不知名 Android 勒贖軟體潛伏 4 小時才發作，能避開防毒軟體偵測

研究人員指出這隻勒贖軟體來自俄羅斯，寄生於知名 app 以感染被害者的裝置，一旦被害者的裝置遭感染後，它會以加密通訊和外部的 C&C 伺服器聯繫，並會蟄伏 4 小時後才活動，躲避防毒軟體偵測。

惡意程式安全公司 Zscaler 發現，一隻 Android 勒贖軟體運用極為高明的手法，能感染合法 App 下載到用戶裝置上，同時潛伏 4 小時躲避所有防毒軟體的偵測。

Zscale 下的 ThreatLabZ 小組研究人員發現，這隻未命名的 Android 勒贖軟體來自俄羅斯，專門鎖定知名 app 執行一系列自動化程序加以感染。其中一個寄生的 app 俄羅斯最受歡迎的娛樂社群 app OK，後者在 Google Play Store 下載數達 5000 萬到 1 億次。它會先反組譯目標 app，在其 AndroidManifest.xml 檔注入必要的指令及 Activity/BroadcastReceiver 變項、複製圖檔及 layout 檔，再寫入勒贖軟體的勒贖文字、字串及攻擊程式感染 apk，等待受害者上門。

不知情的用戶將 app 下載到行動裝置中後數小時，這隻勒贖軟體會展開看似普通的勒贖過程。首先，用戶會看到一個對話框，當中提供數種惡意行為的啟動選項。如果用戶按下「取消」選項，這個對話框會立即再出現，讓使用者沒有時間採取任何動作或卸載 app。若用戶按下「啟動」鍵，手機螢幕會立即被鎖定，發出訊息通知外部 C&C 伺服器，同時出現勒贖文字，以用戶造訪兒童色情內容遭到鎖定，要求用戶在 12 小時內支付 500 盧布作為罰金，

用戶若未付贖金，歹徒就會將用戶行徑公諸於世，而嘗試解鎖者則可能遭到整支手機被鎖，以及個人資料被貼上網的懲罰。

這隻惡意程式手法看起來沒什麼了不起，但它有項超越其他勒贖軟體的能力。研究人員指出，它對外連接的 C&C 伺服器 IP 位址、電話號碼皆以 AES (Advanced Encryption Standard) 加密，而且它所注入的字串、方法及變項都被混淆而難以理解，同時大部份方法是以 Java 映射(Java Reflection)機制呼叫來躲過防毒軟體的狀態分析偵測。

此外，由於大部份防毒程式會針對 app 行為執行數秒到數分鐘的偵測，這隻惡意程式碼竟然會蟄伏 4 小時後才開始活動，藉此躲避防毒軟體的動態分析。

而更糟的是，研究人員發現這隻勒贖軟體並沒有證實用戶是否付款的機制。也就是說，即使用戶付了錢也無法解鎖。

Zscale 表示，從這隻勒贖程式高明感染手法來看，可以想見 Google Play Store 上應該已有不少合法 app 受害。所幸中毒解決方法並不難；只要將手機或平板在安全模式下重新開機，移除被勒贖軟體感染 app 的裝置管理員權限後，將 app 卸載，再重新以一般模式開機即可。目前 Google Play 上也未發現有其他新變種。

資料來源：iThome