保安資訊--今日最新(台灣時間2025/07/15)
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 31 萬 6,100 台受保護端點上總共阻止了 4,910 萬次攻擊。這些攻擊中有 82.1% 在感染階段前就被有效阻止：**(2025/07/14)**

- 在**7**萬**5,600**台端點上，阻止了**2,110**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**6**萬**7,800**台端點上，阻止了**540**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2**萬**1,300**台**Windows**伺服主機上，阻止了**610**萬次攻擊。
- 在**4**萬**4,700**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**78**萬**5,600**次嘗試掃描在**CMS**漏洞。
- 在**3**萬**6,300**台端點上，阻止了**170**萬次嘗試利用的應用程式漏洞。
- 在**6**萬**1,100**台端點上，阻止了**140**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**953**台端點上，阻止了**64**萬**1,100**次加密貨幣挖礦攻擊。
- 在**10**萬**1,200**台端點上，阻止了**820**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**467**台端點上，阻止了**5**萬**7,000**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 28 萬 8,800 個受保護端點上阻止了總計 1,2580 萬次攻擊。**(2025/07/14)**

- 使用網頁信譽情資，在 **278.1K** 個端點上阻止 **12M** 次攻擊。
- 攔截 **27.5K** 個端點上 **349.5K** 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 **7.4K** 個端點上攔截 **162K** 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 **459** 個端點上攔截 **9.4K** 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

2025/07/14

安裝軟體務必從原廠下載～透過假冒軟體的安裝程式暗度陳倉Sainbox遠端存取木馬(RAT)

據報道，有新的網路攻擊行動透過假冒的軟體安裝程式傳播一種被稱為 Sainbox 遠端存取木馬 (RAT) 的 Gh0stRAT 後繼變種。攻擊者將惡意軟體的二進位檔偽裝成中國知名的應用程式，例如：DeepSeek、搜狗或 WPS Office。惡意軟體 .msi 或 PE 安裝程式會被上架在釣魚網站，然後傳送給目標受害者。該攻擊活動被歸屬於名為 Silver Fox 的駭客組織。攻擊者也利用開放原始碼 Hidden rootkit 的變種，在惡意作業期間隱藏任意程序、登錄機碼等。

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.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- 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。

2025/07/14

Cloudflare的臨時通道TryCloudflare遭濫用來提供惡意有效酬載

最近觀察到一起網路攻擊行動濫用合法的雲端服務，例如：TryCloudflare 來託管和傳送高度迴避的遠端存取木馬 (RAT)，例如：AsyncRAT、XWorm、VenomRAT 和 Remcos。攻擊鏈起始於 Dropbox 上代管 ZIP 檔案的釣魚誘餌連結。裡面惡意捷徑檔案會引導受害者進行複雜的多階段執行，包括透過 TryCloudflare 快速通道下載惡意 .LNK 捷徑檔、執行混淆批次腳本，最後擷取並執行 Python 腳本以部署 RAT。使用短暫、未註冊的 TryCloudflare 子網域，讓此基礎架構在邊界控制看來像是合法，使得預先封鎖或列入黑名單變得非常困難。

網路知識：TryCloudflare 是資安業者 Cloudflare 提供的臨時隧道 (Tunnel) 服務，開發者無需設置 DNS 或是調整防火牆組態，就能藉此快速將應用程式或網站於網際網路公開，避免有人直接對伺服器上下其手。然而，這種服務也遭到駭客利用，將其用於埋藏攻擊來源。

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-Base64!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：

- Scr.Malcode!gen
- Scr.Malscript!gen28
- Scr.xSense!gen*
- Trojan.Gen.NPE
- Trojan.Malscript
- WS.SecurityRisk.4
- 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。

2025/07/14

SafePay勒索軟體

SafePay 勒索軟體，第一次被發現是在去年。據報導，該勒索軟體背後的攻擊者已攻擊超過 200 個不同領域的受害者。據了解，威脅者會透過有漏洞的 RDP 或 VPN 點取得存取權，並利用各種就地取材工具在受感染的網路中橫向移動。SafePay 勒索軟體會加密使用者資料，並冠上 .safepay 副檔名。勒索 (贖金支付) 說明則以 readme_safepay.txt 的文字檔形式留存。攻擊者還運用雙重勒索手法，威脅受害者如果不配合如實付贖金，就公開被盜資料。

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-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：

- PUA.Gen.2
- Ransom.Gen
- WS.Malware.1
- 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!200
- Heur.AdvML.C

2025/07/13

安卓行動裝置上的新威脅：Qwizzserial惡意程式

在 2025 年中，研究人員觀察到 Qwizzserial 惡意程式劇增，這是一種新發現的 Android 惡意軟體，專門用來竊取銀行憑證和截取簡訊型的雙重驗證碼。此惡意軟體於 3 月首次被偵測到，它透過模仿合法服務的假冒應用程式進行傳播，引誘受害者安裝這些應用程式。一旦啟動，它就會透過 Telegram 機器人，悄悄將竊取的資料轉寄給攻擊者。此網路攻擊行動主要鎖定烏茲別克的使用者。

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

2025/07/11

CVE-2025-47812--存在Wing FTP伺服器的漏洞在真實網路情境上已遭開採濫用

CVE-2025-47812 是最近被揭露的遠端執行程式碼 (RCE) 漏洞，會影響 Wing FTP 伺服器，這是一個跨平台的檔案傳輸軟體。此漏洞會影響 7.4.4 之前版本的產品，成功開採濫用該漏洞會讓潛在攻擊者在受影響的應用程式中執行任意程式碼。產品供應商已為此漏洞釋出修補程式，但仍有報告指出此漏洞正被廣泛開採濫用。

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：

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: Wing FTP Server CVE-2025-47812

2025/07/11

新發現Pay2Key勒索軟體即服務集團濫用基於匿名技術的隱形網路專案(Invisible Internet Project，I2P)協助駭客集團發動網路攻擊

據報導，在真實網路情境上發現一起租用勒索軟體即服務 (ransomware-as-a-service：RaaS) 營運商：Pay2Key服務的網路攻擊行動。該行動被稱為 Pay2Key.I2P，與 Fox Kitten 進階持續威脅 (APT) 駭客組織有關。攻擊者以 MS Word 圖示偽裝的自解壓縮 (SFX) 檔形式散佈惡意二進位檔。在 cmd 設定腳本和 PowerShell 指令的幫助下，執行下載的壓縮檔會觸發感染鏈，最終導致受感染機器上的資料被加密。注入的勒索 (贖金支付) 通知指示受害者瀏覽攻擊者託管在 I2P (隱形網際網路計畫) 網路上的入口網站。

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-Http!g2
- ACM.Ps-Rd32!g1
- ACM.Ps-Reg!g1
- ACM.Ps-Wbadmin!g1
- ACM.Untrst-RunSys!g1
- ACM.Wbadmin-DlBckp!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.Dropper
- SONAR.SuspBeh!gen616
- SONAR.SuspBeh.C!gen10;
- 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：

- ISB.Dropper!gen4
- ISB.Heuristic!gen50
- ISB.Heuristic!gen58
- Scr.xSense!gen3
- Scr.xSense!gen10
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- Web.Reputation.1
- 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!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。