緊急處理加密勒索軟體威脅 7 原則

現在的加密綁架軟體很可惡！會向受害者勒索金錢，並限時 3 天內付贖金，甚至要求以虛擬貨幣比特幣付款，才能得到可解開加密檔案的私鑰，否則，銷毀私鑰讓受害者再也沒有機會救回檔案

文/羅正漢 | 2015-12-19 發表

現階段，大多數的加密勒索軟體都是透過釣魚郵件入侵，若使用者風險意識不夠，就很可能受害，導致檔案無法存取。

從大多數的加密勒索病毒的執行過程來看，一般都是會向遠端遙控 C&C 主機取得加密金鑰，再暗中加密受害電腦中的檔案，像是先使用 AES 加密檔案，再用非對稱金鑰 RSA 加密來將 AES 金鑰加密，且金鑰長度是 2048 位元，使用戶難以用暴力方式解開加密，因為即便用超級電腦，都要運算個好幾年才能達到目的。

當用戶電腦中的重要檔案，像是 Word、Excel、PowerPoint、PDF、JPG 檔，等近百種常見檔案格式，都被惡意加密後。加密勒索病毒就會跳出要求付贖金的勒索訊息，並限期在很短時間內（像是 3 天）就要給付，否則銷毀金鑰，讓用戶再也無法解開檔案。同時，勒索給付方式上，為了更隱匿蹤跡，會要求以比特幣等金流機制來給付，才能取得解密金鑰。

當使用者看到勒索訊息時，同時也會發現，無法開啟被加密的檔案，文字檔即便開啟，也會是亂碼顯示。而且，新的變種加密勒索軟體，甚至連檔案名稱也能加密，這將使用戶無法分辨哪些檔案無法使用，可能更影響使用者心理狀態，讓用戶焦慮而順從付款。

CryptoWall 是 2015 年最著名的加密勒索軟體

在被害用戶的電腦上，看到螢幕上自動跳出的勒索訊息才知道受害，但這時電腦裡的檔案都被加密，無法正常開啟，而且還是採用超高等級的 2048 位元加密技術，用超級電腦都要花上不少時間才能解開，因此檔案都無法再開啟使用。

加密勒索緊急應變之道

遭受加密勒索軟體入侵後，真的沒有辦法破解嗎？是的，大部分的加密勒索軟體，若都是經由 2,048 位元 RSA 和 AES 加密，幾乎已經不可能自行暴力破解救回檔案。

另一方面，從防毒廠商趨勢的統計資料看出，中小企業為受害對象的比例明顯增加，一旦中小企業真的面臨這種加密勒索威脅時，該如何面對與解決呢？

處置準則 1 中斷網路連線

最近，網路上有不少人詢問，中了勒索軟體該怎麼辦的訊息。防毒廠商趨勢、賽門鐵克等專家的建議都是，先中斷該臺電腦的網路連線，避免災情可能擴大，這是最簡單易做的處理方式，雖然大多數使用者意識到被加密勒索軟體綁

架時，通常災害也已經發生了，但將受害主機隔離這個步驟，仍是不可少的首要處置動作。

檔案無法使用，用戶心急是一定的，公司負責 IT 相關工作的人員，可以先嘗試了解當事人使用情況，像是是否點選可疑的電子郵件，瀏覽了哪些網站，即便使用者不太記得，但也算是多一些參考的資訊。請記得，溝通需要多點耐性，並安撫受駭電腦的使用者，而不是一味指責。

處置準則 2 即刻發現，應立馬關機

若是使用者能夠即時發現，自己電腦中的檔案正在被惡意程式加密，達友科技林皇興表示，這時首要的動作是關機，立刻持續按壓電源鍵，強迫電腦進行關機動作。之後可將該臺電腦的硬碟取出，透過外接方式將其中的未被加密的檔案保存下來。他們也實際這麼做過，結果成功防止其他檔案繼續被加密。但也要提醒大家的是，過程中千萬不能去點選那些已經被加密的受害檔案。

處置準則 3 緊急宣導、清查不可少

就這次我們訪問的防毒、資安廠商等，在他們所接觸到的例子中，大多數加密勒索病毒的感染途徑，都是經由釣魚郵件入侵。

因此，在狀況發生的當下，負責 IT 相關的人員也要立即跟其他部門或同事宣導，提升大家的警覺性，並一一檢視各臺電腦是否也有受害，並通知所有同仁有狀況立即回報。

甚至，IT 人員自行寄送可疑郵件的測試方式，了解是否還有同事沒有提高警覺，以便能針對進行教育訓練，像是教導他們可疑郵件的分辨方式，提醒不要亂點標題聳動的信件，避免點入可疑連結，內文中有亂碼顯示的要特別注意，應多仔細檢查郵件內容。

處置準則 4 評估災情

評估災情是相當必要的一點，知道哪些資料被加密了，才能了解企業損失範圍與嚴重性，同時也要清查這些檔案是否有備份，是否能夠將檔案復原。

萬幸的是，現在也有一些防毒、網路與資安等廠商，例如卡巴斯基、Cisco、Bitdefender 與 Fireeye，已經針對加密勒索軟體推出解密工具與網站，像是中了 CoinVault、Bitcryptor、TeslaCrypt、Linux.Encoder.1 與 CryptoLocker 的受害用戶，就有機會能將檔案解密。儘管，這些工具並不一定保證可以復原檔案，但總是多個機會。然而，要注意的是，也不要病急亂投醫，找到假的解密網站，使用戶再次受害。

處置準則 5 系統重灌，但軟體防護要更注意

若是災情不大，沒有太多重要檔案被加密，或是都有安全備份可以將檔案復原，僅有部分資料需重建，此時，多半使用者會選擇將被感染的電腦硬碟格式化，重灌系統，讓電腦回復成乾淨的原始狀態。

然而，最好在重灌前，也清查受害電腦本身的預防措施，像是 Windows 作業系統是否安裝更新程式，是否安裝防毒軟體，防毒軟體的防護功能是否全部都開啟。因為，除了已知病毒的防護，還要提升未知病毒與最新攻擊的防護力。而且，多數企業防毒軟體在預設上，通常不會將功能全開，主要是這會影響效能，雖然這樣提供使用者選擇的彈性，但無形中也產升一些風險，因為並不是每個用戶能自己衡量並注意。其他還需要留意的像是 Java、Adobe Flash、IE 瀏覽器等，有沒有更新到最新版本。

這有助於了解受害當時電腦本身的風險與狀態，也期望避免該電腦與其他公司電腦，因為同樣的漏洞而再感染。

處置準則 6 保存現場狀況，請求支援

如果想找防毒、資安專家進一步協助，他們也都有提供產品的售後服務，請他們協助了解受害情況也是一種方式。同時，記得也要保存一臺受害主機，以便提供分析環境。

至於是否需要留下當成證據，期待未來能夠成為求償的物證，目前並沒有很好的答案，因為勒索軟體的犯罪偵查有其專業及複雜性，對於一般企業似乎難有即刻的效益。

不過，像是國外 FBI 探員也曾表示，他們也很希望能收集勒索詐騙的訊息，並希望能夠及時了解這些詐騙的不斷發展。國內負責電腦犯罪的相關單位，則是刑事警察局偵九隊。

處置準則 7 沒有辦法中的辦法：付贖金

該不該付贖金，是讓多數受害用戶兩難的問題。基本上，各方面專家的回答都是不建議的，因為這將助長犯罪，更讓惡意駭客為所欲為。

但實際上，企業若是評估災情後，發現影響甚大，有許多重要文件損失，在沒有任何有效辦法的情形下，若只要花不多的金錢就有機會取回，使用者很可能就會買單。但要注意的是，付了款，不一定就能拿到解密金鑰。

在現實生活中，勒索行為已經觸及刑法範疇，只是，網路勒索犯罪都是跨國的事件，加上匿蹤手段高，難以追查，多數人的普遍認知，也都了解這種加密勒索難以追查、破解，因此普遍專家也都沒有針對報警、備案一事給出明確回應，即便美國 FBI 探員也在有提及，花錢消災是解密資料的最快方法。這也顯示加密勒索威脅的惡劣，需艱難面對。

另外，依據臺灣金融機關的規定，遭遇資通安全事件時，金融機構需有通報的動作，告知上級主管機關金管會，但大多數機關單位則沒有這樣的要求。通常只能求助於資安或防毒公司。

若真的沒有辦法，若使用者真的需要購買比特幣支付贖金，其實，臺灣現在遍布全國的全家便利商店的 FamiPort，就與提供比特幣交易服務的 BitoEX 合作，在這種尷尬的情境下，這樣的便利性也不知道是好還是不好。

附帶一提的是，根據調查，初期勒索的金額平均約是 372 元（12 美元）左右，而目前一把解密金鑰的基本價格，已將近 18,600 元（600 美元）。

使用比特幣付贖金，是近年勒索軟體的手段

依加密勒索軟體要求買比特幣付贖金，真的是沒有辦法中的辦法。如果你真的決定要那麼做，購買管道已經有，利用遍布全國的全家便利商店 FamiPort 機臺，選擇繳費、虛擬帳號，輸入 BTC 或 BitoEX 代號，之後依循步驟輸入，就能列印繳費單購買，之後只要接收手機簡訊，依步驟線上兌換 Bitcoin。

搶救只是權宜之計，預防更加重要

當然，普遍中小企業可能受至於人力、成本與規模，無法像大公司能夠導入或規畫完整的資安防護，絕大多數都處於有狀況才對應，也只能進行部分對應，或者是安全機制管理規則或方針，雖然已經決定，卻不知是否確實施行。

對勒索攻擊來說，企業是非常吸引人的攻擊目標。不論企業規模大小，如果沒有相應的安全措施，曝險程度高。而且，加密勒索也只是所有資安的一部份，中小企業至少要能做到基本該做的，像是面對加密勒索威脅時，人員資安意識、軟體系統更新，以及檔案備份，就是很重要的三大步驟，尤其是安全備份這一塊，才能降低加密勒索的風險。面對加密勒索軟體不斷更新、進化，使用者勢必要提高警覺，才不會讓工作成果付之一炬。

以加密對付加密勒索軟體

若是企業已導入以虛擬加密磁區防護形式的檔案加密防護系統，面對這種加密勒索軟體威脅時，也有可能因此免疫，雖然這不是這類系統的主要功能，但也剛好能避免重要檔案被加密。

像是我們問到華鉅科技的 VES 虛擬加密系統，以及優碩資訊的 VDP 虛擬磁區保護機制，由於對應虛擬磁碟機中的檔案能不被勒索軟體加密，算是備份之外，另一種能帶來效果的方式。當然，若虛擬加密軟體更進化，增加對各種虛擬加密磁碟的運行方式來攻擊，那就難說了。

加密勒索軟體真的沒救嗎？

已經有廠商提供解密工具