中華民國 105 年 2 月號
臺東林區管理處

公事家辦無人問，一旦洩密天下知。

預防勒索軟體綁架電腦 三不三要

不上鉤: 標題特別吸引人的郵件務必停看聽！

不打開: 不隨便打開email附件檔

不點擊: 不隨意點擊email夾帶的網址

要備份: 重要資料要備份

要確認: 開啟電子郵件前要確認寄件者身分

要更新: 病毒碼一定要隨時更新

加入FB 粉絲團

勒索軟體更多文章

資安時事案例

“ **煩請確認請款單**…巨集病毒捲土重來

封關民調遇駭 點擊恐被植木馬

個人資料保護法

輕鬆學資安

spear phishing 魚叉式網路釣魚

數位學習

資安小紅帽

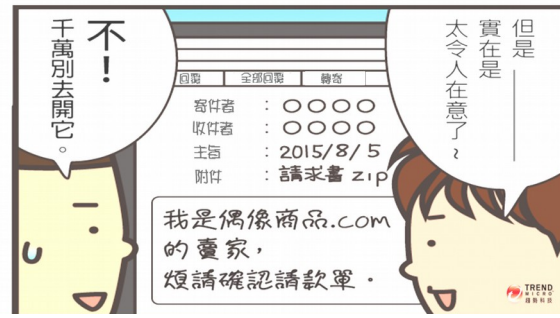
“煩請確認請款單...” "巨集病毒假借公司會議紀錄、內部資料或請款單企圖闖關

巨集病毒捲土重來，當心 Word/Excel 附檔夾帶非法巨集

POSTED ON 2016 年 01 月 06 日 BY TREND LABS
趨勢科技全球技術支援與研發中心

《小廣和小明的資安大小事》清井弟不顧小廣提醒，蠢蠢欲動想打開附件的原因，居然是…。

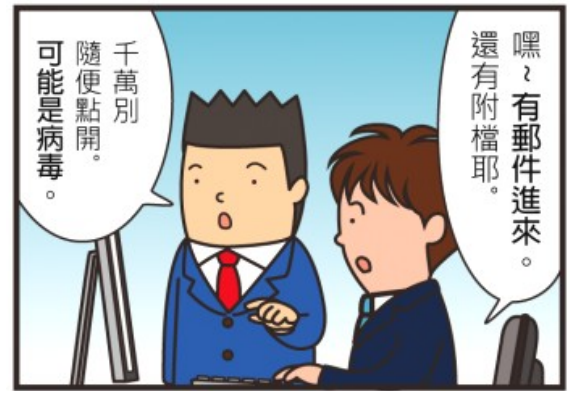
輕井君所收到的是打開附檔就會感染病毒的攻擊郵件。駭客鎖定特定的企業及組織作爲目標，寄出的郵件夾帶了僞裝成公司會議紀錄、內部資料或請款單等的病毒檔案。讓企業員工在沒有防備的狀況下誤開啓了病毒郵件。這一類的手法已日新月異越來越高明。



最近有一種捲土重來再次流行的攻擊手段，就是在附檔的 Word/Excel 文件中被埋進了非法的巨集 (※) 的攻擊郵件。當企業員工企圖將附檔文件打開並執行巨集時，就會感染上病毒。

(※) 巨集 : 是種具備 Word/Excel 等的文書處理及計算的一種軟體，會自動的紀錄複雜的操作步驟，也會多次重覆自動執行的一種機能。

即便如此。在 Microsoft Office 的出廠設定，巨集是無法自動執行的。因此，駭客會在郵件中特別載明「爲了解決亂碼的問題，請開始執行巨集」的註解及設定程序，進而催促用戶執行巨集。此外，在打開郵件時所顯示的「目前巨集沒有被啓用」的訊息中，會提供「請開啓巨集」的快速按鈕，一旦執行後，就會感染上病毒。



起初會用無病毒郵件與諮詢窗口頻繁往來，讓企業員工鬆懈後，再寄出病毒郵件也是其中的不肖手法之一。在點擊文件前如對寄件者和本郵件、附檔名稱及寄件時間等有疑慮的話，請直接以電話與寄件者確認的同時，也請多聽聽網路安全維護人員的意見吧。

HOME

封關民調遇駭 點擊恐被植木馬

自由時報 105 年 41 月 6 日

〔記者顏宏駿／彰化報導〕總統大選民調今起不能公布，但近來中部地區不斷有民眾收到「民調超連結」簡訊，點進去一看，卻不是民調資料，警方表示，這很有可能是駭客入侵，把木馬程式植入受害人手機竊取個資。

鄭姓民眾說，這一個禮拜以來，他手機連續接收到不明來源的簡訊，分別透過「中華電信」、「臉書」、「 line 」傳送，內容提到「總統大選逼近，民調封關，想看各機構最新民調結果請連結 http://… 」、「○ ○ 你好：期待與妳建立Linkedin 關係。接受或取消訂閱請按 http://… 」。

鄭姓民眾表示，由於簡訊一開頭就指出他的名字，覺得很納悶「對方怎會有我的電話」，但因爲電話來源不明，他就沒有點進去。

警方表示，這極有可能是駭客入侵，只要使用者超連結，進入對方所設的網站，就會被植入木馬程式，透過木馬程式，駭客可以取得你的個資，包括私密照、電子錢包。

警方說，駭客從受害者這邊取得手機的密碼、序號、帳號，就能假扮網路買家，大肆到網路店家購買商品，最後帳單都算到被害者頭上。

警方說，看到不明來源電話或簡訊，不要打開，特別是號碼中有「＋」是國際碼，有可能是國際駭客，其次，使用者手機最好自己付費購買手機防毒軟體。

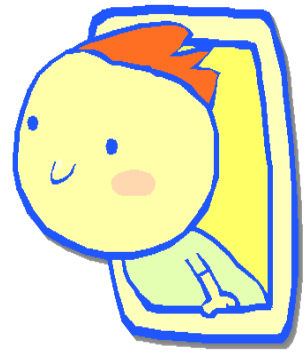
HOME

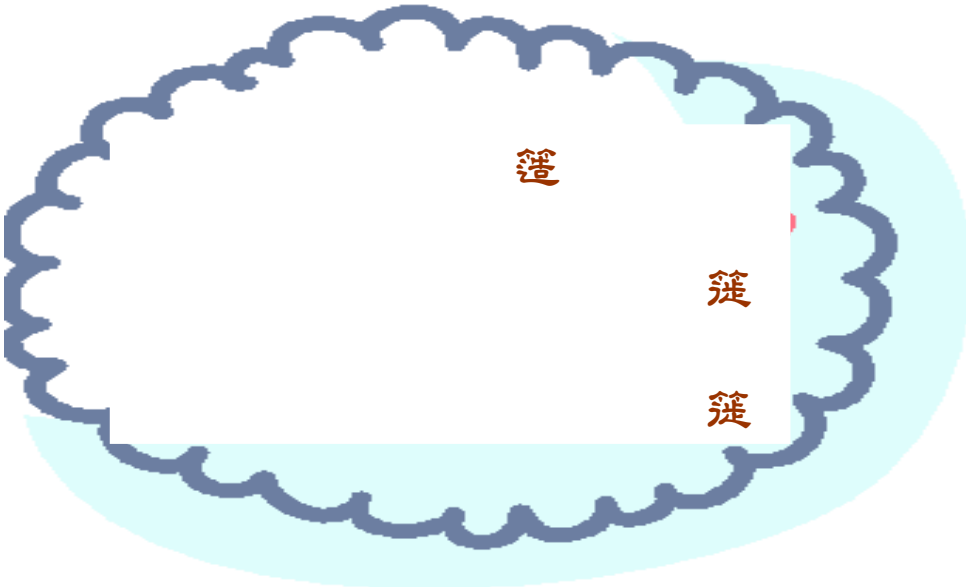
個資保護合理用，避免隱私受侵害！

公務機關之個人資料蒐集、處理（個資法第 15 條）

具有特定目的 + 符合下列情形之一：

1. 執行法定職務必要範圍內。
2. 經當事人書面同意。
3. 對當事人權益無侵害。





防範魚叉式網路釣魚政擊：

保護電子郵件就能防範針對性攻擊

spear phishing 魚叉式網路釣魚

資料出處： NII 產業發展協進會

只針對特定目標進行攻擊的網路釣魚攻擊，通常鎖定之對象並非一般個人，而是特定公司、組織之成員。

HOME