
# 保安資訊--本周(台灣時間2025/08/15)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 33 萬 5,500 台受保護端點上總共阻止了 4,590 萬次攻擊。這些攻擊中有 81% 在感染階段前就被有效阻止：**(2025/08/11)**

- 在**7萬1,700**台端點上，阻止了**1,870**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**7萬2,600**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**2萬1,100**台**Windows**伺服主機上，阻止了**560**萬次攻擊。
- 在**4萬2,300**台端點上，阻止了**140**萬次嘗試掃描伺服器漏洞。
- 在**64萬3,600**台端點上，阻止了**92**萬次嘗試掃描在**CMS**漏洞。
- 在**4萬1,900**台端點上，阻止了**160**萬次嘗試利用的應用程式漏洞。
- 在**7萬3,400**台端點上，阻止了**220**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**766**台端點上，阻止了**73萬4,700**次加密貨幣挖礦攻擊。
- 在**9萬5,600**台端點上，阻止了**800**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**539**台端點上，阻止了**7萬6,200**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 3,100 個受保護端點上阻止了總計 1,260 萬次攻擊。**(2025/08/11)**

- 使用網頁信譽情資，在 **272.4K** 個端點上阻止 **11.8M** 次攻擊。
- 攔截 **28.8K** 個端點上 **666.1K** 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 **159.7K** 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 **420** 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。

## 2025/08/14

## 針對日本U-Next網路影音平台使用者的釣魚郵件構成帳戶接管風險

U-Next 是日本的視訊串流平台 (OTT：Over The Top，透過網際網路直接向用戶提供影音內容的技術)。最近，賽門鐵克偵測到針對 U-Next 使用者及其帳戶的網路釣魚活動。散佈的電子郵件冒充 U-Next 客服，傳送假冒的帳戶使用通知，並誘導收件者點擊確認連結以進行帳戶驗證。該連結會將用戶重導向至一個偽造的登入頁面，目的是竊取他們的憑證。一旦入侵，攻擊者便可存取受害者的 U-Next 帳戶。 電子郵件標題：

- 【U-NEXT】ご利用状況のご確認をお願いします
- 翻譯：【UU-NEXT】請檢查您的使用狀況

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。

## 2025/08/14

## 在真實網路情境上發現Linux平台出現FireWood惡意軟體新變種

一個被稱為 FireWood 的 Linux 平台上的惡意軟體新變種正在真實網路情境上出現。此惡意軟體與 Project Wood 惡意軟體家族有關，並歸屬於 Gelsemium APT 駭客集團。FireWood 後門具有收集受感染機器的資訊、滲透敏感資料以及執行從攻擊者接收的大量命令的功能。新變種的功能與舊版 Firewood 病毒相同，但新版本作了多項配置和執行變更。

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
- Trojan.Gen.NPE
- 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。

---

## 2025/08/14

## 老舊漏洞不補成為駭客的最愛～CVE-2017-11882 漏洞仍會導致惡意感染

CVE-2017-11882 是一個 7、8 年前的陳年老漏洞，會影響 Microsoft Office 中的方程式編輯器元件。如果成功開採濫用此漏洞，攻擊者可能會在目標系統上執行遠端程式碼。雖然該漏洞已存在 8 年之久，但仍會定期觀察到利用該漏洞的新嘗試。本週利用 CVE-2017-11882 漏洞的惡意 Excel Macro-enabled Open XML Add-in 檔案 (.XLAM)，出現新的廣泛散佈。感染鏈會將帶有 .xlam 附件的惡意垃圾郵件發送給受害者，並最終導致感染 VIPKeyLogger 惡意竊密程式。在發現到的惡意垃圾郵件中，附件檔名一些範例如下：

- Purchase order(P.O_T4787074)Kronospan ApS.xlam
- urchase order(P.O_T4787074)Kronospan ApS.xlam
- Nuevo pedido El Corte Inglés 08122025.xlam
- SPARKASSE MPP_1108721468-3107.xlam
- NEW PO .xlam
- Order_05271_Lamela.xlam
- NDue Outstanding .xlam

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。

**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：**

- Bloodhound.RTF.12
- Bloodhound.RTF.20
- Exp.CVE-2017-11882!g2
- Exp.CVE-2017-11882!g3
- Exp.CVE-2017-11882!g5
- MSIL.Packed.19
- Scr.Malcode!gdn34
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Mdropper
- Trojan.SnakeKeylogger
- Scr.Malcode!gen3
- WS.Malware.1
- WS.Reputation.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!200
- 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：

- System Infected: Suspicious Executable Download
- Web Attack: Webpulse Bad Reputation Domain Request

**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。

## 2025/08/13

## BytesFromHeaven勒索軟體

全新的勒索軟體 BytesFromHeaven 已經在真實網路情境上出現。該勒索軟體一旦執行後，會加密使用者資料、冠上隨機的副檔名，並變更桌面桌布來顯示攻擊成功。除了檔案加密之外，BytesFromHeaven 還利用 DLL 側載和偽裝成合法的系統二進位檔來隱蔽地滲透系統。它會主動偵測除錯工具和虛擬機器環境、迴避分析，同時建立持久性／常駐並竊取敏感資訊。混淆和資料竄改使偵測更為複雜，並可能透過 Telegram 頻道進行資料外洩。在加密之後，勒索軟體會注入一個以純文字格式的勒索贖金說明，指示受害者存取一個 Tor 的洋蔥網站，以便進一步溝通。攻擊者只要求比特幣付款，讓受害者只能選擇有限的協商方式。

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.Cryptlocker!g36
- SONAR.Ransomware!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.Gen.HC
- Trojan.Gen.MBT
- 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。

## 2025/08/13

## SmartLoader惡意程式濫用 Github 儲存庫大肆散播

據報導，有新一起網路攻擊行動濫用 Github 儲存庫大肆散播 SmartLoader 惡意軟體。這些儲存庫被偽裝成包含自動化工具、DDoS 保護應用程式、軟體破解或遊戲破解的專案。攻擊者利用搜尋引擎最佳化 (SEO) 中毒手法，使其出現在使用者尋找此類軟體工具或解決方案時的最

高優先搜尋結果中。惡意的有效酬載一旦執行，就會收集系統資訊，並開啟一個通往攻擊者控制的 C&C 伺服器的通道，等待進一步的指令。最近觀察到 SmartLoader 涉入的攻擊行動也伴隨 Rhadamanthys 惡意竊密程式的進一步感染。

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.NPE
- 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。

## 2025/08/13

## 新發現散播PS1Bot惡意軟體網路攻擊行動

資安業者 Cisco Talos 研究人員報告一起全新的惡意行動，傳送 PowerShell 型態的惡意軟體，稱為 PS1Bot。攻擊者利用惡意廣告和搜尋引擎最佳化 (SEO) 中毒手法，將惡意程式載器傳送給毫無戒心的受害者。分散式有效酬載具有模組化架構，其特定元件可讓攻擊者收集和滲透各種資料，例如：系統資訊、鍵盤記錄資料、螢幕擷取、儲存在網頁瀏覽器的資料、憑證、cookies、加密貨幣錢包等。竊取的資料會透過 HTTP POST 請求滲透回攻擊者控制的 C&C 伺服器。

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：**

- Downloader

- Infostealer
- Scr.Malcode!gen43
- Spyware.Keylogger
- Trojan Horse
- Trojan.Gen.NPE
- Trojan.Malscript
- WS.Malware.1
- WS.Malware.2
- XSNet.Heur!gen8
- XSNet.Js!gen1

**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: Scripting Host Processes Making Network Connections
- URL Reputation: Webpulse Bad Reputation Domain Request
- Web Attack: Webpulse Bad Reputation Domain Request

**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。

## 2025/08/13
## 防護亮點：Scattered Spider--企業持續面臨的高風險威脅

Scattered Spider 又稱 UNC3944 和 Octo Tempest，是一個以財務為動機的網路犯罪集團，對機構組織構成重大且持續的威脅。該網路犯罪集團在 2023 年 9 月因對知名的大型飯店與遊戲產業機構發動多起引人側目的攻擊事件後，在國際上聲名大噪。在這些事件中，他們利用社交工程技倆入侵 IT 系統，造成營運癱瘓，並據報竊取近 6TB 的資料。

此威脅發動者以其先進的社交工手法而聞名，通常會冒充 IT 服務台人員，誘騙員工洩露憑證或批准遠端存取。這樣他們就可以使用推送炸彈和 SIM 卡交換等技術繞過多因素驗證 (MFA)。一旦進入網路，他們就會展現「就地取材」(LOTL) 技術的強大能力--濫用合法的管理工具而不被發現。他們的作業通常會進行勒索軟體之部署，而且越來越專注於 VMware ESXi 環境。其結果是造成大規模的作業中斷、資料竊取，以及包括零售、運輸和金融等部門的財務損失。

Scattered Spider 涉入的著名資安事件：

- 2023 年 9 月：一家酒店集團面臨運作中斷，影響酒店鑰匙卡和角子機。另一家公司發生涉及客戶資訊的資料外洩事件。該網路犯罪集團冒充服務台人員取得存取權限。據報導，一名受害業者支付約 1,500 萬美元的贖金；另一名受害者則蒙受超過 1 億美元的損失。
- 2023 年 9 月至 10 月：攻擊者使用竊取的憑證入侵客戶支援系統，竊取所有支援用戶的姓名和電子郵件地址，並進一步進行後續攻擊。
- 2023－2024 年第 2 季：一系列憑證網路釣魚攻擊針對 Microsoft Entra ID 和 AWS 等雲端基礎架構。
- 2024 年中：超過 160 個未啟用多重驗證 (MFA) 的組織其雲端資料遭攻擊者透過竊取的憑

證存取。該組織被追蹤為 UNC5537 (與 Scattered Spider 相關聯)，專注於勒索。

- 2025 年 6 月至 7 月：該組織將範圍擴大至多家航空公司和一家零售業者。社交工程和服務台冒充再次被用來入侵身份服務和中斷營運。

**拆解 Scattered Spider 攻擊鏈 V.S. 自適應防護技術如何拆雷**

攻擊通常從有目標式的社交工程電話開始，打到 IT 服務台，假冒員工要求重設密碼和繞過 MFA 保護。一旦進入，Scattered Spider 會遵循一套結構化的攻擊鏈，展現出對企業環境的透徹了解。

- 階段 1 -- 入侵初期 (Initial Access)／身份濫用：使用服務台冒充、MFA 推送炸彈和 SIM 卡交換來取得最高存取權限。雖然 Adaptive Protection 不會直接介入此階段，但是維持良好的帳號安全習慣仍是非常重要。
- 階段 2 -- 持續潛伏(Persistence)／就地取攻擊 (LOTL)：AnyDesk、TeamViewer、Teleport.sh、ScreenConnect 和 Splashtop 等工具被重新使用，以保持持久性並逃避偵測。自適應防護會強制執行拒絕模式政策，在通常不使用這些工具的環境中自動封鎖這些工具。例如：AnyDesk 或 Teleport 可在特定環境的學習期結束後自動封鎖。
- 階段 3 -- 發現 (Discovery) 以及橫向移動 (Lateral Movement)：透過 Mimikatz、PowerShell scripting、PsExec、WMIC 和 AWS CLI 濫用收集憑證的情況都很常見。Adaptive Protection 包括 36 種以上的 PowerShell 行為規則--涵蓋 LSASS 記憶體讀取、程序注入、Base64 編碼混淆、PE 建立等。就連 WMI 和 PsExec 濫用也受到嚴格控制。
- 階段 4 -- 防禦逃脫 (Defense Evasion) 與核心驅動程式濫用：該群組嘗試透過終止安全進程或安裝惡意 DRM 來停用端點防護。該組織試圖透過終止安全進程或安裝如 STONESTOP 等惡意驅動程式來停用端點防護。自適應防護可以阻止未授權的驅動程式安裝或試圖終止受保護服務的嘗試。
- 階段 5 -- 滲出 (Exfiltration) 與衝擊( Impact)：資料透過 Rclone 或 AWS CLI 等工具外洩。如果未經日常操作的驗證，自適應防護會阻止未經信任的雲端上傳工具，例如：MegaSync、Ngrok 和 Rclone。

**Symantec Adaptive Protection(賽門鐵克自適應防護技術)：專門為複雜威脅的行為保護技術**

Scattered Spider 會利用不斷轉變的公用程式、兩用工具和惡意軟體，因此需要能夠在行為層級進行自適應的防護。賽門鐵克自適應防護正是如此--根據攻擊者的行為，而不只是他們使用的工具，來封鎖惡意活動。

舉例來說，Adaptive Protection 會偵測並阻擋 Scattered Spider 作業中部署的惡意軟體家族常見的相關行為。VIDAR Stealer 常常濫用 PowerShell 來啟動 Rundll32 或 WScript、執行 base64 混淆指令，並在已知的持久化／常駐路徑中建立登錄項目。這些行為，以及不受信任的程序中嘗試產生系統層級元件的情況，都會立即被標記並停止。

同樣地，RattyRAT 會透過 PowerShell 修改註冊表機碼來建立持久性而聞名。自適應防護可防止這些與常見持久性技術相關的關鍵位置的註冊表被變更。DragonForceransomware 會嘗試存取 LSASS 記憶體以盜取憑證、修改服務相關的註冊表項，並使用 PowerShell 和 Rundll32 啟動惡意例程，在這種情況下，所有這些行為都會被主動偵測並阻截。Adaptive Protection 還會監控進行持久性相關的註冊表 run 機碼之修改--這是 DragonForce 攻擊中觀察到的另一種策略。

同時，AveMaria (也稱為 WarZone) 經常濫用腳本引擎和 HTML 主機，以逃避防禦並啟動惡

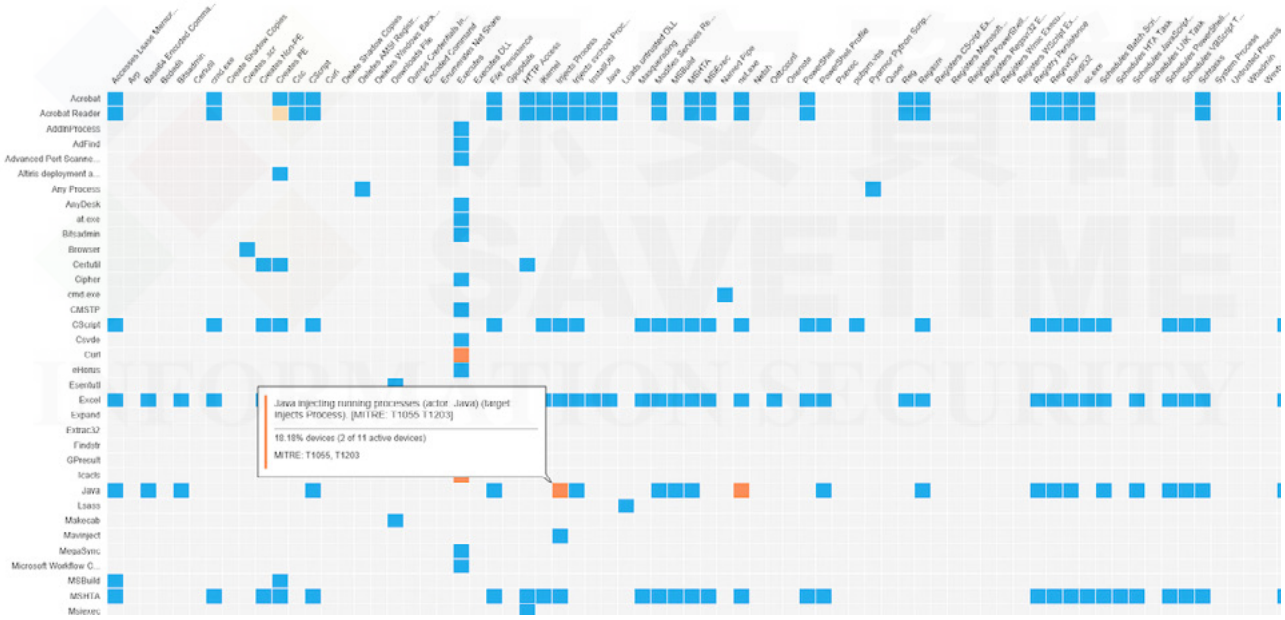
意有效酬載。它使用 mshta.exe 來啟動 PowerShell 或命令列程序，並建立對外 HTTP 連線以進行遠端命令和控制。Adaptive Protection 可偵測這些嘗試，包括透過 HTML 應用 (例如：HTA)、.NET 安裝程式或 WScript 啟動 PowerShell 的情況，並在入侵前阻斷攻擊鏈。

**自適應防護焦點**

- 追蹤的行為：目前有 496 個且跨 69 個應用程式
- 對應：78 項 MITRE ATT&CK 技術
- 受保護的端點：全球超過 290 萬個
- 以拒絕模式封鎖：平均每次部署超過 345 個行為。

賽門鐵克 Adaptive Protection 著重於工具的行為方式，而非僅僅是識別工具，因此可以在不中斷合法業務運作的情況下，同時緩解已知和新型的威脅。想要立即啟用 Adaptive Protection？請參閱此頁面的逐步指南。

Adaptive Protection 現已整合至地端自建的 Symantec Endpoint Protection Manager(SEPM) 管理主控台。透過內建的熱圖視覺化介面，安全團隊可以監控行為的普遍性，並及時採取有根據的決策行動。




請參閱此頁面，了解如何在組織中透過賽門鐵克 Adaptive Protection 最大化降低攻擊面的詳細資訊！對這個功能有興趣的客戶，歡迎與保安資訊聯繫相關導入細節及技術支援。

## 2025/08/12

## Cmimai Stealer惡意竊密軟體

Cmimai 是最近在真實網路情境上發現一種 Visual Basic Script (VBS) 類型的語言全新惡意竊密軟體。該惡意軟體的目標是竊取系統資訊、儲存在系統網路瀏覽器中的資料、cookies、自動填寫資料、憑證等。該惡意軟體以預定的間隔循環執行，每 60 分鐘採集一次新資訊和螢幕截圖。收集到的資料會透過 Discord webhooks 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：

**自適應防護技術(包含於SESC)：**

- ACM.Ps-Wscr!g1
- ACM.Wscr-CNPE!g1
- ACM.Wscr-Ps!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.xSense!gen1
- Scr.xSense!gen3
- Trojan Horse
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- WS.Malware.1
- WS.Malware.2

**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: Scripting Host Processes Making Network Connections
- Audit: System Process Accessing discordapp.com

**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。

## 2025/08/12

## ThrottleStop驅動程式的漏洞被濫用來發動BYOVD攻擊以停用防毒軟體

據報導，巴西發生一場複雜的勒索軟體攻擊，威脅者利用「自帶易受攻擊的驅動程式」(Bring Your Own Vulnerable Driver，BYOVD) 攻擊手法來停用防毒軟體。他們利用 ThrottleStop 驅動程式 (一種合法工具，具有不安全的 IOCTL 介面，允許任意存取記憶體) 的漏洞，搭配惡意的核心模式有效酬載，注入 shellcode、終止安全程序，並部署 MedusaLocker 勒索軟體。

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：

**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.MBT
- Trojan.KillAV
- 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!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。

---

## 2025/08/11

## 新一波針對日本Ticket PIA票務銷售網站用戶的釣魚行動

最近，賽門鐵克發現到針對 Ticket PIA (チケットぴあ) 用戶的網路釣魚活動，該公司是日本最大的活動門票銷售網站之一，提供體育賽事、演唱會和其他娛樂活動的線上和實體票務銷售。該公司透過其網站、行動裝置服務及遍佈全國的實體售票服務據點提供票務服務。威脅者最近發起偽裝成帳戶驗證電子郵件的網路釣魚活動。這些釣魚郵件試圖引誘受害者打開並點擊要求驗證和確認帳戶資訊的釣魚網址。這些電子郵件使用以下主旨：

- 【チケットぴあ】サービス利用継続のためのログインのお願い
- 翻譯：【Ticket Pia】請登入以繼續使用服務

點選電子郵件內的帳戶登入連結，會將使用者重導向到偽造的 Ticket PIA 登入頁面，目的在於竊取憑證。一旦入侵，攻擊者就能存取受害者的 Ticket PIA 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。

---

## 2025/08/11

## Efimer木馬程式以加密錢包為目標

Efimer 木馬程式是一種竊取加密貨幣的惡意軟體，已被發現到透過網路釣魚電子郵件和遭入侵的 WordPress 網站散佈。釣魚誘餌會假冒律師，傳送帶有混淆密碼提示的 ZIP 壓縮檔。執

行時，Windows 腳本檔 (Windows Script File) 指令碼會新增 Windows Defender 排除項目，並透過工作排程或登錄檔的啟動功能部署 JavaScript 類型的木馬。Efimer 會劫持剪貼簿密碼位址、滲透螢幕截圖和加密電子錢包的種子短語 (seed phrase，也稱為恢復短語 (recovery phrase) 或助記詞 (Mnemonic phrase)，並使用 Tor 洋蔥路由加密網路進行 C&C。有些 WordPress 網站會透過假冒的 torrent 連結來託管它，並提供額外的腳本來強制輸入密碼和蒐集電子郵件，以進行大規模的隱匿式擴張。

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
- ACM.Wscr-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。

**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：**

- JS.Redirector
- PUA.Gen.2
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- XSNet.Heur!gen8
- 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：

- Audit: Github Cloud Service Connect Attempt
- Audit: Scripting Host Processes Making Network Connections
- Audit: Suspicious Process Accessing Lets Encrypt Certified Site

**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。

## 2025/08/11

## 下載安裝軟體還是要到原廠～MaaS型態的CastleBot惡意軟體正透過被木馬化的軟體安裝程式散布

CastleBot 是一種透過惡意軟體即服務 (MaaS) 來散佈的惡意軟體，被網路犯罪份子用來傳送惡意有效酬載，其中一個顯著的成果就是勒索軟體。最近一份報告強調 CastleBot 的活動，並將最常見散佈媒介歸屬於被木馬化的軟體安裝程式。成功部署 CastleBot 會導致多個階段，允許收集資訊和傳送進一步的有效酬載。這些階段包括初始下載程式、惡意程式載入器以及最終的後門程式。

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-Rd32!g1
- ACM.Ps-SvcReg!g1
- 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。

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Hacktool.Flooder
- 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
- 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。

## 2025/08/08

## LINE通訊軟體的使用者成為「帳戶接管」釣魚郵件的目標

LINE 在日本是一款廣受歡迎的即時通訊和社交網路應用程式，擁有龐大的使用者群。最近賽門鐵克偵測到針對 LINE 用戶及其帳戶的網路釣魚活動。散佈的電子郵件冒充 LINE 客戶支援，發送假冒的帳戶通知，並要求收件人點擊確認連結，以驗證帳戶詳細資料。該連結會將用戶重導向到一個偽造的登錄頁面，目的是竊取他們的憑證。一旦洩露，攻擊者便可進入受害者的 LINE 帳戶。

電子郵件標題：

- 【重要】lineアカウントの本人確認のお願い
- 翻譯為：【重要】請確認您的 LINE 帳戶身份

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。

---

## 2025/08/08

## 威脅行為者UAC-0099利用惡意HTA檔案進行MatchBoil惡意程式載入器傳送

被稱為 UAC-0099 的威脅組織已被發現到使用惡意 HTA 檔案來傳送 MatchBoil 惡意程式載入器。攻擊者利用含有檔案共享網址 (URL) 的網路釣魚電子郵件，一旦受害者瀏覽這些 URL，就會將其重導向下載惡意 HTA 檔案。受害者執行此檔案後，MatchBoil 惡意程式載入器便會在受感染的端點上啟動惡意活動。此惡意軟體可下載其他任意有效酬載，例如：MATCHWOK 後門或 DRAGSTARE 惡意竊密程式，這兩種程式都是近期 UAC-0099 攻擊行動的一部分。

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.Mshta-CNPE!g1
- ACM.Mshta-CPE!g1
- ACM.Mshta-Http!g1
- ACM.Ps-CPE!g2
- ACM.Ps-Rd32!g1
- ACM.Ps-Mshta!g1
- ACM.Ps-TPs!g1

**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。

**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!gen108
- CL.Downloader!gen203
- Downloader
- ISB.Downloader!gen48
- Scr.Malcode!gen
- Scr.Malcode!gen23
- Scr.Malscript!gen23
- Scr.xSense!gen3
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Web.Reputation.1
- Web.Reputation.3
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.4
- XSNet.Html!gen1

**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。

## 2025/08/08

## Vedalia威脅行為者透過網路釣魚和JPEG隱藏技術部署隱秘的 RoKRAT木馬程式

Vedalia(也稱為 APT37、ScarCruft 或 RedEyes) 是一個與北韓國家有關聯的威脅行為者，透過部署旗下的遠端存取木馬程式 RoKRAT 增強版，持續發展其間諜行動。最近攻擊行動利用嵌入在 ZIP 檔案中的惡意 .lnk 捷徑檔案 (通常透過魚叉式網路釣魚電子郵件傳送)，來執行加密的 shellcode，並將有效酬載直接載入記憶體，經常使用隱匿技術將 RAT 隱藏在合法的 JPEG 影像中。多階段惡意程式載入器會解密並將 RoKRAT 注入受信任的程序，例如：mspaint.exe，以執行無檔案、在記憶體中執行的功能，進而避開傳統的防毒工具。一旦啟動，RoKRAT 會賦予攻擊者完整的遠端控制能力，包括指令執行、資料竊取、螢幕截圖與音訊擷取，以及系統偵察。它還會利用 Dropbox 和 Yandex 等合法雲端平台進行 C&C 通訊和資料滲出。

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：**

- Scr.Mallnk!gen13
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- W32.Beapy
- 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!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。

## 2025/08/08

## Fireant進階持續威脅(APT)駭客組織持續濫用ToneShell後門程式

Fireant 進階持續威脅 (APT) 駭客組織 (又名 Mustang Panda、Earth Preta) 持續使用名為 ToneShell 的後門程式。攻擊者利用 DLL 側載手法在針對政府和軍事組織的攻擊活動中傳送惡意有效酬載。惡意程式在感染後會偽裝成合法的 Google Chrome 程序，並允許攻擊者在受感染的主機上執行各種惡意指令。這些任意動作包括檔案／資料夾操作、登錄修改、建立持久性、執行 shell 指令等。

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
- ACM.Ps-RgPst!g1
- ACM.Ps-Schtsk!g1

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Trojan Horse
- Trojan.Gen.2
- WS.Malware.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**。