遊戲手機藏毒，五步驟自保

趨勢科技指出，在大陸的 Android 第 3 方應用程式商店，發現藏於手機遊戲「Coin Pirate」中的惡意程式，一旦手機遭感染，簡訊中的個資會曝光，簡訊費用也可能暴增。

趨勢科技表示，偵測到的這隻木馬程式名為 ANDROIDOS_PIRATES.A，會隨著使用者下載「CoinPirate」這款遊戲程式感染使用者的智慧型手機；目前「Coin Pirate」已下架，但網路世界無遠弗屆，仍要提醒不小心下載的使用者注意。

過往類似的惡意程式會使用原始碼過濾受害者手機接收的簡訊，而這次的惡意程式則透過監測簡訊中特定關鍵字，像是 cash、money 等，來收集個資，將特定簡訊、國際行動設備識別碼（IMEI）與國際行動用戶辨識碼(IMSI)，相較於以往的惡意程式更具有針對性；還會利用受害者手機轉發簡訊，使受害者付出大筆的簡訊費用。除此之外，這隻木馬程式會將特定網站，以書籤的方式標註於受害者的手機網頁瀏覽器上；這些特定網站不排除藏有其他惡意程式，恐增加受害者瀏覽後中毒的機率。

趨勢科技建議，使用者在安裝任何應用程式時都應謹慎小心，請仔細閱讀程式說明，確定此程式要求使用者授與的權限是否合理。

使用者可以透過下列步驟，檢查自己的手機是否已經遭到這個惡意程式的感染：點選智慧型手機的「設定」，選取「應用程式」中的「正在運作的服務」，若發現有名為「MonitorService」檔案的存在，則手機已經遭受感染。使用者可以

手動刪除此一惡意程式：選取「設定」→「應用程式」→「管理應用程式」，然後刪除此程式。

Android 平台的智慧型手機快速普及，而針對性的惡意程式也更多，Android 智慧型手機用戶可用 5 個簡單步驟自保：

1、確實使用 Android 平台提供的基本手機防護：設定 pin 碼或是開機密碼等，可以讓手機與資料受到基本保護。

2、盡量避免使用 Wi-Fi 自動連線功能：連上開放性的網路服務，如 Wi-Fi，看似相當便利，但此類網路的開放特質如同雙面刃，會讓使用者手機中的資料暴露在輕易被有心人士竊取的風險中。

3、在下載來自第 3 方應用程式商店的應用程式(App)前，請審慎考慮。

4、當有程式或網頁請求授權時，請詳細閱讀其請求授權的內容。

5、安裝具有信譽且有效的智慧型手機防毒軟體，以保護 Android 裝置免受惡意程式威脅。

城鄉發展分署政風室關心您

(資料來源：台中高等行政法院政風室)

6.廉政會報

刪除「本分署業於 100 年 7 月 19 日召開分署廉政會報」連結

7.財產申報

附表一乙：公職人員財產申報表(報政風單位)

連結如下

http://www.moi.gov.tw/files/dcse_download2/dcse_download2_5.doc