以勒索病毒示範 ESET 防毒軟體的功能

https://www.seekinfo.com.tw/
更新日期：2016/3/23

最近勒索病毒大量透過電子郵件散播，有些使用者成為受害者，面對來路不明的信件，就這麼隨意開啟附件，不知是好奇心太強？還是太勇敢？但這就像詐騙一般，總是有人會上當。本文藉由勒索病毒來介紹 ESET 防毒軟體的幾個功能，希望讓大家對現今的防毒軟體有新的認識，不要還停留在單純靠病毒碼辨識病毒的舊觀念。

首先在無病毒防護的狀態下，故意執行勒索病毒，確認此病毒是有效的。請看影片1 https://youtu.be/3-E_WrVSh8k

- 資料夾 ERA6 裡面有許多 PDF 檔，隨意開意其中二個，確認檔案是好的。
- 桌面上的 SKMBT_C48677022466188.zip 是今天凌晨寄來的勒索病毒電子郵件的附件，開啟壓縮檔裡面 .js 檔案，
- 沒多久在 Process Explorer 視窗裡面可以看到有一個 RYMdDzYC.exe 檔案在執行，這就是勒索病毒。檔案在 C:\Documents and Settings\Steven\Local Settings\Temp 裡面。
- 大約在 1:10 秒的位置，可以看到 ERA6 及桌面的檔名被改變了，此時檔案已經被加密，無法救回來了。緊接著，勒索病毒的訊息相繼出現。這部電腦已經成為受害者。

接下來示範，如果在有安裝 ESET 防毒軟體(此影片以 ESET Endpoint Antivirus 6.3.2016.1 為例)，會發生什麼狀況。請看影片2 https://youtu.be/4ISC3IOyOvs

- 首先顯示 ESET 防毒軟體的資訊，並更新病毒碼。
- 然後如同影片1，執行同樣的勒索病毒，執行後，ESET 防毒軟體陸續出現封鎖網址的訊息。因為最近勒索病毒電子郵件附件裡的 .js 的檔案，實際上並沒有加密的功能，很單純只是到某些網址下載檔案來執行，所以如果下載的動作被攔截了，病毒根本沒有機會執行。
- 好，那假設前一道程序失效了，檔案 (影片1 的 RYMdDzYC.exe) 被下載回來執行會發生什麼事？我事先手動下載好放在桌面上，執行後，在 Process Explorer 視窗確認已經啟動。稍等這個勒索病毒開始運作之後，ESET 防毒軟體又開始出現封鎖網址的訊息。因為勒索病毒必須要傳回某些訊息，否則它怎麼知道哪一部電腦解密的 Key 是什麼？到此為止，ESET 防毒軟體的 **Web 存取防護** 功能發揮第一道關卡，成功阻擋了這個勒索病毒。
- 為了進一步測試，接下來我故意關掉 Web 存取防護，讓勒索病毒可以成功連上它想要連線的目標。此時 RYMdDzYC.exe 繼續執行，緊接著 ESET 再度彈出訊息，偵測到記憶體中的 RYMdDzYC.exe 是 Win32/Filecoder.Locky.B 木馬的一個變種。從 Process Exprocess 視窗可以發現 RYMdDzYC.exe 已經關閉了。這個功能是 ESET 防毒軟體的 **進階記憶體掃描** 技術，因為病毒為了躲避防毒軟體的偵測，通常會採用偽裝或加密等各種技術，但是程式一旦在記憶體中執行，就會恢復本來該有的面貌，以這個例子來說，進階記憶體掃描就能判斷出這個檔案是 Win32/Filecoder.Locky.B。
- 接下來用 ESET 防毒軟體掃描 C:\Documents and Settings\Steven\Local Settings\Temp 裡面的 RYMdDzYC.exe，它偵測到是 Suspicious Object。這個是 **ESET LiveGrid** 的功能。如果是依靠病毒碼偵測到病毒，會有明確的病毒名稱，以這個檔為例，病毒名稱應該會是 Win32/Filecoder.Locky 開頭。當 ESET 防毒軟體的病毒碼還無法偵測某些病毒，但是它又透過某些機制 (例如前面提到的，進階記憶體掃描) 認為某個檔案可能是病毒，此時 LiveGrid 的功能會收集這個檔案的資訊，並回傳 ESET 伺服器，這樣即可在數分鐘之內，讓所有 ESET 客戶快速免於這個病毒的威脅。

- 但是剛才 RYMdDzYC.exe 有執行，那檔案被加密了嗎？ 開啟 ERA6 資料夾，檔名完全沒變，隨意開啟二個 PDF 也沒問題。
- 最後，桌面上的檔案用 ESET 防毒軟體掃描一次，結果未發現病毒，所以這個勒索病毒是很新的，ESET 的病毒碼還未更新。

後記

- 現今的防毒軟體並不再是單純靠病毒碼來防範病毒，甚至有好幾種技術來對付各種威脅。不要再完全依賴病毒碼了，如果您認為防毒軟體版本老舊也無所謂，只要有更新病毒碼就可以了。希望這個影片能讓您有不同的看法。(請注意，更新病毒碼還是非常重要的，請勿過度解讀，曲解我的意思)
- 請打開 LiveGrid 的功能，自助助人，所有 ESET 客戶都能受益。如果可以，不要禁止電腦連上 Internet，否則就無法享受 LiveGrid 快速反應的效益，或至少允許連 ESET LiveGrid 的伺服器。
- 以前寫過一篇文章 - ESET 防毒軟體定期掃描 (網址: https://www.seekinfo.com.tw/files/ScheduleScan.pdf)，說明**除非有特別狀況，否則沒有必要做定期掃描**，本文也再次說明，定期掃描沒有太大的用處。試想，本文的例子，病毒碼無法偵測到病毒，掃再多次結果會有差異嗎？
- 影片1 和影片2 使用 Windows XP，單純只是為了方便測試，Microsoft 早已不支援 Windows XP，建議升級到 Windows 7 或更新的版本。
- 每個病毒都不相同，不同時間、不同版本都可能造成不同的反應。影片2 的勒索病毒雖然被 ESET 成功封鎖，並不表示日後新的變種也會完全一樣的反應，對勒索病毒仍要小心應對。請記住，防毒的領域是動態的，隨時都在改變，請持續保持更新資訊。