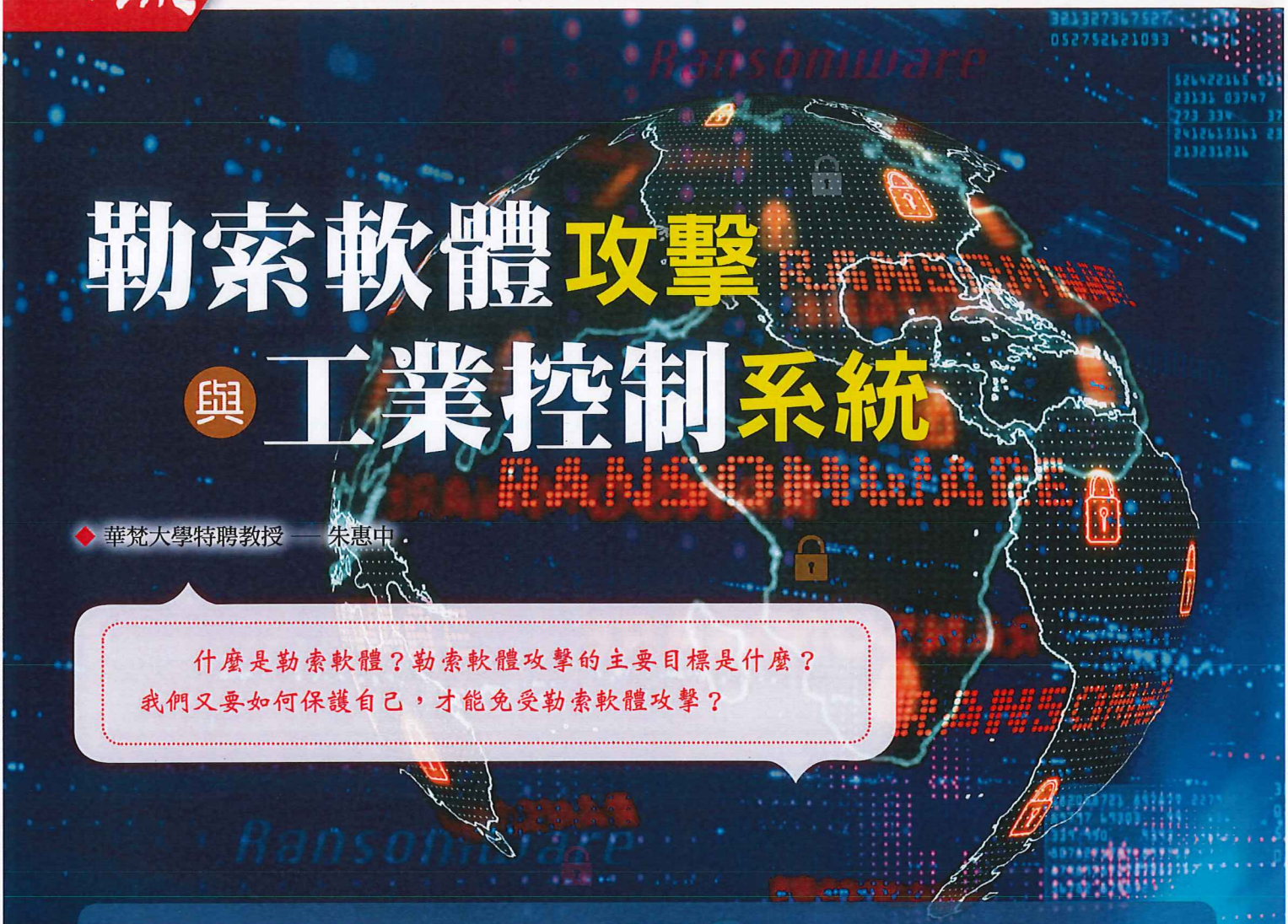


勒索軟體攻擊與工業控制系統

華梵大學特聘教授 — 朱惠中

什麼是勒索軟體？勒索軟體攻擊的主要目標是什麼？
我們又要如何保護自己，才能免受勒索軟體攻擊？

勒索軟體為 2021 年的攻擊主軸，且無趨緩跡象

過去，安全威脅通常涉及從攻擊者可用於其他犯罪（例如身分盜用）的系統中存取資訊。現在，網路犯罪分子通過將受害者的設備和數據作為人質，直接向受害者索取金錢。

自 2013 年以來，這種類型的惡意軟體攻擊（其中資訊被加密【或聲稱是】並提示受害者為恢復存取的密鑰付費）迅速增長，2021 年，勒索軟體更已為當年度四大攻擊主軸之一。本文蒐集及彙整相關資料後，從什麼是勒索軟體？為什麼要了解勒索軟體？勒索軟體攻擊的主要目標是什麼？以及我們如何保護自己免受勒索軟體攻擊等五大面向來一一介紹，以期資安從業人員，特別是關鍵基礎設施之防護者能知己知彼，百戰百勝。

此外根據 Check Point Research 的一份報告，截至 2021 年 5 月，與 2020 年初相比，全球勒索軟體攻擊激增了 102%，而且沒有放緩的跡象。該報告還發現「與 2020 年相比，2021 年上半年全球受影響的組織數量即增加了一倍多。」該報告同時亦顯示，醫療保健和關鍵基礎設施受到最多的攻擊（截至 2021 年 4 月）；亞太地區的組織遭受的攻擊最多，平均每週 51 次（與 2021 年初相比增加了 14%）；自 4 月以來，非洲組織的攻擊增幅最高（34%）。

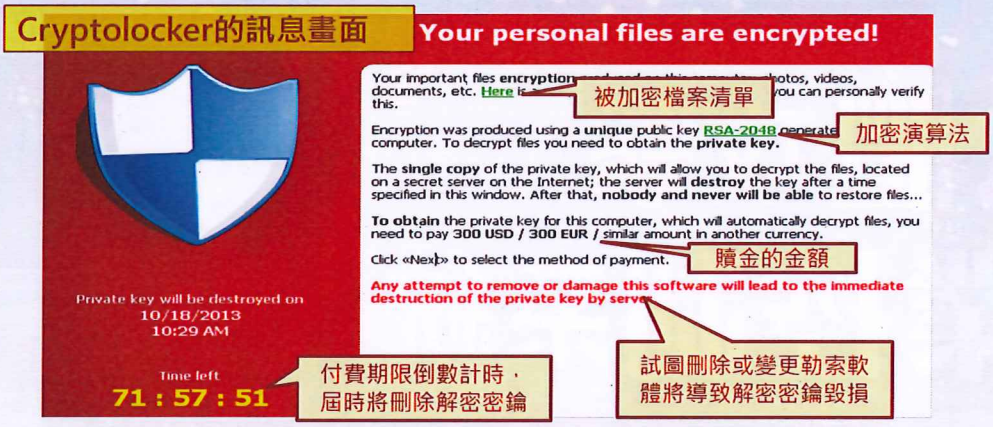


圖 1　Cryptolocker 勒索軟體的訊息畫面

從歷史上看，勒索軟體利用執法機構的形象來強迫受害者付款。這些訊息通常會顯示帶有 FBI 標誌的警告和文字訊息，表明在系統上檢測到非法文件共享，提醒用戶支付罰款或面臨刑事起訴的風險。

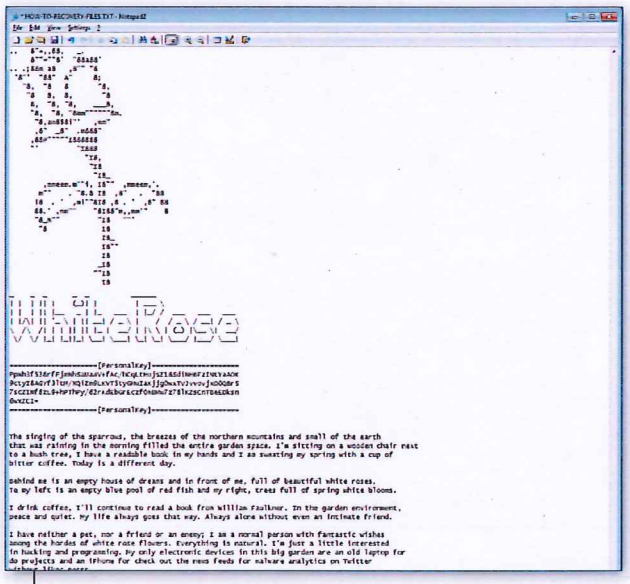
何謂勒索軟體

勒索軟體是一惡意軟體（Malware），勒索軟體係利用非對稱式加密方式，加密受害者的檔案，之後勒索軟體會顯示訊息說明如何付費以獲得解密密鑰，以便在付款後可恢復對資料的存取。攻擊者要求的贖金，費用從幾百到幾千美元不等，通常要求以加密貨幣支付，一種稱為 Cryptolocker 勒索軟體的訊息畫面如圖 1 所示。

基本上，勒索軟體是惡意軟體。駭客通常藉由比特幣或預付信用卡要求受害者付款，以重新獲得受感染設備及其內存儲數據的存取權限。

勒索軟體特徵在於持有設備控制權（因此在本地存儲數據）以獲取贖金，受害者通常以比特幣或其他虛擬貨幣支付贖金。複雜的勒索軟體攻擊採用伺服器、資料庫（原始資料及備份資料）、硬碟或文件級加密，如果不支付駭客要求的贖金，就無法存取文件及資訊，進而影響工作的運行。

隨著勒索軟體攻擊已成為公眾意識，攻擊者開始製作有效軟體，明確表明設備只是被駭客入侵，受害者必須向駭客付費才能返回存取權限。此外，某些的攻擊，例如 WhiteRose 勒索軟體，會向毫無戒心的受害者展示令人費解且幾乎沒有語法的資訊，描述了諸如「駭客坐在灌木樹旁的木椅上」、「一本可讀的書」等田園詩般的環境與「威廉 · 福克納（William Faulkner）在一個偏遠地區的花園裡」等。



WhiteRose 勒索軟體會向受害者展示令人費解且沒有語法的訊息。（Photo Credit: ComplyZoom's twitter, https://twitter.com/ComplyZoom/status/982655350804504577）

工業控制系統是工業廠房中非常重要的系統，用於監視及控制橫跨 IT 及 OT 網路的工業流程。（Photo Credit: Steag, https://commons.wikimedia.org/wiki/File:Leitstand_2.jpg）

勒索軟體的運作方式

勒索軟體攻擊通常透過文件共享網路、經網廣告活動，偽裝成惡意製作的圖像，或附加到電子郵件等方式來進行傳播。

著名的 WannaCry 為最單一勒索軟體攻擊，它利用了 Microsoft SMB 協議中的一個缺陷，使任何未做補（patch）的網路電腦易受到感染。其他攻擊亦有利用不安全的遠程桌面服務（RDP），掃描網際網路以查找易受攻擊的系統。

綜整勒索軟體的運作方式如下：

一、大部分勒索軟體植入電腦的管道為：1. 網路釣魚電子郵件、2. 系統漏洞、3. 軟體／組態更新機制。

二、勒索軟體對檔案進行加密：需要數學密鑰（KEY）才能將檔案解密。

三、畫面顯示訊息要求支付贖款（比特幣）：某些案例中，攻擊者自稱執法機構，要脅因電腦存在色情或盜版軟體而必須關閉電腦，要求支付「罰款」；另一種案例是攻擊者揚言公開受害者的敏感資訊，除非支付贖金。

RaaS（Ransomware-as-a-service）為今年最新型勒索軟體攻擊模式，RaaS 就是在軟體即服務（Software as a Service ）模型中提供勒索軟體。

為什麼要討論勒索軟體

工業控制系統（Industrial Control Systems, ICS）是水電公共設施、工廠以及其他工業廠房當中一項非常重要的系統，用於監視及控制橫跨 IT 及 OT 網路的工業流程。勒索病毒一旦駭入這些系統，就可能造成生產線數日（月）無法營運，進而會增加企業機敏資料（如設計文件、工作流程、專利及應用程式等）外洩至黑暗網路（Dark Web）的風險。

工業控制系統正面臨嚴重的資安挑戰，因為有太多安全上的漏洞，而駭客顯然也緊盯著這些漏洞。美國國土安全部已將勒索病毒的攻擊視為與恐怖主義同樣嚴

重的問題。「他山之石可以攻錯」，本文希望參考美國已有的經驗，來協助我國擁有工業廠房及生產線的企業重新調整其資安措施的焦點、人力部署與相關資源，特別是針對 IT 與 OT 融合後的環境。

勒索軟體攻擊的主要目標

雖然家庭用戶傳統上是勒索軟體的目標，但商業網路越來越成為犯罪分子的目標。此外，服務器、醫療保健和公用事業（例如，Colonial Pipeline 攻擊）亦已成為惡意勒索軟體攻擊者的重要目標。

企業通常是這些惡意軟體特別喜愛攻擊的目標，因為企業會支付較多贖金；然而，那些大企業也可能擁有強大的 IT 運營和經常做備份，故能減輕任何損害並避免支付贖金。

根據 Check 的數據，截至 2021 年，全球勒索軟體攻擊最多的行業是醫療保健，每週平均遭受到 109 次攻擊，其次是公用事業部門，有 59 次攻擊，保險／法律部門則有 34 次。

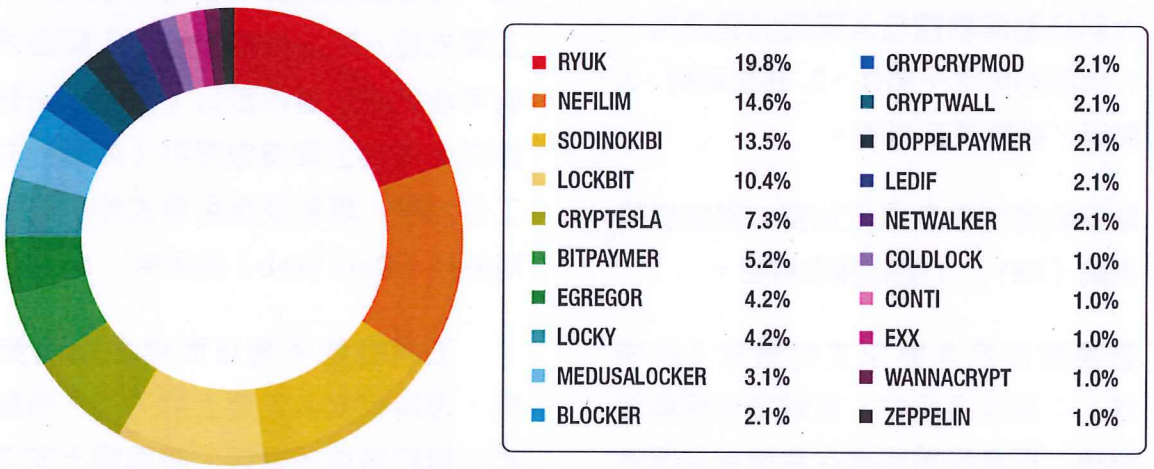
讓問題更加複雜的是，2021 年 NTT Security 的報告指稱，有高達 39% 的新世代網民願意支付勒索軟體的贖金，以便能夠繼續他們的工作，此舉將讓網路犯罪者更加肆意妄為。

常見的勒索軟體攻擊

2020 主要攻擊 ICS 的勒索病毒如圖 2 所示。

全球首次勒索軟體攻擊可以追溯到 1989 年，但第一個廣泛的加密勒索軟體攻擊 CryptoLocker 則始於 2013 年 9 月。駭客剛開始要求 CryptoLocker 的受害者必須在設定的截止日期前付款，後來駭客允許支付受害者以高價金來解密截止日期已過的資料。

圖 2　2020 主要攻擊 ICS 的勒索病毒



Source: Trend Micro, https://documents.trendmicro.com/assets/white_papers/wp-2020-report-on-threats-affecting-critical-industrial-endpoints.pdf.

Locky 是另種早期的勒索軟體，它於 2016 年 2 月首次出現，於 2016 年 12 月停止傳播，僅在 2017 年 1 月和 4 月再次短暫出現。隨著每次消失後又再度出現時，攻擊的方式更為精進。

WannaCry 攻擊於 2017 年 5 月 12 日開始，惟 3 天後即被 GCHQ（英國政府的通信總部，是一個情報和安全組織）發現及鎖住，並確定北韓朝鮮為 WannaCry 攻擊源頭，據估計 WannaCry 攻擊使英國 NHS 損失了近 1 億英鎊。

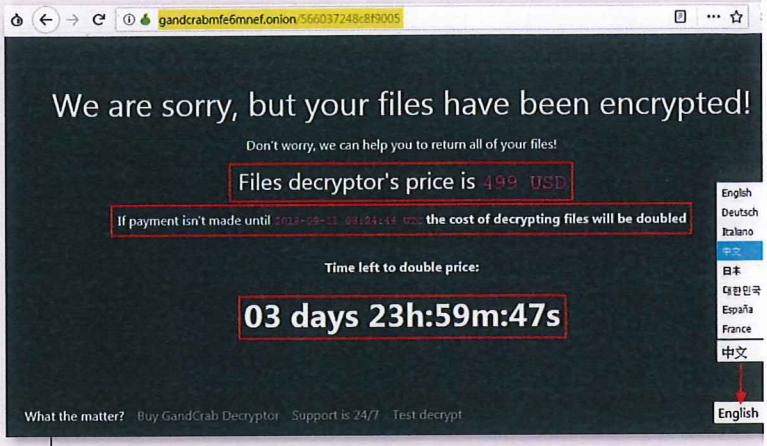
Petya，也稱為 GoldenEye，於 2016 年 3 月首次通過受感染的電子郵件附件傳播；與其他勒索軟體攻擊一樣，它要求以比特幣支付贖金。

2017 年 10 月，Bad Rabbit 開始針對俄羅斯和烏克蘭網民攻擊，並通過企業網絡傳播，影響到德國、南韓和波蘭民眾。

2018 年 1 月發現 GandCrab 勒索軟體，並在 4 月檢測到增強版。GandCrab 主要通過網絡釣魚電子郵件以及 Internet Explorer、Adobe Flash Player 和 VBScript 中的漏洞傳播。

2018 年 3 月，美國亞特蘭大市的電腦網路受到 SamSam 勒索軟體的攻擊，該市預計要支付 260 萬美元才能恢復。

2021 年 5 月 6 日，美國東海岸最大的燃料供應商 Colonial Pipeline 公司遭到勒索軟體攻擊。該公司被迫關閉了部分系統，



GandCrab 勒索軟體主要通過網絡釣魚電子郵件以及 Internet Explorer、Adobe Flash Player 和 VBScript 中的漏洞傳播。（資料來源：臺灣學術網路危機處理中心，https://portal.cert.tanet.edu.tw/docs/pdf/20180926020928283222333270103170.pdf）

暫停運營燃料（包括天然氣、取暖油和汽車用油），造成民眾生活極為不便。

綜上所述，IT 資安與 OT 團隊之間的合作刻不容緩，並應共同盤點如關鍵作業系統相容性及運轉率要求等需求，以便擬定一套更有效的資安策略。

國際知名資安公司之防範建議

綜整如 Trend Micro、Check Point 公司之防範建議如下：

一、應用 IEC62443 4-2/3-3 所揭示的原則，儘速修補、更新終端設備或應用系統至為重要。

二、企業可採用應用程式控管軟體來澈底杜絕駭客入侵時會植入的勒索病毒，此外也可利用威脅偵測及回應工具，透過入侵指標（IoCs）進行清查。

三、管制網路共用資料夾，強制使用高強度的帳號密碼來防止帳號遭暴力登入。

四、採用入侵防護（IDS 或 IPS）來建立正常網路活動的基準數據，如此有助於偵測可疑活動。

五、使用獨立的工具來掃描獨立非連網環境的 ICS 端點。

六、設置專門用來掃描 USB 惡意程式的工作站來檢查所有在獨立非連網端點之間傳輸資料的隨身碟。

七、採取最低授權原則來管制 OT 網路系統管理員與操作人員的帳號。

八、留意木馬程式攻擊，因勒索軟體攻擊通常始於木馬病毒，資訊人員應提防知名木馬如 Trickbot、Emotet、Dridex 等。

九、假日和節日更應提高警覺，很多攻擊發生在較少資訊人員值班的週末和節日。

十、使用反勒索軟體解決方案，可考慮採用具有恢復功能的反勒索軟體解決方案，感染後較快恢復營運。

十一、教育員工辨識惡意電子郵件，許多攻擊始於針對性網路釣魚電子郵件。

勒索軟體未來趨勢與影響

一、專門瞄準工業廠房及生產線的勒索病毒攻擊，正帶來日益升高的當機與機敏資料外洩風險。例如：近年臺廠常遭勒索病毒攻擊，如工業電腦大廠之研華電腦公司。

二、一些存在已久的惡意程式，如：Autorun、Gamarue 和 Palevo 仍會不斷地經由隨身碟在 IT/OT 網路之間散布。

三、製造業者仍會是勒索軟體者的攻擊目標：有鑑於製造業之勒索案件將持續增加，權責機關更應廣加宣傳與進行教育課程。

表 1　近年臺廠遭駭情形

時間	事件
2018/08	●台積電更新機臺遭勒索病毒入侵，損失近 26 億。
2020/05	●中油遭勒索病毒入侵，加油站無法使用部分支付工具。 ●台塑遭檔案病毒入侵，部分辦公室電腦中毒。 ●力成遭勒索病毒入侵，3 廠區緊急關機，損失有限。
2020/06	●欣興遭勒索病毒入侵，部分設備及出貨系統停擺。
2020/07	●台灣國際航電（Garmin）遭勒索病毒入侵，線上服務被迫中斷。
2020/12	●鴻海墨西哥廠遭勒索病毒入侵，索價約 10 億臺幣，經作業系統安全性更新，對營運影響不大。
2021/03	●宏碁遭駭客入侵，勒索 5 千萬美元（約 14 億臺幣）；宏碁未付款，資料也未外洩。
2021/04	●廣達遭駭客入侵，勒索 5 千萬美元（約 14 億臺幣）；廣達稱全面提升資安等級，營運未受影響。

資料來源：自由時報，https://ec.ltn.com.tw/article/paper/1444465。