

勒索病毒的防範

最後更新日期：2017/11/28

[勒索病毒](#) [比特幣](#)



自2017年5月份全球發生大規模勒索病毒軟體攻擊後，勒索病毒成為全球關注的網路安全焦點之一，連美國權威辭典—韋氏辭典近期還增加了「勒索軟體」(ransomware)這個新字。這起大規模的全球勒索病毒事件主角 wannacry，當時攻擊了包括英國、俄羅斯、印度、中國等超過 100 個國家，全球數十萬臺電腦遭受到攻擊。根據媒體報導，臺灣災情並不嚴重，但仍有不少學校以及電力公司的電腦受到感染。

勒索病毒如何勒索？

勒索病毒是一種惡意程式，其散播途徑與一般惡意程式或電腦病毒一樣，一旦感染，它會鎖住受害者的電腦，或者將受害者電腦的硬碟資料加密，進一步要求受害者繳交贖金後，才能夠取回對電腦的控制權或者將硬碟加密解開。以 wannacry 勒索病毒為例，駭客要求的贖金為價值約 300 美元的比特幣。某些勒索軟體會依受害者支付贖金的時間增減贖金，通常越晚支付則贖金的金額會越高；也有些狀況是，即便受害者支付了贖金，電腦也沒有因此被解鎖。

勒索病毒可能帶來嚴重衝擊

近期的勒索病毒發展趨勢是，其攻擊目標逐漸從電腦轉向智慧型手機或其他行動裝置，勒索病毒偽裝成合法 Apps 被使用者下載與安裝後，進而取得手機的控制權。大部分的勒索病毒感染途徑是釣魚電子郵件，當使用者不小心點選釣魚郵件內的超連結，就會開始下載勒索病毒程式；或者是開啟釣魚郵件中的附夾檔案，附夾檔案本身就是惡意程式。這些惡意程式會利用電腦系統漏洞，進一步加密電腦內的各式檔案。英國的國家醫療保健服務就曾經因為遭到勒索病毒的攻擊，影響醫院看診和手術，最後被迫停止門診和取消預約，嚴重影響病人的權益，甚至危害生命安全。

要如何避免資料被綁架？

防範勒索軟體的方式與防範任何惡意程式的方式一樣，平常使用電腦網路的時候應謹慎，以下 5 項由美國消費者報告所歸納的提醒事項，可以讓你降低遭受到勒索病毒侵害的機會：

1. 不輕易點選email內的超連結，如果真的有必要，建議直接在瀏覽器中輸入你所要去的網站網址；
2. 絕不開啟email的附件，除非你知道寄件者並且確定附件內容為何；
3. 不要瀏覽名聲不佳的網站，特別是情色影片網站或是盜版電影網站，因為很可能只要瀏覽這些網站就會受到電腦病毒感染；
4. 不任意下載任何軟體。
5. 定期備份你的檔案或資料在另外一個獨立裝置（如行動硬碟），或者使用雲端硬碟來備份，萬一出事，還可以找回重要資料。