個案分析-

常見於 Facebook 上的惡意連結網址事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2014/12

I. 事件簡介

A. 現今 Facebook(簡稱 FB)已經成為社會大眾主要的社群交友的網路平台，透過 FB 可以訂閱追蹤喜歡的人事物資訊，或者用來與朋友進行溝通傳遞訊息，然而可能也成為駭客利用社交工程入侵的一種方式。

B. 本個案利用 FB 進行社交工程的案例有兩件，分別為事件 A 和事件 B。

C. 事件 A 為近期發現到 FB 上某些人會非自主性的散佈特殊主題的惡意連結誘使朋友去開啟，並且引導下載惡意程式安裝。

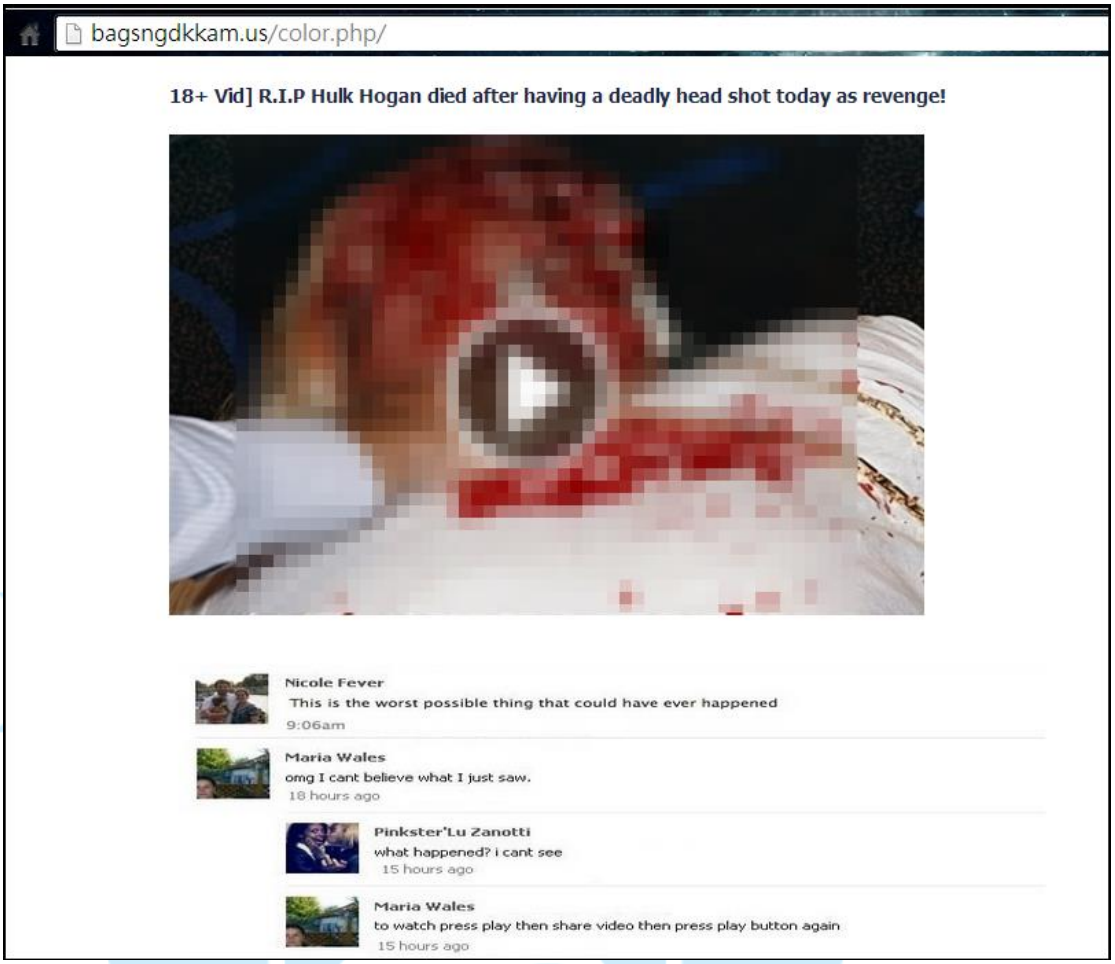
1. 此例為 FB 的朋友會在他人的發表文章底下回覆「Select your favorite color scheme for Facebook layout.」，並提供假的 APP 連結與縮圖供使用者去開啟。

D. 事件 B 為 FB 聯絡人在受害者版上發表惡意 APP 連結，內容包含 FB 釣魚網頁連結，藉以竊取 FB 帳號密碼。

II. 事件 A 檢測

A. 嘗試點入該“Facebook color changer”的連結後，其會自動轉跳至另一網址「http://bagsngdkkam.us/color.php」，並且出現驚悚血腥的圖

片及影片連結吸引使用者去觀看，並且底下還有回覆讓人更容易去開啟。

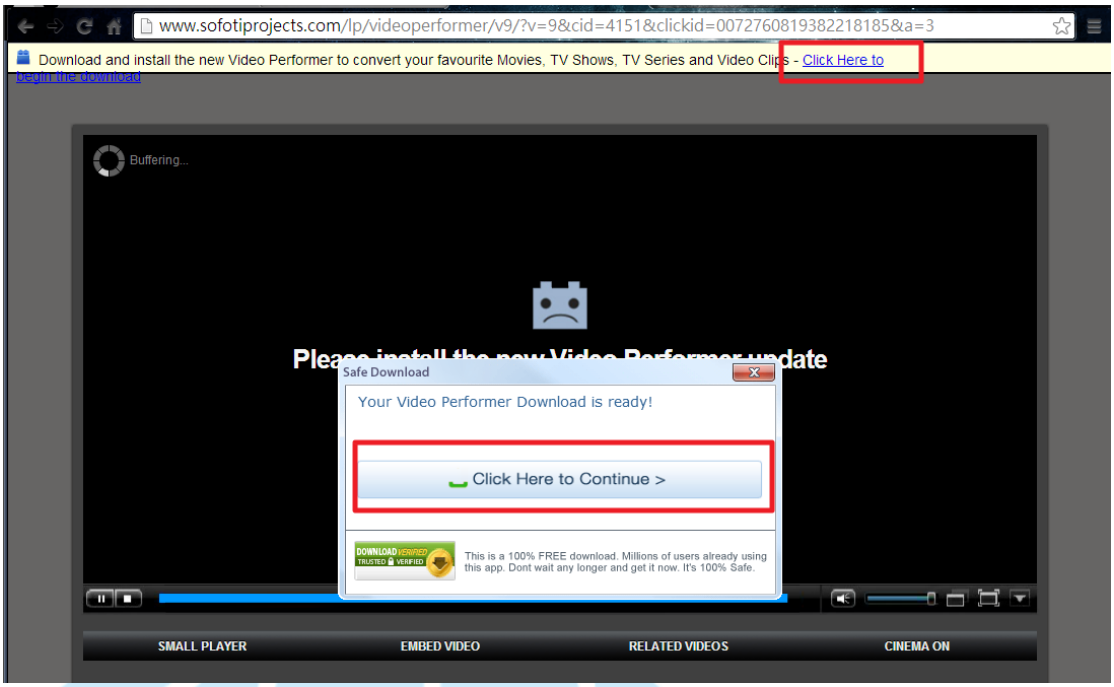


B. 當使用者想去觀看開啟該影片時，畫面中的 PLAY 圖示上會多出「Share this video before watching.」「Share On Facebook」的字樣，提醒使用者觀看前必須分享該訊息至個人 FB 動態上。

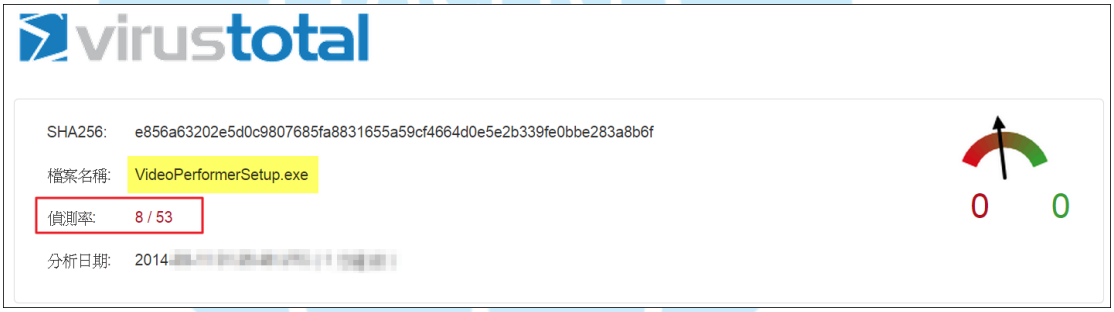
C. 當使用者點擊了確定分享之後，該連結就會自動發布在 FB 個人動態上，進而讓更多朋友去開啟。

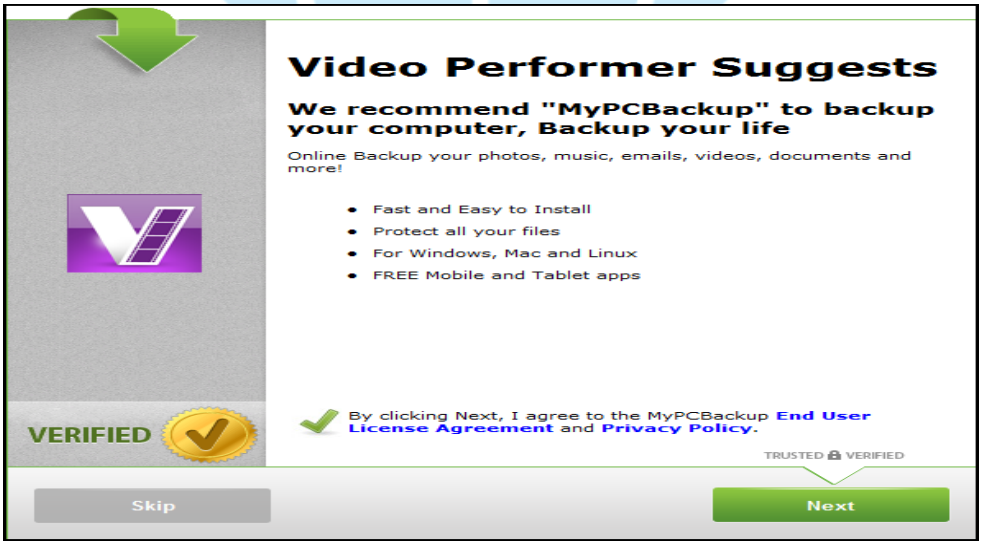
D. 此時網頁並不會立刻撥放該影片，而會轉跳至新的頁面要求下載制式的影片撥放器才能觀看，誘使用戶下載該惡意程式並安裝。

1. 檢查原始碼得知會去 GET /mermaid/redirect.php 後，轉址至 www.sofotiprojects.com 的網站底下。



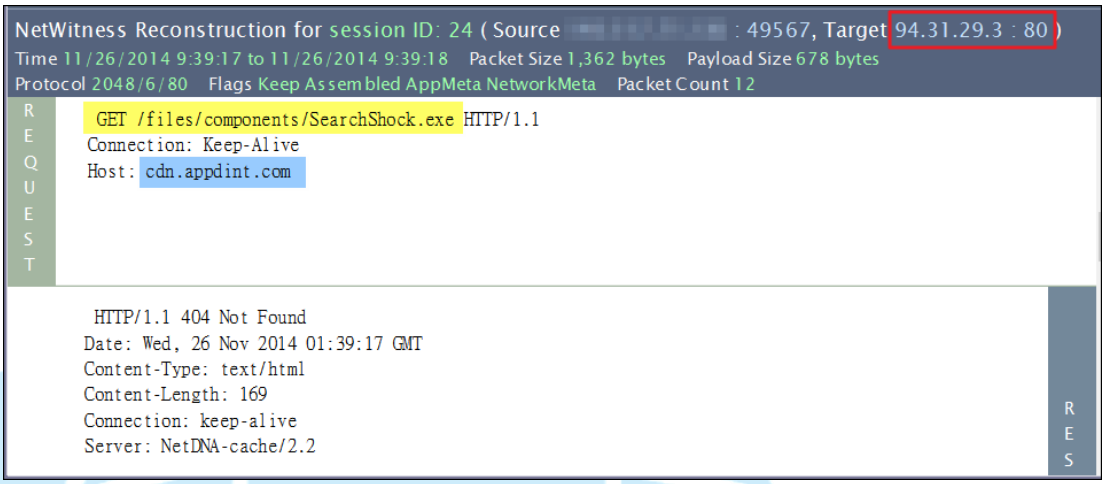
E. 當嘗試點擊連結後會開始下載一個名為 VideoPerformerSetup.exe 的執行檔案，先將該檔案透過 Virustotal 線上掃毒，偵測比例為 8 / 53 的惡意程式。



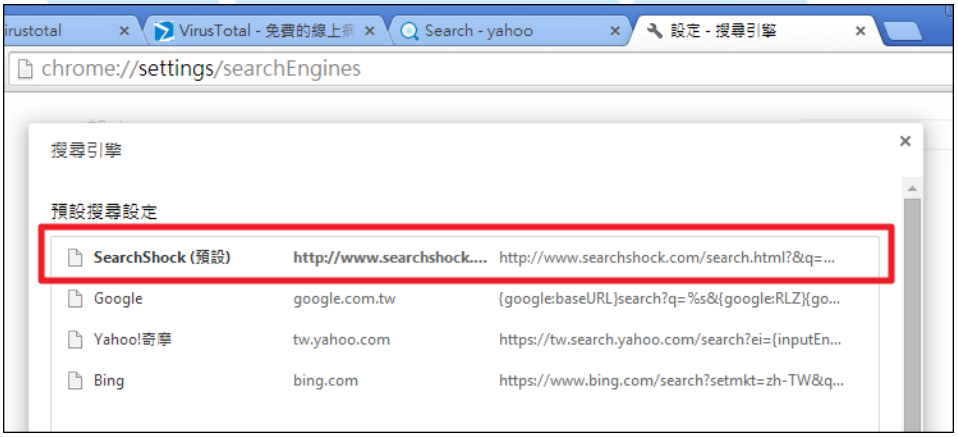


F. 透過封包側錄可以看到當程式 VideoPerformerSetup.exe 在執行安裝時候，會產生一些對外的網路連線，主要會連到英國 IP 94.31.29.3、美國 IP 174.36.241.171 和美國 IP 50.22.175.76。

1. 該程式執行時候會去向網站 cdn.appdint.com 進行下載惡意軟體 SearchShock.exe 執行，此網站 IP 就是 94.31.29.3。

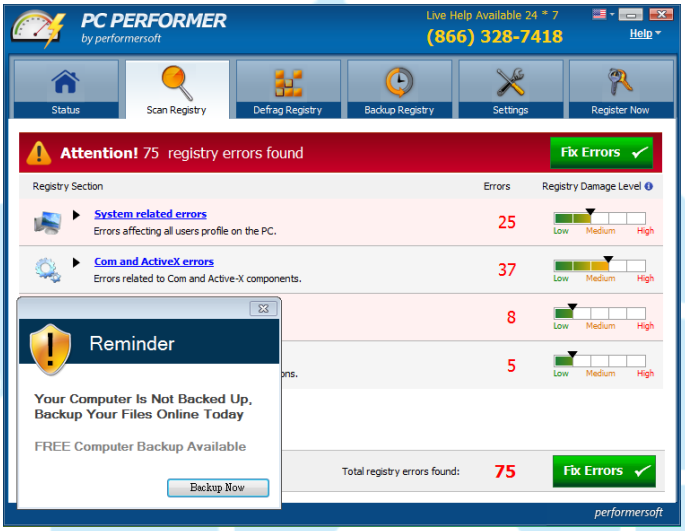


2. SearchShock.exe 安裝後會綁架瀏覽器的首頁，強制改成他的搜尋引擎列，以監控瀏覽器的紀錄或登入密碼。

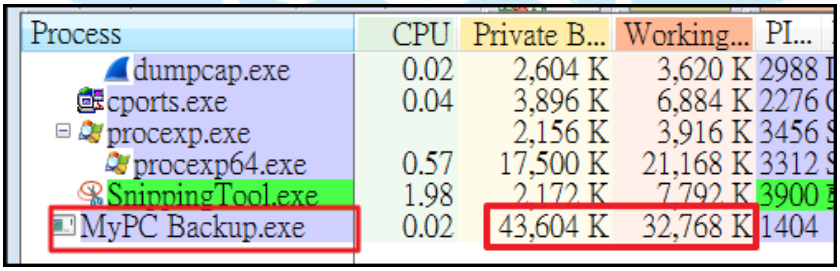


3. 除了 SearchShock.exe 之外，惡意程式還會下載安裝其他檔案，如「ZulaGamesSetupW.exe、UnknownFile.exe、PCPerformerSetup-4.exe、CloudBackup.exe」，這些軟體皆未經由使用者授權就直接安裝，可能會占用主機資源拖慢速度或竊取資料等。

4. 如 PC PERFORMER 看起來是一個系統的修復軟體，事實上剛好相反而會占用主機資源或竄改主機設定。



5. 如 MyPC Backup 則會在背景消耗大量的記憶體資源托慢系統速度。

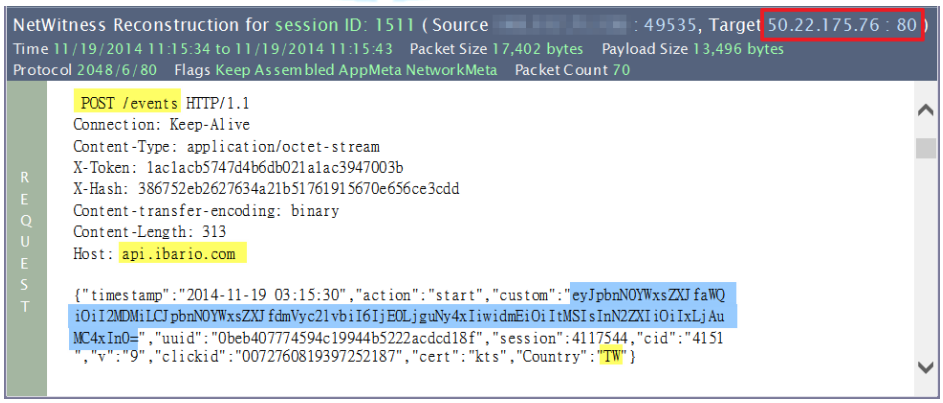


6. 而安裝過程中會將主機的相關資訊透過 HTTP POST 方式上傳到 api.ibario.com，也就是 IP 為 174.36.241.171 和 50.22.175.76，駭客可能利用 Fast Flux 方式動態切換網域名稱對應的 IP。

```
未經授權的回答:
名稱:    api.ibario.com
Addresses:  50.22.175.81
          174.36.241.171
          174.36.241.169
          50.22.175.76
```

a. 透過 Virustotal 檢測該網站 api.ibario.com 的確有被偵測出為惡意網址，比例是 2/61 。

b. 檢視上傳到 api.ibario.com 的封包檔，可以看到報到的路徑是“POST /events”，而內容有標註 timestamp、action、custom、Country 等主機資訊，其中 custom 內文為 base64 編碼，解碼後為「{"installer_id":"603","installer_version":"14.8.7.1","va":"-1","sver":"1.0.0.1"}」，也就是安裝的編號和版本號碼。



III. 事件 B 檢測

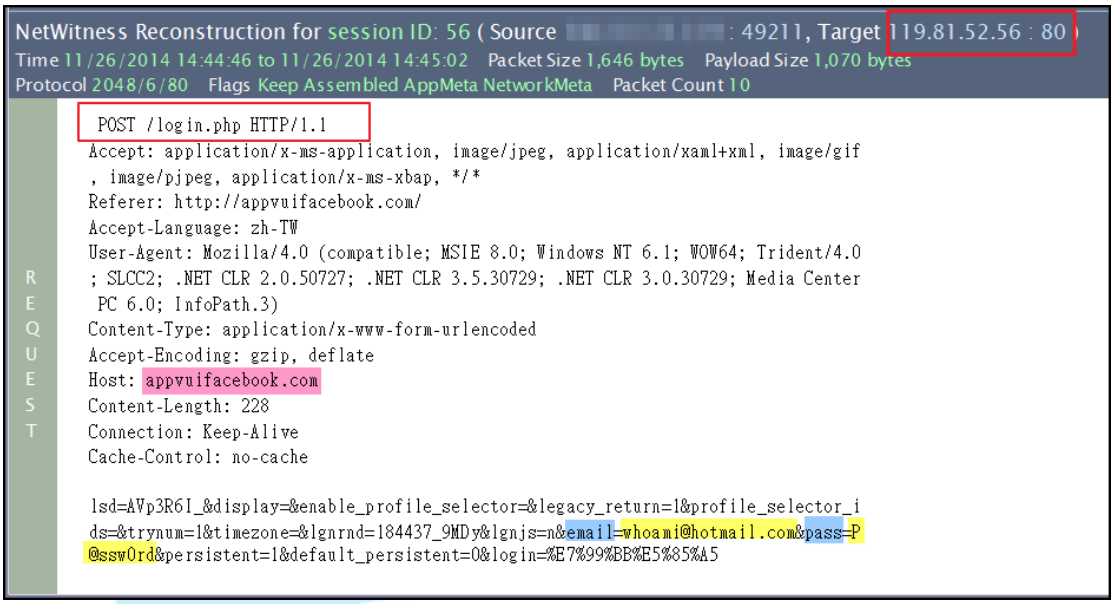
A. 事件 B 中，某 FB 聯絡人向受害者發表一張照片，告知是透過特定 APP 能將生活照轉換成可愛卡通照片，讓使用者去打開附上的連結頁面。

B. 當使用者開啟該頁面後，網頁會轉跳至一個 FB 的名為「Tin Hot 24」社區專頁，此頁面會去執行一些指令碼，故 IE 視窗會跳出詢問是否要停止視窗指令碼的訊息。

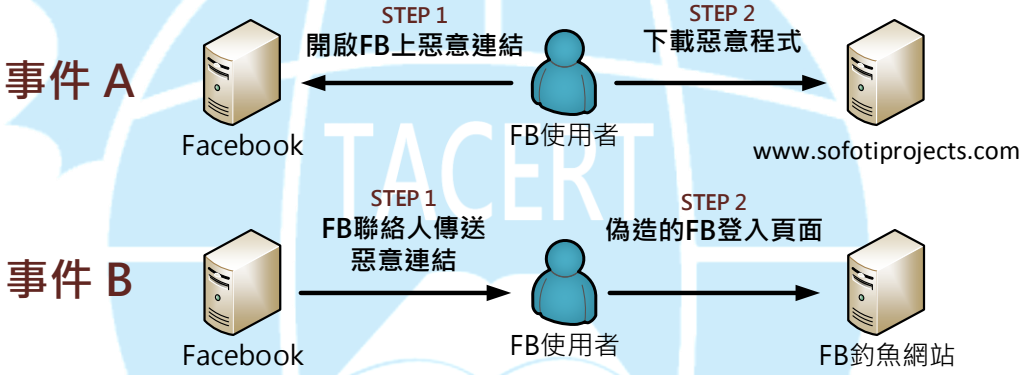
C. 此頁面出現時間很短，不管有無點選「是」或「否」都會在轉跳至另一個網頁，也就是要求重新登入 Facebook 的畫面，此頁面網址為「appvuifacebook.com」的釣魚網頁。

D. 嘗試輸入帳號「whoami@hotmail.com」和密碼「P@ssw0rd」測試，檢查側錄的封包的確有看到該帳號密碼以 HTTP POST 明文方式送出，確實為惡意的釣魚網頁。

1. 釣魚網頁「appvuifacebook.com」的 IP 為「119.81.52.56」，是位於中國河北省廊坊市的主機。



IV.網路架構圖



事件 A：

STEP 1：使用者開啟FB上他人發文的惡意程式連結。

STEP 2：轉址至「www.sofotiprojects.com」並下載惡意程式「VideoPerformerSetup.exe」。

事件 B：

STEP 1：使用者開啟FB聯絡人傳來的惡意連結。

STEP 2：轉址至偽造的FB登入頁面「appvuifacebook.com」

V. 建議與總結

A. 此案例都是經由社交網站 Facebook 進行的攻擊行為，透過聯絡人的信任關係來傳送惡意程式連結或釣魚網站。

B. 事件 A 的聯絡人在自己動態頁面上以留言方式發表惡意的 APP 網址(change color)，讓有興趣的人去開啟安裝。

C. 事件 B 的聯絡人直接在受害者的個人動態留言或私下傳訊息，內容為含有釣魚網站位址，讓受害者登入偽造的 FB 網站以竊取帳號密碼。

D. 這兩個事件共通點為發送惡意連結者可能都不是故意，因為帳號被盜取或者安裝到能夠存取 FB 權限的 APP，自動發送惡意訊息。

E. 事件 A 中受感染者就會在自己的動態上發布惡意網址，表示惡意程式能夠具有自動存取發布 FB 的權限。

F. 建議開啟 FB 的二次驗證功能，於 FB 的安全性設定可以啟用代碼產生器，就算駭客竊取到了帳號密碼還必須輸入時效性代碼方能登入，能有效防範駭客入侵。

G. FB 上的簡訊或留言中的網站連結在開啟前都要特別注意，很有可能為惡意程式連結或釣魚網站。