb等通訊協定
  - 使用http或dns服務，檢查是否有待執行任務
  - 可連接至多個C2域名



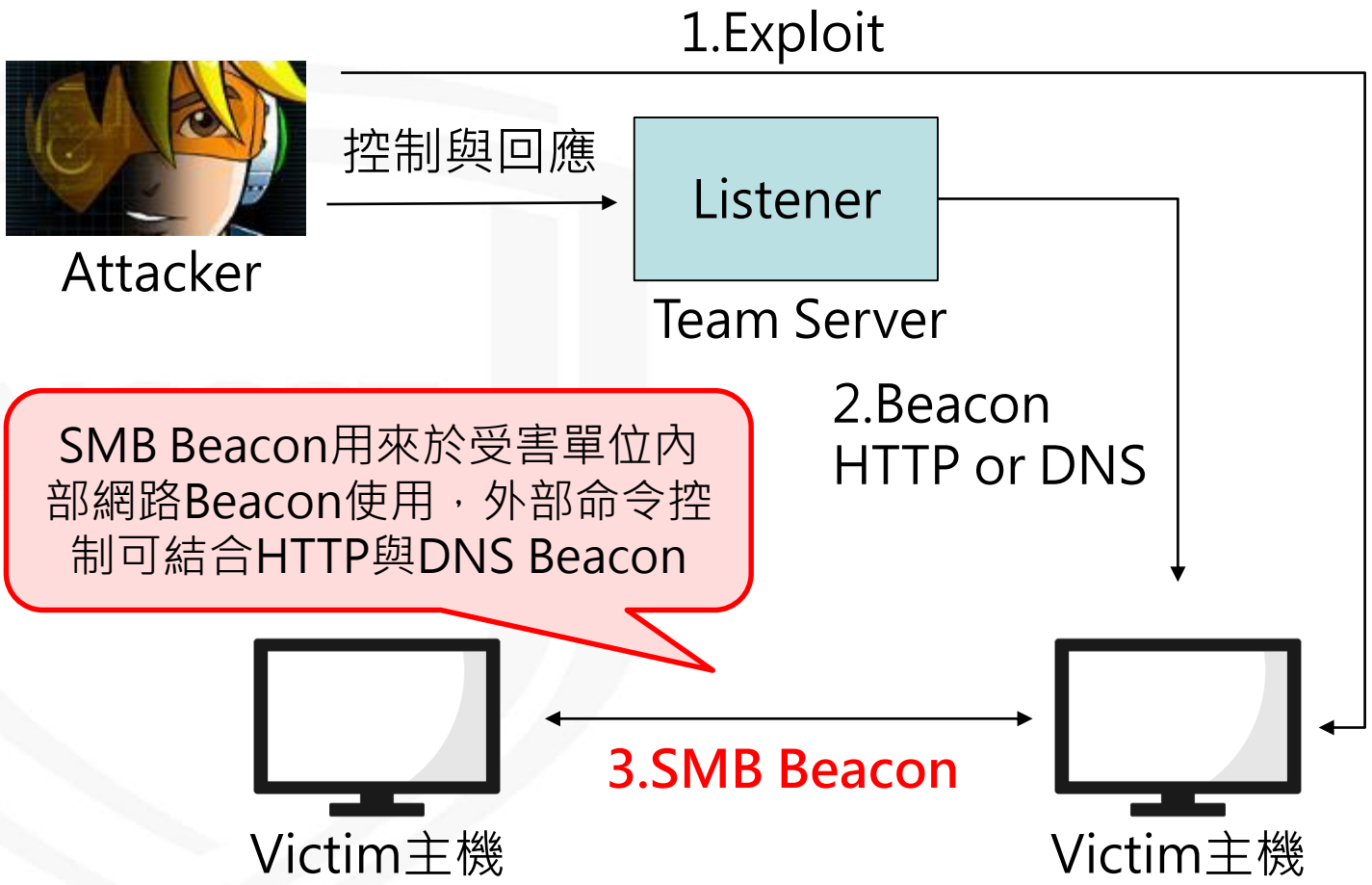
Cobalt Strike Beacon類型(2/3)

- DNS Beacon用於避開防火牆偵測



Cobalt Strike Beacon類型(3/3)

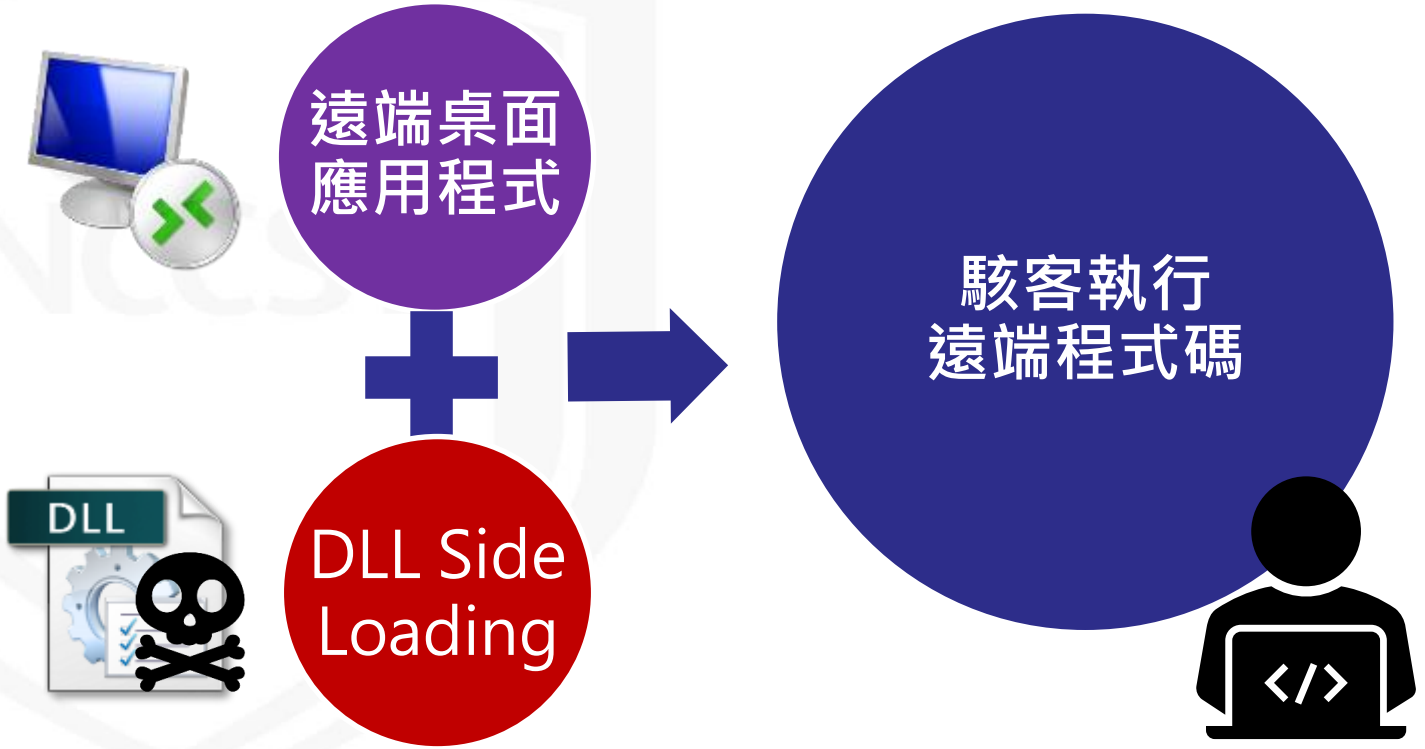
- SMB Beacon用於受害單位內部受害主機溝通使用，目的在於橫向的擴散感染



運用已知軟體漏洞入侵
-DLL Side Loading攻擊

DLL Side Loading漏洞說明(1/2)

- 2020年4月，資安廠商發現利用微軟遠端桌面應用程式之DLL Side Loading漏洞，可讓駭客執行遠端程式碼
- 動態連結函式庫(Dynamic-link library, DLL)是微軟在Windows作業系統中實現共享函式庫之方式



DLL Side Loading漏洞說明(2/2)

- 微軟表示「應用程序目錄DLL植入，被視為深度防禦問題，僅在以後的版本中才會考慮進行更新」，故現階段仍可利用DLL Side Loading攻擊手法

  (資料來源：Microsoft Security Response Center)

- 本次報告將說明Windows桌面應用程式載入DLL時之搜尋順序，並藉由實作驗證利用此搜尋順序，達成DLL Side Loading攻擊手法

DLL Side Loading攻擊成因

應用程式搜尋
並載入DLL

搜尋順序	搜尋位置
1	已載入記憶體之同模組名之DLL
2	Windows Known DLLs列表
3	應用程式所在目錄
4	系統目錄
5	16位元系統目錄
6	Windows目錄
7	當下目錄
8	環境變數PATH中列出的目錄

攻擊者若能將相同名稱之惡意DLL放置於搜尋順序較正常DLL前之位置，讓應用程式優先載入，即有攻擊成功機會

運用已知軟體漏洞入侵
-Zerologon漏洞攻擊
(CVE-2020-1472)

Zerologon漏洞說明

- 資安廠商Secura於2020/9/11揭露，Netlogon遠端協定存在Zerologon漏洞(CVE-2020-1472)
  - 未經驗證之攻擊者可利用偽冒憑證繞過身分驗證，以任意身分與DC建立安全通道，進而取得AD資料庫內容，幾分鐘內就可控管整個網域
  - 與DC建立TCP連線即可駭入，不需加入網域
  - CVSS高達10分之重大漏洞
  - 應儘速安裝修補程式
- 美國國土安全部於9/18發出緊急指令，要求聯邦政府所有機關必須在3天內完成相關修補措施


iThome

Windows重大漏洞Zerologon可讓駭客輕易掌控AD網域

位於Netlogon遠端協定的CVE-2020-1472漏洞，可讓未授權使用者取得管理員權限來控制整個網域。駭客一旦開採成功便能駭入並控制公司Active Directory網域，危及所有連網電腦。微軟在8月Patch Tuesday發布第一階段修補，預計明年第一季進行更完整的修補

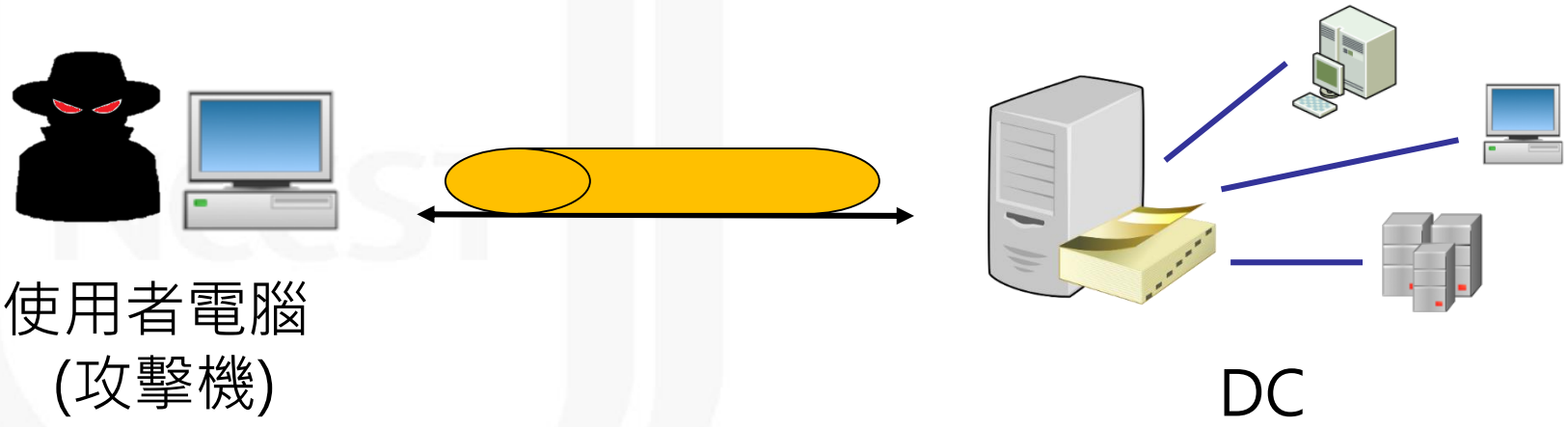

安全防護 新聞

Windows爆出Zerologon重大漏洞專打AD網域 美府發佈緊急修補指令

美國國土安全部上周罕見發佈緊急指令，要求聯邦政府必須在周一午夜之前修補完成Windows Server一項可能導致駭客控制Windows網域重大漏洞。

攻擊情境

- 攻擊者駭進某單位內網使用者電腦後，發現此電腦可連至內網主DC，因此發動Zerologon攻擊，企圖控制整個網域



大綱

- 資安威脅趨勢與案例
  - 全球資安威脅趨勢
  - 政府機關威脅情勢與通報案例
- 近期攻擊手法說明
- 結論與建議

結論與建議(1/3)

- 社交工程攻擊
  - 提升機關人員資安意識，避免開啟非公務相關郵件
  - 落實郵件信箱公私領域區分，避免將公務信箱用於註冊私人用途之應用服務之上
  - 不執行來路不明郵件內夾帶之檔案或連結
  - 不下載非法軟體及檔案
  - 定期更新系統與修補漏洞
- APT類型攻擊
  - 系統漏洞修補及軟體版本更新
  - 執行存取權限控管及採用多因子認證
  - 強化帳號密碼管理，提高系統整體安全

結論與建議(2/3)

- 供應鏈攻擊
  - 要求廠商遵守機關訂定之資安防護規範
  - 關閉不必要通訊埠，限制連線來源
  - 系統串接前完成安全性檢測，包含防毒軟體掃描等
- 物聯網攻擊
  - 變更監視器預設帳號密碼，並停用Admin帳號
  - 定期更新產品韌體與安全性更新
  - 啟用設備提供之安全防護功能
  - 透過防火牆管控存取的來源

結論與建議(3/3)

- 勒索軟體攻擊
  - 定期備份重要的檔案
  - 將最新的更新套用至作業系統與APP
  - 不執行來路不明郵件內夾帶之檔案或連結
  - 不下載非法軟體及檔案
  - 強化端點設備與網路設備的活動監控

報告完畢
敬請指教