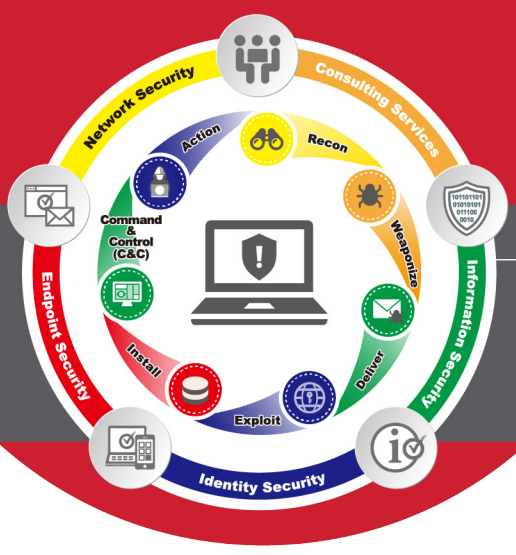


保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

賽門鐵克雲端沙箱，瓦解新興惡意程式的「零日」威脅

2024 年 9 月 3 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

在安全領域中，建立立足點是惡意威脅者在鎖定目標組織中窺探和竊取資訊、執行搜尋和進行橫向移動最重要的第一步。我們經常看見組織收到惡意連結、可執行檔案、Office 文件檔、腳本，包含各種威脅的壓縮檔案或者其中一個作為起點導致另一個的組合，然後在整個威脅鏈中發動隱蔽攻擊，進而入侵目標組織的資訊環境，而目標組織發現時，常常為時已晚，已經造成嚴重的資安事故了。

經矇混程式碼的 VB 腳本

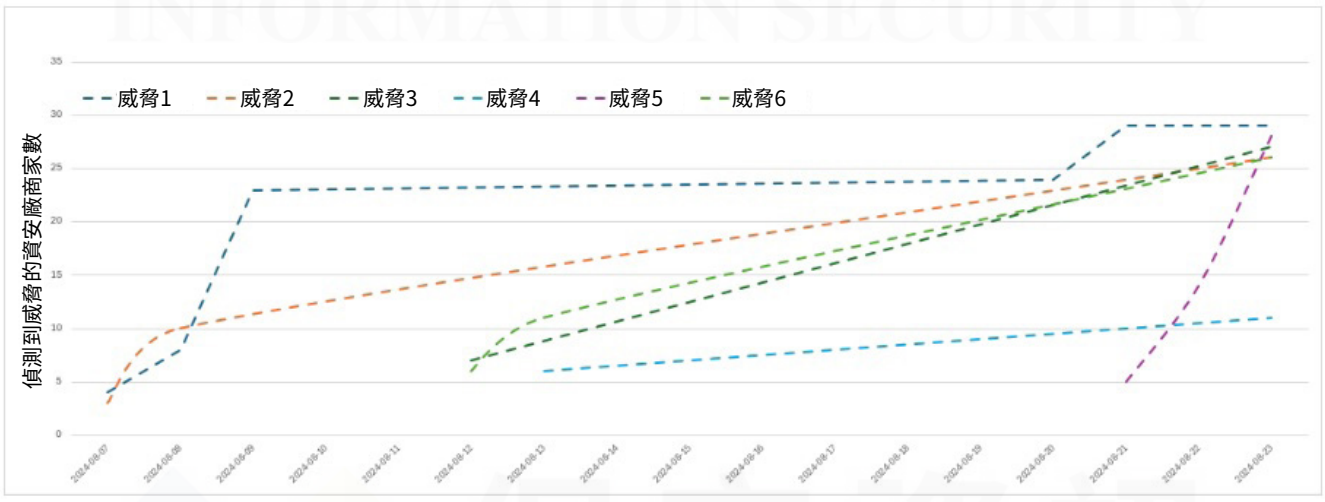
最近，Visual Basic Scripts (VBScript 檔案) 是這種威脅的常見例子。我們觀察到 VBS 和 VBE (已編碼的 VBScript 檔案) 被打包在檔案中，並傳送給不知情的使用者，這些檔案看起來像是圖片檔 (IMG-50012-3067.7z)、文件檔 (Docu_720001.7z)、預訂確認函／收據 (Reservations_00206PDF.7z、Booking_No1162808.rar) 或其他取名為需要使用者開啟和確認的有益無害的檔案。一旦開啟，這些腳本會解密、解壓縮並將較小的有效酬載傳送至本機，或從攻擊者控制的遠端伺服器下載惡意有效酬載。傳統的防毒軟體 (AV) 掃描一直在努力跟上這些攻擊，但由於這些腳本是文字格式，且被 IT 部門廣泛用於日常的業務運作，因此攻擊者可以濫用這些腳本所執行的機器資源來進行掩護、混淆，或使分析變得非常複雜且耗費大量資源。

賽門鐵克雲端沙箱：提供「零日」防護

賽門鐵克雲端沙箱透過利用投入密集的資源的靜態掃描～這是遠超乎運行在端點上模擬偵測技術、頂尖的行為監控和偵測技術 (可關聯所有可用的中繼資料，以偵測此類惡意軟體)，針對上述攻擊提供「零日」防護。這些 VBS／VBE 腳本不斷演進，以躲避包含經混淆的網址和傳統防毒解決方案；然而賽門鐵克雲端沙箱提供更全面的防護，可偵測從混淆機制和可疑技術，到躲避靜態層和被檢測威脅行為的網路物件。在長時間追蹤各種 VB 下載程式後，我們發現賽門鐵克雲端沙箱可提供針對此惡意軟體的「零日」防護 (通常是在檔案建立後幾分鐘內首次出現)，比社群獲得針對這些下載程式的強大防護還要早許多天。

根據「資安術語」的定義：所謂「day zero(零日)」是指前所未見的惡意軟體發佈到真實網路情境上的那一天，因此對資安產品來說完全未知。相對於「zero-day(零時差)」(也稱為 0-day) 一詞，「零時差」是指軟體或硬體中的漏洞，廠商通常不知道該漏洞，也沒有修補程式或其他修復方法。廠商有「零」天的時間準備修補程式，因為該漏洞已被描述或被開採濫用。

偵測到威脅的資安廠商數量



一旦在賽門鐵克雲端沙箱中偵測到特定的檔案，所有沙箱客戶都會立即受惠於已知的處理方式，而所有賽門鐵克客戶則會在幾分鐘內受益於已知的處理方式，因為所有賽門鐵克產品都會參照使用到我們的全球情報網路 (GIN)。

欲瞭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。
欲瞭解更多有關賽門鐵克郵件安全雲端安全服務(Email Security.Cloud)的電子郵件掃描順序，請點擊此處。
欲瞭解更多有關賽門鐵克郵件安全雲端服務(Email Security.Cloud)的郵件威脅偵測和回應(ETDR)功能，請點擊此處。
欲瞭解更多有關賽門鐵克端點安全完整版(SESC)的端點偵測和回應(EDR)功能，請點擊此處。
欲瞭解更多有關賽門鐵克郵件安全雲端服務的(Email Security.Cloud)與資料外洩防護(DLP)的整合功能，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**。