

Summary of the incident

根據洛杉磯時報報導 [1]，2016 年二月五號，Hollywood Presbyterian Medical Center 的醫院資訊系統遭到一款稱作 Locky 的勒索軟體將所有的資料加密。事發當下，門診、病房所有的電腦都無法從醫院資訊系統取得病人資訊，包括影像資料、開藥處方、診斷，因而嚴重影響看診進度，並迫使門診醫師改用紙筆紀錄病歷，所有醫令也只能透過人工傳送。影響最重的莫過於手術室，當天準備接受手術的病患無法按時進到手術室內，因為外科醫師無法於上刀前透過電腦影像規劃術式，當然也無法執行手術。在不到一個禮拜的時間，院方對外宣布已經透過 bitcoin 系統支付 17,000 USD 給駭客以重新取回資料，並已向洛杉磯警方報案，FBI 也已經介入調查。然而警方也承認很難透過 bitcoin 和現有資訊追蹤到駭客的身分。

Impact or implications on modern network security

近年來，駭客將系統檔案加密再來勒索一定金額的 bitcoin 成為一種主流，駭客透過網路系統從遠方在目標系統上針對系統弱點進行攻擊，並執行特定程式碼將所有檔案加密。網際網路代表者個人使用者可以方便地連結全世界的資料，但也意味有心人示可以透過網路到達所有連接上網路並開放特定 ports 的電腦。電腦系統總是會有某些漏洞，比如說 system applications 的 bugs，就可以成為駭客的工具來侵入電腦系統，尤其在許多不再被支援的作業系統，更是容易成為攻擊目標，這個月的 WannaCry 事件也有類似的性質，在 Windows 不再支援的 XP、Vista 等作業系統災情尤其嚴重，而 bitcoin 高度隱私的特性讓 bitcoin 成為駭客勒索的重要支付管道。

Reflection

上課老師提到了未來在 IoT 的時代，security 的重要性不言而喻，尤其當人類高度仰賴電腦系統，反而容易因為系統遭受入侵而帶來更多的風險。醫療體系向來是駭客入侵的一大喜好，主要有以下幾點原因 [2]。首先是醫療體系是一項龐大的盈利事業，不需要駭客都知道要勒索要針對有錢的對象才有獲利，然而有錢，許多產業都有錢，一個更重要的原因是，醫療產業與生命迫切相關，當一個醫療體系無法立即提供醫療服務，最直接的影響就是病患的死亡，醫療的急迫性讓醫院系統在遭受駭客入侵往往只能選擇投降付款。另外，醫療體系本身的資訊系統並不如其他產業容易更新，而資訊相關人才也未必齊全，一旦架設好的資料庫和作業系統上機，就是一路沿用，不再進行太大的更動，畢竟醫院資訊系統是隨時都需要 online 提供服務，無法容許片刻的停機維修。種種特性造成醫療產業容易遭受攻擊，因此在這個月的 WannaCry 事件，英國也有某間醫院遭受池魚之殃。

References

1. [Hollywood hospital pays \\$17,000 in bitcoin to hackers; FBI investigating](#)
2. [Why Hospitals Are the Perfect Targets for Ransomware ?](#)