臺灣大學計資中心網路組
北區學術資訊安全維運中心

資訊安全分析報告

目錄

手持移動裝置惡意程式分析方法簡介

摘要

手持移動裝置使用率激增，成為駭客喜好攻擊的對象，造成手持移動裝置的惡意程式大幅成長，甚至數百個第三方手持移動裝置的軟體下載網站也有惡意程式，導致使用者的個人機敏資料飽受威脅。本文除建議使用者提高警覺及安裝防毒軟體外，也提供多項防護建議措施，並提供手持移動裝置的檢測方式，讓使用者可自行檢測裝置是否存在可疑連線，只要能掌握此一分析方法，將可有效降低機敏資料外洩之風險。

手持移動裝置惡意程式興盛

根據專業網路與資安公司 Juniper Networks 統計，2012 年三月至 2013 年三月，整年度針對手持移動裝置(手機、平板電腦等)所設計的惡意程式大幅成長 614%，有將近 500 個已知的第三方手持移動裝置軟體下載網站有惡意程式，可見針對手持移動裝置所設計的惡意程式正蓬勃發展。

為何針對手持移動裝置的惡意程式會成長如此快速？這可能需要從撰寫此惡意程式之獲利來談了。移動裝置多半較桌上型或筆記型電腦更貼近人們的日常生活，可取得許多個人資訊；如電話個資、私密的文字簡訊、信用卡及密碼等機敏資料，進而結合網路交易以詐騙獲利。駭客利用惡意程式入侵手持裝置，更有機會獲得上述資料，反觀一般企業電腦網路前端多有防火牆與入侵偵測系統等資安設施進行縱深防禦，墊高駭客攻入之困難度。而手持移動裝置多直接暴露於網際網路中，缺少有效的防護機制，駭客轉而攻擊手持移動裝置，以較少的成本與較多的機會獲利。

根據統計全球 65%以上的智慧型手機是 Android 作業系統，所以駭客入侵手持移動裝置也挑選最受歡迎的 Android 系統。近期發生的小額付款簡訊詐騙事件，也是僅針對 Android 作業系統進行攻擊，透過各種詐騙簡訊(*快遞簽收,或信用卡刷卡通知*)誘騙使用者點擊簡訊中的超連結，而這些超連結都經過”縮網址”處理，使用者不易得知將導向哪個網站，如下圖所示。

而超連結通常將導向攻擊者所擁有的雲端空間，並包含一個惡意的 APK 檔案(Android 系統中 APP 安裝檔的副檔名)，一旦使用者點擊下載安裝該 APP 後，惡意程式於背景環境下運作，當攻擊者使用受害手機門號進行小額付款時，所傳送至受害者手機中的簡訊認證碼即會遭竊取，讓駭客得以順利完成小額付款交易。特別的是，即使使用者手機並未 root(取得管理者權限)，一旦點擊超連結並安裝 APK 檔案後亦會受感染。

如何避免手持移動裝置遭植入惡意程式

預防手持移動裝置遭植入惡意程式多半可分為幾類方法，即提高警覺、安裝專用防毒軟體等，本文將再多加說明如何自己進行分析，以做到第一時間防護的層級。

首先是提高警覺，大部分讀者在使用傳統電腦上，應已十分瞭解，但手持移動裝置如上述之統計資料，有近 500 個已知軟體下載網站包含惡意程式，這個情況讓許多使用者上網下載軟體時，很容易就遭植入惡意程式。故在手持移動裝置軟體安裝上，需更加小心與留意其來源位置，對於來路不明的手機程式不要任意安裝，收到來路不明的簡訊，不要打開直接刪除而下載軟體、遊戲等，請至合法官方網站下載。

在防毒軟體部分，相信讀者應不陌生其運作原理，但讀者仍需注意，許多手持移動裝置，會在使用者未同意情況下，將部份資訊送出，這部分是需特別留意，甚至許多來路不明或打著免費旗號的防毒軟體，本身就是惡意程式或間諜軟體，故仍請讀者至合法官方網站下載，降低風險。

建議 Android 平台使用者，將手機設定中"**允許安裝非 Market 應用程式**"或"**允許安裝來路不明的應用程式**"(名稱各 android 版本不盡相同)選項**關閉**

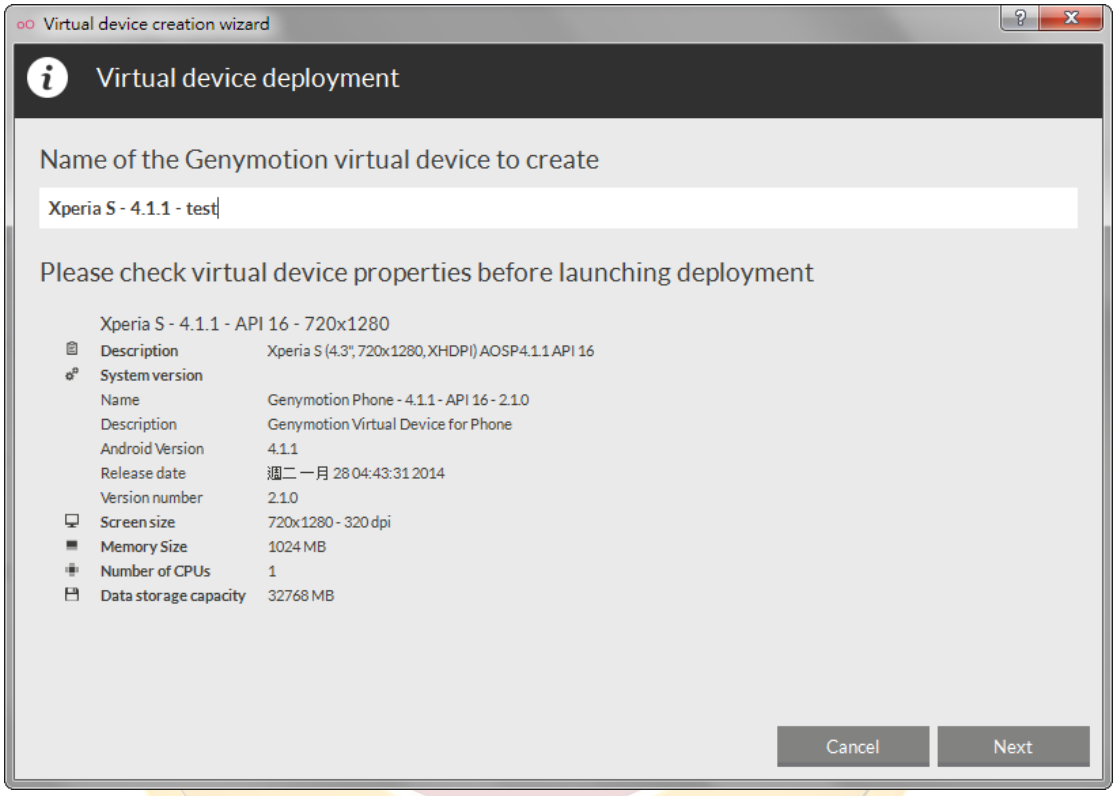
如此一來，使用者即使不小心點擊含有惡意 APK 的網址，惡意程式也會因系統未開放安裝來路不明的應用程式而無法感染系統，確保使用者機敏資料之安全。

除提高警覺、安裝防毒軟體及關閉自動安裝應用程式功能之外，本文將提供更積極做法，使讀者能自行檢測可疑連線，因為建立連線為多數惡意程式運作之第一步驟，只要能掌握此一分析方法，可有效降低資料外洩之風險。

如何自行分析手持移動惡意程式

使用環境:

於本次測試環境中，所使用的 android 模擬器為 Genymotion，模擬環境為 Xperia S, OS 版本為 4.1.1。



接著於模擬器環境中，安裝下列三項軟體：

安智市場

程式網址: *http://www.anzhi.com/soft_1318407.html*

Android Terminal Emulator

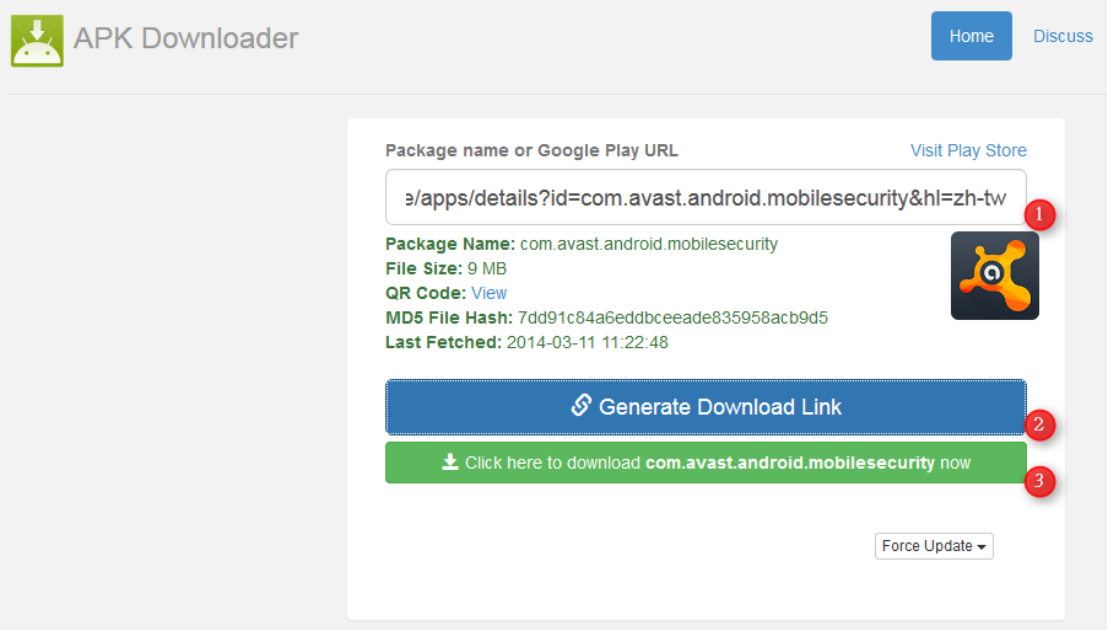
程式網址:

https://play.google.com/store/apps/details?id=jackpal.androidterm&hl=zh_TW

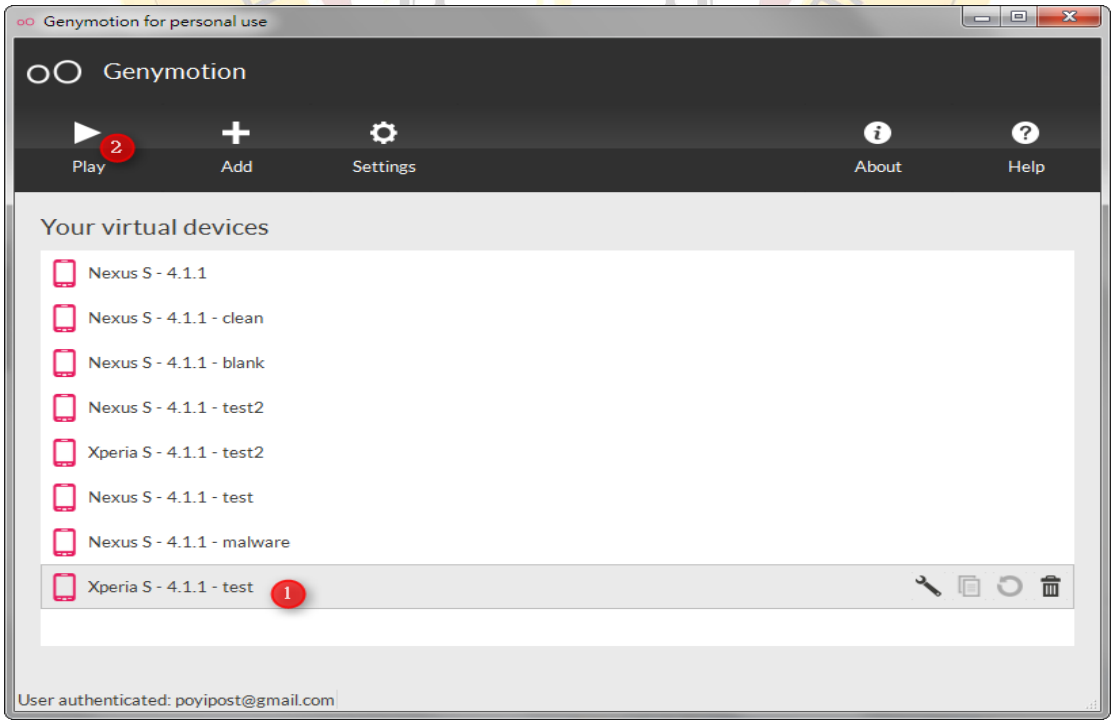
AVG AntiVirus FREE

程式網址: *https://play.google.com/store/apps/details?id=com.antivirus&hl=zh-tw*

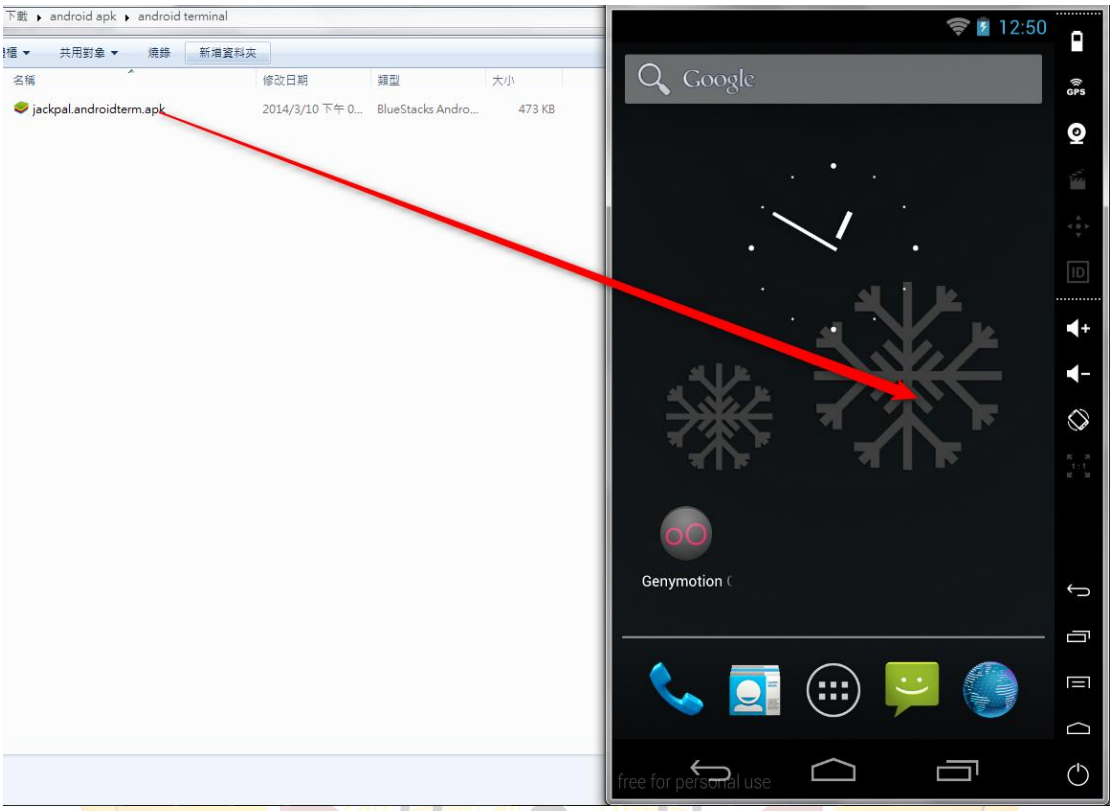
由於本次所使用的模擬環境並沒有內建 Google 相關的服務，因此對於 Google Play 商店中提供的應用程式，我們可以利用 APK downloader 取得 APK；網址為 http://apps.evozi.com/apk-downloader/，只需要將想要取得的 APP 在 Google Play 商店上的網址鍵入即可下載取得該 APP 的 APK 安裝檔。



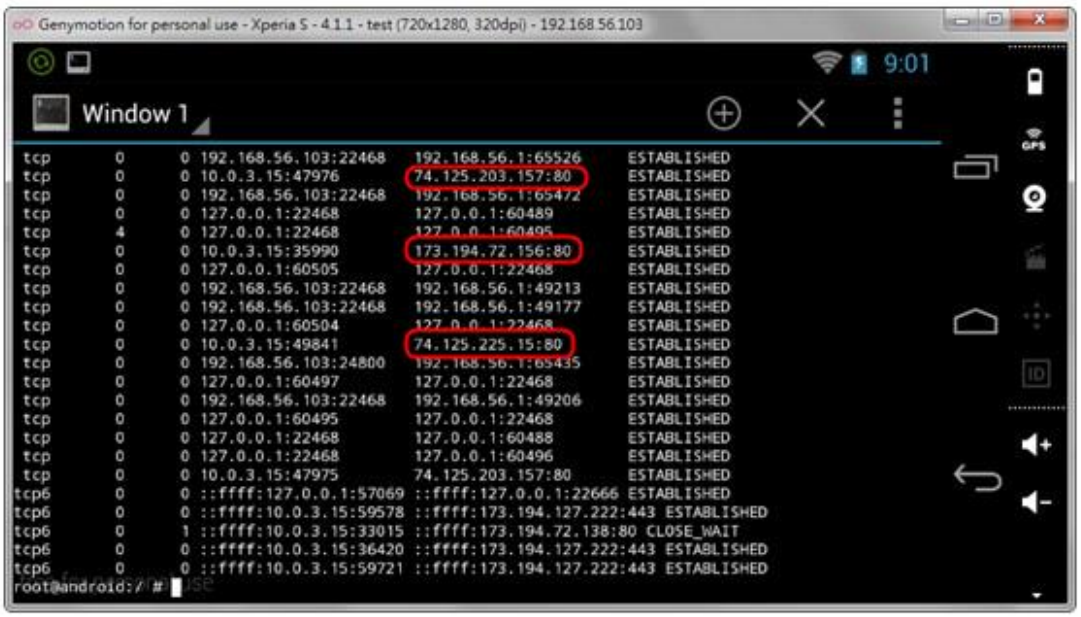
在建立好模擬環境並取得了所需的應用程式後，我們可以開啟模擬環境使用。



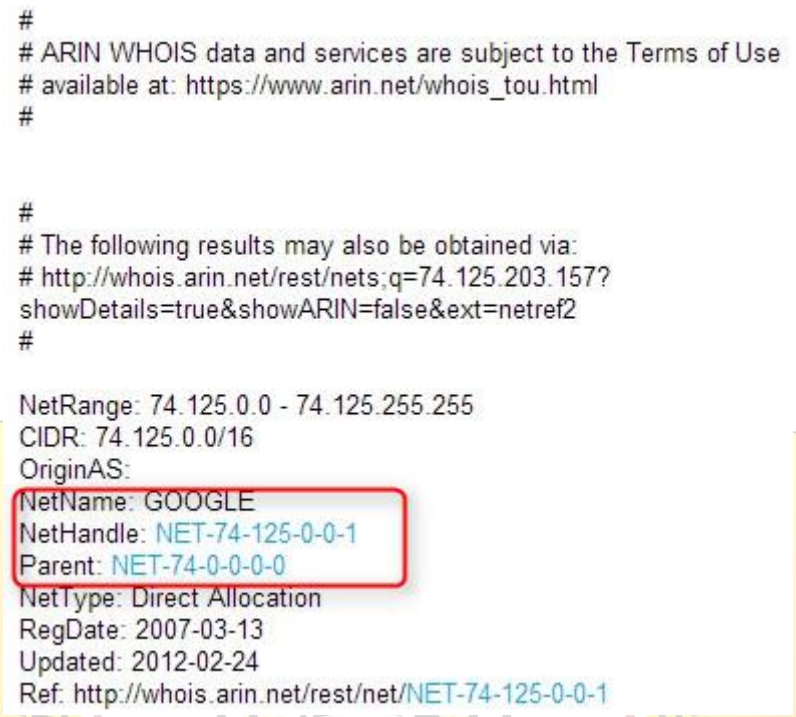
等待模擬環境開啟後可直接將 APK 安裝檔拖拉進模擬器的視窗內，即可在模擬環境裡安裝應用程式。



利用「安智市場」應用程式下載一個惡意軟體進行分析之前，先利用 Android Terminal Emulator 軟體來檢視目前模擬器環境中的網路連線狀況。



可透過 *http://www.whois365.com/tw/about* 查詢 IP 相關資訊，經查詢 74.125.203.157 為 Google 所使用之 IP。



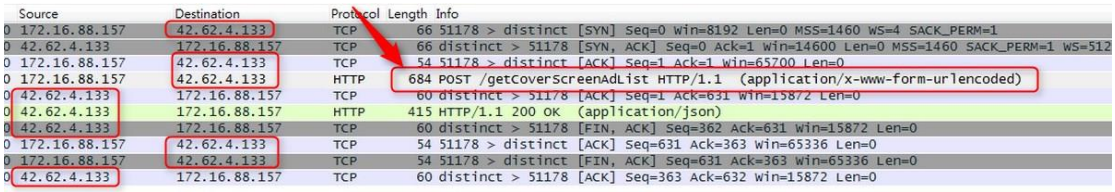
另外對於 74.125.225.15 以及 173.194.127.222 和 173.194.72.138 這三個 IP，也可以查詢出均為 Google 所屬 IP 範圍。到目前為止，可以初步判斷這三個 IP 連線均屬正常。

接著透過「安智市場」應用程式下載並安裝帶有惡意行為的 APP，如下圖所示。

然後利用先前所安裝的 AVG AntiVirus FREE 進行掃描，以證實安裝的 APP 是否為惡意程式。


3:48
應用詳情
簡介
評論
歷史版本
選擇要使用的應用程式
安裝前掃描病毒
程式安裝器
一律採用
僅限一次
吓尿，玩了半天最高分2分，真心太难了，截图
作者： 大虫虫
分享
安裝
收藏
free for personal use

掃瞄結果，該 APP 被 **AVG AntiVirus FREE** 判定為為惡意程式，我們仍進行安裝並利用 Wireshark 軟體側錄網路封包，並且再利用 **Android Terminal Emulator** 軟體檢視網路的連線狀況。我們可以發現在安裝此軟體後，系統與 *42.62.4.133* 建立連線，利用 Wireshark 檢視與此 IP 的連線情形，可發現系統將資料往外傳送。如下圖所示。



透過這些工具及檢測流程，使用者可在 Android 系統中，自我檢測手機程式是否有可疑的行為。於本範例中，在未經使用者授權的情況下，便自行向外傳遞資訊，洩露使用者隱私，更是常見的惡意行為之一。

Android 平台相較於其他移動裝置的作業系統較為開放，造成惡意程式的比例也較高，使用者在下載及使用 APP 時，應慎選軟體來源，切勿安裝來路不明的 APP，或不受信任的第三方軟體，即使是於 Google 官方 Google Play 所下載的 APP，在安裝前也需確認 APP 所需之權限，若對於 APP 安全性有疑慮，則可透過本篇自我檢測方式進行惡意程式的活動分析，進一步確認該 APP 是否有異常行為。

結論

Juniper Networks 指出，超過 500 個第三方 App Stores 上有惡意程式流竄，使得惡意程式擴散更加快速，使用者認為安全的下載平台，居然包含大量惡意程式。另一方面，攻擊者透過電腦將惡意程式傳入行動裝置，此種混合式威脅，加重手持移動裝置遭受感染的機會。

下列為針對手持移動裝置的資安防護建議，依據此建議執行，可大幅降低遭受惡意程式入侵風險。

1. 保持設備資安完整性，勿自行修改或破解行動裝置之安全措施，如越獄與 ROOT，此將讓惡意程式有機會使用最高權限執行程式。
2. 謹慎下載軟體與使用，僅安裝來自可信任來源之軟體，如 Apple Store 與 Google Play，切勿自不明之第三方軟體市集下載軟體。
3. 軟體安裝時所要求之權限是否合理，是否有過多的存取權限，如計算機軟體要求使用自動撥號功能與使用 Internet 等。
4. 定期更新軟體與修補程式。
5. 安裝具公信力之資安防護軟體。
6. 不使用手持移動設備進行重要交易行為。
7. 小心使用公開且無加密之 Wi-Fi 無線網路，極可能會竊取您的機敏資料。

參考資料

1. http://news.cnet.com/8301-1009_3-57591042-83/mobile-malware-grows-by-614-percent-in-last-year/
2. http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=7547
3. http://www.chinatimes.com/realtimenews/20140415002833-260405
4. http://moscoat.pixnet.net/blog/post/176915142-%E3%80%90%E5%B0%B1%E6%83%B3%E8%A9%90%E9%A8%99%E4%BD%A0%E3%80%91%E5%B0%8F%E5%BF%83%E7%B0%A1%E8%A8%8A%E8%88%87%E9%80%A3%E7%B5%90%EF%BC%8C%E5%88%A5%E8%AE%93%E8%87%AA%E5%B7%B1%E8%AA%A4
5. https://www.ezlawyer.com.tw/eb/eb_app.html