關鍵基礎設施之資安防護

◆ 淡江大學國際事務與戰略研究所博士候選人 ── 陳永全

俄羅斯入侵烏克蘭後，美國政府近期持續發出勒索軟體對關鍵基礎設施（CI）的攻擊警告。[1]

俄羅斯將對美國 CI 發起網路攻擊

2022 年 2 月，美國官員警告政府機構和 CI 營運商，[2] 俄羅斯可能會在對烏克蘭發動軍事攻勢的同時，對烏克蘭和美國發起網路攻擊。聯邦調查局（FBI）和國土安全部（DHS）警告執法人員、軍事人員和 CI 營運商，要特別留意俄羅斯在網路上的行動，因為他們發現俄羅斯掃描美國網路次數增加，且其製造的假訊息也越來越多。

CI 為國家命脈

CI 提供一個國家的國家安全、社會民生、經濟發展、政府運作等持續營運所需要之基本功能或各項服務，一旦遭受天然災

[1] 在俄羅斯入侵烏克蘭後，美國持續發出關鍵基礎設施的勒索軟體攻擊警告，其中包括政府、金融以及食品和農業等目標。“Feds Warn About Critical Infrastructure Ransomware Attacks, Vulnerabilities”，https://www.esecurityplanet.com/threats/critical-infrastructure-ransomware-attacks-vulnerabilities/。

[2] “FBI and DHS Warn of Russian Cyberattacks Against Critical Infrastructure”（聯邦調查局和國土安全部警告俄羅斯對關鍵基礎設施的網絡攻擊），https://www.natlawreview.com/article/fbi-and-dhs-warn-russian-cyberattacks-against-critical-infrastructure。

由於科技的快速發展及全球化的概念，使人類活動大量仰賴網路互動，舉凡政治、能源、金融、交通等均包含在內，未來如何整合串聯虛、實兩個不同的領域，對國家的穩定運作極其重要。

害、人為破壞，都可能造成政府及企業運作中斷，形成骨牌及擴大效應，衝擊經濟發展與民心士氣，甚至嚴重影響政府運作。

全球化的概念將人與人的實際接觸邁向虛擬空間的交流，舉凡政治、社會、能源、商業、物流、金融與交通運輸等，均大量仰賴網路互動。未來如何整合，串聯虛、實兩個不同的領域與世界，對國家的穩定運作極其重要。

網路攻擊事件倍數增長

2021 年統計數據顯示，勒索軟體攻擊頻率呈倍數成長，在威脅持續提升下，政府及資安業者呼籲企業組織需更強化資安機制，以避免重要關鍵基礎設施的運作系統遭癱瘓或機敏資料遭竊，同時更需強化人員的資安防護意識與技能。

2021 年網路威脅趨勢，以勒索軟體利用資安漏洞和供應鏈入侵攻擊為主，駭客趁 COVID-19 疫情，政府企業分工分流、異地或居家辦公、遠端工作等時機大舉實施。據統計，勒索軟體攻擊在 2021 年 6 月至 12 月間內飆升 93%。另據全球知名網路安全公司最新報告指出，2021 年全球的網路攻擊量創下歷史新高；[3] 臺灣受攻擊次數遠高於亞太地區平均值，每週平均被攻擊 2,644 次。[4]

[3] Check Point Software 公司的《網路攻擊趨勢：2022 年安全報告》指出，與 2020 年相比，2021 年教育／研究部門每週被攻擊次數為 1,605 次（增加 75%），緊隨其後的是政府／軍隊每週被攻擊 1,136 次（增加 47%）和通信每週被攻擊 1,079 次（增加 51%），https://www.checkpoint.com/press/2022/check-point-softwares-2022-security-report-global-cyber-pandemics-magnitude-revealed/。

[4] 《中共網軍壓境！台灣去年遭網路攻擊大增 38% 遠高亞太平均值》，https://news.ltn.com.tw/news/politics/breakingnews/3815742。

新興攻擊態樣

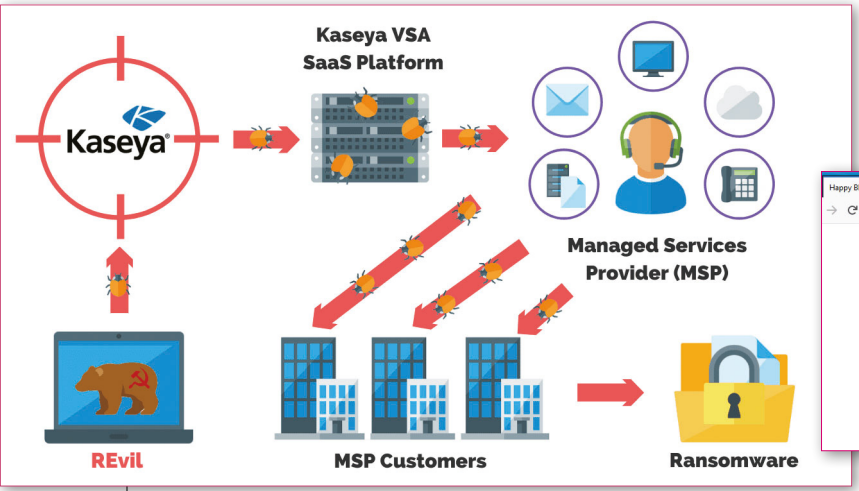
新興的勒索軟體攻擊，例如 “Triple Extortion”（三層勒索），其攻擊方式，係從企業網路中竊取機敏數據、威脅受害對象、要求付款、否則將公開發布其所竊取之機敏寶貴資訊，尤有甚之，攻擊者針對該受害組織的客戶、協力廠商、合作夥伴，亦要求給付高額贖金。

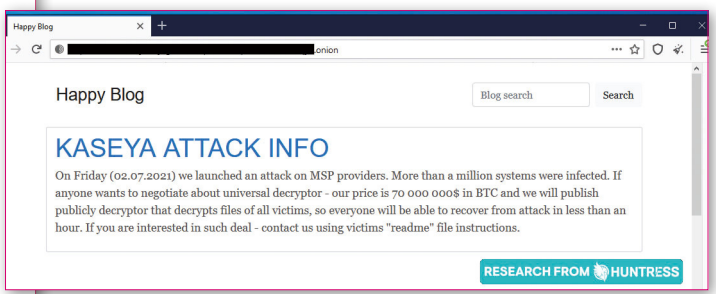
供應鏈攻擊案例，以 2021 年的 SolarWinds 攻擊最著名，其他複雜的供應鏈攻擊尚有 2021 年 4 月份的 Codcov，以及 7 月初的 Kaseya 攻擊，規模與影響均不容小覷。

另有許多惡意軟體正迅速擴展中，例如：Trickbot、Dridex、Qbot 和 IcedID 等；網路駭客正採取更具滲透力的軟體工具，使其攻擊更有威力與效力；儘管各國執法部門加強取締，但勒索軟體增長速度卻未因此而減緩。這種虛實之間的攻與防，日益變化的攻擊手段與趨勢，將對 CI 營運商造成極大的損害，需採取更嚴密的防範策略來因應。

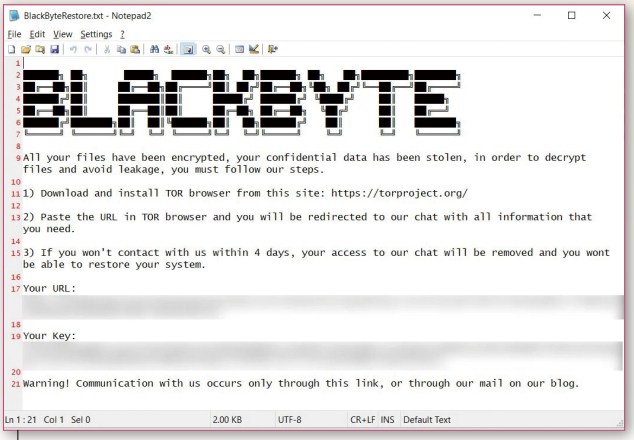
美國關鍵基礎設施頻傳遭駭客攻擊

美國聯邦調查局（FBI）發出警告，曾於 2021 年 7 月首次現身的 “Black Byte” 勒索軟體服務組織（RaaS），已再次活躍於網路世界中，截至 2022 年 3 月為止，美國至少已有三個關鍵基礎設施部門遭 Black Byte 入侵攻擊，分別是：政府部門設施、金融服務機構和食品農業設施等。此外，該組織同時鎖定全球多個企業目標，準備針對各大企業資訊安全漏洞發起攻擊行動，進而竊取並將文件加密進行勒索。

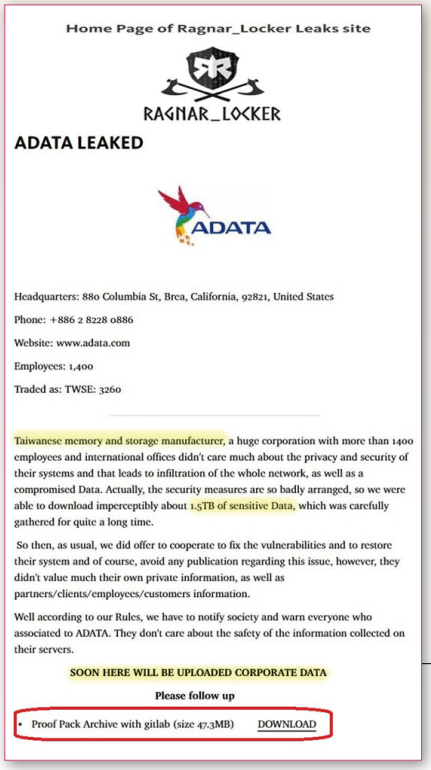




Kaseya 是一家為管理服務商（MSP）和 IT 公司提供 IT 管理軟體的公司，遭到俄國駭客團體 REvil 勒索威脅，其聲稱已感染超過 100 萬臺設備，並要求支付價值 7 千萬美元的比特幣作為贖金。（Photo Credit: PurpleSec, By Josh Allen, https://purplesec.us/kaseya-ransomware-attack-explained; Huntress, By John Hammond, https://twitter.com/_JohnHammond/status/1411868939903246338）



截至 2022 年 3 月為止，美國至少已有 3 個關鍵基礎設施部門遭 Black Byte 入侵攻擊，其同時鎖定全球多個企業目標，準備針對各大企業資訊安全漏洞發起攻擊，並竊取文件加密進行勒索。（Photo Credit: SOCRadar, https://socradar.io/who-is-the-blackbyte-ransomware-group-and-how-does-the-decryptor-works）



Ragnar Locker 在網站宣稱他們駭入 ADATA 的系統，並已盜出 1.5TB 機密資訊。（圖片來源：竣盟科技，https://blog.billows.com.tw/?p=1137）

FBI 另發現至少有 52 家橫跨十大關鍵基礎設施領域的企業組織，遭到 Ragnar Locker 勒索軟體入侵，[5] 涵蓋製造、能源、金融服務、政府及資訊科技等領域企業；可怕的是，Ragnar Locker 在執行加密過程中，電腦仍可正常執行而不會被受害者發現。[6] Ragnar Locker 2020 年曾攻擊全球第四大貨櫃船運業者—達飛海運集團公司（CMA CGM），[7] 臺灣記憶體大廠威剛公司在 2021 年也遭到 Ragnar Locker 攻擊。[8]

整合 3T 科技

當 CI 營運商為了強化自身資訊安全防護能力，布署添購多項的資訊安全監控與管理工具，例如入侵偵測防護系統、防毒軟體系統、防火牆之後，資訊系統管理人員是否就可無後顧之憂？資訊安全設備每日產出的記錄檔，少則數千筆，多則上萬筆甚至千萬筆，是否能妥切分類並且進行正確分析？統計分析完成後，是否確定哪些是相關聯的？哪些是個別的事件？又有哪些是緊急的事件需要即刻進行處置？一旦緊急事件被資訊管理人員歸納出來後，是否能夠立即確認該事件之攻擊手段？

上述問題精髓，均在於虛實環境的認識與整合，CI 營運商必須有效整合資訊科

[5] Ragnar Locker 犯罪組織主要對大型企業發動攻擊，並在加密前先行取走檔案，以迫使受害單位支付贖金。《全球第四大貨櫃船運業者 CMA CGM 遭 Ragnar Locker 勒索軟體攻擊》，https://www.ithome.com.tw/news/140261?fbclid=IwAR279_IVLDPG2hpep1aSmpucGcHfKSTsM_ma8Ibzx9Z1SyzG8RYUMGpdZ6k。

[6] FBI 除提供該勒索軟體的入侵指標（IOCs Indicator of compromise security）外，也督促受害者主動向主管機關舉報並提供相關細節以追蹤駭客，避免其他組織再度受害。

[7] https://www.cma-cgm.com/local/taiwan-agencies。

[8] 《威剛遭勒索軟體 Ragnar Locker 攻擊》，https://www.ithome.com.tw/news/144910。

技（IT, Information Technology）、操作科技（OT, Operation Technology）與通訊科技（CT, Communication Technology），再進一步結合開放式數據平臺，形成智慧企業整合架構，據以鏈結雲端資料分析應用，把設備控制層、現場管理層、企業營運層及協同商務層整合，一路貫通串接，使上下各類型資訊皆趨向透明化且能即時呈現；循此，CI 營運商便可建構出智慧型戰情監控室，採全天候、全時段、即時根據運作生產狀況，傳送資訊至雲端進行大數據分析，可迅速作出反應，確保運行順利。

CI 營運商必須有效整合 IT、OT 與 CT，再進一步結合開放式數據平臺，鏈結雲端資料分析應用，建構出智慧型戰情監控室，採全天候、全時段、即時根據運作生產狀況進行大數據分析，確保運行順利。

CI 營運商之資安防護作法

揆諸過往，有別於傳統軟體病毒攻擊都是由具備專業技術的駭客組織發起，然隨著 RaaS 勒索軟體服務這類新興組織的崛起，其背後集結來自不同專業領域的技術人員，包含開發者、測試人員及談判人員等，以專業分工團隊的型態，提供向買家出售或出租勒索病毒的服務，從中抽取佣金與租金的非法獲利，此行為被視為是促使勒索病毒攻擊迅速擴散的主因之一。

因此，CI 營運商在面對虛實的網路世界與實體世界環境中，如何落實資安防護，有效降低遭攻擊的風險，可遵循下列六點：

一、使用獨特且高強度的密碼。

二、執行多重身分驗證。

三、操作系統和軟體需保持在最新版本。

四、刪除對管理網路共享不必要的訪問。

五、使用基於主機的防火牆。

六、為搭載 Windows 系統的電腦啟用文件受保護的檢視機制。

在 IT、CT 及 OT 與設備之相依性位置圖建置版本管理、維護協力廠商緊急連絡電話等相關訊息方面，均須符合資通安全管理等相關規範。[9] 另輔以運用「政府組態基準」（Government Configuration Baseline, GCB）規範的一致性安全設定（如密碼長度、更新期限等），以降低資安風險。上述資訊在「行政院資通安全會報技術服務中心」中可獲得解答。[10]

[9] 「有效運用資安弱點通報機制」（Vulnerability Alert and Notification System, VANS），結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實資通安全管理法之資產盤點與風險評估應辦事項。

[10] 政府組態基準目的在於規範資通訊設備（如個人電腦、伺服器主機及網通設備等）的一致性安全設定（如密碼長度、更新期限等），以降低成為駭客入侵的管道，進而引發資安風險。該專區提供 GCB 說明文件、相關資源及常見問答，能協助各機關進行導入規劃與實作。https://www.nccst.nat.gov.tw/GCB。