保安資訊--今日最新(台灣時間2025/09/22)
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。

點擊此處獲取--關於賽門鐵克原廠防護週報

2025/09/19

BeaverTail惡意軟體利用ClickFix社交工程伎倆在macOS和Windows平台上大肆散播

ClickFix 社交工程伎倆透過偽造的驗證碼，誘騙使用者執行惡意指令。根據 Gitlab 報告指出，近期發現到利用此技倆的攻擊行動正散播新型 BeaverTail 惡意軟體。該惡意軟體背後的進階持續威脅 (APT) 駭客組織先前鎖定軟體開發者，如今已將目標轉向行銷、加密貨幣交易及零售產業。

BeaverTail 是一種基於 JavaScript 的惡意軟體，其主要功能是讓攻擊者竊取機密資料、加密貨幣錢包資料及系統憑證，隨後部署名為 InvisibleFerret 的 Python 惡意竊密軟體與遠端存取工具。近期散佈的 BeaverTail 變種已開始鎖定 macOS 系統，其惡意程式以經編譯過的二進位檔形式傳遞，透過 .pkg 和 PyInstaller 等工具製作，此特性有別於早期 JavaScript 變種。該 macOS 惡意軟體安裝包會嘗試竊取用戶密碼，並下載額外的有效酬載二進位檔。

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：

- OSX.Trojan.Gen
- Trojan.Gen.NPE
- WS.Malware.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。

2025/09/19

Leafperforator進階持續威脅(APT)駭客組織利用尼泊爾反政府抗議運動進行惡意軟體傳播

StrikeReady 資安研究人員近期揭露的活動顯示，地緣政治事件正成為目標式網路威脅的熱門誘餌。Leafperforator 進階持續威脅 (APT) 駭客組織 (亦稱Sidewinder) 近期將攻擊目標鎖定於關注尼泊爾抗議活動的個人。該駭客組織採用多管齊下的攻擊手法，結合行動裝置與 Windows 惡意軟體，並輔以網路釣魚攻擊。其中一種觀察到的戰術是偽裝成尼泊爾緊急服務機構竊取用戶憑證。另一顯著案例則是冒充尼泊爾陸軍代理參謀長阿肖克・西格德爾將軍 (截至 2025 年 9 月)，藉此部署行動惡意軟體。所散佈的有效酬載具備隱蔽功能，能將文件與圖像竊取至攻擊者控制的 C&C 伺服器。

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：

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
- Trojan.Gen.NPE

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

賽門鐵克的端點防護行動裝置版本(IOS/Android)已將其歸類為以下威脅並提供最完善的保護能力：

賽門鐵克的端點防護行動裝置版本 (IOS/Android) 還能夠分析簡訊內容的鏈接。它利用比對賽門鐵克全球資安情資網路 (GIN) 重要來源之一 Symantec WebPulse 中的威脅情報檢查簡訊內容中的網址，並在該鏈接為可疑時會及時提醒用戶，以保護用戶免受簡訊 (SMS) 網路釣魚攻擊。

- AdLibrary:Generisk
- Android.Reputation.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。

2025/09/18

DarkCloud惡意竊密軟體涉入歐洲能源、金融及海事領域的目標式攻擊

賽門鐵克偵測到一起散播 DarkCloud 惡意竊密軟體的垃圾郵件散播行動，該行動利用發票／運送主題的誘餌來散佈 Windows 平台上惡意竊密軟體。攻擊者偽造兩家德國工業供應商 (分別為工業機械供應商及儲槽／儲存設施建造公司) 身份，同時運用物流與發票方式的社交工程手法。

電子郵件 (主旨：『URGENT!! - Cambodia to Hong Kong[...]「*緊急!!－柬埔寨至香港[...]」』及『TOP URGENT!!－Invoice No-E26EXP00780[...]*「最高緊急!!－發票編號-E26EXP00780[...]」』)內含壓縮檔附件，解壓後會產生名為「1250 Fibro Rotary Tables India Private Limited/1250 Fibro Rotary Tables India Private Limited.exe」的 PE 檔案，該檔案即為 DarkCloud 惡意程式。

DarkCloud 是一款首次於 2022 年現身的主流惡意竊密軟體。其典型竊取目標包含：瀏覽器儲存的密碼與 Cookie、電子郵件／FTP 憑證，以及剪貼簿資料 (含加密貨幣錢包資訊)。

此二進位檔會嘗試建立持久化機制，並將資料外洩至攻擊者控制的管道 (本案例透過 Telegram API 傳輸)。已觀察到的 (混淆處理) 終點：

- hxxps://api[.]telegram[.]org/bot8419968582:AAGRs4ffljMSYb6T1ADt95vBLuhOSYI6qew/sendDocument
- hxxps://api[.]telegram[.]org/bot/8419968582:AAGRs4ffljMSYb6T1ADt95vBLuhOSYI6qew?id=5366689155

攻擊目標橫跨多個產業與國家，包括：

- 能源業--丹麥
- 公共／開發部門--丹麥
- 銀行／金融業--克羅埃西亞
- 航運／海事業--希臘
- 能源／工業部門--荷蘭

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

基於行為偵測技術(SONAR)的防護：

- 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。

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：

- MSIL.Packed.19

基於機器學習的防禦技術：

- Heur.AdvML.B

Symantec
A Division of Broadcom

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。

保安資訊
KEEPSAFE
INFORMATION SECURITY

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，以及基於比原廠更熟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**。

業界公認 **保安資訊**--賽門鐵克解決方案專家
We Keep IT Safe, Secure & Save you Time, Cost

服務電話：0800-381500｜+886 4 23815000｜http://www.savetime.com.tw