

小心！利用武漢肺炎的病毒與網釣郵件已開始流竄

駭客開始利用大眾對於武漢肺炎的恐懼心理，製造各式偽裝成官方感染數據或衛教資訊的惡意檔案，發動網釣攻擊

文/陳曉莉 | 2020-02-03 發表 iThome

新型冠狀病毒肺炎（武漢肺炎）令全球人心惶惶，而駭客也利用使用者的擔憂發動了惡意攻擊，包括以武漢肺炎為名的病毒及網釣郵件攻擊。

專門提供企業安全意識培訓服務的 KnowBe4 表示，他們在日前發現了一則假冒來自美國疾病管制與預防中心（CDC）的電子郵件，在郵件內容中呼籲使用者要小心防範武漢肺炎，並附上一個可以得知使用者城市確診案例的列表連結，但使用者點選後，出現的卻是要求使用者輸入 Outlook 憑證的網頁。

而卡巴斯基則發現了多個以武漢肺炎為名的各種檔案，它們的檔案格式不一，但都夾帶了病毒，這些檔案可能是 PDF 檔、MP4 檔或 Docx 檔，駭客暗示這些檔案含有如何保護自己免受武漢肺炎侵襲的資訊，但其實它們不是木馬程式就是蠕蟲，可能會破壞、變更、複製或封鎖使用者電腦上的檔案，甚至是干預使用者的網路操作。

IBM X-Force 亦揭露駭客已利用人們害怕武漢肺炎的心態，藉由偽造的電子郵件通知來遞送金融木馬程式 Emotet。

其實只要坊間出現熱門的新聞或消息，都很快就會成為駭客利用的工具，武漢肺炎當然也不例外。

資安專家建議使用者不要隨便輸入自己的憑證，避免點選可以的連結，也應仔細觀賞所下載之檔案的副檔名，並安裝有效的防毒產品。