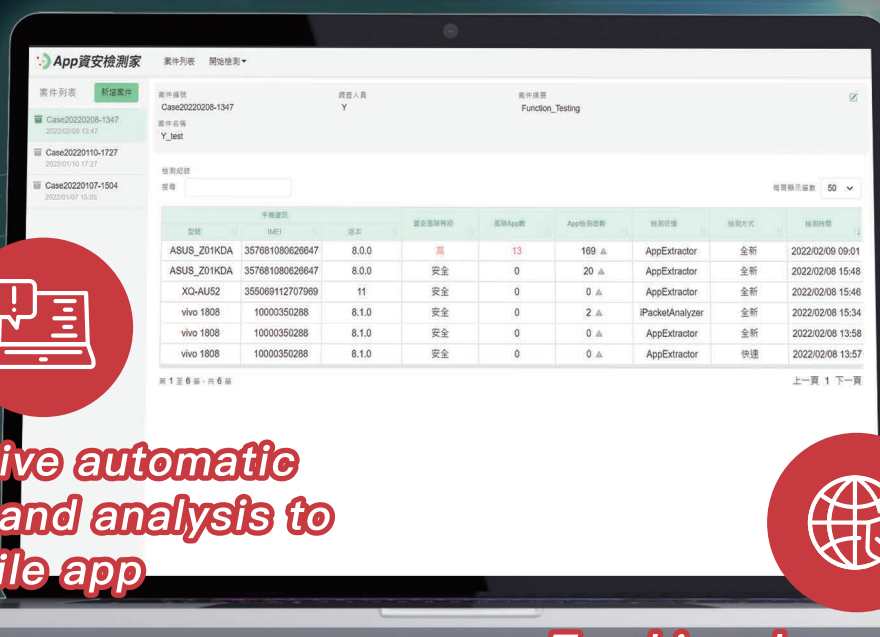




AppDetector



App資安檢測家

案件列表 開始檢測

案件編號: Case20220208-1347 檢定人員: Y 檢中檔案: Function_Testing

案件名稱: Y_test

檢定紀錄

| 型別 | 手機號碼 (IMEI) | 版本 | 安全風險等級 | 惡意App數 | App檢出總數 | 檢出設備 | 檢出方式 | 檢出時間 |
|-------------|------------------|-------|--------|--------|---------|-----------------|------|------------------|
| ASUS_Z01KDA | 357681080628647 | 8.0.0 | 高 | 13 | 169 | AppExtractor | 全新 | 2022/02/09 09:01 |
| ASUS_Z01KDA | 357681080628647 | 8.0.0 | 安全 | 0 | 20 | AppExtractor | 全新 | 2022/02/08 15:48 |
| XQ-AU52 | 3550698112707969 | 11 | 安全 | 0 | 0 | AppExtractor | 全新 | 2022/02/08 15:46 |
| vivo 1808 | 10000350288 | 8.1.0 | 安全 | 0 | 2 | iPacketAnalyzer | 全新 | 2022/02/08 15:34 |
| vivo 1808 | 10000350288 | 8.1.0 | 安全 | 0 | 0 | AppExtractor | 全新 | 2022/02/08 13:58 |
| vivo 1808 | 10000350288 | 8.1.0 | 安全 | 0 | 0 | AppExtractor | 快速 | 2022/02/08 13:57 |


第 1 頁 共 5 頁



Non-invasive automatic examination and analysis to mobile app




Tracking down App-related information security risks with ease



Fast security analysis and risk level evaluation to target mobile device via app inspection



Conduct effective and thorough information security inspection via data verification with international security database



Straight-forward visualization and forensic report. Get the result with speed and seal the deal

Main Functions



«AppDetector» is a non-invasive, automatic app inspection and security risk evaluation solution. With its robot-based process, packet networking analysis, data verification, and risk level evaluation can be done with ease and speed. «AppDetector» has been utilized in different sectors and scenarios, including law enforcement, other government agencies, information security auditing, internal investigation, etc.

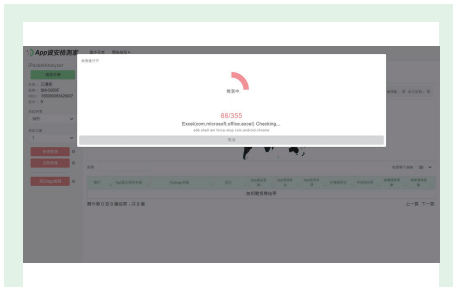
| 警告 | App程式檔案名稱 | Package名稱 | 版本 | App安裝日期 | App安裝評估 | App使用來源 | App風險評估 | 防護層評估 | 防護層來源 |
|----|--------------------------|---|------------------|---------|---------|---------|---------|-------|-------|
| 異常 | Device configuration | android.autoinstalls.config.asus.pai | 1013 | 低 | 有 | 外部傳真 | 無比對資料 | 無檢測來源 | |
| 異常 | Certificate Installer | com.android.certinstaller | 8.0.0 | 低 | 有 | 外部傳真 | 無比對資料 | 無檢測來源 | |
| 異常 | Package Access Helper | com.android.defcontainer | 8.0.0 | 低 | 有 | 外部傳真 | 無比對資料 | 無檢測來源 | |
| 異常 | Android Easter Egg | com.android.egg | 1.0 | 低 | 有 | 外部傳真 | 無比對資料 | 無檢測來源 | |
| 異常 | BatteriesOH_v1.0.0.5 | com.asus.batteriesoh | 1.0.0.5 | 低 | 有 | 外部傳真 | 無比對資料 | 無檢測來源 | |
| 異常 | FM Radio | com.asus.fmradio | 1.61.0.62_18040g | 低 | 有 | 外部傳真 | 無比對資料 | 無檢測來源 | |
| 異常 | com.asus.fmservice | com.asus.fmservice | 1.62.180321 | 低 | 有 | 外部傳真 | 無比對資料 | 無檢測來源 | |
| 異常 | FocusAppListener | com.asus.focusapplistener | 2.1.0.38_180116 | 低 | 有 | 外部傳真 | 無比對資料 | 無檢測來源 | |
| 異常 | ASUS ZenUI | com.asus.res.defaulttheme | 4.0.0.2_170801 | 低 | 有 | 外部傳真 | 無比對資料 | 無檢測來源 | |
| 異常 | TermsAndConditionWebView | com.asus.setupwizard.suwinspi.resusushmviewer | 4.0.0.13_180528 | 低 | 有 | 外部傳真 | 無比對資料 | 無檢測來源 | |
| 異常 | Gmail | com.google.android.gm | 2022.01.08.4234 | 低 | 有 | 外部傳真 | 無比對資料 | 無檢測來源 | |

AppDetector

1 Supports non-invasive, automatic data verification and analysis to mobile apps.



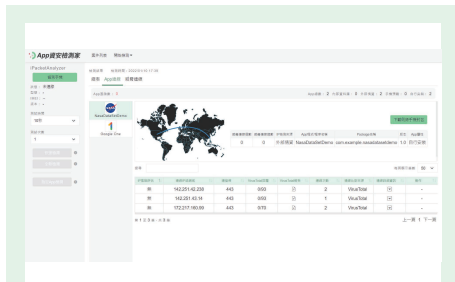
2 Aside from apps on local device, AppDetector can also automatically download apps from app marketplace and conduct automatic analysis.



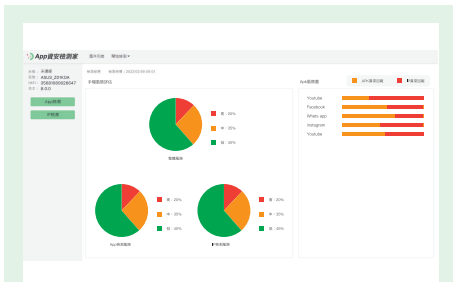
3 Supports packet capture and packet networking analysis. Detect connection in which risky IPs and URLs are involved.

| 警告 | App程式檔案名稱 | Package名稱 | 版本 | App安裝日期 | App安裝評估 | App使用來源 | App風險評估 | 防護層評估 | 防護層來源 |
|----|--------------------------|---|------------------|---------|---------|---------|---------|-------|-------|
| 異常 | Device configuration | android.autoinstalls.config.asus.pai | 1013 | 低 | 有 | 外部傳真 | 無比對資料 | 無檢測來源 | |
| 異常 | Certificate Installer | com.android.certinstaller | 8.0.0 | 低 | 有 | 外部傳真 | 無比對資料 | 無檢測來源 | |
| 異常 | Package Access Helper | com.android.defcontainer | 8.0.0 | 低 | 有 | 外部傳真 | 無比對資料 | 無檢測來源 | |
| 異常 | Android Easter Egg | com.android.egg | 1.0 | 低 | 有 | 外部傳真 | 無比對資料 | 無檢測來源 | |
| 異常 | BatteriesOH_v1.0.0.5 | com.asus.batteriesoh | 1.0.0.5 | 低 | 有 | 外部傳真 | 無比對資料 | 無檢測來源 | |
| 異常 | FM Radio | com.asus.fmradio | 1.61.0.62_18040g | 低 | 有 | 外部傳真 | 無比對資料 | 無檢測來源 | |
| 異常 | com.asus.fmservice | com.asus.fmservice | 1.62.180321 | 低 | 有 | 外部傳真 | 無比對資料 | 無檢測來源 | |
| 異常 | FocusAppListener | com.asus.focusapplistener | 2.1.0.38_180116 | 低 | 有 | 外部傳真 | 無比對資料 | 無檢測來源 | |
| 異常 | ASUS ZenUI | com.asus.res.defaulttheme | 4.0.0.2_170801 | 低 | 有 | 外部傳真 | 無比對資料 | 無檢測來源 | |
| 異常 | TermsAndConditionWebView | com.asus.setupwizard.suwinspi.resusushmviewer | 4.0.0.13_180528 | 低 | 有 | 外部傳真 | 無比對資料 | 無檢測來源 | |
| 異常 | Gmail | com.google.android.gm | 2022.01.08.4234 | 低 | 有 | 外部傳真 | 無比對資料 | 無檢測來源 | |

4 Supports risk level and security score evaluation according to the analysis and verification results.



5 Support visualization of packet networking analysis with world maps, helping investigators track down information security risks.



6 Supports visualization of inspection summary with statistical charts/graphs (e.g. quantity of analyzed apps, risk level percentage of apps, etc.)



7 Supports forensic report generation, making it easy and effective for investigators to present analysis result.