# 保安資訊--今日最新(台灣時間2025/05/12)
# 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 34 萬 900 台受保護端點上總共阻止了 5,410 萬次攻擊。這些攻擊中有 83.6% 在感染階段前就被有效阻止：**(2025/05/06)**

- 在**8**萬**2,500**台端點上，阻止了**2,340**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**7**萬**6,200**台端點上，阻止了**570**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2**萬**3,900**台**Windows**伺服主機上，阻止了**670**萬次攻擊。
- 在**5**萬**3,700**台端點上，阻止了**220**萬次嘗試掃描伺服器漏洞。
- 在**1**萬**4,700**台端點上，阻止了**1**萬**1,000**次嘗試掃描在**CMS**漏洞。

- 在**4**萬**8,700**台端點上，阻止了**200**萬次嘗試利用的應用程式漏洞。
- 在**9**萬**5,200**台端點上，阻止了**200**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,300**台端點上，阻止了**67**萬**2,100**次加密貨幣挖礦攻擊。
- 在**9**萬**1,100**台端點上，阻止了**640**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**484**台端點上，阻止了**6**萬**2,100**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 15 萬 3,600 個受保護端點上阻止了總計 670 萬次攻擊。**(2025/05/06)**

- 使用網頁信譽情資，在 **147.5K** 個端點上阻止 **630** 萬次攻擊。
- 攔截 **17.3K** 個端點上 **268.2K** 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 **4.6K** 個端點上攔截 **94.2K** 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 **285** 個端點上攔截 **3K** 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**

**2025/05/09**

### Earth Kasha威脅份子在最近的網路攻擊行動中以台灣和日本為目標

趨勢科技研究人員最近回報，Earth Kasha 威脅組織持續以台灣和日本的使用者為攻擊目標。攻擊者利用內嵌巨集功能的 EXCEL 檔案來掩護稱為 RoamingMouse 惡意軟體植入器的感染。該攻擊鏈的後續階段也會使用 ANELLDR 惡意軟體載入器、Anel 後門的全新變種、SharpHide 工具以及第二階段 NoopDoor 後門。該攻擊行動被認為主要是針對潛在受害者的間諜活動，以及從受攻擊的端點竊取資訊。

賽門鐵克已經於第一時間提供多種有效保護 **(SEP／SESC／SMG／SMSMEX／Email.Security.cloud／DCS／EDR)**。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

**VMware Carbon Black 產品的防護機制：**

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

**檔案型(基於回應式樣本的病毒定義檔)防護：**

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

**基於機器學習的防禦技術：**

- Heur.AdvML.A!500
- 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。

**2025/05/09**

### 在針對巴西的惡意攻擊行動中部署遠端監控與管理(RMM)工具

Cisco Talos 研究人員報告一項針對巴西使用者的全新惡意網路攻擊行動。攻擊者利用各種商用遠端監控與管理 (RMM:Remote Monitoring and Management) 工具，例如：PDQ Connect 和 N-able 遠端存取軟體。攻擊鏈透過惡意垃圾郵件引爆，將受害者導向下載託管在 Dropbox 檔案共用上的惡意安裝程式。安裝該 RMM 工具後，攻擊者便可遠端存取受攻擊的端點。以這種方式取得的存取權／憑證，可被涉入惡意攻擊行動的初始入侵管道掮客或稱初始存取掮客 (Initial Access Broker：IAB) 出售給其他威脅份子。

**網路知識**：初始入侵管道掮客或稱初始存取掮客（Initial Access Broker:IAB），就是專門收集可存取特定組織的帳密資料的角色，可以想像為專門竊取大門鎖匙賣給小偷的人，如果重要的IT基礎架構的帳密被竊且轉賣給駭客，就如同門戶大開完全沒有門禁，任何的防護措施也都沒用。

賽門鐵克已經於第一時間提供多種有效保護 **(SEP／SESC／SMG／SMSMEX／Email.Security.cloud／DCS／EDR)**。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

**基於行為偵測技術(SONAR)的防護：**

- SONAR.TCP!gen6

**VMware Carbon Black 產品的防護機制：**

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

**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：**

- Trojan Horse
- Web.Reputation.3
- 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。

**2025/05/09**

### Mamona勒索軟體

Mamona 勒索軟體是在商品化勒索軟體商圈中新上架的新威脅，它完全是離線運作，沒有外部通訊或資料外洩。該惡意軟體使用自訂的加密規則來加密使用者檔案，並冠上 .HAes 副檔名。它採用混淆技術，例如：使用 ping 進行時間延遲，以避免被偵測到。儘管勒索 (贖金支付) 說明通知，宣稱資料會被竊取，但實際上並沒有資料外洩。已有功能性解密工具可讓受害者復原檔案。

賽門鐵克已經於第一時間提供多種有效保護 **(SEP／SESC／SMG／SMSMEX／Email.Security.cloud／DCS／EDR)**。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

**基於行為偵測技術(SONAR)的防護：**

- SONAR.RansomPlay!gen1
- SONAR.Ransomware!g16

**VMware Carbon Black 產品的防護機制：**

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

- 賽門鐵克 EDR 能夠監控和標記該威脅攻擊者的策略、技術和程序 (Tactics、Techniques、Procedures，TTPs)。
- 賽門鐵克新增了特定惡意軟體的威脅搜尋查詢，客戶可以在 iCDM 控制台上觸發這些查詢。有關這些查詢的更多資訊，請參閱此鏈接：https://github.com/Symantec/threathunters/tree/main/Trojan/IcedID
- 賽門鐵克的端點偵測與回應 (EDR) 最新簡報檔，請點擊此處。

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Ransom.Gen
- Trojan Horse
- Trojan.Gen.MBT

**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。

### 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**