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

無懈可擊的組合～賽門鐵克行為分析--SONAR＋賽門鐵克雲端沙箱--Cynic

2025 年 6 月 10 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

行為分析

行為分析是當應用程式在電腦上執行時，偵測潛在惡意行為的即時防護。賽門鐵克的行為分析使用啟發式方法和信譽資料來偵測新興和未知的威脅。它提供「零時差」保護，因為它能在傳統病毒和間諜軟體偵測定義建立之前偵測到惡意行為，以解決威脅。行為分析使用啟發式系統，利用賽門鐵克的線上情報網路與用戶端電腦上的主動本機監控來偵測新興威脅。它也會偵測用戶端電腦上應受監控的變更或行為。

賽門鐵克行為分析--SONAR(Symantec Online Network for Advanced Response)

賽門鐵克的行為分析技術 (簡稱「SONAR」) 會持續監控所有程序，不論是否受信任。它會追蹤檔案、登錄、進程、服務、注入線程、DLL 側載和進程空洞化等複雜的攻擊鏈。它還會追蹤攻擊鏈中合法進程的使用情況。這些包括就地取材 (LOTL) 程序和兩用工具。一旦識別出惡意載體，SONAR 會移除惡意檔案、登錄項目和進程，並終止攻擊中使用的任何 LOTL 和兩用進程，進而解除整個攻擊鏈。

賽門鐵克雲端沙箱--Cynic

我們以雲端為基礎的沙箱分析平台 (稱為「Cynic」非常貼切)，利用 SONAR 行為偵測為賽門鐵克郵件安全雲端服務 (ESS：Email Security.cloud Service) 提供攔截能力，在目標攻擊進入收件匣之前就被偵測出來。

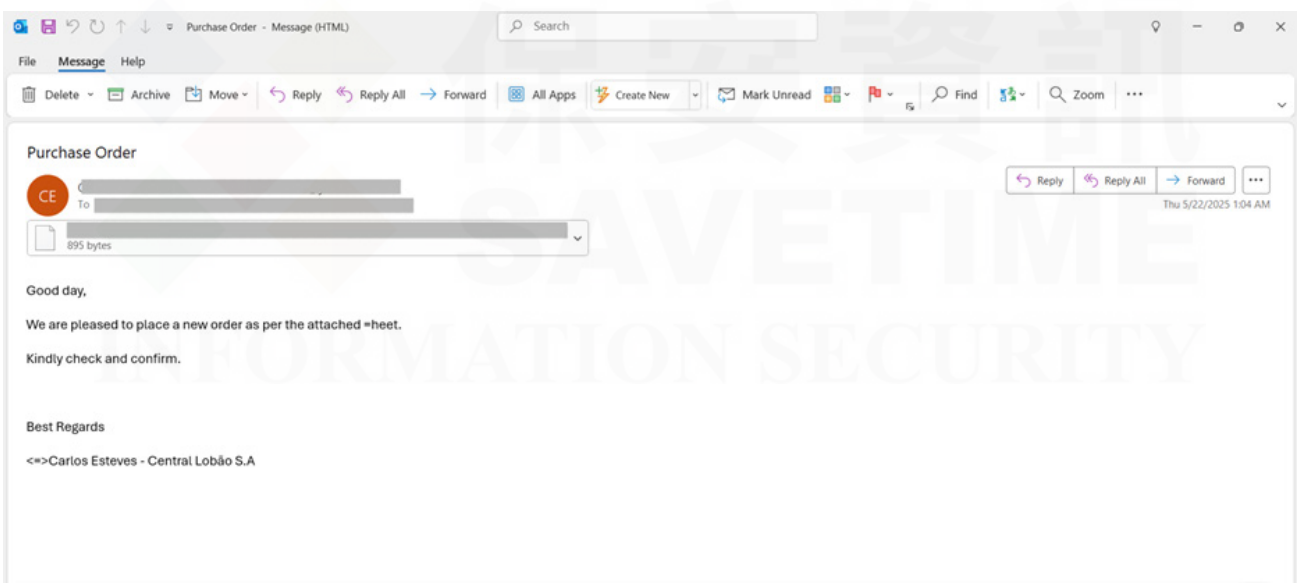
目標式 (有針對性的) 攻擊通常會從精心製作的釣魚電子郵件開始，誘導使用者開啟附件，而使用者並不知道附件會在背景中隱匿進行的複雜攻擊足以癱瘓整個網路。偵測這些攻擊最可靠的方法之一，就是監控完整的攻擊鏈，並在一連串行為被識別為惡意攻擊時啟動偵測。

如果我們可以透過觀察其自然行為來偵測攻擊，而不讓網路暴露在任何風險之下，那會如何？甚至在使用者看到釣魚電子郵件之前。

透過在賽門鐵克郵件安全雲端服務 (ESS：Email Security.cloud Service) 中使用 Cynic，我們就可以做到這一點。來自可疑電子郵件的附件會被轉寄給 Cynic，以便在雲端沙箱中進行分析。Cynic 的一個關鍵元件是來自 SONAR 引擎的沙箱特定行為偵測模型。

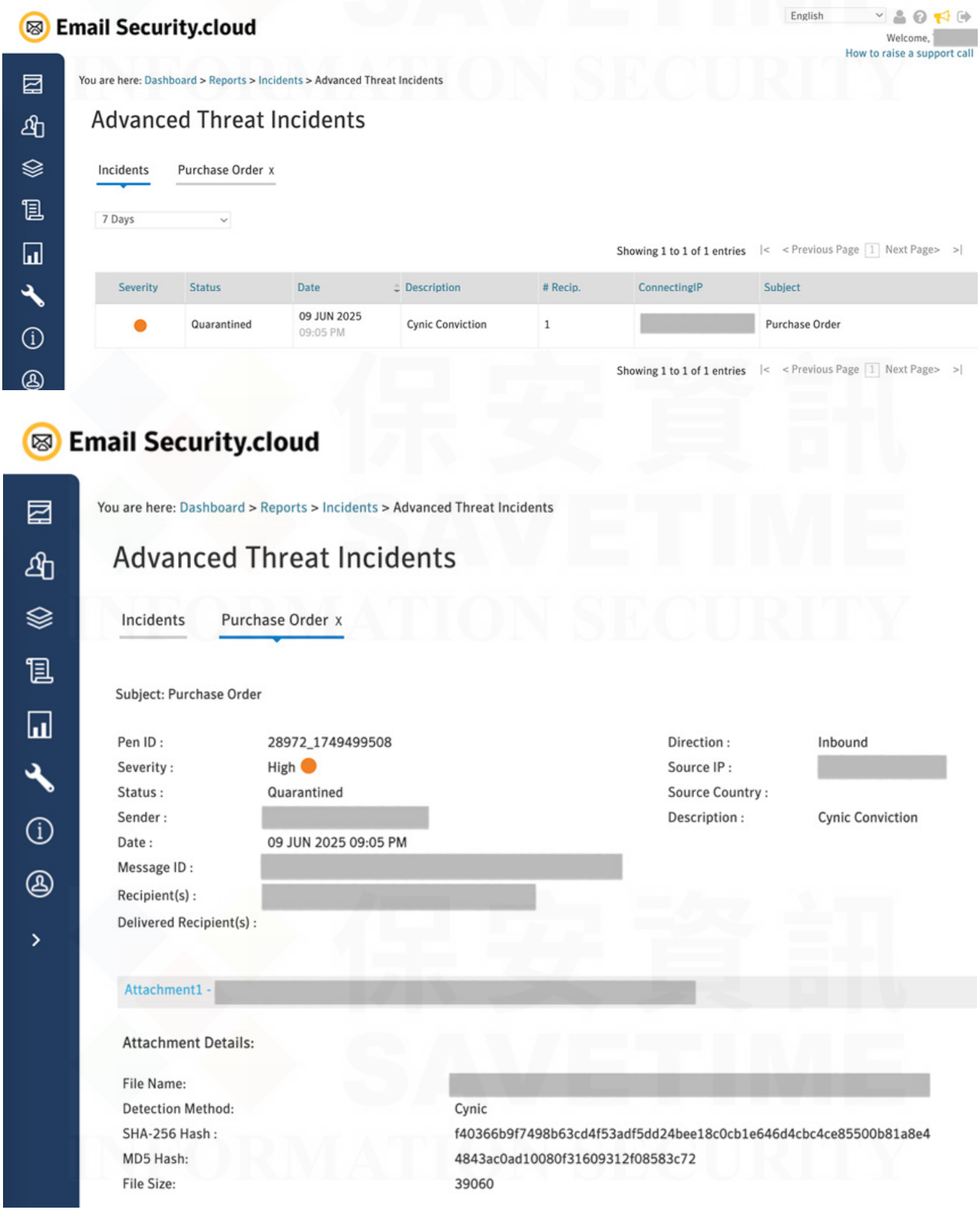
舉個最近的例子

賽門鐵克郵件安全雲端服務 (ESS：Email Security.cloud Service) 掃描一封包含壓縮檔附件的電子郵件。該附件被傳送至 Cynic 進行分析，而壓縮檔內容則會被引爆。在 Cynic 內，我們執行特殊的 SONAR 組態，該組態經過客製調整，可偵測和報告引爆環境中的可疑行為。



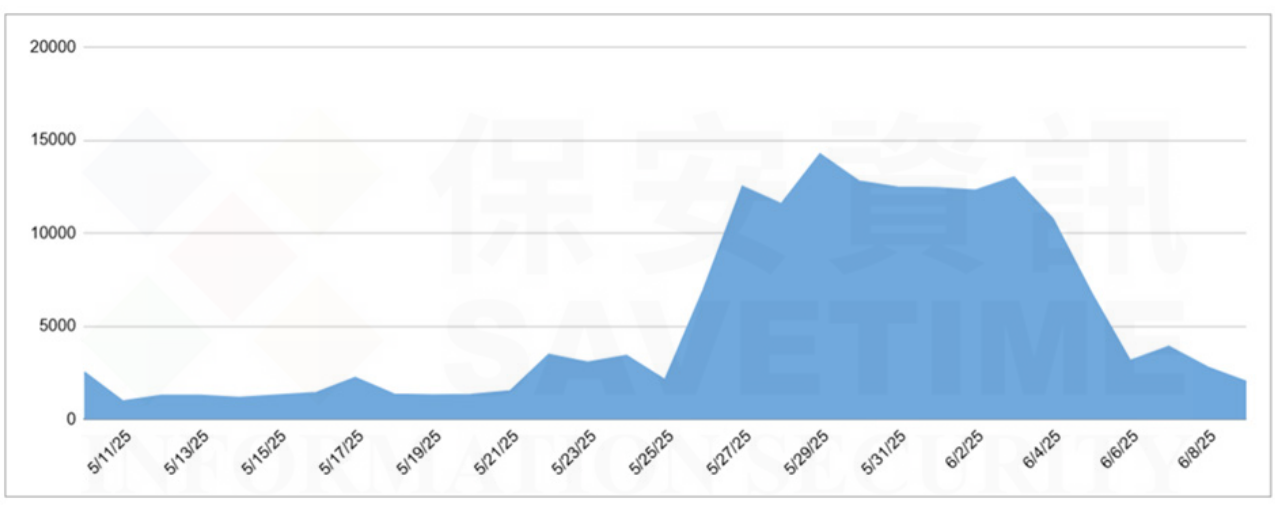
從 Cynic 引爆所獲得的大量資料中，我們能夠分析整個攻擊鏈並報告下列行為及偵測結果：

- 削弱防禦能力 (MITRE T1562)：啟動 PowerShell 執行個體時 (instance) 停用 Windows Defender。
- 處理程序挖空 (Process Hollowing) (MITRE T1055)：將 regsvcs.exe 挖空以注入 Snake Keylogger，我們透過深入掃描程序記憶體發現這一個情況。根據這些指標，Cynic 能夠確認電子郵件附件為惡意，讓賽門鐵克郵件安全雲端服務 (ESS：Email Security.cloud Service) 能夠保護網路免受這次釣魚嘗試的攻擊。



答案都在這裡，你只要登入並瀏覽賽門鐵克郵件安全雲端服務 (ESS：Email Security.cloud Service) 的管理介面。而在 SONAR 寶貴協助下，Cynic 的能力遠超壞人所能想像。

SONAR 攔截的電子郵件



欲了解有關 Symantec Endpoint Protection 的行為分析技術 SONAR 的更多資訊，請點擊此處。
欲了解管理行為分析 (SONAR)，請點擊此處。
欲了解 SONAR 如何與賽門鐵克雲端沙箱 (Symantec Cloud Sandbox) 整合，請點擊此處。
欲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。

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**。