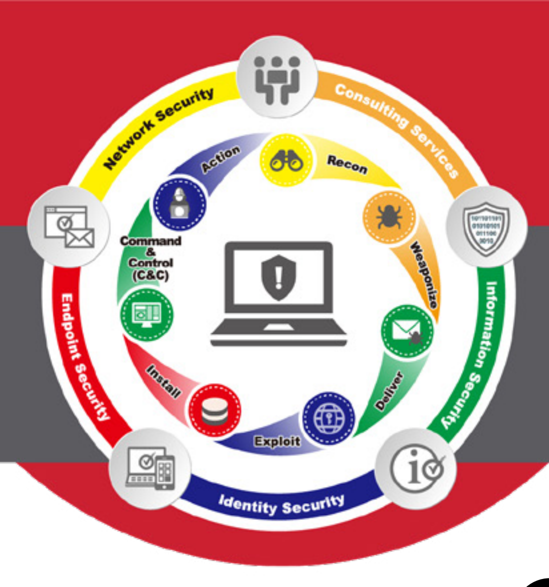

保安資訊--今日最新(台灣時間2025/04/01)
賽門鐵克原廠防護公告重點說明

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 37 萬 4,200 台受保護端點上總共阻止了 4,480 萬次攻擊。這些攻擊中有 82.5% 在感染階段前就被有效阻止：**(2025/03/24)**

- 在**7**萬**9,000**台端點上，阻止了**1,710**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**7**萬**8,400**台端點上，阻止了**640**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2**萬**4,000**台**Windows**伺服主機上，阻止了**590**萬次攻擊。
- 在**4**萬**9,500**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1**萬**1,900**台端點上，阻止了**92**萬**9,200**次嘗試掃描在**CMS**漏洞。
- 在**4**萬**3,800**台端點上，阻止了**170**萬次嘗試利用的應用程式漏洞。
- 在**10**萬**8,200**台端點上，阻止了**240**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,700**台端點上，阻止了**78**萬**1,100**次加密貨幣挖礦攻擊。
- 在**11**萬**400**台端點上，阻止了**720**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**555**台端點上，阻止了**7**萬**9,800**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 17 萬 2,100 個受保護端點上阻止了總計 730 萬次攻擊。**(2025/03/24)**

- 使用網頁信譽情資，在 **165.2K** 個端點上阻止 **700** 萬次攻擊。
- 攔截 **19.5K** 個端點上 **269.2K** 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 **5.7K** 個端點上攔截 **109.7K** 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 **186** 個端點上攔截 **2.9K** 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

2025/03/31

SnakeKeylogger惡意竊密軟體涉入一起多階段的資訊竊取行動

SnakeKeylogger 是一款惡意竊密軟體，會收集憑證和其他敏感資料。目標是常見的應用程式，例如：Google Chrome、Mozilla Firefox 等網頁瀏覽器，以及 Microsoft Outlook 和 Thunderbird 等電子郵件用戶端程式。它也會從 FileZilla 擷取儲存的 FTP 認證。此多階段攻擊由一封包含 IMG 檔案附件的惡意垃圾郵件開始，當開啟此附件時會建立一個虛擬磁碟機。在虛擬磁碟中，可執行檔案會偽裝成 PDF 文件，以增加收件者開啟的可能性。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1

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：

- Scr.Malcode!gen43
- Scr.Malcode!gen139
- Trojan.Gen.MBT
- 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
- 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。

2025/03/31

安卓平台出現的全新手機惡意軟體：Crocodilus

Crocodilus 是最近在威脅生態圈出現安卓平台上的全新行動銀行特洛伊木馬。該惡意軟體具有廣泛的遠端控制和資訊竊取功能，可讓攻擊者進行應用程式覆蓋攻擊、遠端存取遭攻擊的裝置、竊取儲存在行動裝置上的憑證／資料、鍵盤記錄和執行從 C&C 伺服器接收的指令等。與許多其他手機惡意軟體一樣，Crocodilus 須先取得目標裝置上的存取服務，才能進行惡意作業。

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：

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。

- Android.Reputation.2
- AppRisk:Generisk

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。

2025/03/31

威脅生態圈出現全新的惡意軟體載入器：CoffeeLoader

CoffeeLoader 是一款全新的精密惡意軟體載入器，用來執行次要有效酬載，同時逃避偵測。此惡意軟體載入器利用在系統 GPU 上執行程式碼的打包程式。CoffeeLoader 可透過 Windows 工作排程建立持久性／常駐能力，並可透過預先寫死在程式碼的工作排程來維持持久性。對於 C&C 通訊，它使用 HTTPS 與預先寫死在程式碼的伺服器進行通訊。如果這些伺服器無法連線，它會使用動態網域產生演算法 (DGA，Domain Generation Algorithm)，並使用憑證綁定 (certificate pinning) 的方式以確保安全性。

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：

自適應防護技術(包含於SESC)：

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

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 Horse
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Reputation.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.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。

2025/03/30

MassLogger惡意竊密程式涉入多起網路釣魚行動，以採購業務相關誘餌來引誘全球企業上鉤

MassLogger 是一款種專門擷取受害者憑證、擊鍵和剪貼簿資料的惡意竊密程式，在威脅生態圈已有明顯的影響力，全球各地已發現不同規模和受害者類型的攻擊行動。

在最近一次攻擊行動中，有人觀察到一名攻擊者假冒一家在中東經營航空燃料和潤滑油、海事、運輸、科技、包裝、旅遊、水處理和房地產的公司的採購人員，以假亂真來降低受害者的警覺。

惡意電子郵件會施壓收件者確認、簽署虛構的 XLS 文件並蓋章，以增加急迫感。如果使用者開啟惡意附件，Excel 檔案 (PO 23-179、PO 23-181.xls) 將開採濫用 CVE-2017-0199 漏洞，此漏洞是 Microsoft Office 的陳年老漏洞，當開啟精心製作的檔案，就會執行遠端惡意指令碼。接續就會觸發下載和執行 HTA(HTML 應用程式) 檔案，進而呼叫和執行 MassLogger。

目標行業：航太、農業、汽車、建築、人力仲介與就業服務、能源、工程、娛樂、金融服務、醫療保健、工業氣體過濾、IT 服務、實驗室服務、物流、製造、遠洋與離岸、專業服務、公共部門、科技、公用事業。

目標國家：美國、比利時、挪威、阿聯酋、荷蘭、希臘、芬蘭、瑞士、瑞典、沙烏地阿拉伯、馬來西亞、印度、澳洲、南非、法國、新加坡、台灣、印尼、土耳其、肯亞、日本、香港、阿曼、摩洛哥和以色列。

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。

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：

- CL.Downloader!gen12
- ISB.Downloader!gen80
- Scr.Malcode!gen59