Quark Engine 廣告宣傳手冊

Quark Engine 是什麼?

Quark Engine 為針對 Android 平台之惡意程式評分系統。藉由解構犯罪行為階段論，設計出 Android 惡意行為 5 階段檢查。除此之外，Quark 也開發 2 種類型之分析報告，以及 4 種圖形化分析情資，提供惡意程式分析師獨特之分析視角，並提升其分析效率。

Quark Engine 為 rule-base 分析引擎，目前已精選出 192 條規則，且規則會持續更新。除此之外，惡意程式分析師可依其需求，自行撰寫惡意行為偵測規則。

此外，我們也開發 Dalvik Bytecode loader (Dalvik 為執行 Android 應用程式之核心)。該技術為 Quark 做到汙點分析 (Tainted analysis) 並且可抗基本混淆技術 (隨機更改變數與函式名稱)。

Quark Engine 為 Github 平台之開源專案，其 Github 頁面可於 [1] 查閱。Quark 在 Github antivirus 分類中，為星星數 PR 96 之專案。成為開源專案使 Quark 能與全世界共享其技術，同時，也能吸收來自世界各地之開發能量。到目前為止，已有許多開發人員為我們貢獻新功能，以及協助維護 Quark，同時也獲得許多合作機會與成長力量。

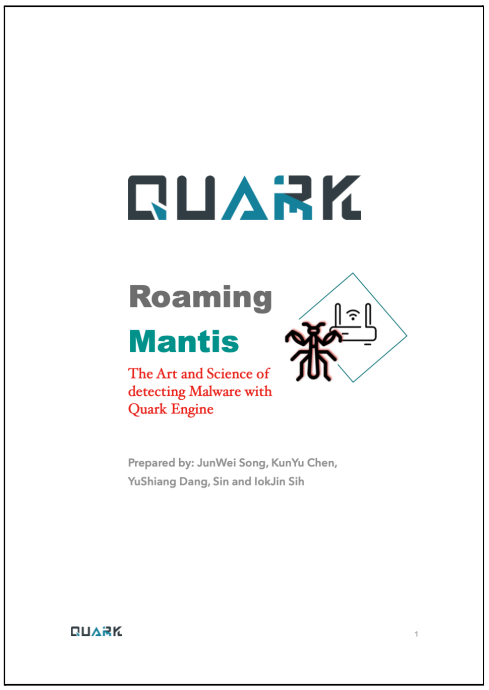
Quark Engine 之特點與優勢

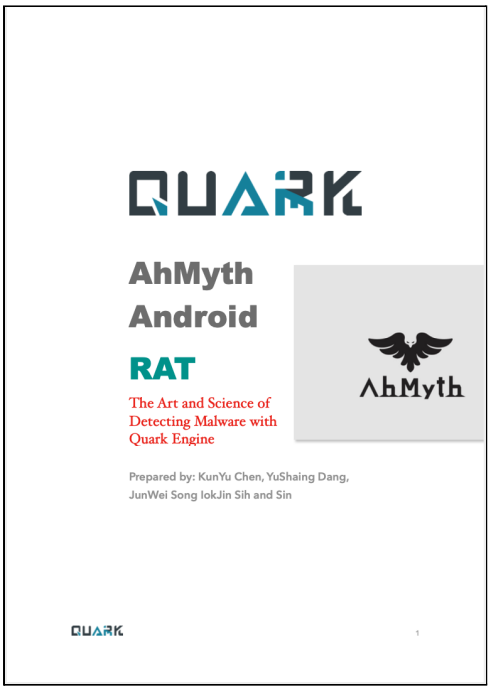
Quark Engine 提供簡潔易懂之概覽報告 (Summary Report)，以語意方式描述分析標的潛在之惡意行為。並輔以 Call Graph, Behavior Map, Label-based Report 以及 Behaviors Comparison Radar Chart 等分析功能，提供惡意行為原始碼、呼叫關係、分析標的惡意行為種類，及不同分析標的之惡意行為比較等情資，大幅提升惡意程式分析師工作效率。Quark 各項功能詳細說明可於 [1] 查閱。

雖然 Quark 可人工撰寫偵測規則，然而在毫無線索之情況下 (拿到未知樣本)，撰寫規則實屬不易。除此之外，以人工撰寫規則所耗費之時間及人力成本過高，且規則好壞取決於分析師資安經驗是否豐富。因此，我們開發出自動化規則生成系統，藉由生成分析標的使用之原生 API 組合，從中篩選出真正有惡意行為之組合，並生成為 Quark 偵測規則，以此減少分析師大量工作時間。分析師只需取得惡意程式真正 payload，即可透過此系統生成之規則，透徹理解惡意程式之行為。

Quark Engine 從發展至今受到許多國際專家與組織關注，已是資安領域知名開源專案，並已累積許多合作專案與貢獻者，例如 IntelOwl (瑞典資安公司 Certego 旗下之開源專案) 以及一位 Fortinet 首席研究員。除此之外，Quark 也在許多國際知名資安研討會上發表成果 (例如: DEFCON 與 BlackHat)，其影響力受到國際認可。

Quark Engine 分析 Ahmyth 與 Roaming Mantis 兩支經典惡意程式樣本，並釋出分析報告。其結果表明，兩樣本之行為確實能被 Quark 偵測出，證明 Quark 具有偵測惡意行為之能力。兩樣本之分析報告如下圖所示，並可於 [2] 查閱。





Quark Engine 與 Google Summer of Code

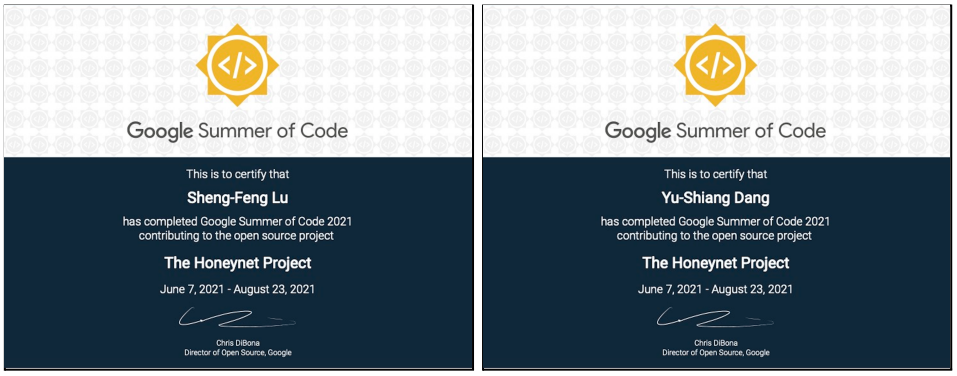
Google Summer of Code (GSoC) 為 Google 舉辦，媒合貢獻者與開源專案之計畫。由開源專案成員指導貢獻者完成計劃，並由 Google 支付貢獻者獎學金。開源專案則可提升該專案之開發能量，甚至發掘潛在核心成員，為一舉數得之計畫。

自 2010 年起，參與 GSoC 組織數量為 150 至 201 個，其中不乏如 Python, Debian, Metasploit 等具知名度與指標性之組織與開源專案。經統計，每年開源專案之入選率僅 10% 左右，貢獻者僅 20-25%。因此，入選 GSoC 對開源專案亦或貢獻者皆為不易之事。

Quark 於 2021 年透過 The HoneynetProject 組織，入選 GSoC 2021，為台灣第一個參與 GSoC 之開源專案。並且於 GSoC 2021 期間，成功指導兩位貢獻者完成計畫。

Shen-Feng Lu 幫助 Quark 將核心分析函式庫替換成 Rizin，以及優化 Quark 效能。
Yu-Shiang Dang 幫助 Quark 開發新自動化規則生成系統，以及執行 Quark Everywhere 策略。兩位貢獻者之 GSoC 證書如下圖所示，其貢獻成果可於 [3] 查閱。

2022 年 Quark 再次參與 GSoC，並正在指導一位來自不同國家之貢獻者。該貢獻者計畫開發新功能 Quark Script，使 Quark 能快速聚焦、探索及分析惡意程式之行為。為壯大 Quark 社群並吸引更多優秀貢獻者，參與 GSoC 將是 Quark 每年例行規劃。



Quark Engine 與知名開源專案之合作

Quark 截至目前為止，已透過互利互惠模式，與 8 個知名資安開源專案合作，如下圖所示。其中，Kali Linux、Jadx、Ghidra 與 MobSF 為資安領域中，具有相當知名度之專案。

Kali Linux 將 Quark 整合至其工具庫，以增加該專案 Android 逆向分析之能量。Jadx、Ghidra 與 MobSF，則與 Quark 整合並開發出 Code Overview 功能，讓使用者能夠快速找出惡意行為之原始碼，提升惡意程式分析師工作效率。

除此之外，上述專案皆是資安領域中具指標性之專案。與這些專案合作，不僅能提升使用者之工作效率，也能大幅增加 Quark 知名度，達到 1+1 大於 5 之效益。相關合作資料可於 [4] 查閱。

Quark Engine 參與之國際研討會

為保有世界級競爭力，Quark 不斷保持與世界頂尖資安人員交流與互動。每年，我們也積極於國際資安研討會上，發表 Quark 最新研發成果。到目前為止，Quark 已參與至少 7 個知名資安研討會，如下圖所示。其中，DEFCON 與 BlackHat，為資安界中最頂尖、最具指標性之研討會。

Quark 從發展至今，積極與世界接軌，並不斷達成新穎、具突破性之目標。我們很榮幸能夠在這些頂尖研討會上，與全世界共享成果。這些成果也證明 Quark 是具有影響力且被國際認可之開源專案。

Reference

以下為 Quark 其他相關資訊之連結：

[1] Quark Github 頁面：https://github.com/quark-engine/quark-engine
[2] 分析報告之連結：https://github.com/quark-engine/quark-reports
[3] Quark GSoC 貢獻者之報告：https://quark-engine.github.io
[4] Quark Reference：https://github.com/quark-engine/ref