【解牛集】

網絡風險管理「迫埋身」

許佳龍

科大資訊、商業統計及營運學系教授

繼 WannaCry 之後，一隻名為 Petrwrap 的病毒上周首先在歐洲發動攻擊，進行勒索。一批報稱受勒索軟件攻擊的公司，包括總部設於倫敦的全球最大廣告公司 WPP、烏克蘭國有能源公司及基輔主要機場等飽受蹂躪。有防毒軟件專家指出，今次勒索軟件所利用的程式漏洞，跟 WannaCry 用的一樣，他形容 Petrwrap 是 WannaCry 變種。

當「欲哭之聲」稍告靜下來之際，Petrwrap 又接踵而來。很明顯，電腦犯罪，尤其勒索軟件肆虐所帶來的問題，網絡犯罪對我們生活的衝擊、對社會造成潛在的破壞，大家有需要及早認識，並作出必要的防範。今日，互聯網應用愈來愈廣泛，並與我們很多日常活動緊扣一起，故無論是機構或個人，面對的風險也愈來愈高，因此，對於網絡的風險管理，防患於未然，是一個「貼身」的問題。

利用加密技術犯案

可以預見，網上軟件勒索的犯罪行為將會愈來愈流行。繼 WannaCry 後，如今又有 Petrwrap，用戶中招後，若交不出贖金，手機裡所有文件都會被刪除。

細心觀察，早期的網上勒索，黑客多利用「分散式阻斷服務攻擊」（distributed denial-of-service attack， DDoS）犯案。針對的對象多為大機構或支援交易的公司。因為只要令到攻擊對象的網站無法運作，就可成為勒索的籌碼，使這些企業或網站就範。如今隨著互聯網技術的進步，今天犯案人會利用加密的方式進行勒索，因為加密勒索可針對的對象更為廣泛。

WannaCry 的作案手法其實很簡單，透過一些途徑，如電腦病毒，或用戶不小心下載一些惡意程式——這程式其實就是加密程式，一進入電腦後，便把電腦上所有檔案加密，使用戶無法開啟，被迫要付出贖金取得解碼。真是「傷心欲淚」。

如何保護電腦安全，避免受襲，筆者與資訊科技界的朋友交流，他們都會提議，謹記安裝防毒軟件、避免開啟可疑電郵附件及網頁連結、定時更新電腦系統，以及作檔案備份。然而，這些防範措施，如更新電腦系統，一般人都會做，筆者認為，此舉其實很被動，也不足夠。

檔案備份防「毒侵」不足夠

無可否認，錯手或不小心點擊了一些連結也相當普遍，尤其在網上瀏覽影片時，「手快快」點擊，結果讓「有毒軟件」長驅直入。另一種普遍情況是，當我們看到一些好像與自己相關的電郵時，禁不住開啟，一旦啟動了當中的附件，便告馬上「中毒」。所以，即使定期更新電腦系統，「防毒」措施並不足夠。

在檔案備份方面，一般人以為備份了便有足夠安全，但看深一層，如今用戶往往依賴在雲端系統進行備份。這又衍生出一個問題，這些勒索軟件運作的模式，並非把用戶的電腦完全鎖死，只是把電腦上所有的檔案加密。當用戶電腦上的檔案已被加密，則無論是同步或定時上載到雲端系統的原檔案，即會被「更新版本」（已遭加密）的檔案所取代，結果也遭到加密，用戶也無法開啟。若不付出贖金取得解碼，還是無法解決問題。

對於這種弊端，個別雲端系統供應商有一些應對建議。如 Dropbox 提供一個三十日或更長的存檔備份服務，用戶可以在 Dropbox 下載回三十日內之前上載的原檔案。這無疑有助解決備份一些不足的缺點，但畢竟並非人人都採用這種相對高昂的付費服務。退一步說，即使肯付款買一個「網絡保險」，黑客日後也有可能會採取一些攻擊策略，令已遭入侵的客戶不能輕易取回原來的備受檔案(例如在一段長時間內逐步地加密個別的電腦檔案)。所謂「道高一尺，魔高一丈」。

生活「數碼化」的網絡風險

其中一個最好的方法，包括資訊業界的朋友都有建議，就是進行離線備份，並把這些檔案與互聯網「絕緣」，有需要時才用來應急。雖然，離線備份對一般個人用戶或可以做到，但企業或大機構用戶便會有困難，因為其電腦運作系統會相對複雜，要求它們長期保留一套離線備份，而又需要時常定期更新，委實有困難，而且成本也不菲。

回到現實，面對資訊科技日新月異，互聯網的發展一日千里， 今日，我們每個人的生活和行為活動，都離不開網絡，需要電腦的支援。事實上，我們必須意識到，我們已把自己的生活「數碼化」，與電腦世界交融在一起。十多年前，這

個問題可能並不如今日那麼嚴重，因為當時使用電腦，很多集中在商業交易上。因此，即使電腦被鎖死，或用戶的網站遭入侵，不能運作，充其量是損失一、兩周的交易凍結、或網站無法正常運行，僅此而已，對於個人的人身安全，還沒有大問題。

然而，今時不同往日，隨著電腦科技愈來愈廣泛利用，黑客作案的影響範圍亦已溢出商業交易領域，並且滲入到個人的人身安危層面。譬如醫院。在香港的醫療領域有一個電子醫療紀錄互通系統，無論是公立或私人執業的醫生，均可透過電子醫療紀錄，馬上掌握到病人的病歷，為病者作出及時疹治。若在緊急治療情況下，一旦醫院的電腦系統遭加密勒索，病人得不到及時對症下藥治療，必然危及病者的生命安全，因此，醫院往往別無選擇，唯有付出贖金。

整體安全更為重要

除了醫院，還有電力公司、公共交通運輸系統，都是黑客攻擊的高危對象，尤其醫院，更是常見的攻擊目標，美國便曾有多起例子。很明顯，目前犯案的黑客十分聰明，他們不僅懂得找勒索對象，得手後，所開出的解密贖金金額，也不會「獅子大開口」，索取天文數字款項，他們一般會開出一個受害人可以承擔、可以忍痛付款的金額水平。

由此來看，就算離線備份亦只可以保護「檔案資料」的安全性，更重要一點是，我們需要以更寬闊的目光，考慮到備份的整體作業模式，亦即想及公司的運作，如果沒有互聯網，還可以維持基本的運作嗎？例如醫院，一旦沒有互聯網，是否仍然可以維持基本的功能，包括手術可以照常進行，藥物配給也可以如常配送。筆者認為，當下，無論個人和機構的生活與行為，很多都和電腦網絡融匯一起，因而這個網絡風險問題就必須有所思考、有所警惕和有所應對。除了醫院，那些管理重要基礎設施的機構，都應該有如此的思維。當短暫沒有互聯網時，有沒有一個應對的方案，能夠提供基本的服務，設立了一個備份的作業系統。例如，地鐵可以如常提供服務，電力繼續供應如常。

物聯網下的個人安全

再看今日很多人都在講「物聯網」，即我們身邊的很多事物，都會被接駁上互聯網。除了電腦，還有電視、微波爐、冷氣機，甚至患有心臟毛病的人內置到身體裡的心臟起搏器等。事實上，今日電子醫療愈來愈普及，不少初創公司正密鑼緊鼓，加快研發透過把一些個人身邊的「事物」，將個人的身體健康狀況，直接與醫生緊密連繫起來，從而提高個人保健醫療的效率。這些產品不少已在準備進入市場階段之中。很清楚看到，今日互聯網的影響力無遠弗屆，也愈來愈

大，我們面對的風險也愈高。

從黑客的勒索軟件犯案，我們從中窺察到，網絡的安全，不僅僅是警惕黑客的攻擊和勒索，還應看到互聯網應用愈來愈廣泛，對個人和機構用戶所帶來的風險管理問題。

必須重視網絡風險管理

對個人來說，離線備份基本上可以起到保護電腦資料安全的作用，但一些日常生活重要的活動，若然是透過物聯網上的設施進行，便需要好好想一下，當沒有這網絡時，自己的生活會否受到衝擊和損害，要有防範未然的思想和對應方案的準備。

對企業來說，把檔案資料離線備份，有助保護這些資料的安全，但更重要的是，企業或機構本身，必須考慮到整體作業的安全，尤其是一些醫療和重要公共機構，一旦暫時沒有互聯網，基本操作是否還可以如常持續，因而一個整體作業備份系統，即使要付出成本，企業或機構還是值得作出「兩手準備」。

事實上，機構或企業透過互聯網，節省了不少操作上的交易成本，使利潤額得到擴大，盈利率提高，故其管理高層也不應該只想到從互聯網中得益，而完全不付出一分一毫代價。從這個角度看，從利潤中撥出部分資源，作為支援這個後備系統的設立、維繫和更新，是合理的政策選擇，尤其提供廣泛影響社會公眾的基礎設施，設立後備運作系統的費用和成本，完全值得付出，而且更是風險管理不可或缺的部分。