Crypt0L0cker 病毒介紹(白育澄 撰稿)

Crypt0L0cker 病毒之類型爲「文件加密」，屬勒索軟體。通常，Crypt0L0cker 病毒來自惡意網站，或被駭客(Hacker)入侵之合法網站。如果同仁們上一些色情網站，或者開啓「不知名的」網路郵件，更會大大增加電腦被感染的機會，被感染時，出現的訊息，如下圖所示：

目前，這種病毒，會入侵所有版本的 Windows 作業系統，包括：Windows XP、Windows Vista、Windows 7 和 Windows 8 等。此病毒，會對你電腦內的所有文件檔案，進行加密(Encryption)；被加密的文件檔案，其副檔名後面，會加入**.encrypted** 字樣，好像在告訴你：「呵，你的檔案，已被我加密了。」若不幸中了，會讓你欲哭無淚，如下圖所示：

m_104勞務委託需求單_itri_0409_final_black.doc.encrypted	2015/12/22 上午 ...	ENCRYPTED 檔案
m_104勞務委託需求單_itri_0409_final_color.doc.encrypted	2015/12/22 上午 ...	ENCRYPTED 檔案
m_104實支細項_itri_0409_final_color.doc.encrypted	2015/12/22 上午 ...	ENCRYPTED 檔案
m_2015_aCEA_四人學經歷.docx.encrypted	2015/12/22 上午 ...	ENCRYPTED 檔案
m_遴聘相關研究人員簽呈_20150413.doc.encrypted	2015/12/22 上午 ...	ENCRYPTED 檔案

Crypt0L0cker 病毒，採用 AES-265 和 RSA 加密，因爲在人的有生之年內，無法解，所以中毒的電腦，別無選擇，使用者只能「購買私鑰」，達到入侵者(Intruder)對你勒索的目的。這個勒索軟體，創造了一個 DECRYPT_INSTRUCTIONS.txt 的勒索信；很「貝戈戈」的是：它會在該文件已被中毒且加密的每個所屬文件夾中，具文此次勒索贖金支付網站相關的訊息。透過這些訊息，可以讓你清楚了解，如何進行付款的程序；目前，中毒者被勒索的錢，皆爲「比特幣」。若你不付贖金，經過某一期限，其勒索贖金會加倍；若不信邪，再不支付，其勒索贖金會翻倍，成爲天價。這時，就看你的文件，重不重要，值不值得付款了。有位中毒者，付了約台幣 15,000 元，才獲得部分檔案的回復。

因此，本中心對全校同仁，要做重要呼籲與宣導，如下：

1. 不要用學校的電腦，上色情網站，對於不熟悉的網頁與不明郵件附件或連結，請勿開啓，避免感染病毒。
2. 不要在學校的電子信箱中，開不明寄信者的郵件。這是教育部規定的，而且每年會對各校的執行情形，給予評比；同時，教育部會故意用陌生郵件，來測試學校教育行政人員及老師，是否點選來路不明的郵件。這項評比，取名爲：社交工程演練。
3. 不要用學校的電腦，執行臉書(Facebook)與 LINE 中，不明的影片，不明的音樂，不明的圖片，或不明的軟體，以保護您電腦中的公務文件。
4. 目前此病毒感染之檔案無法救回；因此，同仁們須於每週週末，定期拷貝您電腦的公務文件，除了備份

(Backup)於外接式硬碟或光碟外，最好將重要檔案，分別備份於 2 台以上電腦，做好異地資料備援(Offsite Data Storage)的工作，以策安全。

5. 對於不明軟體，或破解軟體，請勿安裝。瀏覽網頁時，彈出式視窗，請不要點選或安裝，避免感染病毒。

對於蠕蟲、木馬、後門、間諜軟體等，有些同仁們可能在不知不覺中被感染，如果您對自身電腦有疑慮，可至本中心確認之下列網站，下載免費掃瞄程式。

注意：掃瞄時最好利用電腦空檔時刻執行，切勿執行其它程式或開啓任何檔案，以利掃瞄程式順利進行。

https://www.malwarebytes.org/antimalware/

http://www.bleepingcomputer.com/download/junkware-removal-tool/

【一般宣導】

1. 敬請尊重智慧財產權，有關校園網路使用規範、智慧財產權之宣導及注意事項，請多予關注，相關網址如下：http://www.takming.edu.tw/cc/。
2. 請勿安裝來路不明之非法軟體，以免觸法。