親愛的客戶您好， 這是來自研展資訊的關心提醒信件 ：

由於近日來加密勒贖病毒越來越嚴重，若程式資料遭綁架會對公司造成極為嚴重的損失，所以請大家一定要小心。**一但發現檔案被修改、或是沒在操作電腦，但是電腦變慢硬碟狂閃的現象，請立刻關閉電腦**並通知集前窗口及相關人員進行處理。

＊ **加密勒贖病毒的特性:** 病毒會在背景運作然後將本機及網路上的共享資料進行加密，直到最後才會跳出付費視窗連結或留下付費的相關訊息。**加密後的檔案要解密，除了和駭客交易外(不一定有用)，暫無其它解密辦法。**

＊ **加密病毒目前的主要來源: 以電子郵件及網頁為主**，病毒現在並不會主動攻擊，所以**最重要的是加強個人使用郵件及網頁行為及主動預防部份強化防毒及備份系統。**

加強個人使用郵件及網頁行為: 需告知使用者要做好以下有關郵件及網頁的基本注意事項。

郵件方面 :

常見是利用自己寄自己等內容來吸引使用者，主要是信件中含有 word、excel、pdf、zip、rar 這類附件。**壓縮檔內如含 exe、js、vbs 等執行檔，也很有可能是對方中毒或是駭客所寄出的信件 ，在確認寄件者及信件內容前不要去開啟不明的附件。**

網頁方面:

大多是使用者**瀏覽了不可明網頁並點擊特殊連結**所造成，像是大陸網站、免費破解軟件下載、廣告連結，往往都會有可能造成電腦中毒。

防護系統的部份:

針對這波加密攻擊 ，**常見的免費及破解防毒軟體 ，因為病毒碼的更新速度比不上使用原版的防毒軟體 ，所以還是會建議使用原版防護軟體，且能夠隨時更新到最新的疫苗**，防毒系統掃毒的效果才能發揮防禦效力，由於各版本都有不同的效果，**如果可以選擇含有網路防護模組最佳。**

備份加強部份:

日常需要做好完整的資料離機備份，建立相關的保護機制，如 NAS 網路備份 、二次備援 、異地備份 等等，當問題不幸發生時才能有效的還原資料。
另外本機硬碟、USB 隨身碟 ，都算本機備份，加密病毒發作也會連同本機上的儲存設備進行感染。

研展資訊關心您

感謝資料提供者: 集前資訊