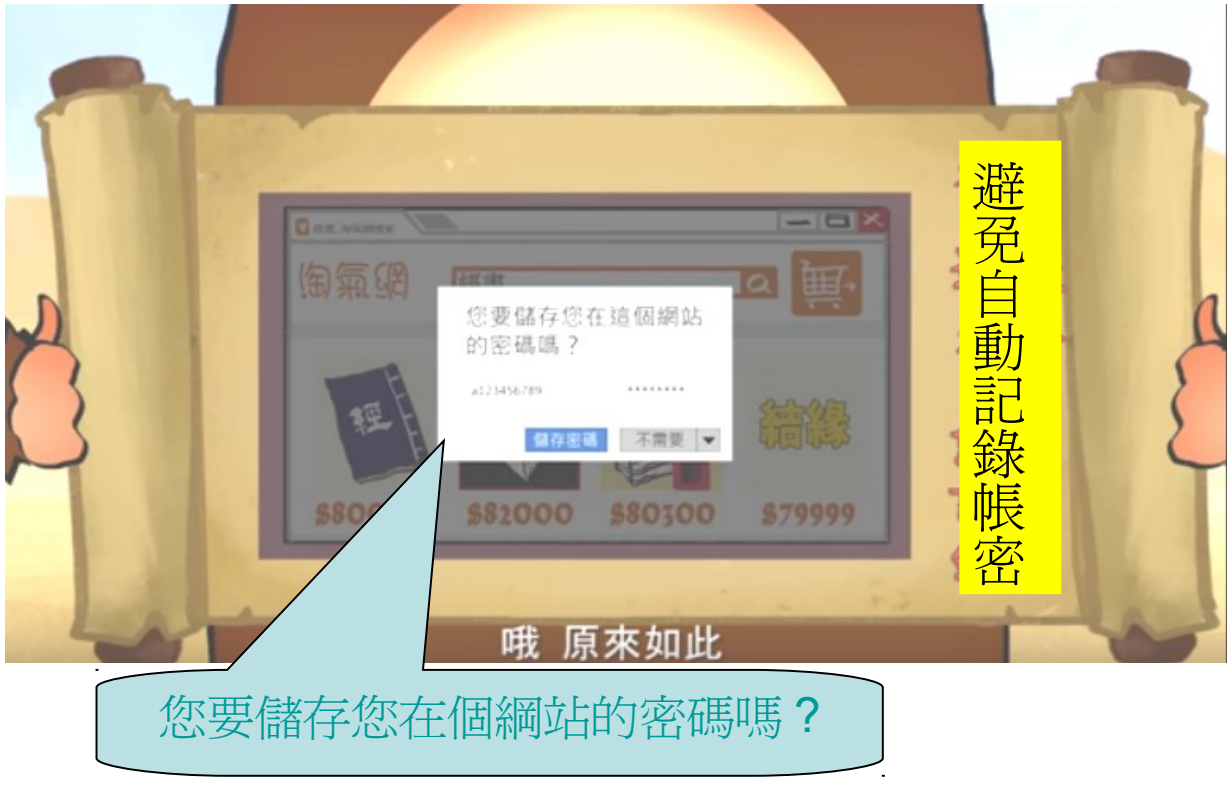
臺東林區管理處

中華民國 106 年_ 5 月
號

公務機密不留意，對人對己都不利。



資安時事案例

用雲端硬碟小心！勒索病毒變種假冒 Drop box 也淪陷

可以給我驗證碼？ 小心上詐團賊船

個人資料保護法 Q&A

輕鬆學資安

Time bomb 時間炸彈

數位學習 105 年資安動畫金像獎

唐三資安 on

用雲端硬碟小心！勒索病毒變種假冒 Dropbox 也淪陷

中央社 2017/04/08

資安大廠趨勢科技發現勒索病毒「 TorrentLocker 」變種， 攻擊時會假冒受害者的供應商， 寄送含 Dropbox 連結的假發票下載點，進而散布惡意程式碼。

趨勢科技表示，儘管 TorrentLocker 勒索病毒已過了它的巔峰期，但它至今依然活躍，而且由於偵測率不高，歹徒一直能夠暗中攻擊不知情的受害者。

TorrentLocker 的最新變種在行爲上與趨勢科技之前所偵測到的類似，主要的差異只在於散布方式，以及惡意程式執行檔的包裝方式。

比方說，新的 TorrentLocker 變種在攻擊時，會先假冒受害者的供應商，用電子郵件寄一份發票給受害者。這份「發票」不是隨信附上，而是透過一個 Dropbox 連結來下載。

除此之外，爲了增加郵件的真實性，郵件內容還包含了帳單、發票和帳戶編號等資訊。 TorrentLocker 之所以使用 Dropbox 連結， 就是爲了躲過郵件閘道防護產品的偵測，因爲郵件當中不含附件，而是使用指向正派網站的連結。

使用者一旦點選了郵件中的連結， 就會下載一個 JavaScript 檔案（ JS_NEMUCOD ）到電腦上，這就是假發票。當使用者試圖開啓這份假發票時，會再下載另一個經過編碼的 JavaScript 檔案到記憶體中，進而下載 TorrentLocker 的惡意程式碼到系統中執行。

新的 TorrentLocker 變種有一項不同之處是其檔案會包裝成 NSIS 安裝檔以躲避偵測，一些其他常見的勒索病毒也使用同樣的技巧， 如： CERBER 、 LOCKY 、 SAGE 和 SPORA 。

從 2017 年 2 月 26 日至 3 月 6 日這段期間，趨勢科技的 Smart Protection Network 偵測到 54688 封含有 Dropbox 連結的垃圾郵件，分散在 815 個不同的 Dropbox 帳號。此項威脅絕大多數都出現在歐洲，尤以德國和挪威的比率最高。挪威境內的威脅在 2 月底到達高峰， 3 月初開始慢慢轉移到德國。

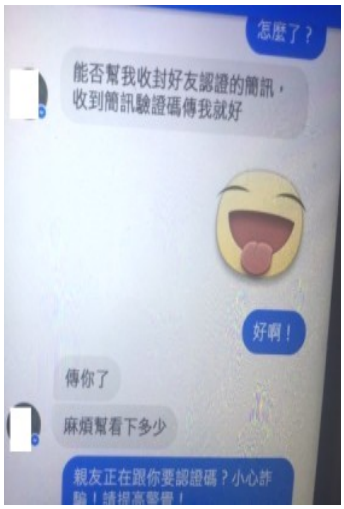
此外，威脅大多集中在平日出現，週末會暫時消失。而且趨勢科技發現，上午 9 時至 10 時之間的感染數量會突然飆高，這剛好是每天的上班時間左右，很可能是因爲員工剛進辦公室開始看信的緣故。由於企業經常使用 Dropbox 來管理及傳送檔案，因此員工很容易因爲缺乏戒心而受騙開啓信中的連結。

目前，趨勢科技正與 Dropbox 密切合作來解決這項問題。根據 Dropbox 資安團隊表示，在消息發布當時，所有相關的惡意檔案都已全部撤下，而相關的使用者帳號也都已遭封鎖。

趨勢科技指出，有鑑於 TorrentLocker 新變種與其他類似勒索病毒所採用的欺騙手法，企業應該格外小心提防社交工程攻擊。首先，企業應教育員工如何防範網路釣魚，時時提防可疑的電子郵件，例如：仔細查看寄件人的姓名及郵件內隨附網址顯示的文字是否與實際相符。事實上，一般使用者最好盡量避免下載附件檔案或點選郵件中的連結，除非確定郵件的來源百分之百可靠。

除此之外，使用者也應採取一些額外步驟來備份資料，例如「 3-2-1 」原則： 至少 3 份備份、 2 種儲

可以給我驗證碼？ 小心上詐團賊船



自由時報　2017 年 4 月 3 日

〔記者許國楨／台中報導〕台中市阮姓婦人接到詐團冒充友人透過通訊軟體傳訊息，要求查看並回傳手機簡訊上的認證碼，阮婦不慎給了認證碼後發現臉書出現警語嚇得向警方求助，警員立即請阮婦取消手機內小額付款功能、更改臉書及 Line 密碼等程序，並請阮婦知會好友提高警覺，及時阻止詐團藉此對親友詐財。

警方指出，阮婦上月底接獲騙徒冒充友人以臉書通訊軟體 Messenger 傳來訊息，請她收一封「好友認證」的簡訊，並要求回傳簡訊驗證碼，阮婦不疑有他，回傳驗證碼後卻發現臉書系統出現「親友正在跟你要認證碼嗎？小心詐騙」的警語。

阮婦驚覺有問題先撥打 165 反詐專線，隨後在丈夫陪同下就近向第五分局北屯派出所求助，女警洪玫君及副所長陳亦豐研判是詐團技倆，當機立斷請阮婦按照員警提供步驟行動。 1. 取消手機內小額付款功能。 2. 更改 Messager 密碼並關閉 Facebook 。 3. 更改 Line 密碼並取消 Line 的「允許至其他裝置登入」功能。

警方同時請阮婦於 Line 群組廣發訊息給親朋好友和臉書發文，告知自身帳號可能被盜用，若收到要求借錢訊息即是詐騙，切勿輕信；洪員事後再又撥打電話關懷，阮婦表示還是陸續有親友收到借錢訊息，所幸有先知會親友故無人遭詐。

警方對此呼籲，詐團常假冒親友，透過 line 、 Facebook 等通訊軟體，以換手機爲由套問被害人電話號碼，再請被害人代收認證簡訊請你告知簡訊認證碼，得手後隨即註冊新帳號後向親友借錢，或用來更改被害人的拍賣網站密碼、手機小額付費藉此詐財，提醒民眾小心防範！

HOME

個資法 Q&A

債權人應如何向監理機關申請查詢債務人車籍相關資料，方符合個資法？

資料來源：法務部全球資訊網 張貼日期： 2015/10/29

答：

本部 102 年 12 月 26 日法律字第 10203514550 號函說明四所述「債權人既已循民事救濟途徑取得強制執行法第 4 條所定各款執行名義，其債權確屬實際存在，若不許其以執行名義文件或法院執行處之通知，向有關機關申請查詢債務人之車籍相關資料」，係指法院依強制執行法第 18 條第 1 項開始強制執行程序後，依同法第 19 條第 1 項規定，對於強制執行事件，認有調查之必要時，命債權人查報之通知。是以，債權人執憑強制執行法第 4 條第 1 項各款執行名義之一，向相關機關查詢債務人之個人資料，限於強制執行程序進行中，並應提出法院命債權人查報之相關證明，方得向相關機關提出申請查詢債務人之財產狀況等資料。

(摘自「法務部 104 年 1 月 29 日法律決字第 10300716620 號書函」 - 本函全文可於本部全球資訊網點選「法務部主管法規查詢系統」查詢）

Time bomb 時間炸彈

資料出處：行政院國家資通安全會報技術服務中心

顧名思義，此乃一段隱藏的程式碼，當執行一段時間後，將於特定某個時間造成電腦系統的損害或損失。時間炸彈不像邏輯炸彈 (Logic Bombs) 般設計精密，時間炸彈僅關心系統日期，並非某些特定事件的發生。除非系統日期改變或程式碼被移除，否則不管發生什麼事，時間炸彈將於特定日期引爆。預防抵抗此類程式碼的方法是經常性進行資料備份，將損害或損失減至最低。

HOME