保安資訊--本周(台灣時間2025/07/04)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 32 萬 6,200 台受保護端點上總共阻止了 4,820 萬次攻擊。這些攻擊中有 81.7% 在感染階段前就被有效阻止：**(2025/06/30)**

- 在**7萬6,000**台端點上，阻止了**2,160**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**7萬8,100**台端點上，阻止了**560**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬1,700**台**Windows**伺服主機上，阻止了**560**萬次攻擊。
- 在**4萬5,900**台端點上，阻止了**150**萬次嘗試掃描伺服器漏洞。
- 在**9萬5,000**台端點上，阻止了**68萬2,400**次嘗試掃描在**CMS**漏洞。
- 在**38萬**台端點上，阻止了**160**萬次嘗試利用的應用程式漏洞。
- 在**6萬1,900**台端點上，阻止了**120**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,500**台端點上，阻止了**70萬9,600**次加密貨幣挖礦攻擊。
- 在**11萬400**台端點上，阻止了**820**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**522**台端點上，阻止了**6萬9,700**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 29 萬 1,500 個受保護端點上阻止了總計 1,220 萬次攻擊。**(2025/06/30)**

- 使用網頁信譽情資，在 **280K** 個端點上阻止 **11.6M** 次攻擊。
- 攔截 **28.6K** 個端點上 **416.2K** 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 **8.4K** 個端點上攔截 **194.1K** 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 **463** 個端點上攔截 **7.8K** 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。

2025/07/03

遠端監控與管理(RMM)工具常遭濫用～以ConnectWise實例說明

在過去的幾個月中，我們觀察到勒索軟體集團、始存取掮客 (Initial Access Broker-IAB)、進階持續威脅組織 (APT) 和其他網路犯罪份子惡意使用熱門的遠端監控與管理 (RMM) 工具 ConnectWise 的情況急遽增加。這些攻擊目標是全球公私部門的組織。

在這份防護公告中，我們將分享本週觀察到的攻擊行動的簡要見解。這些攻擊主要以電子郵件為主 (附件和／或惡意網址連結)，使用 ConnectWise RMM 用戶端偽裝成假冒的例行業務或政府相關文件，最終授予網路罪犯遠端存取權。

觀察到的檔案名稱：

- InvoiceReceipt_404243.exe
- SSAValidationLocator.exe
- Statement.exe2024+SCHEDULE+C,+MY+ORGANIZERpdf.exe
- SSA.exeE-Statment-819950.exe
- JaxOffice.exe
- Recently_S_S_A_Statement6484451.exe
- SSAverificationupdates.exeRevisedContract.exe
- NotaFiscal-978.exe
- ANZLiveSupport.exe
- INVO_DF42EC51-0238-4963-843A-0908BC35F462-87707F03.exe

- SocialSecurityAdministration.exe
- SA_US_9709181.exe
- AccountStatement_MonthYear.pdf.Client.exe
- Statement.exe
- 401K_Partners.exe

觀察到的惡意網址連結：

- hxxp[:]//s33ewq[.]s3[.]us-east-2[.]amazonaws[.]com/cpataxpreparer-2024manage-returnaccts/2024+BUSINESS+K1+COMPLETE+ORGANIZERpdf[.]exe
- hxxps[:]//groupons[.]pages[.]dev/InvoiceReceipt_404243[.]exe
- hxxps[:]//janetss3[.]s3[.]us-east-2[.]amazonaws[.]com/cpataxpreparer-2024manage-returnaccts/2024+BUSINESS+K1+COMPLETE+ORGANIZERpdf[.]exe
- hxxps[:]//lenshioz[.]s3[.]us-east-2[.]amazonaws[.]com/2024returns-k1-business-trisha/2024+SCHEDULE+C,+MY+ORGANIZERpdf[.]exe
- hxxps[:]//myaccel[.]blue/SSA[.]ORG/ScreenConnect-3025147[.]ClientSetup%20(1)[.]exe
- hxxps[:]//postil[.]ceo/InvoiceReceipt_404243
- hxxps[:]//relocq[.]s3[.]us-east-2[.]amazonaws[.]com/2024-cpareturnscustomefcopy-sandra/2024%20BUSINESS%20K1%20COMPLETE%20ORGANIZERpdf[.]exe
- hxxps[:]//relocq[.]s3[.]us-east-2[.]amazonaws[.]com/2024-cpareturnscustomefcopy-sandra/2024+BUSINESS+K1+COMPLETE+ORGANIZERpdf[.]exe
- hxxps[:]//s33ewq[.]s3[.]us-east-2[.]amazonaws[.]com/cpataxpreparer-2024manage-returnaccts/2024+BUSINESS+K1+COMPLETE+ORGANIZERpdf[.]exe
- hxxps[:]//scheme[.]silabel[.]net/wp-content/SSA[.]exe
- hxxps[:]//social-ssa[.]site/
- hxxps[:]//ssavalidation-cooperation[.]pages[.]dev/SSAValidationLocator[.]exe

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 Horse
- Trojan.RemoteAdmin!g1

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: ScreenConnect Remote Support Software Activity

- Audit: ScreenConnect Remote Support Software Activity 2
- Audit: ScreenConnect Remote Support Software Activity 3
- System Infected: Suspicious ScreenConnect Activity
- System Infected: Suspicious ScreenConnect Activity 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。

2025/07/03

散播Remcos的垃圾郵件行動以.tar壓縮檔附件引人上當

最近觀察到 Remcos 攻擊行動以一封包含 .tar 壓縮檔附件的惡意電子郵件觸發。該壓縮檔包含一個 .lnk 檔案，會啟動 PowerShell 下載 Remcos 有效酬載。Remcos 惡意軟體會注入負責持久性／常駐能力的其他元件。成功入侵後，攻擊者便可完全控制系統。

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.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：

- Infostealer.Bancos
- Scr.Malcode!gen
- Scr.Mallnk!gen6
- Scr.xSense!gen3
- Scr.Mallnk!gen13
- Scr.xSense!gen10
- Trojan.Gen.NPE
- Trojan Horse
- 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

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。

2025/07/03

Janela遠端存取木馬(RAT)在最近的網路攻擊行動中展露頭角

Janela 遠端存取木馬 (RAT) 是源於 BX RAT 的後繼改良版本。Janela RAT 之前曾在針對拉丁美洲地區銀行使用者的攻擊行動中散播。根據報導，目前有新的攻擊行動散佈此惡意軟體。攻擊者利用從 Gitlab 儲存庫傳送給受害者惡意的 .MSI 套件。執行下載的安裝程式會觸發任意指令碼，導致感染 Janela RAT 有效酬載，並安裝惡意瀏覽器擴充套件，從受攻擊的端點竊取資料。

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-CPE!g2
- ACM.Ps-Reg!g

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：

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：

- Downloader
- Trojan Horse
- Web.Reputation.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。

2025/07/03

Blackmoon銀行木馬程式不斷擴充的破壞力

以鎖定線上金融服務使用者 (尤其是韓國) 而聞名的 Blackmoon 銀行木馬程式，已演變成更具欺騙性的多功能威脅。傳統上，它著重於網頁流量重導向和憑證竊取，通常透過釣魚電子郵件、遭入侵或接管的網站和惡意下載傳播來感染 Windows 系統。一旦啟動，它會改變系統設定，並注入假冒的銀行登入頁面以竊取使用者憑證。

最近，Blackmoon 經常被觀察到偽裝成合法的中文安全軟體，並使用與受信任的安全工具相關的名稱。它透過 autorun 和機碼變更等手法建立持久性，並使用 USB 傳播、DLL 側載和程序注入來混入系統環境。除了竊取憑證之外，該惡意軟體還結合資料外洩和挖礦劫持，反映出朝向模組化、多用途攻擊鏈的轉變。

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-Reg!g1
- ACM.Ps-RgPst!g1
- ACM.Ps-Wscr!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.Gen.2
- Trojan.Gen.6
- Trojan.Gen.MBT
- Trojan.Zbot
- W32.XiaobaMiner
- 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

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。

2025/07/02

DEVMAN--源於DragonForce勒索軟體的最新變種

DEVMAN 是源於 DragonForce 勒索軟體家族的全新自訂勒索軟體變種。該惡意軟體會加密資料，並冠上 .DEVMAN 副檔名。注入的勒索 (贖金支付) 說明是直接套用 DragonForce 勒索軟體家族。除了使用者資料之外，該惡意軟體目前似乎也在加密自己的索 (贖金支付) 說明檔。這和其他少數被發現的 DEVMAN 樣本的行為顯示這個勒索軟體可能仍在開發中。

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.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：

- Ransom.DragonForce
- 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

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：

- Attack: Ransom.Gen Activity 46

2025/07/02

GIFTEDCROOK惡意軟體推出強化版，可透過Telegram竊取文件

據報導，由 UAC-0226 威脅組織所運營的 GIFTEDCROOK 惡意軟體出現強化版，與 2025 年 2 月首次觀察到的初期功能相比有顯著升級。GIFTEDCROOK 最初專注於瀏覽器憑證竊取，現在已演變為全面的資料外洩平台，能夠針對敏感的 Office 和 PDF 文件進行攻擊。該組織使用以軍事為主題的誘餌文件，通常寄給烏克蘭政府和軍方人員，誘騙受害者啟用文件中嵌入的惡意巨集。一旦觸發，巨集就會下載並安裝惡意軟體，然後透過 Telegram 殭屍頻道悄悄地將資料外洩。

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：

- Scr.Malcode!gen
- Trojan Horse
- Trojan.Gen.MBT
- 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
- Heur.AdvML.B
- 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
- Audit: Untrusted Telegram API Connection
- System Infected: Trojan.Backdoor Activity 564
- System Infected: Trojan.Backdoor Activity 654

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。

2025/07/01
防護亮點：IPS稽核特徵改變遊戲規則的價值～有效攔截勒索軟體攻擊鏈中的RMM工具濫用

在當今節奏快速的數位世界中，IT 團隊仰賴遠端監控與管理 (RMM) 工具來維持一切運作順暢。這些工具對於生產力來說是不可或缺的，但事實上，勒索軟體駭客組織正在利用這些工具入侵網路、部署惡意軟體，並脅迫 貴公司的業務。

但您如果能扭轉局面呢？如果您有一個預警系統，可以在可疑的 RMM 活動演變成昂貴的勒索軟體噩夢之前就發現它，那可以怎麼辦？

有了**賽門鐵克入侵防護系統 (IPS) 的稽核特徵功能**，您就可以做到。它們是您對付最陰險之勒索軟體攻擊的主動防禦工具。

詭異的威脅：勒索軟體如何劫持 IT 團隊仰賴遠端監控與管理 (RMM) 工具

勒索軟體駭客組織很聰，知道您使用合法的 RMM 工具，例如：AnyDesk、ScreenConnect、TeamViewer 和 Splashtop。他們不是以新奇的零時差入侵，而是濫用您賴以提高工作效率的這些常用工具軟體。我們已經看到頂尖的勒索軟體家族，例如：LockBit、BlackCat、Hive 和 AvosLocker 屢次濫用這些常見的 RMM 平台：

- 取得初始存取權
- 在網路中建立據點
- 在系統之間自由移動
- 竊取敏感資料
- 最後，釋放其破壞性的有效酬載

突破勒索軟體的挑戰：主動偵測、不中斷作業

這就是 IPS 稽核特徵創造巨大價值的地方。與其等待破壞發生，這些特徵會一直觀察，充當您的隱密守護者。

這就是核心價值主張：

1. **早期預警，發揮最大的影響力**：IPS 稽核特徵會主動監控可疑的 RMM 行為：
   - 向外與 RMM 基礎架構的非預期連線
   - 未經授權的 RMM 代理安裝
   - 不尋常的遠端會話啟動和檔案傳輸。
2. **稽核模式**：預設情況下，IPS 稽核特徵以**稽核模式**運作，記錄所有活動並觸發警報。這可為您的安全團隊提供無價的早期可視性，讓您建立正常、經核准的 RMM 使用基準。這對於識別真正的威脅是非常重要的，而不會持續出現誤判。
3. **不會中斷 IT 的關鍵業務**：與可能會阻礙合法 IT 作業的解決方案不同，IPS 稽核特徵 (Audit Signatures) 專為精確而設計。您可以在不妨礙基本 IT 支援功能的情況下抓到壞人。建立基準後，您可以選擇性地將特定特徵切換至**封鎖模式**，主動防止風險最高的未授權或惡意 RMM 活動。
4. **強化您的資安監控中心 (SOC)**：對於您的 SOC 團隊而言，這些特徵可改變遊戲規則。它們可將模糊的懷疑轉換為可採取行動的情報：
   - **情境豐富的警示**：每個警示都提供重要的詳細資訊：哪個 RMM工具、來源／目的地 IP、時間戳記和活動類型。

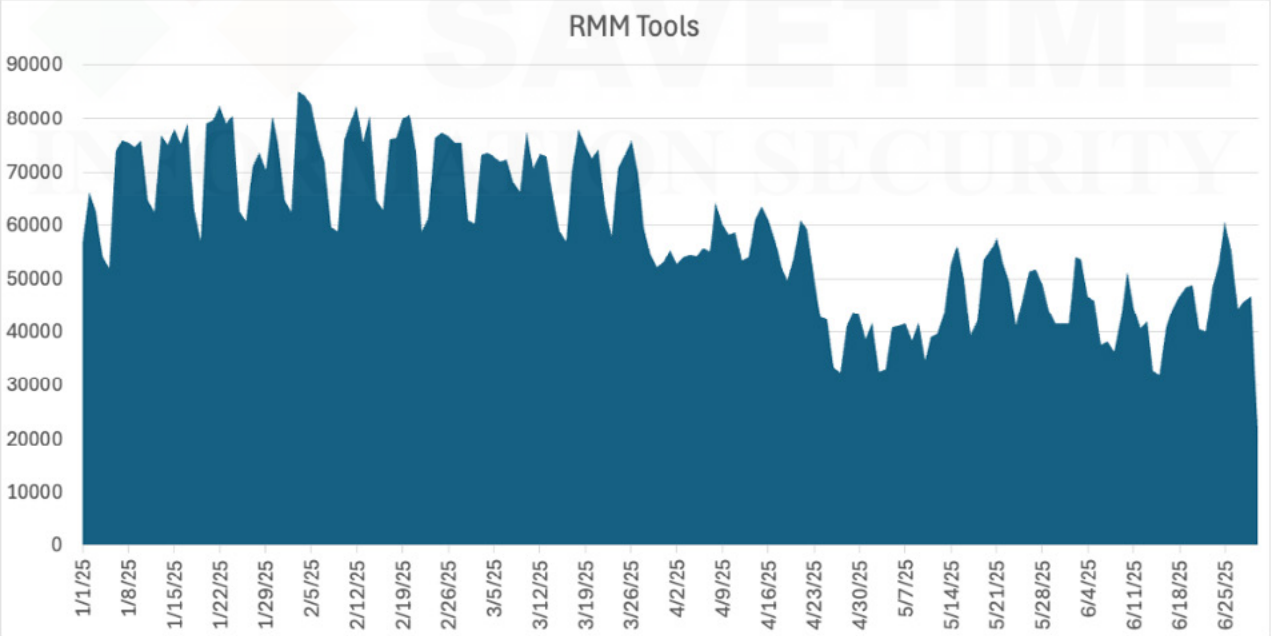
- **具體指出異常**：快速發現來自未經授權裝置的 AnyDesk 會話、可疑電子郵件後的 ScreenConnect 安裝程式，或非辦公時間的 ZohoAssist 使用情況。
- **強化威脅攔截**：來自稽核特徵的豐富記錄可成為主動偵測威脅的寶貴資料，協助您揭露隱藏的攻擊者。
- **統一安全態勢**：此遙測可與您的 SIEM 和 EDR 解決方案無縫整合，提供網路和端點活動的全面性整體檢視，以強化事件回應。

您的行動計畫：立即強化您的防禦

若要真正發揮 IPS 稽核特徵的威力，並大幅改善您的勒索軟體復原能力，請遵循此策略路線圖：

1. **大範圍的應用**：針對整個網路上所有已知的 RMM 工具啟用稽核特徵。
2. **針對您的環境調整**：針對您特定的網路使用情況微調這些特徵。這對於建立合法活動的精確基準、減少誤報並確保您的安全團隊專注於真正的威脅非常重要。
3. **優先進行每日檢閱**：優先進行每日警示檢閱，並將重點放在異常的端點、非工作時間的活動，或出現新的、未經核准的 RMM 工具。
4. **執行白名單**：維持經核准的 RMM 工具和授權管理員的嚴格白名單，以進一步簡化調查工作。
5. **策略性封鎖**：一旦確認正常行為，針對確定的威脅啟動封鎖模式，立即關閉惡意活動。

切換至封鎖模式後，賽門鐵克 IPS 稽核特徵會封鎖 RMM 工具



必須強調的事實：投資於主動式勒索軟體防禦

在對抗勒索軟體的戰鬥中，早期偵測不僅是一項優勢，更是一項必要條件。透過部署稽核模式 IPS 特徵碼，您可以為組織提供主動、不中斷且高效的方式，偵測濫用 RMM 工具以來 發動勒索軟體攻擊的關鍵階段。這項功能對於預防會造成後患無窮的入侵、保護您的資料，以及確保持續的業務運作至關重要。

儘早做好萬全準備，不要坐等勒索軟體來襲。使用賽門鐵克稽核模式 IPS 特徵碼 (Symantec IPS Audit Signatures) 能加強您的防禦能力，翻轉網路威脅的趨勢。

建議客戶在桌機/筆電和伺服器上啟用 IPS，以獲得最佳保護。請點擊此處瞭解啟用 IPS 的說明。欲瞭解如何整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站，請點擊此處。沒有使用 SEP 也行？可使用賽門鐵克瀏覽器防護服務保護您的瀏覽器。

2025/07/01

Braodo惡意竊密軟體在GitHub上託管下載的元件

最近觀察到 Braodo 惡意竊密軟體所涉入的攻擊行動，利用 GitHub 來放置可供下載的攻擊鏈中所需多個元件。該攻擊鏈包括一個初始 .bat 檔案，它會啟動 PowerShell 來下載第二階段所需的原件，即另一個 .bat 檔案。這個次要的 .bat 檔案負責從 GitHub 下載其他元件，包括建立持久性和執行最後 Braodo 惡意竊密軟體有效酬載的元件。最終有效酬載以 .zip 壓縮檔的形式送達，其中包含 Python 腳本形式的惡意竊密軟體。

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-FlPst!g1
- ACM.Ps-Http!g2

基於行為偵測技術(SONAR)的防護：

- SONAR.Powershell!g98

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：

- Downloader
- ISB.Downloader!gen348
- ISB.Dropper!gen4
- Scr.ObfBat!gen3
- Trojan Horse

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: Github Cloud Service Connect Attempt
- Audit: PowerShell Process Accessing Github

2025/06/30

CVE-2025-4322：存在WordPress Motors主題中的提權漏洞

CVE-2025-4322 是存在 WordPress Motors 主題中的高嚴重等級的提權漏洞 (CVSS 風險評分：9.8)，在 5.6.67 之前的版本中影響 WordPress Motors 主題。開採濫用該漏洞，攻擊者可在未認證或身份驗證的情況下，重設任何使用者 (包括管理員) 的密碼。此漏洞已影響超過 22,000 個 WordPress 網站，主要是汽車經銷商及租賃服務業者所使用的網站，此漏洞可透過管理員帳號接管導致整個網站受到攻擊。此漏洞已在 GitHub 上公開記錄，強調立即修補或減緩的迫切性。

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：

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：

- Attack: WordPress Motors Theme CVE-2025-4322

2025/06/30

好工具往往淪為幫兇：EmailJS和HubSpot在CCMA網路釣魚計劃中遭濫用

一個全新網路釣魚行動假借南非調解仲裁委員會 (Commission for Conciliation、Mediation and Arbitration，CCMA) 的法律傳票，利用緊迫感和恐懼感迫使收件者採取行動。此網路釣魚行動鎖定在南非營運的組織 (企業和政府相關機構)，以及在南非設有辦事處、客戶或營運的跨國公司。

這封電子郵件的標題為「RE：SUBMISSION OF SUMMON DEMAND DOCUMENTS」，冒充一家知名的跨國跨洲的德國金融科技公司，並附上一份 PDF 附件，聲稱其中包含需要立即處理的官方法律文件。

附件檔案名為 Demand Notice.pdf，包含一個隱藏連結，可將受害者重定向至 HubSpot CDN 基礎架構上託管的 HTML 頁面。這是利用合法平台試圖逃避內容檢查和網域封鎖清單的威脅份子常用的手法。在 6 月較早前的攻擊行動中，他們使用的是 Files FM，一個位於歐洲的雲端儲存和檔案分享服務。

在此案例中，釣魚網頁偽裝成法律通訊，背景模糊，模仿南非 SARS 機構的官方信箋抬頭。在此頁面之上，還有虛假 Microsoft Office 365 登入提示，要求使用者輸入其電子郵件和密碼。

EmailJS 是基於 JavaScript 的合法服務，可讓電子郵件直接從瀏覽器傳送，無需後端伺服器。網路釣魚頁面並非將憑證滲透到攻擊者控制的網域，而是使用用戶端腳本透過 EmailJS 的公開 API 傳送竊取的登入資料。這種無伺服器方法試圖繞過傳統的偵測機制，這些機制依賴於監控離埠網路連線或標示可疑網域。網路釣魚表格也封鎖 Gmail 等免費電子郵件供應商，顯示其明顯專注於竊取價值較高的企業憑證。

雖然 EmailJS 廣泛用於合法用途，例如：聯絡表單和通知，但對於網路釣魚工具包來說，它仍是一個很有吸引力的工具。

網路知識：

◎ EmailJS 允許開發者直接從應用的前端向特定電子郵件帳號發送郵件，無需建置自己的郵件伺

服器。開發者可使用 EmailJS 提供的 API，並使用預設樣板來處理表單提交後的郵件傳送工作。這樣的方案讓我們能夠快速地實現聯絡表單功能，並將表單內容以郵件的形式發送出去。

◎ HubSpot 是全球第一套 Inbound Marketing 集客式行銷的行銷工具，可以幫助客戶吸引使用者、轉換潛在客戶、促成銷售的成長。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Phish.Pdf
- Phish.Html

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)。

2025/06/27

Lotus Spider駭客組織發動的網路攻擊，利用Lotus V2惡意程式載入器

據報導，在一起新的網路攻擊行動中發現 Lotus V2 惡意程式載入器涉入其中，並歸咎於 Lotus Spider 駭客組織。該攻擊鏈利用虛假的 CAPTCHA 式傳送策略，引導受害者執行 PowerShell 腳本，進而下載並執行惡意的 .MSI 安裝程式。.MSI 檔案會將 .DLL 檔案側載到遭入侵的機器上，並啟用與攻擊者伺服器的 C&C 通訊。成功感染 Lotus V2 惡意程式載入器後，就可以散佈第二階段的有效酬載。

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。

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.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A!400

- 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。

2025/06/27

免費的永遠最貴～軟體被重新打包成為惡意軟體傳播的重要手法

研究人員發現一種正在上升的趨勢，網路罪犯重新包裝合法的商業軟體 (例如：SonicWall 的 SSL VPN NetExtender) 來傳送惡意竊密程式。從視訊轉檔程式到系統公用程式等熱門應用程式，都被修改為包含惡意有效酬載，並透過釣魚電子郵件、破解的軟體平台和欺騙性廣告散佈。

這些特洛伊木馬安裝程式看似真實，但一旦執行就會悄悄地竊取敏感資料，例如：登入憑據、瀏覽器 cookies、加密錢包和系統資訊。

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：

自適應防護技術(包含於SESC)：

- 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：

- Infostealer
- Trojan Horse
- Trojan.Malmsi

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**。