Forensics 鑒真數位
專業數位資訊鑑識公司

iForensics App Sandbox

行動應用App沙箱檢測平臺

採用先進實體機沙箱技術，忠實呈現App的惡意行為分析

- 搭配實體機進行檢測，使App不會因偵測到模擬環境而終止
- 透過瀏覽器即可進行動靜態分析，不遺漏存取行為及連線資訊
- 分析結果直接警示是否有危險權限使用，並視覺化呈現對外連線之IP地理位置

主要功能

iForensics App Sandbox 行動應用App沙箱檢測平臺
App資安檢測利器，採用實體機沙箱技術，忠實呈現App的惡意行為分析

鑒真數位鑑識檢測實驗室

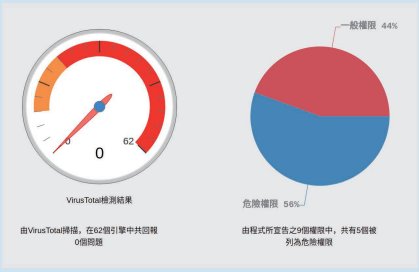
專案索引　報告檢視　專案建立　權限批准　專案維護　分析進度　登出　目前使用者:admin

Report ID:　SD - apptest_du.tri.register 2020/12/18 10:46:07

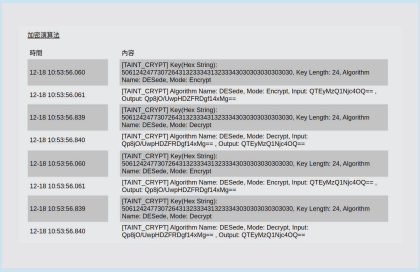
行為分析

行為	動態	靜態	行為	動態	靜態	行為	動態	靜態
使用JNI			手機號碼存取			網路通訊行為	✓	✓
電話撥接行為			藍芽存取		✓	行事曆存取		✓
NFC存取			簡訊收送			Wi-Fi存取		✓
SD卡存取			聯絡人存取			手機資訊存取		✓
GPS存取		✓	相機存取		✓	檔案增刪改異動		✓
程式提權			溫度感應器存取		✓	電源狀態存取		✓
開機啟動			加密演算法	✓	✓	資料庫存取	✓	✓

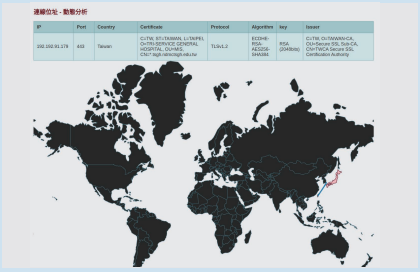
1 獨家動態分析模式，直接觸發可疑檔案，以模擬更精準且實際之惡意行為



2 支援 App Hash 並自動查驗VirusTotal惡意程式評比，搶先鎖定可疑權限

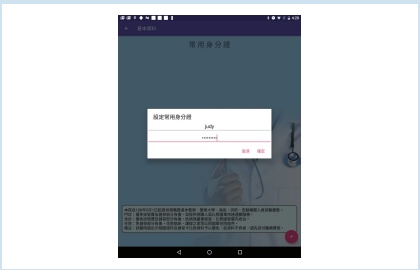


3 以動態分析捕捉App所採用之加密演算法及金鑰，以更快確認是否有敏感資訊被寫死在程式中

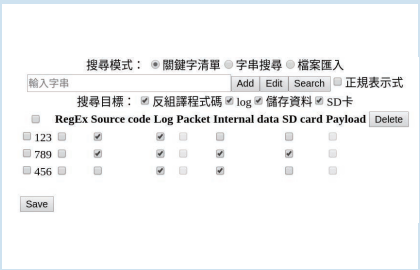


4 可直接側錄及解析未加密之網路封包，並鎖定目的端IP之地理位置

5 同一沙箱可執行多次App分析，大幅減少作業程序



6 可手動分析彈性處理案件，並更容易鎖定特定目標



7 支援事先定義關鍵字群組，用於不同App之檢測結果比對，並進行交叉分析

www.iforensics.com.tw

Forensics 鑒真數位
專業數位資訊鑑識公司

電話：(02)2517-2532　service@iforensics.com.tw
傳真：(02)2517-1097　台北市中山區松江路309號11樓之5