下表為駭客集團偽冒中華郵政之惡意木馬後門 APP 資訊

| | |
|---|---|
| 偽冒對象 | 中華郵政 |
| 樣本名稱 | post.apk |
| 樣本生成時間 | 2020-04-07 01:01:48 |
| MD5 | a39cb8c75d4e8e49bbfff7813d41ba80 |
| SHA-256 | 3d4c132e052323dd8d98762aa9c383ed50ce3e36305e32116494ffaaf8b08130 |
| 下載連結 | http://upsp-us[.]top/post.apk |
| 下載站 IP | 154.9.205.199 |
| 下載站國家 | 美國 |
| 中繼站 IP | 195.123.228.134 |
| 中繼站國家 | 保加利亞 |

提供以下三種方法判別用戶 Android 行動裝置是否遭感染：

1 查看 APP 圖示是否有白邊且 APP 名稱是否正確

1.1 偽冒 APP 圖示未使用透明背景，故以非白色圖片為主畫面背景，將「中華郵政」APP 圖示放置於主畫面，可判斷出惡意木馬後門 APP 帶有白邊的圖示，詳見圖 1。

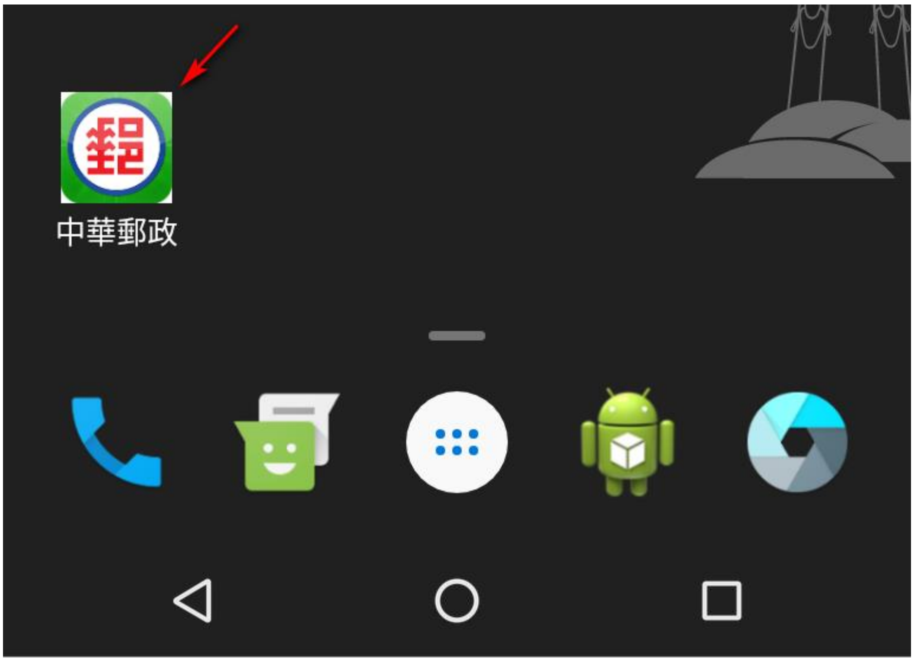


圖1 偽冒惡意木馬後門 APP 圖示

1.2 中華郵政官方 APP 名稱應為「e 動郵局」，而非「中華郵政」。以非白色圖片為主畫面背景，將 APP 圖示放置於主畫面，可看出中華郵政官方正常的 APP 圖示為完整透明背景，圖示並無帶有白邊，詳見圖 2。

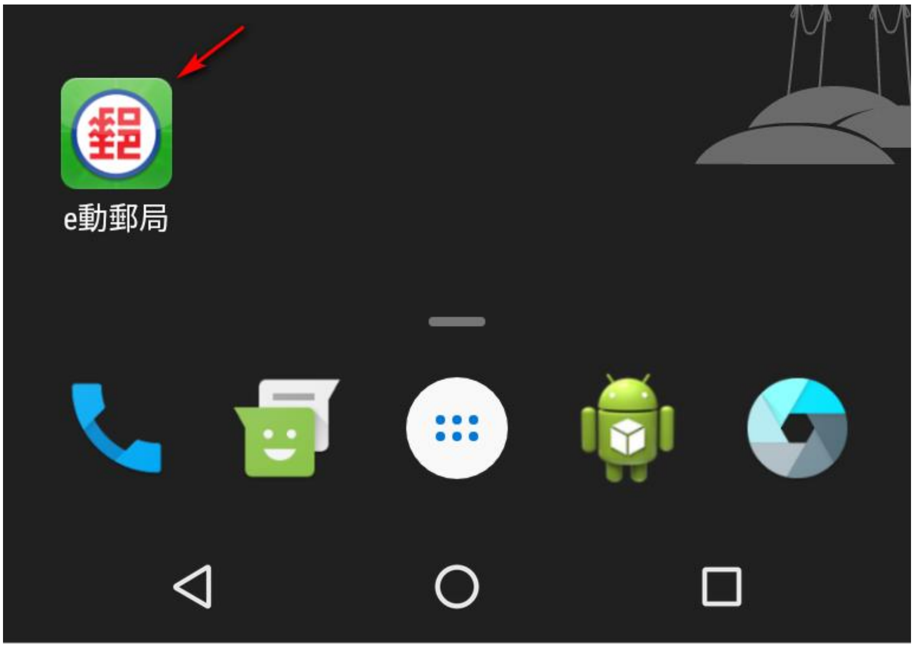


圖2　中華郵政官方正常的 APP 圖示

2　APP 啟動時的畫面

2.1　惡意木馬後門 APP 第一次啟動時，會出現請求使用者變更預設簡訊應用程式的詢問視窗，並要求「允許應用程式一律在背景執行」之權限，以達到攔截設備簡訊之目的，詳見圖 3。


圖3　惡意木馬後門 APP 第一次啟動時的畫面

2.2　中華郵政官方 APP 僅詢問存取裝置中的相片、媒體和檔案之權限，與顯示交易安全之提示訊息，並不會要求使用者變更預設簡訊應用程式與允許應用程式背景執行之權限，詳見圖 4。


圖4　中華郵政官方 APP 第一次啟動時的畫面

3　透過開發人員功能查看是否有異常 APP 在背景運行

若上述方法皆無法分辨，則可開啟開發人員功能(開啟方法請查詢各廠牌行動裝置說明書或產品支援說明)，進入[設定]→[系統]→[開發人員選項]→[正在運作的服務]，點選可疑中華郵政圖示進行檢查。正常的中華郵政 APP 下方字串為「com.mitake.android.epost」，且通常不會常駐於背景執行。但惡意木馬後門 APP 下方字串為隨機英文字，如：「da.hao.pao.bin」，詳見圖 5。


圖5　惡意木馬後門 APP 執行處理程序