保安資訊--本周(台灣時間2025/09/19)
賽門鐵克原廠防護公告重點說明

前 言

賽門鐵克原廠首要任務就是保護我們的顧客，被譽為賽門鐵克解決方案專家的保安資訊更能發揮我們被高度認可的專業知識與技能、豐富經驗以及專為幫助客戶成功的服務熱忱，與顧客共同創造賽門鐵克解決方案的最大效益，並落實最佳實務的安全防護。攻擊者從不休息，我們更不會。一支技術精湛且敬業的團隊不斷創造新的防護措施，以應對每天發布成千上萬的新威脅。儘管不可能詳述我們已經可以防禦的每種新威脅，但該站點至少反映了我們的努力。這些公告分享針對當前熱門新聞話題有關威脅的保護更新，確保您已知道自己受到最佳的保護。點擊此處獲取賽門鐵克原廠防護公告 (Protection Bulletins)。

關於 保安資訊有限公司 | 從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

在端點啟用賽門鐵克入侵預防系統(IPS) 的好處(以下皆為美國時間)

賽門鐵克的入侵預防系統 (IPS) 是業界一流的深層封包檢測技術引擎，可保護包括財富 500 強企業和消費者在內的數億個端點(桌機／筆電／伺服主機)。

過去的 7 天內，SEP 的網路層保護引擎 (IPS) 在受保護端點上總共阻止了 6,700 萬次攻擊。這些攻擊中有 87.2% 在感染階段前就被有效阻止：**(2025/09/03)**

- 在受保護端點上，阻止了**2,940**萬次嘗試掃描**Web**伺服器的漏洞。
- 在受保護端點上，阻止了**510**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**Windows**伺服主機上，阻止了**480**萬次攻擊。
- 在受保護端點上，阻止了**310**萬次嘗試掃描伺服器漏洞。
- 在受保護端點上，阻止了**200**萬次嘗試掃描在**CMS**漏洞。
- 在受保護端點上，阻止了**250**萬次嘗試利用的應用程式漏洞。
- 在受保護端點上，阻止了**97**萬**1,600**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在受保護端點上，阻止了**56**萬**9,500**次加密貨幣挖礦攻擊。
- 在受保護端點上，阻止了**810**萬台次向惡意軟體**C&C**連線的嘗試。
- 在受保護端點上，阻止了**8**萬**6,400**次加密勒索嘗試。

強烈建議用戶在桌機／筆電／伺服主機上啟用 IPS (不要只把SEP/SES當一般的掃毒工具用，它有多個超強的主被動安全引擎，在安全配置正確下，駭客會知難而退)，以獲得最佳保護。點擊此處獲取有關啟用 IPS 的說明，或與保安資訊聯繫可獲得最快最有效的協助。

有憑有據!SEP的瀏覽器延伸防護功能，在上周所帶來的好處？

賽門鐵克的入侵預防系統 (IPS) 是業界最佳的深度資料包檢測引擎，可保護數億個端點(桌上型電腦和伺服器)，其中包括財富 500 強企業和消費者。

賽門鐵克端點安全 (SES) 或賽門鐵克端點防護 (SEP) 代理透過谷歌 Chrome 瀏覽器和微軟 Edge 瀏覽器的延伸供瀏覽器保護。這些延伸有兩個組成部分：

- 瀏覽器的入侵預防，利用 IPS 引擎保護客戶免受各種威脅的侵害。
- 網頁信譽，可識別可能包含惡意軟體、欺詐、網路釣魚和垃圾郵件等惡意內容的網域和網頁帶來的威脅，並阻止瀏覽這些網頁。

在過去 7 天內，賽門鐵克透過端點防護的瀏覽器延伸防護功能，在受保護端點上阻止了總計 1,330 萬次攻擊。**(2025/09/03)**

- 使用網頁信譽情資，在端點上阻止了 **12M** 次攻擊。
- 在受保護端點上攔截 **1.1M** 次攻擊，這些攻擊試圖將用戶重定向到攻擊者控制的網站上。
- 在受保護端點上攔截 **147.2K** 次瀏覽器通知詐騙攻擊／技術支援詐騙攻擊／加密劫持嘗試。
- 在受保護端點上攔截 **7.7K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。

建議客戶啟用端點防護 (SEP) 的瀏覽器延伸，以獲得最佳防護。按下此處獲取：整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站的說明。

2025/09/18

HybridPetya--具備UEFI開機套件的Petya／NotPety惡意軟體最新變種

ESET 安全研究人員發現名為 HybridPetya 的全新惡意軟體樣本，其具備 2016 至 2017 年間造成重大影響的 Petya 與 NotPetya 攻擊行動的特徵。儘管尚未偵測到實際部署案例，但這些樣本的顯著差異在於採用 UEFI 開機套件，可對 NTFS 格式化分割區的主檔案表 (MFT) 進行加密。該報告進一步揭露技術細節，並指出其試圖利用 UEFI 安全啟動漏洞 (CVE-2024-7344) 進行攻擊。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 **(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)**，並以下述的命名及對應的防護機制來提供具體說明：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Ransomware!g7
- SONAR.TCP!gen1

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Zombie
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

2025/09/18

IBM X-Force新發現散佈SnakeDisk蠕蟲與Toneshell後門程式的最新攻擊行動

IBM X-Force 新發現一項歸屬於 Fireant(又稱 Hive0154、Mustang Panda) 駭客組織所發起的惡意攻擊行動。此攻擊行動利用源於惡意程式 ToneShell 的更新版本：Toneshell9，透過使用本地配置的代理伺服器進行指令與控制 (C&C) 通訊來規避偵測，並允許建立兩個並行的反向殼層 (reverse shells)。近期歸屬於該駭客組織的另一惡意軟體為 SnakeDisk，此為新型 USB 蠕蟲專門鎖定擁有泰國 IP 位址的裝置。SnakeDisk 與 Tonedisk 存在程式碼相似性，同樣利用 USB 裝置作為傳播媒介。感染後會部署 Yokai 後門程式--該後門曾於 2024 年 12 月針對泰國官員的攻擊行動中出現。Yokai 使惡意攻擊者能在受感染主機上執行任意指令。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (**SEP**/**SESC**/**SMG**/**SMSMEX**/**Email.Security.cloud**/**DCS**/**EDR**)，並以下述的命名及對應的防護機制來提供具體說明：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Ps-RgPst!g1

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool.Flooder
- Phish.Gen
- Trojan Horse
- Trojan.Gen.MBT

- Trojan.Gen.NPE
- WS.Malware.1
- WS.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.B
- Heur.AdvML.B!200
- Heur.AdvML.C

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/09/18

內建整合式系統配置工具的XillenStealer惡意竊密軟體～讓阿貓阿狗也能當網路偷賊

資安廠商 CYFIRMA 旗下的資安研究人員在最新報告中，揭露一款基於 Python 開源惡意竊密軟體：XillenStealer，可於 GitHub上輕易取得。此惡意軟體運用模組化腳本與 Windows 原生功能竊取敏感資料，核心功能包含竊取系統資訊、加密貨幣錢包、瀏覽器資料與網路設定，並能擷取螢幕截圖。

該惡意竊密軟體內建整合式系統配置工具，可以簡化客製化與部署流程，降低攻擊者所需技術門檻。名為「Builder V3.0」的整合式系統配置工具提供圖形化介面，可配置並編譯客製化資訊竊取二進位檔。其支援透過 Telegram 機器人進行資料外洩，並具備模組化選項，能鎖定 Discord、Steam、Telegram、遊戲啟動器或加密貨幣錢包等特定應用程式。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)，並以下述的命名及對應的防護機制來提供具體說明：

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen1

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer
- Trojan Horse
- Trojan.Gen.2
- WS.Malware.2

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/09/16

RevengeHotels網路犯罪集團，採用新戰術大肆散播強悍的VenomRAT遠端存取木馬程式(RAT)

Securelist 研究人員已確認名為 RevengeHotels(亦稱TA558) 的網路犯罪集團，專門鎖定酒店及旅遊產業竊取信用卡資料。其典型攻擊手法是偽裝成發票的釣魚郵件，引導受害者前往詐騙網站。這些網站會觸發惡意腳本檔案下載，進而使系統感染遠端存取木馬程式 (RAT)。近期行動中，RevengeHotels 開始運用人工智慧生成的程式碼作為初始感染與下載機制。這種 AI 輔助開發產生的程式碼更為簡潔，包含註解與佔位符 (Placeholders)，與先前混淆的自訂程式碼形成顯著差異。該犯罪集團現正透過 JavaScript 載入程式與 PowerShell 下載程式散佈 VenomRAT--此為源自 QuasarRAT 的強力遠端存取木馬。其當前鎖定巴西酒店業為攻擊目標，並計劃將行動擴展至西班牙語系市場。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (**SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR**)，並以下述的命名及對應的防護機制來提供具體說明：

自適應防護技術(包含於SESC)：

- ACM.Ps-Enc!g1
- ACM.Ps-Http!g2
- ACM.Ps-Rd32!g1
- ACM.Ps-Wscr!g1
- ACM.Wscr-CNPE!g1
- ACM.Wscr-Ps!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!gen1
- SONAR.Powershell!g110
- SONAR.SuspStart!gen2
- SONAR.TCP!gen1

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen*
- Scr.Malcode!gdn*
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.xSense.C

- XSNet.Js!gen1
- XSNet.Ps1!gen1
- Web.Reputation.1
- WS.Malware.1
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Audit: Bad Reputation Application Activity
- System Infected: Trojan.Backdoor Activity
- URL Reputation: Webpulse Bad Reputation Domain Request

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/09/17

供應鏈攻擊～WhiteCobra威脅組織鎖定開發工具進行資料竊取

資安業者 Koi 研究發現名為 WhiteCobra 技術精湛的高階威脅組織，其持續一年之久的攻擊行動鎖定微軟 Visual Studio Code(VSCode)、AI 驅動的程式碼編輯器 (IDE)：Cursor 及 Windsurf 用戶。該威脅組織先前曾涉及重大加密貨幣竊盜案與惡意擴充功能，其縝密的「Operation Solidity Pro」攻擊行動可拆解為五個階段：惡意 VSIX 封裝、偽裝上架至擴充市集、社群媒體宣傳、人為製造下載量以營造社群證明，以及即時資料竊取。該駭客組織透過 X 平台實施激進的社交工程攻擊，運用預製模組並偽裝成具影響力的開發者帳號，製造假冒緊急與社群背書。其多階段混淆式酬載傳遞機制可隱藏惡意程式碼，並部署平台專屬酬載。這些酬載隨後會下載並執行，例如：LummaStealer 等惡意竊密軟體，從加密貨幣錢包、雲端基礎設施、通訊平台及密碼管理器竊取敏感數據。此攻擊行動代表 WhiteCobra 戰術的重大進化，其核心目標在於開發者生態系統內的軟體供應鏈入侵。

網路知識：Windsurf 建立在 VS Code 的基礎上，提供更好的 UI、更快的效能以及「寫入模式」等創新功能，您可以在其中直接根據提示寫入和生成文件，或者只需關閉寫入模式即可，像您一樣使用聊天功能在傳統的助理中。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護（SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)，並以下述的命名及對應的防護機制來提供具體說明：

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen1

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- OSX.Trojan.Gen
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Zbot
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/09/17

由AI撰寫程式碼的惡意軟體：EvilAI偽裝成合法工具

趨勢科技研究人員指出，名為 EvilAI 的全新惡意軟體正透過偽裝成合法生產力工具及 AI 工具展開攻擊。此木馬程式採用專業介面並具備有效數位簽章，使其極難被使用者及傳統安全解決方案偵測。EvilAI 憑藉其欺騙性特質，能在引發警報前潛入系統並建立持久存取權限。該惡意軟體的感染範圍遍及全球，其中歐洲、美洲及亞太中東非洲地區的感染率最高。製造業、政府機構與醫療保健等關鍵領域成為主要攻擊目標，顯示出其採用廣泛且不分對象的攻擊策略。

惡意軟體 EvilAI 透過新註冊的仿冒供應商入口網站、惡意廣告及搜尋引擎優化操縱進行傳播，誘使用戶下載看似有用的應用程式。該惡意軟體運用人工智慧生成乾淨且具隱蔽性的程式碼，並將惡意有效酬載與功能性應用程式捆綁，在執行有害活動時確保用戶滿意度且不被察覺。其感染鏈通常始於透過 Node.js 執行的 JavaScript 有效酬載，並藉由工作排程、登錄檔機碼及啟動捷徑建立持久性。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護（SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)，並以下述的命名及對應的防護機制來提供具體說明：

自適應防護技術(包含於SESC)：

- ACM.Ps-Wscr!g1

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- JS.Redirector
- PUA.Gen.2
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- WS.SecurityRisk.3

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/09/16

釣魚郵件偽裝成內部郵件訊息，散佈手法精湛的SHTML憑證圈套

賽門鐵克新發現的釣魚攻擊行動，利用偽裝成密碼保護的 SHTML 附件竊取員工憑證。這些郵件精心偽裝成內部發送--例如：將 account@<org> 偽裝成 user@<org>--並附帶諸如 EmployeeName_EFT_PAYMENT-CBA004233-00009_PDF.shtml 等文件名稱。

開啟檔案後，可見模糊的試算表背景疊加著登入提示。受害者被要求「解鎖」這份所謂的文件，但輸入的任何憑證都會被暗中收集。腳本會讀取密碼欄位 (pwd_key) 及使用者識別碼，透過 api[.]ipify[.]org 取得受害者的 IP 位址，並透過 Telegram Bot API 將竊取的資料轉送給操弄者。

Telegram 廣大用戶與加密通訊特性使其成為極具吸引力的資訊洩漏管道，相關行動可完美融入合法通訊流中。該行動同時運用蜜罐領域偵測自動化操作、刻意安排的錯誤訊息能延長互動時間，並在嘗試失敗後將用戶導向合法網域--所有設計目的皆在提升可信度。

針對特定網域的分析顯示，受害者類型呈現多元化，主要集中於金融服務與保險、酒店與旅遊、媒體與出版、工業與能源供應商、物流業、醫療保健供應商及教育領域。

該行動顯然聚焦於歐洲 (特別是英國、愛爾蘭、丹麥、瑞士和土耳其)、中東 (以色列、阿曼、黎巴嫩和巴勒斯坦) 以及非洲部分地區 (迦納、馬拉威、南非)，凸顯出其刻意針對戰略經濟領域與地區的組織進行滲透的企圖。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)，並以下述的命名及對應的防護機制來提供具體說明：

郵件安全防護機制：

不管是地端自建 (SMG／SMSEX) 的郵件過濾／安全閘道及主機防護、雲端郵件安全服務 (E-mail Security.Cloud) 以及郵件威脅隔離 (ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護 (威脅不落地)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Phish.ScrTgHtml!gen1

2025/09/16

NPM套件生態圈正遭受自我複製的蠕蟲感染

多個來源通報的惡意活動已觀察到影響 npm JavaScript 儲存庫中的眾多套件。該活動由名為Shai-Hulud 的自我複製蠕蟲所主導，此蠕蟲感染本地的 NPM 後，會根據使用者存取權限搜尋並感染其他可存取的套件。其行為包含竊取機密資訊、外洩資料，並將受影響使用者的私人 GitHub 專案標記為公開。

網路知識：npm 全名為 Node Package Manager，是 Node.js 的套件 (package) 管理工具，npm 可以讓 Node.js 的開發者，直接利用、擴充線上的第三方套件庫 (packages registry)，加速軟體專案的開發。

此攻擊運作模式如同真正的蠕蟲，透過將自身重新發佈至遭入侵者維護的其他套件中，實現自主傳播。其運作流程包含：下載目標套件、修改其 package.json 檔案以植入自我複製 hook、嵌入惡意有效酬載，最後利用維護者的憑證重新發佈已植入木馬的套件。此自動化循環機制使惡意軟體能持續透過維護者合法發佈權限，在 npm 生態系統中進行持續感染與擴散。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)，並以下述的命名及對應的防護機制來提供具體說明：

自適應防護技術(包含於SESC)：

- ACM.Ps-Wscr!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Malscript

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- URL Reputation: Webpulse Bad Reputation Domain Request

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

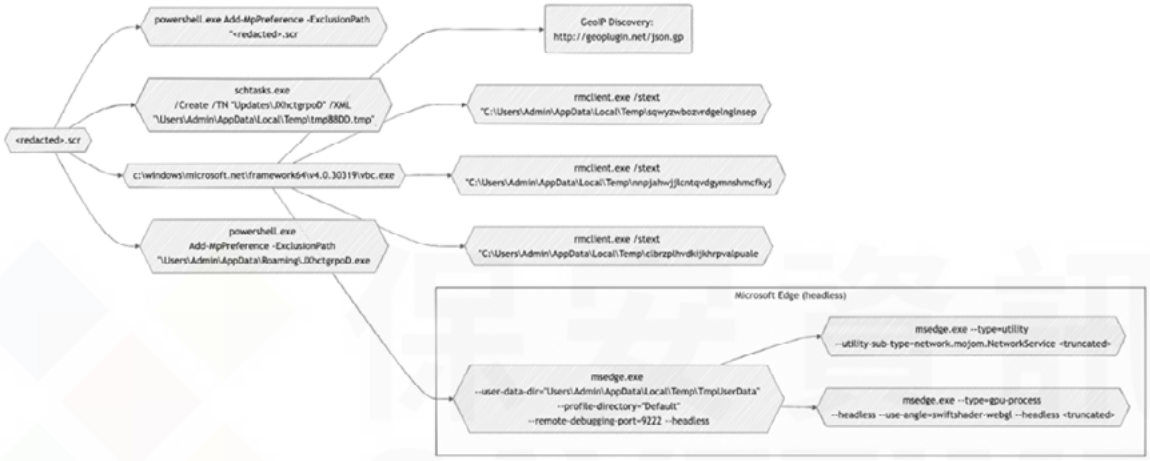
被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/09/16
防護亮點：「駕輕就熟」力抗進階惡意軟體的賽門鐵克雲端沙箱

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。

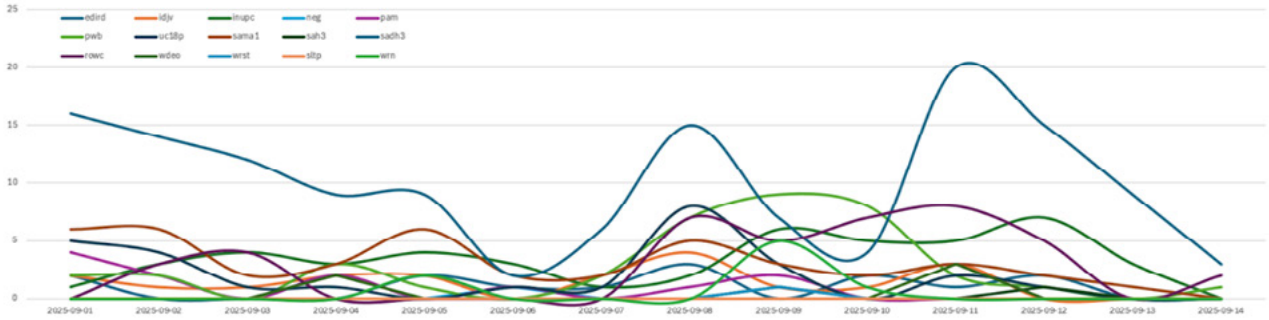
實際的威脅偵測來自多種引擎、運用多重技術，從觸發過程識別非良性特徵及觸發期間產生的行為與檔案痕跡：

- 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。

2025/09/16
CVE-2025-5086--存在Delmia Apriso的嚴重等級安全性漏洞

CVE-2025-5086 是一項近期披露的嚴重等級的漏洞 (CVS風險評分：9.0)，涉及對不可信任資料的反序列化處理，影響 DELMIA Apriso 製造營運管理 (MOM) 軟體。若成功利用此漏洞，攻擊者可能在受影響應用程式環境中執行任意程式碼。此漏洞已在上星期被美國網路安全暨基礎設施安全局 (CISA) 列入「已遭成功利用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中，顯示該漏洞在真實網路情境中已遭大肆開採濫用。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)，並以下述的命名及對應的防護機制來提供具體說明：

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Web Attack: Delmia Apriso CVE-2025-5086

2025/09/16
Maranhão Stealer惡意竊密軟體涉入的攻擊行動

Cyble研究人員近期發現一起「Maranhão Stealer」惡意竊密軟體涉入的攻擊行動。該攻擊透過雲端平台託管的社交工程網站鎖定遊戲用戶。此惡意竊密軟體自 2025 年 5 月前後開始活躍並持續發展，其利用盜版軟體安裝檔案、遊戲修改器及破解遊戲啟動器誘騙受害者。其傳播手法多與惡意 Inno Setup 安裝程式的 ZIP 壓縮檔有關。

Maranhão Stealer 惡意竊密軟體採用多種精心策畫的戰術達成其目標。它透過登錄檔機碼與工作排程建立持久性，以系統屬性與隱藏屬性掩飾惡意酬載，並執行全面的主機偵察，蒐集硬體規格、網路配置及地理位置等詳細資訊。其運作的核心環節在於竊取憑證、Cookie、瀏覽紀錄及加密貨幣錢包資料。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)，並以下述的命名及對應的防護機制來提供具體說明：

自適應防護技術(包含於SESC)：

- ACM.Ps-Reg!g1
- ACM.Ps-RgPst!g1
- ACM.Untrst-Csc!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!gen1
- SONAR.Stealer!gen1

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有

類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Trojan
- Infostealer
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.C

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- URL Reputation: Webpulse Bad Reputation Domain Request

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/09/16

kkRAT：新發現的遠端存取木馬涉入針對中文使用者發動的惡意軟體攻擊

針對中文使用者發動的惡意軟體攻擊行動已被發現，該行動除部署已知的 ValleyRAT 與 FatalRAT 外，更使用先前未曾記載過的 kkRAT。根據 Zscaler 報告指出，此惡意軟體透過託管於 GitHub 的釣魚頁面傳播，這些頁面偽裝成熱門軟體。kkRAT 採用類似 Ghost RAT 的通訊協定，並新增加密與壓縮功能，具備剪貼簿劫持、遠端監控能力，並能透過「自帶漏洞驅動程式」(BYOVD) 伎倆規避防毒／EDR 工具。其指令集包含替換加密貨幣錢包位址、部署遠端管理工具，以及中繼網路流量以繞過防火牆等功能。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (**SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR**)，並以下述的命名及對應的防護機制來提供具體說明：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspDriver!g30

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt
- Hacktool.Gen
- Trojan Horse
- Trojan.Dropper
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.C

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Audit: Bad Reputation Application Activity
- URL Reputation: Webpulse Bad Reputation Domain Request

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/09/15

Buterat後門程式鎖定企業與政府網路

資安公司　Point Wild 的 Lat61 威脅情報團隊發現名為 Backdoor.Win32.Buterat 的複雜惡意軟體，其設計目的在實現持久性的長期網路感染。此進階後門程式使攻擊者得以滲透系統、竊取敏感資料並部署其他惡意工具。Buterat　採用強大的持久化機制與指揮控制 (C&C) 基礎設施的自適應通訊方式，通常透過釣魚攻擊、惡意電子郵件附件或遭入侵的軟體下載進行傳播，特別鎖定企業與政府網路。執行時，Buterat 優先採用隱蔽策略，將其程序偽裝成合法系統任務，修改登錄檔機碼以實現持續執行，並運用加密或混淆通訊方式規避網路檢測。初步靜態分析顯示存在類似混淆字串，可能包含與惡意檔案執行及下載相關的關鍵 API 呼叫，凸顯其多元化的惡意功能。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護（SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)，並以下述的命名及對應的防護機制來提供具體說明：

自適應防護技術(包含於SESC)：

- ACM.Ps-RgPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.SuspBeh!gen57

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cycbot
- Infostealer.Scapzilla
- SMG.Heur!gen
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- W32.Changeup!gen*
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.3

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.C

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- System Infected: Trojan.Backdoor Activity 634

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/09/15

持續如火如荼進行中的Contagious Interview攻擊行動

資安公司 SentinelLABS 已發現並揭露與「Contagious Interview」攻擊行動及主導該行動相關的北韓威脅行為者，其展現出高度複雜的運作安全策略。這些惡意行為者正積極運用網路威脅情報 (CTI) 平台--包括 Validin、VirusTotal 及 Maltrail--監控自身基礎設施是否出現暴露與偵測跡象。最新發生「Contagious Interview」行動 (亦稱「ClickFake Interview」) 主要鎖定加密貨幣產業從業者，其目標涵蓋情報蒐集與加密貨幣資產直接竊取。該行動引誘受害者方面成效顯著，2025 年 1 月至 3 月期間已確認逾 230 名受害者。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (**SEP**/**SESC**/**SMG**/**SMSMEX**/**Email. Security.cloud**/**DCS**/**EDR**)，並以下述的命名及對應的防護機制來提供具體說明：

自適應防護技術(包含於SESC)：

- ACM.Ps-Wscr!g1

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Web.Reputation.1

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

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**。