保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

「駕輕就熟」力抗進階惡意軟體的賽門鐵克雲端沙箱

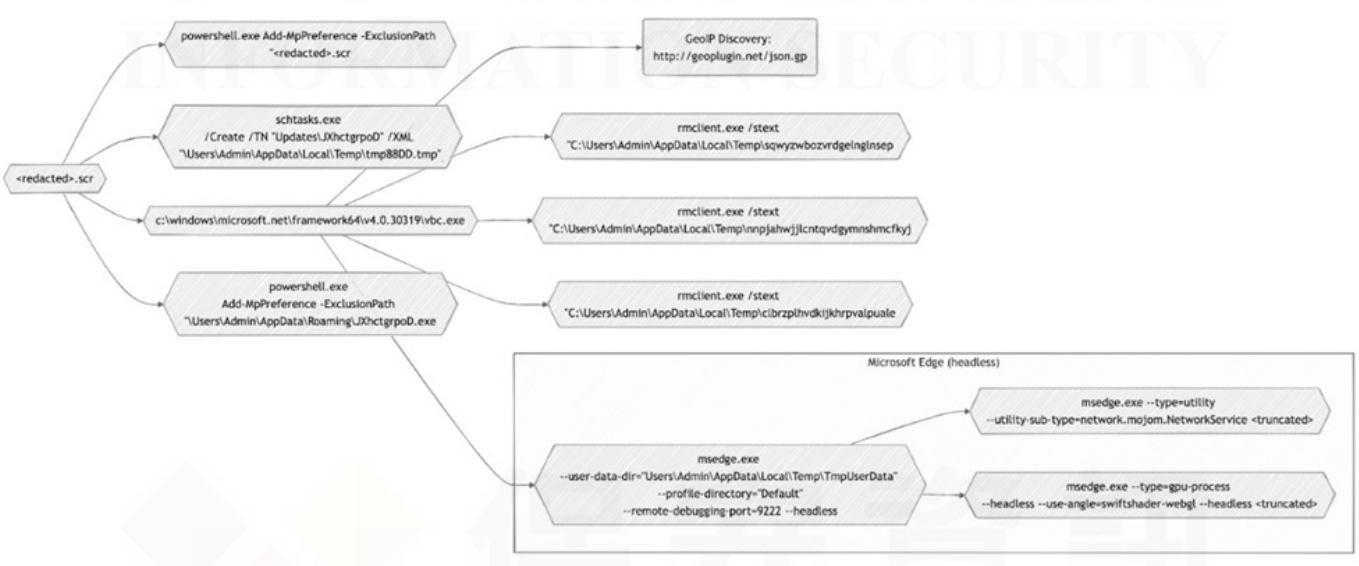
2025 年 9 月 16 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

賽門鐵克雲端沙箱透過提供進階惡意軟體偵測功能，強化現有防護、偵測與分析產品。此沙箱運用賽門鐵克完整的偵測架構及針對雲端資源優化的多重引擎，得以偵測那些在有限資源下難以識別的惡意軟體。

以下是 Remcos 惡意軟體的實例，該軟體在零時差攻擊階段成功躲避靜態分析偵測。此惡意軟體利用包含 Office 文件檔與可執行檔的 zip 壓縮檔，誘使用戶執行惡意樣本。

雲端沙箱引爆惡意軟體流程圖



當整合雲端沙箱功能的解決方案運行掃描時，會接收大量智慧分析與惡意偵測資訊，這些資訊有助於偵測惡意軟體。除偵測功能外，雲端沙箱掃描產生的metadata可歸納如下：

惡意軟體分析：觀察到戰術、技術與程序(TTPs)

此分析詳述惡意樣本所觀察到的 TTPs，並對映 MITRE ATT&CK 的戰術、技術與子技術框架進行分類。

「執行」戰術階段：

- 使用者執行 (T1204.002)：惡意軟體透過使用者開啟偽裝成電子郵件附件『<redacted>.scr』檔案而執行。
- 指令與腳本編譯器 (T1059.001)：利用 PowerShell 執行指令，特別是用 powershell.exe Add-MpPreference 以實現自我保護。

「防禦繞過」戰術階段：

- 破壞防禦機制 (T1562.001)：停用或修改工具：初始樣本及後續釋放的惡意軟體均使用指令 powerShell.exe Add-MpPreference -ExclusionPath，明確試圖規避偵測。
- 受信任開發者工具代理執行 (T1127.001)：惡意樣本啟動 vbc.exe 執行惡意活動。
- 混淆檔案或資訊 (T1027) 的分析與檢測：將可執行檔使用 .scr 檔案副檔名如名稱為『<redacted>.scr』，是常見偽裝成合法螢幕保護程式的技術。

「發現」階段：

- 系統資訊發現 (T1082)：惡意軟體查詢大量登錄檔機碼，並運用多種工具將系統資訊匯出至本機檔案。
- 系統位置發現 (T1614)：惡意軟體會依據遭駭電腦的 IP ，到 geoplugin.net 判斷遭駭電腦的地理位置／國別。

「持久化」戰術階段：

- 開機或登入自動啟動執行(T1547.001)：惡意軟體在用戶的 AppData\Roaming 目錄中建立 jxhctgrpod.exe 檔案，並建立工作排程以實現其自動啟動。

「命令與控制」以及「資料竊取」戰術階段：

- 透過 C2 通道外洩資料 (T1041)：惡意軟體連接到遠端 IP 位址並外洩大量資料。

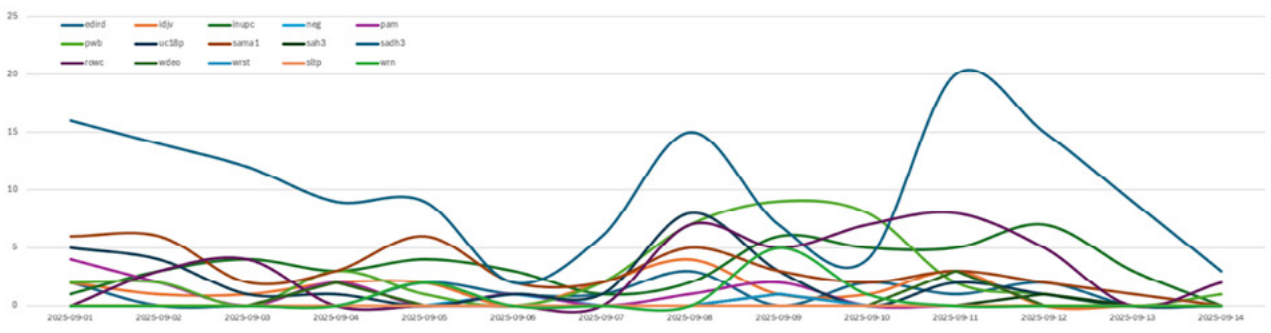
實際的威脅偵測來自多種引擎、運用多重技術，從觸發過程識別非良性特徵及觸發期間產生的行為與檔案痕跡：

- 直接偵測特徵
- 進階機器學習
- 沙箱內啟發式行為群組追蹤
- 網路偵測堆疊
- 沙箱內觀察結果的關聯分析

受益於雲端沙箱的強大功能

在賽門鐵克雲端沙箱中，此威脅透過多種偵測工藝被識別，並由安全應變團隊與自動化系統持續監控，進而強化雲端沙箱的防護效能。我們每日對賽門鐵克雲端沙箱進行優化，不僅追蹤個別惡意軟體樣本的演變，更同步掌握威脅態勢的變化趨勢，藉此為客戶提供全面防護。透過分析上述參考樣本中的各項偵測結果，我們得以追蹤採用相同或相似技術的多重威脅，使雲端沙箱能持續為客戶提供防護。

雲端沙箱的多元檢測工藝可以隨時掌握多個惡意軟體家族的動向提供安全所需的可視性



賽門鐵克雲端沙箱透過整合多種威脅偵測工藝、引擎及監控機制，針對威脅環境中不斷進化的技術手法提供零時差防護。集結研究與應對能力的協同效應優勢，持續強化雲端沙箱服務在新型威脅出現時偵測零時差威脅的能力。

欲深入了解更多有關賽門鐵克雲端沙箱功能，請點擊此處。
欲深入了解更多有關賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，請點擊此處。
欲了解更多有關啟動賽門鐵克雲端沙箱在端點偵測和回應(EDR)的環境，請點擊此處。
欲了解更多有關賽門鐵克的端點偵測和回應(EDR)功能，請點擊此處。

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片）軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶使用情境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。
保安資訊連絡電話：**0800-381-500**。