個案分析-

# Facebook 常見惡意網址之『linkee.com』事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2014/01

I. 前言：

A. 現今 Facebook (簡稱 FB)已為世界知名且最多人使用的網路社交軟體，但是近期出現一些惡意的網址或程式在 Facebook 流竄，若不小心開啟可能嚴重侵害到個人或者他人的權益，導致個人資料外洩或者成為一個 BOT 危害其他 FB 使用者。

B. 駭客往往喜歡使用聳動的影片標題去誘使 FB 使用者去點開連結觀看。

C. 因此我們嘗試去開啟執行這些疑似惡意程式，並將受感染的過程及結果做個簡單的說明。

D. 我們用一個新創的 FB 帳號對近期出現的可疑連結做測試。

II. 測試環境：

A. VMware: Win7(x64)

B. 瀏覽器版本： Google Chrome

C. 創立一個測試用空白的 FB 帳戶去開啟惡意連結。

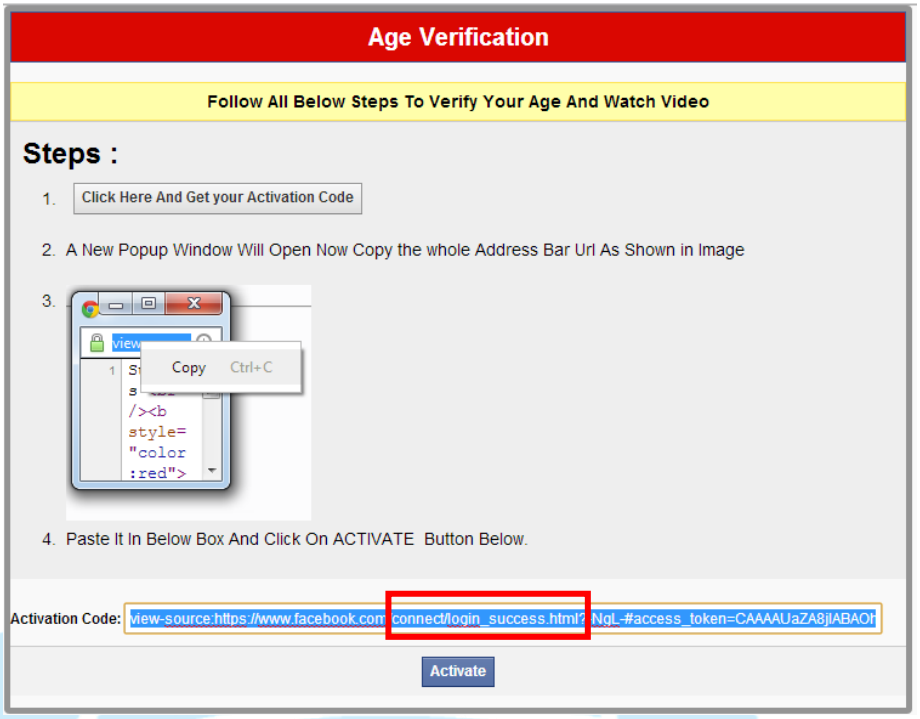
III. 測試過程：

A. 在 FB 上搜尋到一個使用者 Rakib 在他人的發文中做留言，此留言只有一串可疑網址 http://linkee.com/VmFE0j，初步判斷為惡意連結。

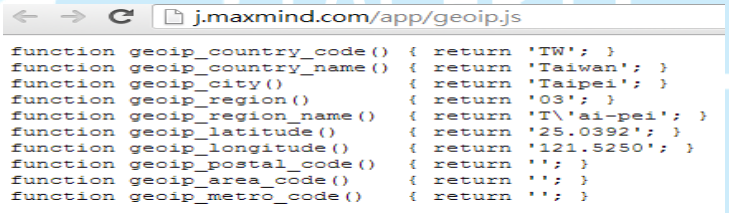

B. 再點下該網址後 FB 跳出一個警告視窗，表示此網站可能不安全，我們點選非垃圾訊息觀察會出現什麼畫面。


C. 此時會出現一個頁面 “http://tknngl.altervista.org” 要求做 Age Verification，

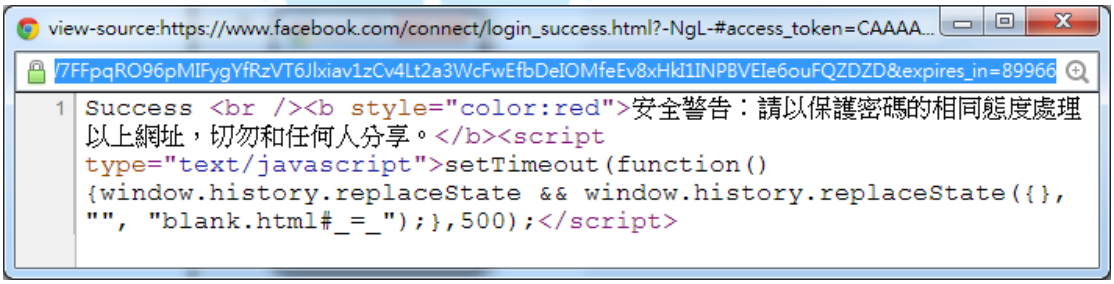
並有教學圖示引導受害者跟著做，看到這邊有警覺心的人應該就會發現是個釣魚網站。



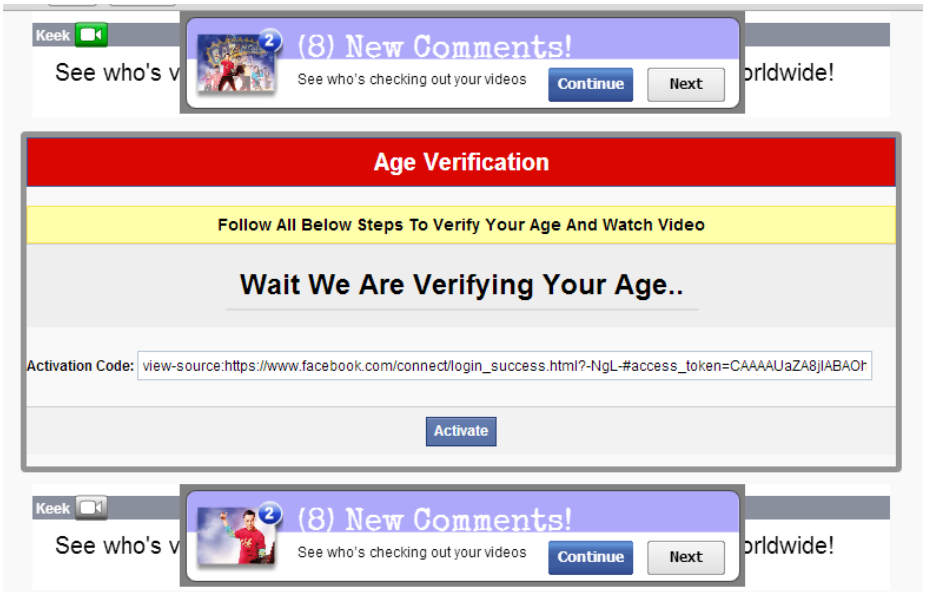

1. 此頁面原始碼會執行"http://j.maxmind.com/app/geoip.js" 收集受害者 IP 資訊。



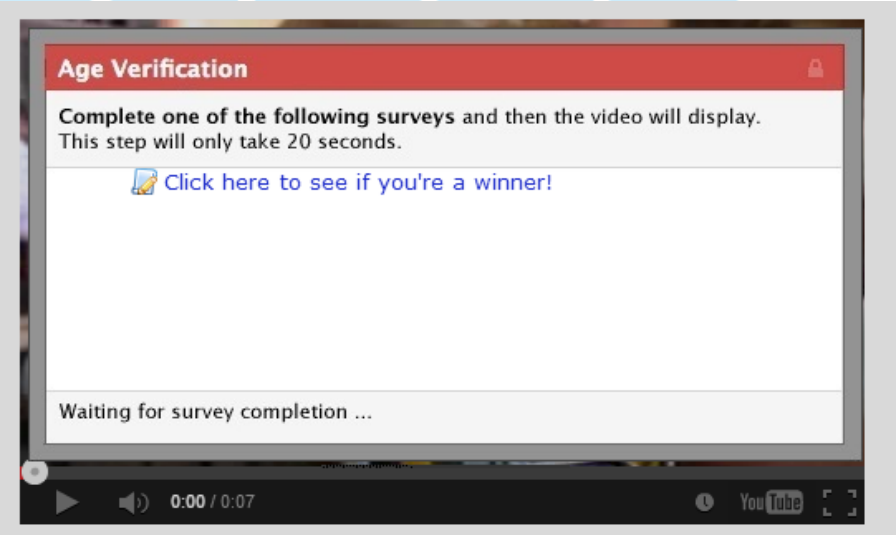

2. 第一步執行完果然跳出一個小視窗，內容還會顯示安全警告告知受害者保護此 Activation code，但實際上是背景執行一支 javascript。裡面隱含了 FB 登入成功的密鑰字串，部分為 /login_success.html? 應為登入密碼。




3. 第二步複製以上網址後再貼到下方的 Activation code 欄位，並點下方的 Activate 圖示。
4. 接著會出現一個畫面顯示 “Wait We Are Verifying Your Age..”的訊息。




5. 接著會出現網址“http://buzzingcl.info/cl/twfbd”的頁面顯示 “Waiting for survey completion”，此時 FB 帳號已經被入侵了，然而背景的 Youtube 根本無法點選撥放，只是一個偽造的圖案。




6. 若點選 “Click here to see if you’re a winner” 則會跳出另視窗 “rewardzone.onlineacutions.com” 告知可以獲得 3C 產品，因明顯為釣魚網站，故此網頁我們則無繼續點選。


IV. 測試結果：

A. 我們發現到個人的動態時報開始出現奇怪的發文和不雅照片，且照片的說明即為另一網址連結，誘導使用者好奇去點取以觀看該影片。(截圖經過馬賽克處理)


B. 受害者 FB 會自動去追蹤其他使用者或發出交友邀請。


C. 受害者 FB 會自動對某些“粉絲專頁”按讚，以訂閱他們奇怪的文章。


D. 若將剛自行發布的成人照片網址開啟，則又會跳到“tknngl.altervista.org”的相同釣魚頁面，目的誘使其他觀看者上鉤，成為另一受害者。

E. 有些發過的圖文離奇的被移除，但從 FB 的登入 IP 紀錄來看為正常。

1. 在之後從新登入 FB 被官方偵測有異常行為，主要是散佈一些垃圾訊息。


2. FB 官方提出下列警告果然就是相同作法將自己的登入權限外放讓第三者使用。


V. 解決方式：

A. 刪除瀏覽器 Facebook 的所有 cookie。

B. 刪除 FB 所發布的任何文章，取消相關按讚的專業訂閱。

C. 刪除自動發出的交友邀請。

D. 盡快更改 FB 的密碼，建議使用兩次驗證機制。

VI. 結論建議：

A. 此惡意連結並非出現 FB 啟動應用程式中。

B. 會自動散步惡意貼文以及標註朋友，且 FB 的個資可能已經外洩。

C. Facebook 上時常會有朋友分享一些影音連結，不確定的網址連結請勿輕易打開，多半會用短縮網址方式顯示來轉址，使人看不出來真正位址。

D. 加強 FB 帳號安全設定，例如使用安全驗證碼登入功能。
(手機驗證或二次驗證碼)

E. 盡量避免使用瀏覽器自動記憶密碼登入功能。