保安資訊--本周(台灣時間2025/09/05)
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) 在受保護端點上總共阻止了 6,700 萬次攻擊。這些攻擊中有 87.2% 在感染階段前就被有效阻止：**(2025/09/03)**

- 在受保護端點上，阻止了**2,940**萬次嘗試掃描**Web**伺服器的漏洞。
- 在受保護端點上，阻止了**510**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**Windows**伺服主機上，阻止了**480**萬次攻擊。
- 在受保護端點上，阻止了**310**萬次嘗試掃描伺服器漏洞。
- 在受保護端點上，阻止了**200**萬次嘗試掃描在**CMS**漏洞。
- 在受保護端點上，阻止了**250**萬次嘗試利用的應用程式漏洞。
- 在受保護端點上，阻止了**97**萬**1,600**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在受保護端點上，阻止了**56**萬**9,500**次加密貨幣挖礦攻擊。
- 在受保護端點上，阻止了**810**萬台次向惡意軟體**C&C**連線的嘗試。
- 在受保護端點上，阻止了**8**萬**6,400**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，在受保護端點上阻止了總計 1,330 萬次攻擊。**(2025/09/03)**

- 使用網頁信譽情資，在端點上阻止了 **12M** 次攻擊。
- 在受保護端點上攔截 **1.1M** 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。
- 在受保護端點上攔截 **147.2K** 次瀏覽器通知詐騙攻擊／技術支援詐騙攻擊／加密劫持嘗試。
- 在受保護端點上攔截 **7.7K** 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。

2025/09/04

APT28駭客集團推出NotDoor後門程式

LAB52 發現一種被稱為 NotDoor 的全新後門程式，該惡意程式被歸屬於與俄羅斯情報機構有關聯的駭客集團 APT28。NotDoor 透過 Microsoft OneDrive 以 DLL 側載方式傳播，利用 Outlook VBA 巨集監控電子郵件中的觸發字詞，進而實現指令執行、資料竊取及檔案上傳功能。該後門透過修改登錄檔維持持久性／常駐，並採用混淆技術與自訂字串編碼，凸顯 APT28 針對北約成員國不斷進化的攻擊手法。

網路知識：LAB52 是西班牙網路安全公司 S2 Grupo 威脅情報部門，它專門從事針對各種組織的網路威脅情報分析和報告。

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-Enc!g1
- ACM.Ps-Http!g2
- 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
- Trojan.Gen.NPE

2025/09/04

印尼語版本的「Agent Tesla」攻擊行動鎖定東南亞企業

賽門鐵克發現到一起鎖定東南亞組織的新型「Agent Tesla」攻擊行動，目標涵蓋當地企業及大型跨國公司的區域分支機構。

攻擊者假冒知名印尼餐飲服務公司，發送主題為「Kekeliruan Invoice Pembayaran」(付款發票錯誤) 的惡意垃圾郵件。這封印尼文郵件聲稱付款金額不符，並敦催促收件者財務部門檢視附件檔案。

附件為一個 RAR 壓縮檔 (Invoice Pembayaran.PDF.rar)，內含惡意執行檔 (ssVC.exe)。此執行檔啟動後會釋放並執行 Agent Tesla 程式，該惡意竊密程式能竊取瀏覽器憑證、電子郵件登入資訊及剪貼簿資料，並將資料傳回攻擊者控制的基礎設施。

分析顯示此攻擊行動廣泛鎖定東南亞地區，目標涵蓋當地企業與跨國公司的區域分支機構。受影響產業及總部所在地包括：

- 汽車與製造業--印尼子公司 (日本母公司)
- 食品與消費品--當地生產商與經銷商 (印尼企業)
- 保險與金融服務--印尼及馬來西亞地區分支機構 (總部位於美國與日本)
- 醫療保健與製藥業者--亞洲營運據點 (全球母公司總部位於美國)
- 電信業--馬來西亞 (馬來西亞營運商)
- 工業與能源業--於印尼及歐洲設有營運據點的機構 (總部位於比利時與日本)

本次攻擊中出現的 Agent Tesla 二進位檔展現了橫跨多個 ATT&CK 類別的戰術：

- 執行階段 (TA0002)：運用PowerShell (T1059) 與腳本編寫 (T1064) 執行指令並修改 Windows Defender 設定。
- 特權提升與防禦規避 (TA0004／TA0005)：運用程序注入 (T1055）、混淆與打包 (T1027、T1027.002)、時間戳篡改 (T1070.006)、隱藏視窗 (T1564.003) 及安全工具修改 (T1562、T1562.001)。
- 憑證存取與蒐集 (TA0006／TA0009)：收集儲存的電子郵件憑證 (T1003、T1552、T1552.001)、竊取網頁會話 Cookie(T1539)、蒐集 Thunderbird 資料 (T1114)、擷取螢幕截圖 (T1113) 及收集系統資訊 (T1082)。
- 指令與控制 (TA0011)：利用應用層通訊協定 (T1071) 進行資料外洩與遠端控制。

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

基於行為偵測技術(SONAR)的防護：

- SONAR.Stealer!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。

基於端點偵測與回應(EDR)：

- 賽門鐵克的郵件安全解決方案可以提供這類型攻擊的完整保護，並且電子郵件威脅隔離 (ETI) 技術為我們的客戶提供了更深層的保護。
- 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訊息，請參閱此 GitHub 儲存庫：https://github.com/Symantec/threathunters/tree/main/Trojan/Remcos 。

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：

- MSIL.Packed.19

基於機器學習的防禦技術：

- Heur.AdvML.C

2025/09/04

伊朗駭客組織--Nexus，濫用阿曼外交部郵箱發動的攻擊行動

近期針對阿曼外交部發動的攻擊行動，最初由 ClearSkyhgew 所揭露，隨後 Dream Security 研究人員進一步提供深入分析。這起隱蔽的魚叉式網路釣魚行動，利用遭入侵的外交部郵箱向全球外交網路散佈偽裝成註冊表單的惡意 Word 文件。這些附件內含隱藏的 VBA 巨集程式碼，運用多種進階規避技術：包括將有效酬載從數字 ASCII 編碼解碼、插入延遲以繞過沙箱偵測、將可執行檔偽裝成無害日誌檔案，並透過修改登錄檔與 DNS 實現持久化／常駐。收集到的系統資訊隨後經加密 HTTPS 通道外洩至遠端指令控制伺服器 (C&C)。

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-RgPst!g1
- ACM.Untrst-RgPst!g1
- ACM.Word-CPE!g1
- ACM.Word-RgPst!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh.C!gen2

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：

- Backdoor.Cobalt
- Trojan Horse
- 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

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。

2025/09/03

全新勒索軟體：Jackpot出現

一款被稱為 Jackpot 全新勒索軟體已經出現，其與 MedusaLocker 勒索軟體家族有相關聯，採用雙重勒索策略，結合檔案加密與竊取敏感資料。該勒索軟體具備反虛擬機與反偵錯功能以規避分析，一旦執行，便會在被加密檔案冠上「.jackpot[數字]」的副檔名，同時更改受害者桌面布景並放置名為 READ_NOTE.html 的勒索贖金支付說明文件。該說明文件以公開資料威脅要求付款，提供特定聯絡電子郵件地址，並設定嚴格 72 小時期限，逾期贖金金額將提高。此種技術性規避手段與心理壓力的結合，凸顯勒索軟體戰術持續進化以最大化影響力與贖金收益的趨勢。

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-RgPst!g1
- ACM.Ps-Wbadmin!g1
- ACM.Untrst-RgPst!g1
- ACM.Untrst-RunSys!g1
- ACM.Vss-DlShcp!g1
- ACM.Wbadmin-DlBckp!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.RansomLckbit!g3
- SONAR.Ransom!gen107
- SONAR.SuspLaunch!g18

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.Gen.HC
- Ransom.GlobeImposter
- Ransom.Zombie
- 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!100
- Heur.AdvML.B!200

2025/09/03

MystRodX後門程式

根據 XLab 最新報告，一種名為 MystRodX 新型後門程式已被發現，該程式以 C++ 語言編寫，具備廣泛的功能範圍。其支援檔案管理、通訊埠轉發、反向殼層存取及 socket 管理，同時內嵌反偵錯與反虛擬機技術以規避安全分析。與傳統後門程式不同，MystRodX 以隱蔽性與靈活性著稱，能依據配置動態啟用或停用功能。其靈活特性包含：可選擇透過 TCP 或 HTTP 通訊，並能決定以明文傳輸資料或採用 AES 加密傳輸。

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：

- Linux.Mirai
- Trojan Horse
- Trojan.Gen.NPE

2025/09/02

Masslogger涉入的郵件攻擊鏈已從直接附加檔案轉換為Discord CDN網址

Masslogger 是一款自 2020 年起開始活躍的惡意竊密軟體，至今仍位居最普遍威脅之列。其設計目的在竊取儲存於瀏覽器、電子郵件用戶端及通訊應用程式中的憑證資訊。一旦執行，該惡意軟體可透過 FTP／SMTP 協議竊取資料，並利用 Telegram 機器人與攻擊者控制的基礎設施進行通訊。多年來，其後繼版本不斷演進，並且採用不同層級的混淆與規避策略。

近幾週觀察到，某個攻擊者正利用惡意 64 位元 PEDLL 執行多起惡意垃圾郵件行動，藉此部署 Masslogger 木馬程式。活動初期主要透過電子郵件直接傳送壓縮檔附件，但該攻擊者已轉而利用 Discord CDN 等合法託管服務，企圖規避郵件檢測機制。

近期攻擊行動範例：

- 攻擊鏈：電子郵件 → 網址 (Discord CDN) → ZIP 檔案 → PEDLL (64 位元可執行檔)
- 主旨：Bank Transfer Ft 56-57-58
- 寄件者：冒用香港食品進出口企業名義
- 連結：hxxps[:]//cdn[.]discordapp[.]com/.../proof_of_payment[.]zip

整體而言，該攻擊者在攻擊行動中冒充物流公司、工程公司、政府機關、媒體機構、消費品牌、金融機構及科技供應商。惡意電子郵件常偽裝成貨運通知、採購訂單、緊急查詢或付款確認函。

常見的主旨包括：

- Urgent Order* 緊急訂單
- DHL Express Shipment Notification* DHL快遞貨件通知
- PO# 202556* 採購單號202556
- AB_PO 01-LEZ-2025
- Shipment Notification--EPP* 貨件通知
- New Order* 新訂單
- Urgent Inquiry* 緊急查詢

對這些攻擊行動的分析顯示，其攻擊目標涵蓋廣泛的產業與地域，包括：

- 產業領域：金融與銀行、物流、能源、媒體、政府、製造、科技、消費品及旅遊業。
- 地區：歐洲 (英國、芬蘭、比利時、奧地利、德國、西班牙、瑞士)、中東 (黎巴嫩、以色列、沙烏地阿拉伯)、北美、亞洲 (日本、印度、香港)及非洲 (南非、馬爾地夫、波札那)。

此類廣泛鎖定目標的行為凸顯了攻擊行動的投機性質，其目標涵蓋企業與政府機構。

觀察到的攻擊行動廣泛運用混淆技術、程序注入及偽裝手法以規避偵測。MITRE ATT&CK 框架對應的攻擊階段包含：憑證存取 (T1003、T1552)、防禦規避 (T1027、T1564)、持久化 (T1547) 以及資料竊取 (T1045、T1041 對應項目)。

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

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.Gen.MBT

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。

2025/09/02

Desolator勒索軟體

Desolator勒索軟體集團 (也稱為Desolated Collective) 是近期在真實網路情境裡發現到相對較新的勒索軟體集團。據稱受害者包括拉丁美洲與南歐的建築工程公司，以及東南亞的一家科技與軟體開發商。

成功執行後，被加密檔案將被冠上 .desolated 的副檔名，並在多個目錄中放置勒索贖金支付說明文字檔 (RecoverYourFiles.txt)。該說明強調攻擊者與政治或國家組織無關聯，宣稱其動機純粹是為了金錢利益。受害者被要求在 48 小時內透過 Session Messenger 聯繫攻擊者，否則將永久失去一次性解密金鑰。該集團聲稱會提供可解密的能力證明，示範解密一個小於 100MB 的非敏感檔案。

與 Desolator 相關的勒索軟體二進位檔展現了混淆、持久化與影響技術的融合，其行為模式符合現代勒索軟體家族的特徵。

- 執行與持久化：運用命令列譯器 (T1059)、Run key 與 Winlogon 登錄檔進行持久化機制 (T1547.001、T1547.004)
- 防禦規避：堆疊字串混淆、透過XOR加密配置檔 (T1027)、偽裝二進位檔 (T1036)
- 影響範圍：檔案加密 (T1486)、刪除陰影副本與備份目錄 (T1490)、選擇性資料破壞 (T1485)
- 偵測與憑證存取：系統及網路共用清單列舉 (T1083、T1135)、瀏覽器資料擷取、登錄檔查詢

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.Ransomware!g6
- SONAR.SuspWrite!g6

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

基於機器學習的防禦技術：

- Heur.AdvML.C

2025/09/02
防護亮點：守護關鍵基礎設施--為何傳統系統仍然很重要

現代資訊科技 (IT) 不可或缺的隱形骨幹

在雲端原生應用程式、容器化工作負載與 AI 分析工具主導當今 IT 的焦點技術背後，存在著更為低調卻同樣關鍵的基礎架構：UNIX 與 Windows 這類傳統的企業系統。實際上從金融、醫療到製造業及政府部門，這些系統始終是經營運作的核心樞紐。它們承載核心銀行應用程式、管理醫療資料、交易處理系統、儲存戶籍謄本等公民個人資料--這些功能絕非能輕易在一夜之間就宣告終止支援。

事實上，儘管科技創新一路往前飛奔，大型企業仍高度依賴傳統的 Windows 與 Unix 系統來確保穩定性、合規性與可靠性。保護這些系統不僅關乎回溯相容性，更是守護企業營運基礎架構的關鍵所在。

為何傳統系統依舊持續在關鍵性任務有關的重要系統扮演重要角色

- 核心業務工作負載：銀行系統仍仰賴大型主機與 Unix 交易處理器執行高吞吐量、低延遲作業。航空公司透過過去數十年來通過高韌性考驗的傳統系統來調度機隊。
- 合規完善度與監管：醫療與金融產業面臨嚴格規範。傳統系統常儲存稽核與合規所需的病歷紀錄或交易檔案。
- 經長久驗證過的企業擴展成長所需之可靠性：傳統 Unix 系統專注於穩定性與業務持續正常運作時間 (Uptime) 的優化。對許多跨國企業而言，使用三十年的核心系統仍比全新的雲端原生應用程式更值得信賴。

這些平台不僅未退流行，反而已轉化為值得傳承的資產--而非負債。

系統終止支援的挑戰：刻不容緩的漏洞危機

隨著 Windows Server 2012 等傳統平台進入終止支援 (EOL) 的現實階段，企業面臨嚴峻挑戰：供應商不再發布修補程式，官方支援全面終止。然而，由於極度依賴這些系統，不得讓許多具漏洞風險的系統仍持續運作於生產環境中。

這幾年的重大資安事件的前車之鑑歷歷在目，沒有加裝任何保護措施的已終止支援系統總是成為首要的攻擊目標：

- WannaCry (2017年) 利用未修補漏洞的 Windows Server 2003/2008 系統，導致全球醫療與物流業的癱瘓。
- BlueKeep (2019年) 使數百萬未修補的 Windows Server 2008 及 XP 系統暴露於遠端程式碼執行風險。
- PrintNightmare (2021年) 凸顯 Windows 環境中長期存在的元件仍具高度吸引力。

若缺乏主動式防護機制，無論是傳統的 Unix 或 Windows 伺服器，皆會成為勒索軟體、內部威脅及進階持續性攻擊者建立一個擴大的攻擊面。

產業趨勢帶來全新的緊迫感

- 混合IT的現實：80% 企業表示關鍵工作負載仍分散於雲端、Unix 及傳統基礎架構。
- 勒索軟體激增：攻擊者鎖定生命週期終止與未修補系統，因防禦方可選擇的安全防禦方案有限。
- 使用生命週期被迫延長：經濟環境與整合複雜性常迫使企業將傳統系統使用期限大幅延展至原廠官方支援時限之外。
- 數位轉型壓力：企業必須在不中斷關鍵業務的前提下推動現代化--要在這兩種對立的想法之間取得微妙平衡，會是一大挑戰，其中保護傳統資產更是不可妥協的底線。

DCS：不止於為老舊作業系統打造的防禦解決方案

賽門鐵克重要主機防護系統：DCS～Data Center Security 專為保護 Unix、Linux 及傳統 Windows 系統抵禦現代威脅而設計。有別於高度依賴特徵檔或修補週期的被動式工具，DCS 提供主動式策略防護機制，強化關鍵伺服器韌性，使其能抵禦零時差攻擊、內部人員威脅及勒索軟體攻擊。

重要功能

- 強制最小權限原則：即使 root 使用者亦受限於被核准的動作，降低內部人員濫用風險並防範權限提升攻擊。
- 微分段技術：將應用程式與伺服器分組至安全容器中，阻斷橫向移動並在攻擊者擴散前隔離受感染系統。
- 系統強化與持續監控：DCS 持續監控虛擬與實體伺服器，提供即時合規性檢查並鎖定易受攻擊的設定。
- 零時差漏洞防護：透過應用程式隔離與白名單機制，DCS 可阻斷未授權程序，並在修補程式發布前即保護記憶體免受緩衝區溢位、遠端程式碼執行攻擊及應用程式漏洞侵襲。
- 入侵防護系統 (IPS) 與檔案完整性監控 (FIM)：預建的 Unix 基準政策 (Unix baseline policies) 監控特權指令、系統強化狀態、登入活動及檔案完整性，即時偵測異常行為。
- 針對 Unix 特定威脅的防禦機制：從類似 Shellshock 的 Bash 漏洞到 Linux.Gomir 後門程式，DCS 可阻止惡意程式碼執行，強制對敏感設定實施唯讀保護，並將變更行為與核准的管理流程綁定。
- 網路流量控制：精細可微調的政策可精準限制未受信任之連線、縮小攻擊面，並將通訊範圍限制於已知且經授權的系統。
- 威脅情報整合：透過整合賽門鐵克的全球威脅情報與機器學習技術，DCS 能阻擋針對 Linux／Unix 系統的新型惡意軟體家族，防止惡意程式建立持續機制及指揮與控制通訊。

成功案例

- 穩定是金融服務的基石：全球前五大銀行持續透過逾二十年歷史的 Unix 伺服器處理每日數百萬筆交易。將這些工作負載遷移至雲端不僅成本高昂，更伴隨營運風險。透過部署 DCS，該銀行達成：
  - 即時防堵未修補漏洞。
  - 資安事件應變處理時間縮短 45%。
  - 實現混合 IT 環境的持續合規性報告。
- 守護醫療基礎設施：某大型醫療機構運用 DCS 對仍運行但生命週期已終止的 Windows Server 上

關鍵醫療系統實施唯讀保護。此舉在不中斷重要服務的前提下，有效阻止勒索軟體篡改病患資料，並確保符合 HIPAA 規範。

保護過去，確保未來

企業絕不能將傳統系統視為過時的遺物。它們是是活生生、會呼吸的資產--全球營運的支柱。保護這些資產不是可有可無的選項，而是面對勒索軟體、監管壓力與數位轉型時，企業韌性的核心所在。

透過 DCS 解決方案，組織能延長最值得信賴系統的安全與合規生命週期，確保舊系統不再成為負擔，而是堅不可摧的堡壘。

關於賽門鐵克的重要主機防護系統：DCS～Data Center Security 的完整資訊可點擊網頁說明或最新簡報檔。網頁或簡報如有說明不夠清楚的地方，歡迎與保安資訊的業務或技術顧問提供建議。

2025/09/02

TinkyWinkey鍵盤側錄程式

外部威脅態勢管理平台公司 Cyfirma 分析發現一款名為 TinkyWinkey 的全新 Windows 鍵盤側錄程式，該程式透過服務型的持久化模型與受信任程序中的 DLL 注入技術，在持續監控的同時規避偵測。此惡意軟體不僅執行系統剖析，更運用低階鍵盤掛鉤技術擷取全面性的按鍵輸入，涵蓋特殊按鍵及跨多語言佈局的 Unicode 字元。

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：

- PUA.Gen.2
- 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!100
- Heur.AdvML.B!200

2025/09/02

北韓駭客組織：Vedalia* 維達利亞發動名為「Operation HanKook Phantom」的間諜擴大行動

稱為「Operation HanKook* 韓泰 Phantom」的間諜行動，據稱由北韓威脅行為者 Vedalia(亦稱 APT37、ScarCruft) 策劃，據資安公司 Seqrite 通報，它正鎖定南韓學術與研究機構。攻擊者透過魚叉式網路釣魚郵件誘騙受害者，郵件偽裝成新聞通訊主題，並附帶惡意 .LNK 捷徑檔附件。載入程式執行後，將啟動多階段感染鏈：透過無檔案 PowerShell、反射式 DLL 注入及 XOR 加密記憶體執行技術，解密並啟動 RokRAT 遠端存取木馬。該惡意軟體具備系統指紋識別、虛擬機器規避、螢幕擷取功能，並能透過 Dropbox、pCloud、Yandex 及 Google Drive 等合法雲端服務傳送竊取的資料。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.Powershell!g20

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.Mallnk!gen13
- Scr.Mallnk!gen20
- Trojan Horse
- Trojan.Gen.NPE

2025/08/29

流行也是詐騙的幫兇～遠端桌面軟體ScreenConnect以AI主題的影片為誘餌被安裝用於佈署後續的Xworm 遠端存取木馬程式

近期發現到一起利用人工智慧主題為誘餌的攻擊行動，誘騙受害者下載偽裝成影片檔案且具有數位簽章的遠端桌面軟體 ScreenConnect 安裝程式。執行後，該安裝程式會秘密建立隱藏遠端連線並啟動多階段感染鏈。攻擊鏈中，.BAT的批次腳本會從 GitHub 擷取混淆的 Python 有效酬載，繼而透過程序注入與空洞化技術部署 Xworm 遠端存取木馬 (RAT)。該惡意軟體在隱藏的桌面會話中運行，並透過修改登錄檔取得常駐能力，讓攻擊者能夠長期遠端控制與憑證竊取。

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-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 Horse
- Trojan.Gen.MBT

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: Remote Access Tool ScreenConnect Activity

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。

2025/08/29

方便不等於隨便～安卓手機行動裝置平台上的SpyNote遠端存取木馬正透過偽造的 Play 商店網站傳播

一起新型攻擊行動正透過偽裝成 Google Play 商店頁面的欺騙性網站散佈安卓手機行動裝置平台上的 SpyNote 遠端存取木馬 (RAT)，誘騙用戶安裝具有注入功能的 .APK 獨立安裝檔。安裝後，注入程式會使用從套件名稱衍生的 AES 金鑰解密內嵌有效酬載，並運用 DEX 元件注入技術在執行階段植入惡意程式碼，進而規避靜態分析。攻擊鏈最終部署出功能完整的 SpyNote 惡意程式，具備遠端監控、竊取資料及裝置控制能力，包含鍵盤記錄、麥克風／相機存取權限，以及濫用輔助服務 (Accessibility Services)。為躲避偵測，近期樣本採用控制流混淆、動態 DEX 載入技術，並透過 WebSocket 網路通訊協定且使用輪替網域的 C&C 伺服器進行效率、即時的通訊。

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：

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
- Andriod.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**。