2021年具影響力的網路安全事件

◆ 華梵大學資管系特聘教授 — 朱惠中

駭客獅子大開口要求贖金的行徑，越來越肆無忌憚，因為攻擊者明白，關鍵基礎設施機關業者，願意不惜一切代價來恢復營運。

2021年，網路安全行業的多事之秋

對網路安全行業而言，剛剛結束的2021年是個非常多事的一年。從年初以關鍵基礎設施為攻擊目標之「前所未有」的勒索軟體浪潮，到2021年底以臭名昭彰的Log4j漏洞結束為止（威脅並未降低），勒索軟體已對世界各地政府機關及私有企業造成嚴重且持續的威脅。

如何提昇工業控制系統（Industrial Control System, ICS）安全以避免關鍵基礎設施被攻擊，已成資訊安全的顯學。2021年上半年，在ICS中發現的漏洞有所增加，暴露出攻擊的高風險。同時，隨著企業持續將設備連接到互聯網並將IT系統與運營技術（OT）融合後，如何儘早應用美國國家標準與技術研究院（National Institute of Standards and Technology, NIST）所發

布的資安框架（CyberSecurity Framework, CSF）[1] 指導範例，在新的平臺上執行辨識（Identify）、保護（Protect）、偵測（Detect）、回應（Respond）和復原（Recover），將比過往任何時候都更加重要。

前事不忘後事之師，根據 darkreading 網站資料，整理 2021 年重大網路資安攻擊事件，指出潛在威脅並試著提出改善方案。

美國東海岸最大的油品供應商遭勒索事件

美國東海岸最大的油品供應商 Colonial Pipeline 在 2021 年 5 月遭到勒索軟體攻擊，使得汽油、柴油、家用暖氣用油與軍用油品等供應均受到嚴重衝擊，影響到 18 州數百萬人的生活。美國聯邦機動運輸安全管理局（Federal Motor Carrier

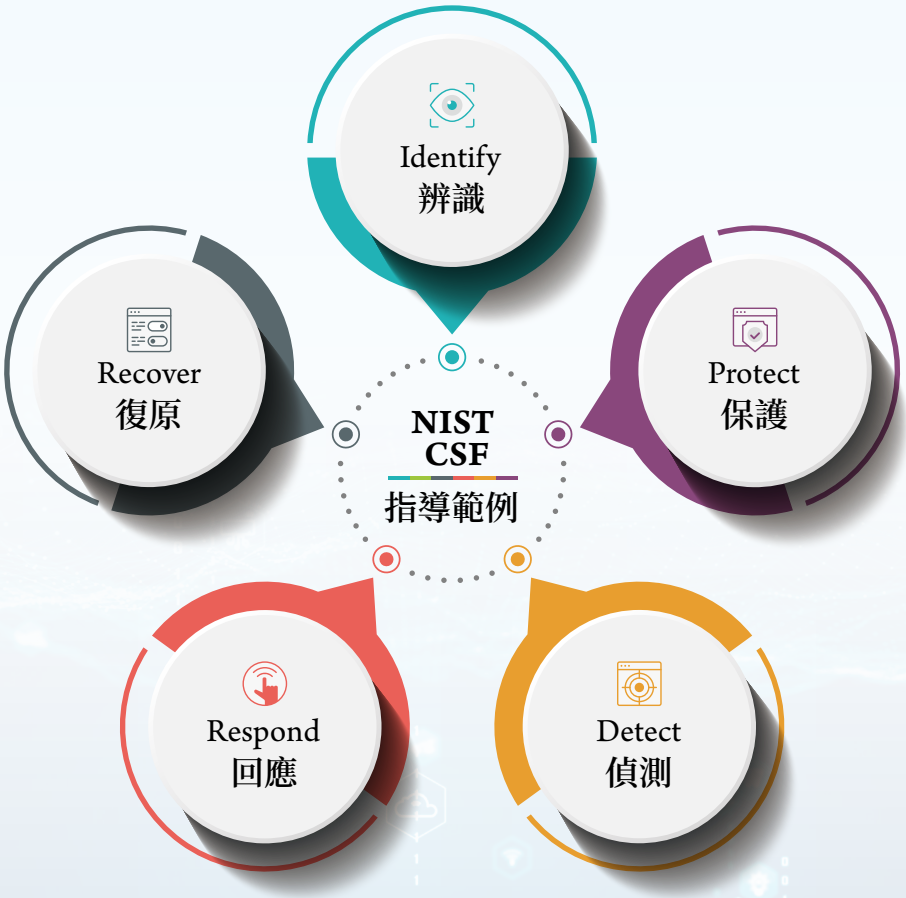


圖 1　NIST 資安框架指導範例

[1] NIST 的 CSF 為各國公部門與企業採用之資安框架，臺灣也不例外。

Safety Administration, FMCSA）在該等州發布緊急狀態，以緩解油品供應中斷問題。

美國聯邦調查局（FBI）確認此次攻擊的元凶是來自東歐的 DarkSide 駭客集團，其是銷售勒索軟體即服務（RaaS）[2] 的俄羅斯網路犯罪組織，此次攻擊除將該公司電腦系統鎖死外，DarkSide 還竊取了超過 100 GB 的企業資料。

攻擊事件導致三成加油站都無油可賣，油品供應中斷影響車輛運輸。在 Colonial Pipeline 遭駭客攻擊 5 天後，該公司依舊沒辦法完全恢復營運。為回歸正常生活，除政府發布囤積禁令外，該公司以支付 440 萬美元的比特幣贖金 [3] 方式解決。

本事件不僅成為全球頭條新聞，而且還揭示勒索軟體攻擊能演變影響到實體世界。由於 DarkSide 疑是通過利用未使用多因素身分驗證（Multi-factor Authentication, MFA）[4] 的帳戶，復以該公司系統建置於 1960 年代，資安防護效果薄弱，故駭客可輕易獲得對 Colonial Pipeline 系統的存取權限。

英國資安公司 Sophos 專家深入研究後，對勒索軟體的防範，提供以下建議：

一、分析所有端點使用者的電腦，確保它們已經安裝修補程式，並要求任何遠距存取必須採用多因素驗證及限制能存取的網段。

二、確認系統的DMZ已經與區域網路隔離，並且鎖定伺服器不得執行 PowerShell 和未經授權的二進位檔案。[5]

三、在所有電腦（尤其是伺服器）上執行進階端點保護。[6]

Colonial Pipeline 成立於 1961 年，系統建置老舊，資安防護效果薄弱，駭客有機可乘，使石油運輸管道暫停運作，嚴重影響民生運輸。（Photo Credit: Pete D, https://flic.kr/p/22b51Mc; Famartin, https://w.wiki/4qej）

[2] Ransomware-as-a-Service，係出售或出租勒索病毒。亦即，勒索軟體程式已再不需要自行開發，透過網路交易便可取得。

[3] 據報其中 230 萬美元後來被美國政府追回。

[4] 使用者要通過 2 種以上的認證後，才能得到存取控制電腦的授權。

[5] 如開源工具 RClone 等，並需儘快（不超過 5 天）安裝好所有修補程式。

[6] 最厲害的攻擊者大多都不會鎖定桌上型電腦或筆記型電腦；相反的，他們會鎖定於伺服器，因為伺服器最不可能被及時修補並執行適當的安全工具。

美國佛州一家水處理廠曾遭駭客入侵，其意圖改變飲用水中 NaOH 之添加量；皮膚若接觸未稀釋的 NaOH 會引發不適，嚴重時會造成灼傷。左圖為淨水系統示意圖，右圖為遭 NaOH 灼傷的皮膚。（Photo Credit: Blazius, https://commons.wikimedia.org/wiki/File:Sodium_hydroxide_burn.png）

四、監控所有日誌和感應器的異常活動，並追蹤警示和可疑活動，調查它們為什麼發生。[7]

五、備妥備份和災難復原計畫，以防在調查過程中若發現部分系統遭駭需要離線重整，才能及時因應。

美國佛州水處理設施遭駭事件

2021 年 2 月，駭客利用遠端桌面通訊協議（Remote Desktop Protocol, RDP）入侵佛州奧茲馬鎮（Oldsmar）內的一家水處理廠（關鍵基礎設施）的水質控制系統，試圖改變飲用水中氫氧化鈉（NaOH）的含量。[8] 值得慶幸的是，該公司值班人員適時發現，順利阻止受汙染的水流向公眾。這攻擊揭示了沒有安全遠端存取系統所面臨的風險，以及 ICS 保護措施的重要性。所幸駭客行為即時被發現，但此事已驚動白宮及聯邦調查局。

事後對該事件調查分析顯示，該廠水質控制系統密碼與該廠使用的 TeamViewer 軟體的**預設密碼疑似相同**，所以駭客利用其連上內部人員電腦，並取得該水廠操作員的存取權限，幸好，駭客作為即時被員工發現，進而取消此項作業。

這攻擊已將美國關鍵基礎設施的脆弱性暴露無遺，特別是證明了飲用水處理設施系統[9] 竟可被輕鬆地入侵。此一事件促使美國 CISA[10] 向關鍵基礎設施運營商發出警告，提醒他們使用過時之桌面共享軟體

[7] 由於伺服器不會與使用者互動，因此每個伺服器警示都可能是遭到攻擊的徵兆。

[8] 駭客將 NaOH 添加量由 100ppm 設定至 11,100ppm（超過 1 百倍）。NaOH 是種具腐蝕性的鹼液，小量使用能調整水的酸鹼度，未稀釋時則有毒，會引發眼睛、皮膚不適。

[9] 監控和數據採集系統（supervisory control and data acquisition, SCADA）。

[10] 美國國土安全部之網路安全暨基礎架構安全局（Cybersecurity and Infrastructure Security Agency, CISA），職責在於維護關鍵基礎設施安全。

全球最大肉類供應商 JBS 遭駭客攻擊，導致澳大利亞、加拿大和美國的工廠關閉，並摧毀了美國工廠近 1/5 的肉類加工能力，食品價格因此高漲。

SolarWinds 公司為美國專門研發系統、網路、基礎設施管理軟體的業者，全球客戶數為 30 萬家，包括眾多美國公部門機構。（Source: solarwinds, https://www.solarwinds.com/zh/federal-government/government-partners）

或不再提供維護之軟體（如 Windows 7）的危險。

全球最大肉品供應商遭勒索事件

全球最大的肉類供應商 JBS 遭到俄國駭客 RaaS 集團 REvil 的攻擊，導致澳大利亞、加拿大和美國的工廠關閉，並摧毀了美國工廠近 1/5 的肉類加工能力，此次攻擊事件導致北美與澳洲地區之肉品處理產線被迫中斷，食品價格高漲。

依 iThome 報導，因 JBS 有備份系統，故公司能即時恢復操作，JBS 也強調尚未有證據顯示客戶、供應鏈或員工的資料遭到危害或濫用。另據報導，該公司向攻擊者支付 1,100 萬美元的贖金，以恢復其營運能力。[11] 整起事件凸顯企業與政府機關資安系統的脆弱，駭客獅子大開口要求贖金，越來越肆無忌憚。

美國基礎設施軟體管理業者 SolarWinds 遭駭事件

2020 年 12 月，傳出美國財政部與商務部遭到國家級駭客攻擊，且與這些機構所使用的 IT 監管平臺 SolarWinds Orion 有關；美國 CISA 發布緊急指令，要求所有的聯邦機構檢查網站，立即關閉或斷開所有該平臺產品。CISA 指出，此事件為聯邦網路帶來了無法承受的安全風險。

SolarWinds 公司為美國專門研發系統／網路／基礎設施管理軟體的業者，全球客戶數為 30 萬家，包括眾多美國聯邦機構。SolarWinds 坦承安裝含漏洞版本 [12] 的

[11] JBS 美國子公司 11 月 9 日證實，為避免遭到進一步的威脅與傷害，該公司做出「艱難的決定」，已支付駭客約新臺幣 3.07 億元贖金，https://www.rti.org.tw/news/view/id/2102222。

[12] 為 2020 年 3 月到 6 月間釋出的 SolarWinds Orion Platform 2019.4 HF 5 至 2020.2.1 版本。

客戶接近 1.8 萬家。駭客藉由公司的安全漏洞滲透到客戶內部網路，並可藏匿於受害者系統長達數月之久。

勒索軟體的發展階段

RaaS 已成為新興的商業模式，因為**它允許任何人**利用漏洞並發起攻擊，它也被證明是一種**有利可圖**的商業模式；如同 Colonial Pipeline 與水廠事件，當營運中斷或遭惡意入侵時都可能危及生命。攻擊者瞭解到關鍵基礎設施組織是有利可圖的目標，他們不僅有足夠財力，且他們將不惜一切代價以恢復營運。

重要的是，許多民營食品飲料廠原始設計，從未考量到未來會連接到互聯網上，亦即沒有資安的設計；隨著數位化轉型，許多食品廠將實現製造流程自動化，這意味著與民眾切身相關的民生必需品供應將面臨到更大的安全威脅。

趨勢公司研究後得出以下結論：

一、勒索病毒是存在已久卻仍在持續演進的威脅：從 DarkSide 最近活動就能看出，今日勒索病毒在許多方面都已進化，包括更大的攻擊目標與更進階的勒索技巧。

二、勒索集團不再只滿足於將電腦鎖死，讓企業無法動彈來獲得贖金；現在，他們還會深入挖掘企業網路以找到更多獲利方法。例如，遭駭客入侵的雲端伺服器可能再經歷另外的攻擊流程，資料遭竊轉賣。已遭入侵的企業資產，在地下市場可說是暴利商品。

三、趨勢科技總監 Jon Clay 列出勒索病毒發展階段：

第 1 階段：單純只有勒索病毒。將檔案加密，留下一封勒索訊息，然後等著收錢。

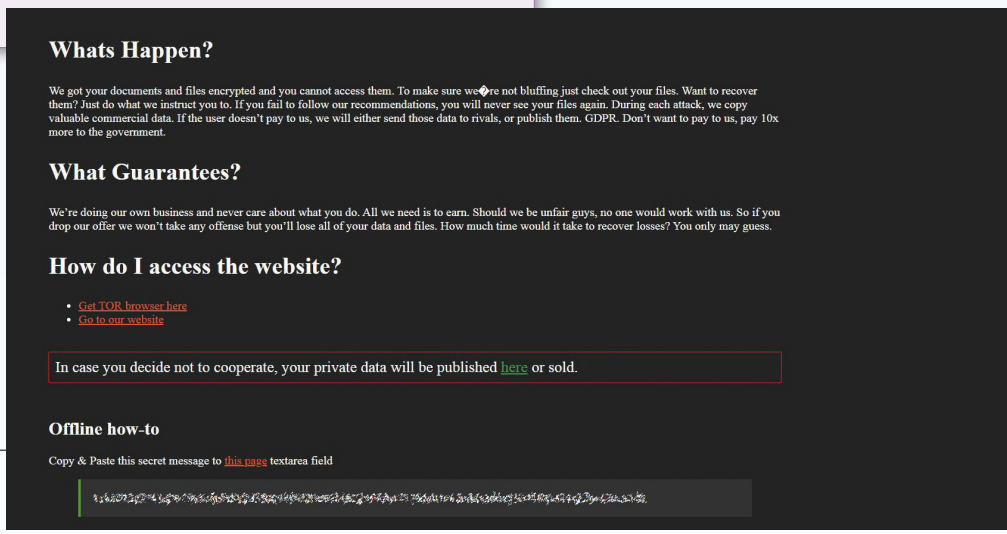
第 2 階段：雙重勒索。第 1 階段＋將資料外傳然後威脅公開資料。Maze 是第一個採用此手法的已知案例。

第 3 階段：三重勒索。第 1 階段＋第 2 階段＋ DDoS 攻擊威脅。SunCrypt、RagnarLocker 和 Avaddon 是率先採用此手法的已知案例。

第 4 階段：四重勒索。第 1 階段＋（可能搭配第 2 階段或第 3 階段）＋直接發送郵件給受害者的客戶，或者雇用電訪中心跟客戶聯繫。

未來，勒索病毒仍會不斷演進，不幸的是，有些機構迄今仍未把網路資安列在第一順位，例如有資安專家就指出 Colonial Pipeline 仍在使用含有漏洞的舊版 Microsoft Exchange，而且還存在其他漏洞。未來，一旦民生必需服務業遭駭客攻擊，將對社會各層面帶來損害，因此，確保這類服務的安全，絕對是機關與企業的優先要務。

勒索病毒第一階段就是將檔案加密，留下勒索訊息。（圖片來源：作者提供）



勒索病毒第二階段除了檔案加密外，另外留下威脅公開資料之訊息。（圖片來源：竣盟科技，https://blog.billows.com.tw/?p=476）

「供應鏈攻擊」為 2022 年新戰場

後疫情時代，預判有 2 種資安攻擊手法，除勒索軟體外，「供應鏈攻擊」亦將成為 2022 年的網路攻擊主流。

根據趨勢科技研究，「供應鏈攻擊」可歸納如次：

一、「供應鏈攻擊」是一種間接入侵單位的攻擊方式，網路犯罪分子會透過找尋與單位合作的第三方服務供應商，從中找到可以橫向至單位的攻擊路徑，這類攻擊存在於各種產業、生產製造、系統、軟體或委外服務架構中，目前常見的攻擊類型有：版本更新感染、派送脅持嫁接、程式庫感染、第三方元件感染、軟體漏洞及臭蟲等。

二、供應鏈資安有三大破口，分別發生在軟硬體供應鏈、產業垂直合作水平連結、外包維護廠商。

「供應鏈攻擊」將使得企業受害層面擴大至供應鏈上下游，造成企業面臨勒索事件發生時的危機處理更為艱困。