保安資訊--本周(台灣時間2025/08/08)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 9,100 台受保護端點上總共阻止了 5,380 萬次攻擊。這些攻擊中有 83.4% 在感染階段前就被有效阻止：**(2025/08/04)**

- 在**7萬6,700**台端點上，阻止了**2,330**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**7萬3,100**台端點上，阻止了**530**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬2,100**台**Windows**伺服主機上，阻止了**570**萬次攻擊。
- 在**4萬7,000**台端點上，阻止了**190**萬次嘗試掃描伺服器漏洞。
- 在**1萬5,700**台端點上，阻止了**100**萬次嘗試掃描在**CMS**漏洞。
- 在**4萬7,500**台端點上，阻止了**200**萬次嘗試利用的應用程式漏洞。
- 在**6萬2,400**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**794**台端點上，阻止了**69萬2,900**次加密貨幣挖礦攻擊。
- 在**9萬6,700**台端點上，阻止了**830**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**537**台端點上，阻止了**7萬1,700**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 28 萬 3,800 個受保護端點上阻止了總計 1,250 萬次攻擊。**(2025/08/04)**

- 使用網頁信譽情資，在 **273.6K** 個端點上阻止 **11.8M** 次攻擊。
- 攔截 **27.9K** 個端點上 **475.6K** 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 **6.8K** 個端點上攔截 **153.2K** 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 **377** 個端點上攔截 **8.4K** 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。

2025/08/07

營運Project AK47駭客工具組的駭客在這一波SharePoint的ToolShell之零時差漏洞攻擊中擔任要角

Palo Alto Networks 威脅情報小組 Unit 42 的研究人員發現針對最近遭開採濫用的 SharePoint 漏洞 (又稱 ToolShell) 的攻擊活動，與利用名為 Project AK47 工具集 (C&C 的客製化命令與控制框架) 的攻擊活動之間存在所關聯。此工具集是由中國的威脅份子所為，其中包括一個後門、採用側載的惡意程式載入器和勒索軟體。此工具集的涉入，Unit 42 評估該威脅份子有財務動機。由涉入 ToolShell 的漏洞攻擊來看，相信此網路犯罪者也有涉入網路間諜活動。

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.Psxec-Lnch!g1
- ACM.Psxec-Masq!g1
- ACM.Ps-Rd32!g1
- ACM.Ps-RgPst!g1
- ACM.Ps-SvcReg!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
- Ransom.Lockbit
- Trojan Horse
- Trojan.Gen.MBT
- 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
- Heur.AdvML.C

2025/08/06
CVE-2025-34300--存在問卷平台設計軟體Lighthouse Studio的漏洞

CVE-2025-34300 是一個最近揭露的範本注入漏洞，會影響問卷平台設計軟體：Sawtooth Lighthouse Studio，這是一個受歡迎的調查研究平台。如果成功開採濫用此漏洞，未經驗證攻擊者可能會透過特製的請求執行任意程式碼。此漏洞已在 9.16.4 或更新的版本中獲得修補。

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: Lighthouse Studio CVE-2025-34300

2025/08/06
新發現散播PXA Stealer惡意竊密程式的網路攻擊行動

PXA Stealer 惡意竊密程式最早在去年被發現。此惡意軟體目的在收集和滲透各種敏感資料，包括憑證、信用卡記錄、瀏覽器 cookies、Discord 權杖、加密貨幣錢包以及來自第三方應用程式（例如：密碼管理器或 VPN 客戶端）的資訊。最近在真實網路情境上觀察到散佈此惡意竊密程式的全新多階段攻擊行動，目標受害者來自全球 60 多個國家。攻擊者採用新型的規避技術，例如：透過合法簽署的軟體二進位檔進行側載、隱藏惡意 DLL 或模仿常見檔案類型的壓縮檔。

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.Ps-RgPst!g1
- ACM.Ps-SvcReg!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.Dropper
- 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。

2025/08/06

CVE-2025-54309--存在CrushFTP零時差漏洞在真實網路情境上已遭開採濫用

CVE-2025-54309 是最近被揭露一個未受保護的替代通道漏洞，會影響 CrushFTP 管理檔案傳輸軟體。如果成功開採濫用此漏洞，未經認證的遠端攻擊者可透過 CrushFTP 取得管理存取權限，而導致遠端程式碼執行。產品供應商已針對此漏洞釋出 CrushFTP 軟體的修補版本。此漏洞已被美國網路安全暨基礎設施安全局 (CISA) 列入「已遭成功利用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中，顯示該漏洞在真實網路情境中已遭大肆開採濫用。

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: CrushFTP CVE-2025-54309

基於安全強化政策(適用於使用DCS)：

賽門鐵克的重要主機防護系統：DCS～Data Center Security，預設鎖定政策會拒絕所有遠端連線，因此可保護底層 UNIX／Windows 伺服器免受此漏洞攻擊。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2025/08/06

JSCEAL惡意竊密程式，透過惡意廣告傳播鎖定加密貨幣使用者

根據 Check Point 發佈一份報告顯示，一場大規模的惡意廣告攻擊行動，正在透過假冒的 Binance、MetaMask 和 Kraken 等應用程式廣告，鎖定加密貨幣使用者為攻擊目標。受害者會被誘騙下載遭篡改 (加料) 的安裝程式，這些安裝程式會與攻擊者託管的 JavaScript 一同執行，這是一種逃避偵測的雙重執行手法。惡意軟體使用 PowerShell 腳本來剖析系統，然後再部署以 Node.js 編譯的 JavaScript(JSC) 惡意軟體，稱為 JSCEAL，它會竊取加密錢包憑證、瀏覽器 cookies、Telegram 存取權杖和密碼。JSCEAL 擁有超過 35k 個惡意廣告，全球曝光率可能超過 1 千萬使用者，透過社交工程和隱匿的反分析技術造成嚴重威脅。

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.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!500
- 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：

- URL reputation: Browser navigation to known bad URL

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。

2025/08/05

SAP存在的CVE-2025-31324漏洞，已遭Linux平台上的後門程式：Auto-Color開採濫用

Auto-Color 是一種隱匿的 Linux 遠端存取木馬程式 (RAT)，已被發現到開採濫用 CVE-2025-31324 漏洞 (SAP NetWeaver 中允許遠端檔案上傳的嚴重漏洞) 來取得 Linux 系統的初始存取權。惡意程式透過包含 ELF 有效籌載的惡意 ZIP 檔案傳送，並透過修改 ld.so.preload 檔案和部署惡意共用物件，在以 root 存取權限執行時建立常駐能力。Auto-Color 具有模組化的指令集，支援反向

shell、檔案執行、代理設定及自我刪除。它使用 DNS tunneling 和 TLS 與它的命令控制伺服器通訊，如果在沒有 root 權限的情況下執行，或 C&C 伺服器無法連線時，Auto-Color 會保持休眠狀態，以逃避偵測。

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.Gen.NPE
- WS.Malware.1

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: SAP NetWeaver CVE-2025-31324

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。

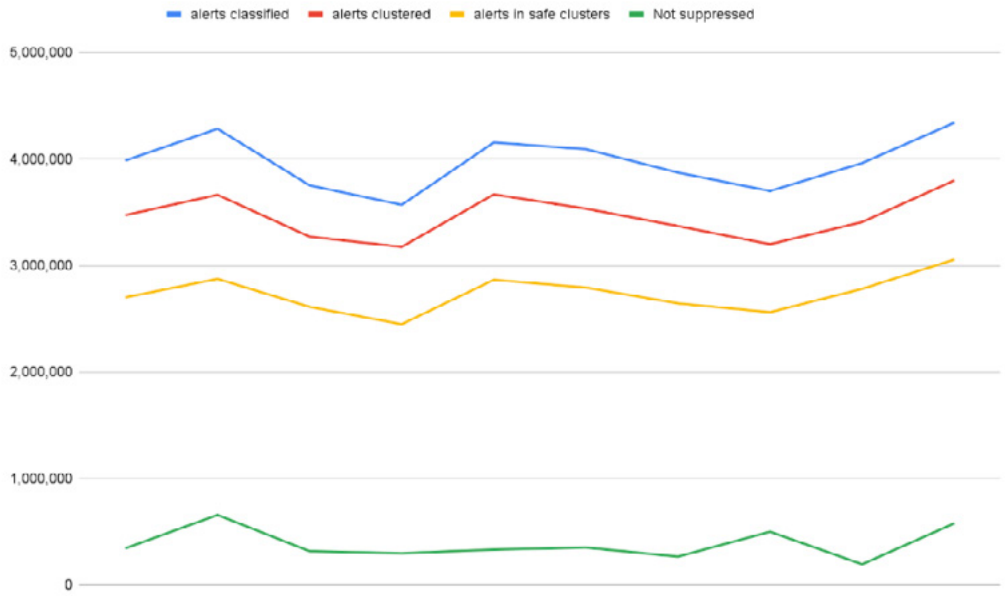
2025/08/05
防護亮點：破除雜訊：智慧型異常分類如何強化資安營運中心(SOC)作業

資安營運中心 (SOC) 的效能經常受到一個無聲無息、無處不在的敵人影響：「警報通知疲勞轟炸」。當資安營運中心 (SOC) 分析師被大量的安全警示淹沒時，就會出現這種現象，其中許多都是誤報、低優先順序或多餘的警示。不分優先順序的警報持續不斷，會導致敏感度降低、倦怠，最重要是可能真的會遺漏真正的重要威脅。

「警報通知疲勞轟炸」後果非常嚴重。分析師難疲於奔命，回應時間變慢，組織的整體安全狀態也會被弱化。大量的警報讓人很難從看似良性事件中分辨出真正的惡意活動，導致時間浪費、營運成本增加，以及遭成功入侵的風險提高。

為了避免這個關鍵問題，賽門鐵克開發創新的抑制技術：異常分類 (Anomaly Classification)。此系統利用人工智慧 (AI) 和機器學習 (ML) 的力量，同時採用監督和非監督模型來智慧地抑制良性警示，並提高真正惡意警示的能見度。我們的新監督模型是根據遙測特徵與數以千計的客戶回饋輸入進行訓練，讓我們能有效結合無監督與有監督技術，達到更高的抑制率。

有了新引入的模型，我們取得重大突破。在我們初步實驗中，我們已經壓制 94% 的警報，但隨著改良模型的到位，我們進一步將未壓制的警報減少原來值的三分之二，合計壓制率達到 98%。其餘的高優先級警報應由 SOC 小組進行分流。這可大幅降低 SOC 代理的工作量，讓他們能將專業知識專注在真正重要的威脅上。



為 SOC 團隊帶來的好處

實作我們的異常分類系統，可為飽受「警報通知疲勞轟炸」的 SOC 團隊帶來多種好處：

- 大幅降低警報量
- 更專注於真正的威脅
- 更快的事件回應
- 提高分析師士氣和留任率
- 提高效率並節省成本
- 主動的安全態勢。

欲深入了解賽門鐵克的端點多層次防護解決方案中「進階機器學習」防護技術，請點擊此處。

2025/08/05

網路釣魚行動濫用Proofpoint 與Intermedia兩家資安業者惡意網址檢測服務

研究人員報告一起協同式的網路釣魚行動，利用 Proofpoint 和 Intermedia 的連結防護服務 (Link-Wrapping) 功能來掩飾惡意 URL，並將使用者重導向至 Microsoft 365 的憑證蒐集頁面。攻擊者取得受保護電子郵件帳號的存取權，然後使用 Bitly 和其他短網址來混淆目標，產生多層重導向連結。他們濫用受信任網域 (urldefense.proofpoint.com 或 url.emailprotection.link)，以提高點擊率，並試圖繞過信譽過濾。誘餌包括假冒的語音郵件通知、共用的 Teams 文件和 Zix 安全訊息提示，所有這些都會導向假冒的 Microsoft 登入頁面。

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：

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)。

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。

2025/08/05

新出現以仿冒日本航空(JAL)「補登哩程」通知郵件的網路釣魚

賽門鐵克偵測到新一波針對日本使用者的網路釣魚，他們使用偽造的日本航空（JAL）電子郵件。這些電子郵件的主旨：マイル加算手続きのご案内 -> (翻譯：「里程積分規程訊息」)

這些郵件被偽裝成通知郵件，其中提到由於用戶帳戶中的註冊資訊存在差異，導致里程未被計入。為了解決這個問題，要求用戶點擊所提供的 URL 並確認會員資料。

點擊所提供的連結，使用者就會被轉到偽造的日航登入頁面，以竊取憑證。一旦入侵，攻擊者便可存取受害者的 JAL Mileage 帳戶。

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：

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)。

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。

2025/08/04

4l4md4r勒索軟體

一個被稱為 Mimo Gang 的勒索軟體駭客組織最近聲名大噪，他們的勒索軟體稱為 4l4md4r。成功入侵後，勒索軟體會在被加密檔案中冠上 .4l4md4r 副檔名，並在多個目錄中留下贖金說明。他們的攻擊鏈還包含 PureHVNC，這是一種用於監視和控制的遠端存取特洛伊木馬。

根據贖金說明的內容，該行駭客組織似乎沒有採取雙重勒索策略 (即威脅若不滿足要求就出售或洩露資料)。相反的，他們只專注於在加密的勒索上，要求價值 500 美元的比特幣。

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

基於機器學習的防禦技術：

- Heur.AdvML.C

2025/08/04

惡意軟體冒充印度金融機構APP，竊取安卓手機／行動裝置上的資料並耗損電力

研究人員發現有安卓手機／行動裝置上的惡意軟體透過釣魚網站，模仿可信賴的金融服務 APP，以印度語系的行動裝置為目標。惡意 APP 最初看似無害，在安裝有效酬載之前會先充當驅動程式，竊取憑證和個人資料，同時還會透過 Firebase 指令使用 XMRig 隱秘地挖掘門羅幣。

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。

- 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。

2025/08/04

針對印度政府與國防單位的網路釣魚攻擊

一場由 APT36 駭客組織(也稱為 Transparent Tribe) 發起的網路釣魚攻擊行動已經浮出水面，目標是印度政府和國防單位，他們利用透過錯別字 (打錯字) 的域名或模仿合法的類似域名 (typo-squatting) 伎倆來模仿官方入口網站。根據報導，該攻擊透過提示受害者輸入電子郵件密碼和來自印度 Kavach 認證系統的即時一次性密碼 (OTP) 來獲取憑證。

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：

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)。

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。

2025/08/03

傳播SilverFox遠端存取木馬(RAT)的網路釣魚行動

發現一起 SilverFox 遠端存取木馬 (RAT) 涉入的全新網路釣魚行動，攻擊者透過搜尋引擎佳化 (SEO) 或購買關鍵字排行的惡意網站來進行水坑式攻擊，冒充合法軟體 (例如：Feishu) 的下載連結。研究人員發現超過 2,600 個相關的惡意網站。當使用者被成功誘騙時，他們會下載一個偽造的安裝程式壓縮檔，其中包含一個未簽署的可執行驅動程式，該驅動程式會部署 SilverFox 遠端存取木馬程式 (RAT)，這是一個可自訂的模組化後門。

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.SuspDriver!g30

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

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。

2025/08/03

Plague(*瘟疫)--Linux平台新出現的後門程式

最近發現一個被稱為 Plague(*瘟疫) 的隱匿式 Linux 後門，它以惡意 PAM(Pluggable Authentication Modules，即可插入的驗證模組) 的形式嵌入，悄無聲息地繞過系統認證，並建立持續 SSH 存取權限。研究人員指出，自 2024 年 7 月以來已觀察到多個變種，顯示出強大的迴避能力。Plague 使用不斷進化的多層混淆、反偵錯檢查、硬編碼 (寫死在程式碼內) 憑證，以及抹除 SSH 連線痕跡的技術，在系統更新後仍能保持活躍，並留下最少可供鑑識採證的跡證。

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：

- Trojan.Gen.NPE

2025/08/01

DoubleTrouble～安卓手機行動裝置平台出現的銀行金融惡意軟體

據報導，一種複雜名為 DoubleTrouble 安卓手機行動裝置平台上的銀行金融惡意軟體，透過冒充歐洲銀行機構的釣魚網站以及最近在 Discord 上分享的惡意連結傳播。此惡意軟體結合先進的覆蓋攻擊、螢幕錄影、鍵盤記錄和即時裝置操控，讓網路罪犯能夠收集銀行憑證、攔截一次性密碼 (OTP)，甚至執行自動化動作，例如：模擬點擊、刷卡或啟動應用程式。其有效酬載隱藏在具有欺騙性的合法應用程式之資源／原始目錄中。一旦安裝後，DoubleTrouble 會濫用 Android 的輔助功能服務 (Accessibility Services)，以隱匿的方式劫持裝置控制權並擷取敏感資料，即使在實施多因素驗證的情境也是如此。

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。

- AdLibrary:Generisk
- AppRisk: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。

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**。