Kryptowire 榮獲
2019 IDC MarketScape MAST 領導者殊榮

kryptowire

04

你安裝的 Mobile App 安全嗎？

2018 年美國國土安全局委託 Kryptowire，針對 Google Play Store、Apple App Store 兩大平台商店上，北美區最熱門 Top100 的應用程式進行檢測，經過 Kryptowire 檢測後，發現前百大 Android App 有 9% 的 APP 存在憑證安全問題，iOS App 有 15% 的 App 使用強度不足的加密方式。

關於 Kryptowire

成立於 2011 年，總部位於弗吉尼亞州泰森角（Tysons Corner），由美國國防高級研究計劃局（DARPA）和美國國土安全部（DHS S & T）獨立出來成立的技術單位。主要提供企業、政府機關組織自動化軍用級軟體保證和合規性測試技術。現有美國政府機構、國家有線電視公司等客戶。

產品介紹

現今開發的行動應用程式數量不斷增加，檢測技術人員數量無法滿足行動應用程式增加的速度，同時人工檢測的流程曠日費時，難以滿足現今企業頻繁更新行動應用程式版本的需求，企業期望公司發行的行動應用程式符合行業、政府所訂定的資訊安全、隱私標準和法規。透過 Kryptowire 可在軟體發佈上線之前自動檢測行動應用程式合規性，並提供完整跟詳細的資安測試報告。

優良表現

2018
Kryptowire 資安檢驗發現 33 個 CVE 的資安風險與弱點（涵蓋 13 個 Android 供應商）

2019
Kryptowire 資安檢驗發現 146 個 CVE 的資安風險與弱點（涵蓋 29 個 Android 供應商）

2019
Kryptowire 與伊利諾伊大學供同組隊開發的自動網絡安全系統獲得美國國土安全部頒發的邦克獎（Bang for the Buck Award）

Kryptowire 產品的獨特之處

免原始碼
免提供原始碼即可進行完整的資安檢測

快速提供檢測結果
數小時即可取得檢測報告，並附上問題說明以及解決方案

雙平台支援
業界唯一完全支援 iOS 跟 Android 平台

多元檢測結果
提供行動應用程式的安全、隱私、裝置授權情況

全自動化檢測
只需上傳 .apk 跟 .ipa 檔案，無需人工介入即可完成測試

傳輸資料分析
提供行動應用程式的傳輸方法、流向、資料內容

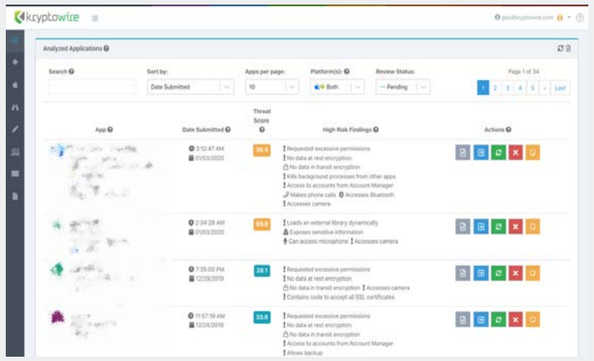
支援多項國際規範
OWASP、NIAP、NIST、GDPR、PCI、 HIPAA、等國際規範

動態程式分析
支援雙平台動態程式碼的執行分析報告

Web 操作介面

簡易操作，快速上手

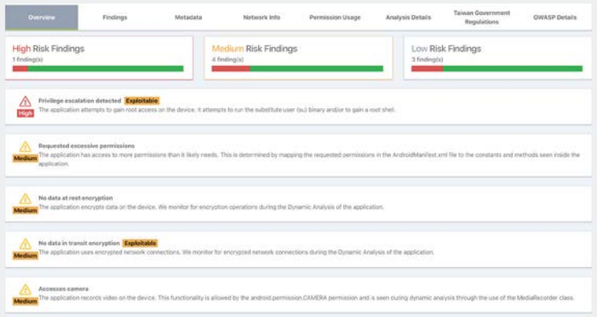
操作介面、檢測方式簡便，讓工具變成程式開發者、管理者的堅強後盾。



完整分析報告

提供詳細分類清楚的資安分析報告

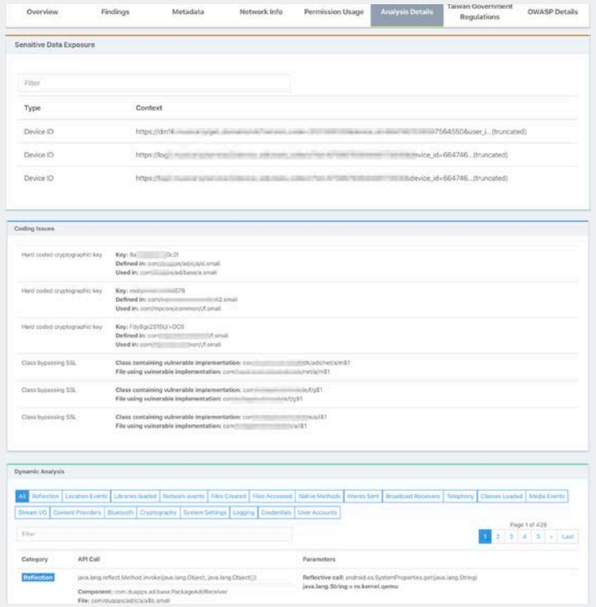
條列資安風險的類型與問題、完整的隱私權與裝置權限使用情況。



動態程式分析

呈現程式執行時的真實面貌

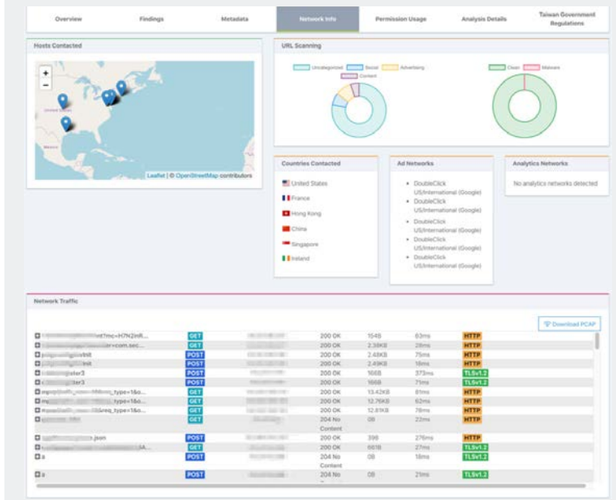
透過動態分析資料，可條列出程式執行時使用的 Library、Function、 Framework、變數、參數等資訊以及程式的資安問題。



資料流向報告

確實掌握資料流向

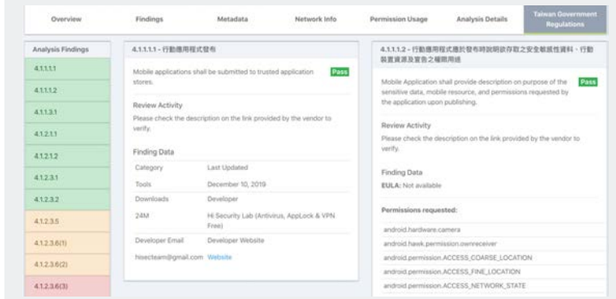
提供行動應用程式對於資料傳輸時，採用的傳輸方式、內容、協定等資訊，並記錄資料傳送到之位址以及網路傳輸是否使用安全的傳輸的規範。



標準行動應用 App 基本資安規範

由經濟部工業局推動，提升國內重要單位、企業之 App 安全

Kryptowire 可協助公司自我檢測，確認 App 是否符合政府訂定之安全規範，提升 App 安全層級同時達到保護客戶隱私的目的。

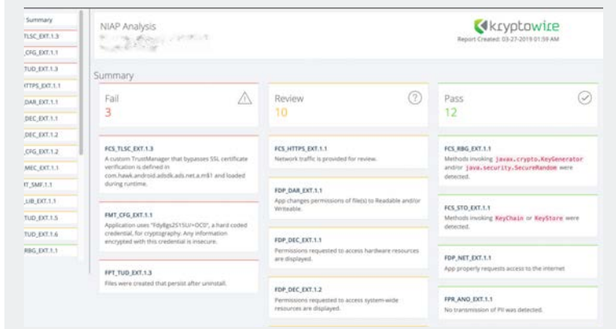


支援美國聯邦政府使用之檢測標準

(NIAP Protection Profile for Application Software)

美國國家資訊安全保障組織 (NIAP) 針對 Mobile App 訂定之檢測標準

使用 Kryptowire 讓公司的 App 可與國際資安標準接軌，進而提升 App 安全，提高資安能量是對消費者的保障，更是公司的提升資訊安全最佳的捷徑。

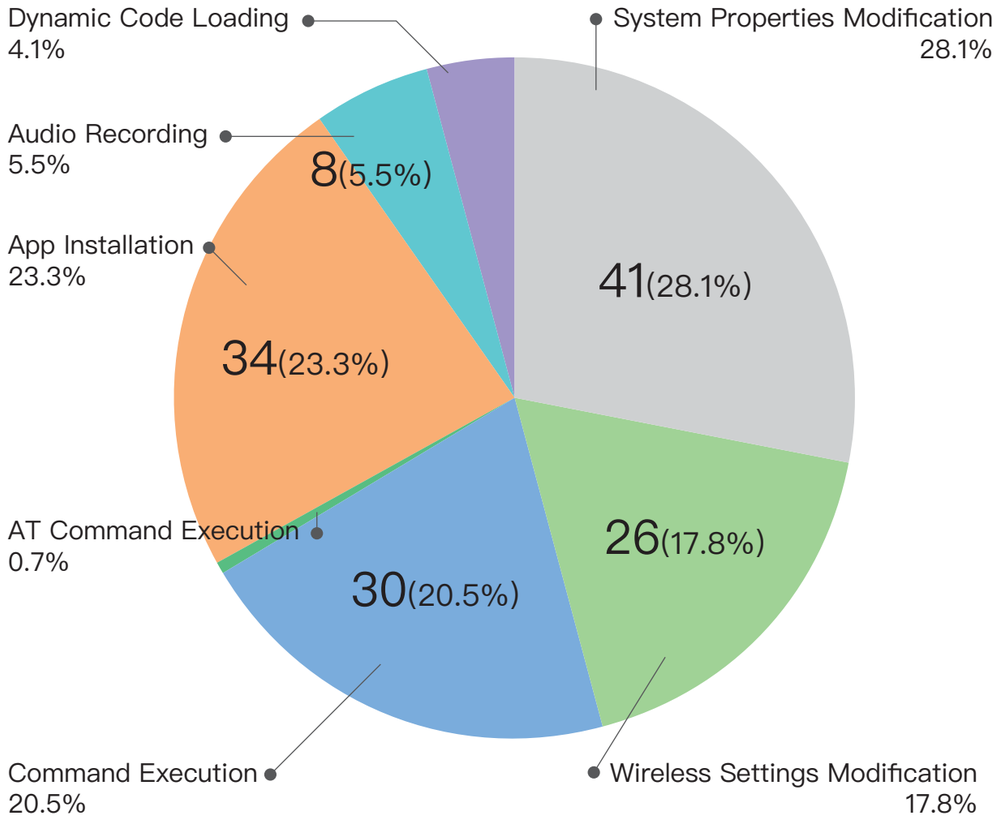


你的物聯網裝置韌體安全嗎

Android 作業系統的物聯網裝置，在出廠時已預載了應用程式和韌體。預載的應用程式大多數功能無法提供使用者主動關閉並且在預設設定上擁有較高的權限 (Root) 可直接存取系統功能。除此之外，裝置預載的應用程式、韌體恐因以下幾種原因，導致發生潛在遠端和本地端之可利用漏洞、存在 " 後門 " 功能、主動洩漏裝置資料等漏洞或惡意行為。

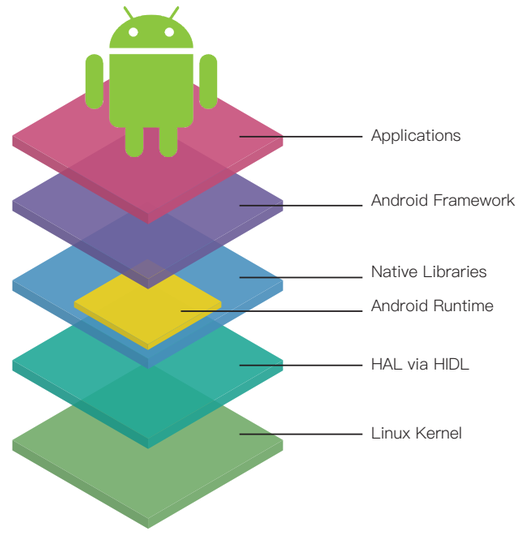
- 無法確認供應商提供官方程式碼安全性
- 無法確認硬體供應商提供軟體安全性
- 非 / 故意暴露敏感性功能 (如：側錄麥克風、網路傳輸資料等)

為了量化 Android 作業系統裝置上之預載的應用程式和韌體中存在漏洞以及隱私暴露程度，Kryptowire 分析各種 Android 供應商和運營商的裝置，在 2019 年共發現的 146 個 CVE 弱點，其中的弱點種類分如下：

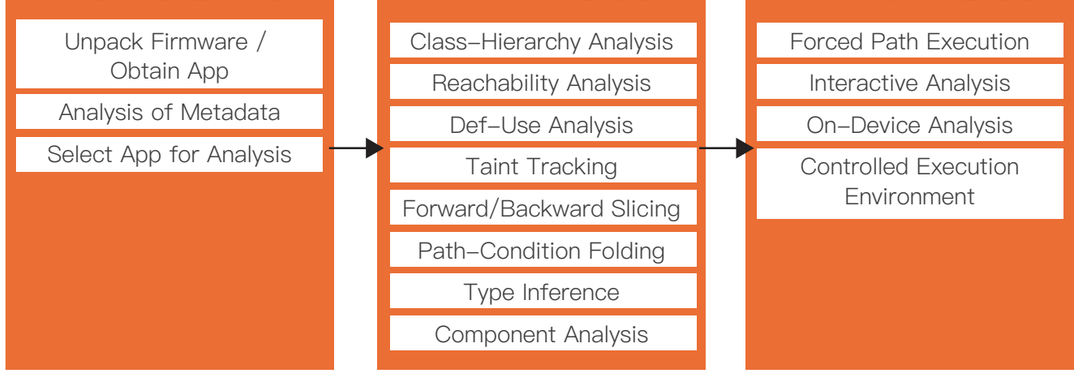


Krytpowire 韌體掃描

1. **取得 Mobile App 和韌體**
   將韌體 Image 檔以及內部 App 傳入分析系統中 (雲端檢測服務或建置離線檢測系統)
2. **發現的漏洞**
   系統會報告漏洞的類型（如：命令執行、竊取個人資料）和相關漏洞佐證的資料
3. **產生的漏洞**
   顧問人員可利用自動化系統的輸出來驗證和生成概念驗證漏洞。POC 可以在實際環境中進行測試和驗證



Krytpowire 弱點發現引擎



Kryptowire 弱點檢測模組

- PII leakage
- Command execution
- Record audio
- Record audio
- Capture screenshot
- SMS sending
- Modification of system properties
- App installation
- Sending AT commands
- Logcat leakage
- Factory reset
- Dynamic code loading and execution
- Modification of wireless setting