保安資訊--本周(台灣時間2025/05/23)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 8,900 台受保護端點上總共阻止了 4,870 萬次攻擊。這些攻擊中有 81.3% 在感染階段前就被有效阻止：**(2025/05/19)**

- 在**8萬1,800**台端點上，阻止了**1,980**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**8萬800**台端點上，阻止了**620**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬2,600**台**Windows**伺服主機上，阻止了**600**萬次攻擊。
- 在**5萬800**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1萬700**台端點上，阻止了**71萬3,800**次嘗試掃描在**CMS**漏洞。
- 在**5萬300**台端點上，阻止了**190**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**140**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,400**台端點上，阻止了**68萬6,700**次加密貨幣挖礦攻擊。
- 在**10萬600**台端點上，阻止了**840**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**552**台端點上，阻止了**8萬1,000**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 16 萬 8,400 個受保護端點上阻止了總計 750 萬次攻擊。**(2025/05/19)**

- 使用網頁信譽情資，在 **162.2K** 個端點上阻止 **720** 萬次攻擊。
- 攔截 **17.6K** 個端點上 **229.9K** 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 **4.9K** 個端點上攔截 **110.5K** 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 **279** 個端點上攔截 **2.3K** 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。

2025/05/22

8年前的漏洞還不進行修補嗎?～駭客組織SideWinder利用舊版Office陳年老漏洞發動攻擊

駭客組織 SideWinder 最近針對孟加拉、巴基斯坦和斯里蘭卡的高知名度政府機構進行網路間諜行動。攻擊者利用魚叉式釣魚誘餌搭配地理圍籬 (知道所在地理位置，然後決定是否觸發) 有效酬載，以確保只有特定國家的受害者才會收到惡意內容。為了啟動感染程序並部署 StealerBot 惡意軟體，需要結合開採濫用陳年老舊漏洞 (CVE-2017-0199(遠端程式攻擊漏洞) 和 CVE-2017-11882(憶體毀損漏洞))。當受害者開啟自訂的 RTF 檔案時，就可以利用這些漏洞透過載入外部內容的惡意 Office 文件執行遠端程式碼，並利用傳統 Equation Editor 中的記憶體損毀漏洞，產生潛在的系統危機。攻擊和漏洞利用的最後階段是部署憑證竊取惡意軟體，用於資料外洩和持續存取／常駐。

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-Sc!g1
- 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：

- Bloodhound.RTF.12
- Bloodhound.RTF.20
- Scr.Malcode!gen
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- Trojan.Mdropper
- Web.Reputation.1
- Web.Reputation.3
- WS.Malware.1
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- 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。

2025/05/22

越方便越不安全：安卓 v.s. IOS～GhostSpy安卓平台(手機)惡意軟體

GhostSpy 是一種安卓平台 (手機) 惡意軟體，最近被發現在真實網路情境裡被大肆散播。與其他流行的行動惡意軟體類似，GhostSpy 利用裝置的輔助服務 (Accessibility Services) 在目標裝置上側載惡意 .apk 套件。感染後，遠端存取木馬程式 (RAT) 可讓攻擊者完全控制受攻擊的裝置、遠端執行指令、鍵盤記錄、錄音／錄影功能等。它還會竊取各種資訊，包括銀行憑證、2FA 認證碼、簡訊內容、通話記錄、聯絡人等。

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：

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
- 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。

2025/05/22

假冒的KeePass安裝程式，涉入鎖定ESXi環境的攻擊中被大肆散佈

KeePass 是一款廣受歡迎的開放原始碼密碼管理應用程式。最近報導指出，有人正在散佈針對 ESXi 環境的偽造 KeePass 安裝程式。該惡意軟體被稱為 KeeLoader，其功能包括從 KeyPass 資料庫收集資料／憑證、啟動任意元件，以及確保在受攻擊的機器上持久存在等。據報導，該攻擊行動已持續數月，攻擊者試圖在受感染的機器上安裝 Cobalt Strike 信標、滲透敏感資料，甚至部署勒索軟體有效酬載。此惡意活動據信與勒索軟體駭客 Black Basta 過去相關的初始存取掮客 (Initial Access Broker-IAB) 有關聯。

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.TCP!gen6

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：

- Backdoor.Cobalt
- Trojan.Dropper
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- 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：

- Audit: Bad Reputation Application Activity
- System Infected: Trojan.Backdoor Activity 634

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。

2025/05/22

CVE-2024-7399 & CVE-2025-4632：存在Samsung 數位顯示器軟體 MagicINFO Server 9存在的嚴重等級漏洞，已被駭客大肆開採濫用

CVE-2024-7399 是存在 Samsung 數位顯示器軟體 MagicINFO Server 9 的未認證遠端程式碼執行 (RCE) 漏洞。此漏洞可讓攻擊者透過未認證的 POST 請求上傳惡意 .jsp 檔案，並有效執行任意的作業系統指令。雖然該漏洞早在 2024 年 8 月就已被披露並修補，但針對該漏洞的詳細說明最近才被發佈。在 PoC 發佈後不久，又有一個新的繞過漏洞 (追蹤為 CVE-2025-4632) 被公開。據報導，這兩個漏洞都在真實網路情境裡已遭開採濫用，成為壯大 Mirai 殭屍網路火力的幫兇。

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: Malicious Java Payload Upload 17
- Web Attack: Malicious Java Payload Upload 19
- Web Attack: Malicious Java Payload Upload 25
- Web Attack: Metasploit JSP Payload
- Web Attack: Samsung MagicINFO CVE-2025-4632

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 預設的防禦規則將阻止任何上傳和執行 webshell(本例中為 jsp)。這主要是透過控制可以寫入檔案的位置，以及可以在 JSP 腳本執行的沙箱上執行哪些指令來達成。
- 預設 Windows 強化政策中的 DCS 網路規則會封鎖與網際網路的連線，因此可降低攻擊面。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2025/05/22

假冒日本電子稅務的偽造電子郵件通知，成為網路釣魚行動的誘餌

E-Tax 是日本國家稅務局的線上稅務網站，可協助企業報稅及繳稅。最近，賽門鐵克發現有人模仿 e-Tax 進行網路釣魚，誘使使用者開啟偽造的通知郵件。該電子郵件提到最近進行的稅務驗證，要求使用者立即註冊並更新所有個人資訊。這些詐騙電郵目的在誘騙使用者點擊釣魚網頁。當受害者點擊電子郵件內容中的釣魚網頁後，就會被騙進入憑證收集網頁。

電子郵件標頭(mail header)：

- 電子郵件主旨：務署からのお知らせ【宛名の登録確認及び秘密の質問等の登録に関するお知らせ】
- 翻譯：機關通知 [關於收件人註冊確認和安全問題註冊等的通知]。

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。

2025/05/21

路邊撿到的槍常常會自炸，使用AI工具務必到原廠網站～惡意廣告引誘受害者瀏覽偽造Kling AI網站

威脅者利用社交媒體惡意廣告引誘受害者進入冒充 Kling AI 平台的偽造網頁。此行動會引誘訪客使用該平台製作 AI 生成高質量的影片和圖片。然而，偽造 Kling AI 網站並未提供使用者所要求的內容，反而提供惡意圖片或影片輸出以供下載，結果發現這是一個偽裝的可執行檔案。當使用者期待預覽偽造 AI 所產生的內容時，最後會啟動惡意軟體載入程式。一旦執行，惡意竊密程式會滲透瀏覽器儲存的憑證、會話權杖和其他敏感資料等。

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-RgPst!g1
- ACM.Untrst-RgPst!g1
- ACM.Untrst-RunSys!g1
- ACM.Untrst-Schtsk!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g5
- SONAR.ProcHijack!g51
- 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：

- Infostealer
- Trojan Horse
- Trojan.Gen.MBT
- W32.Silly!gen
- WS.Malware.1

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。

2025/05/20

防護亮點：賽門鐵克IPS引擎～新增JA3指紋識別技術智取迴避偵測手法的威脅

在現今快速演進的威脅環境中，網路罪犯不斷開發新技術以繞過傳統安全防護的偵測。以定義檔為基礎的偵測雖然仍有價值且需要，但惡意軟體作者可能會利用多樣態、變種和其他混淆方法來逃避偵測。在賽門鐵克，我們致力於透過不斷創新的安全技術來領先這些威脅。因此，我們很高興與您分享，我們先進的入侵防護系統 (IPS) 引擎現已結合 JA3 指紋技術，以提供更卓越的威脅偵測能力。

了解挑戰：真實世界中的迴避偵測手法的威脅

傳統的安全解決方案通常依賴識別已知的惡意程式碼模式或網路特徵。然而，現代惡意軟體的設計經常會改變其外觀和行為，使其很難僅使用這些方法來偵測。這些威脅可能會使用：

- 多樣態：改變程式碼結構以避免與特徵相符。
- 網域產生演算法 (DGA)：動態產生網域名稱以避開黑名單。
- 加密：加密通訊以隱藏惡意流量。

這些規避手法可讓惡意行為者在您的網路中建立據點，並在被偵測到之前造成重大損害。這就是 JA3 指紋技術發揮作用的地方。

JA3：更智慧的端點威脅偵測方法

JA3 是指分析 TLS／SSL(傳輸層安全／安全 Sockets 層) 用戶端和伺服器交握階段 (handshake) 特徵的指紋技術。這些交握是客戶端和伺服器建立安全連線時的初始協商過程。JA3 並非著重於加密通訊的內容，而是分析交握本身的具體細節，例如：

- 支援的 SSL／TLS 版本
- 提供的密碼套件
- 使用的 TLS 擴充套件

這些特性獨特組合為每個用戶端和伺服器建立獨特的指紋。惡意行為者經常在通訊中使用特定的函式庫或預先建立的工具，這會產生一致且可辨識的指紋，可利用這些指紋進行偵測。

JA3 如何增強賽門鐵克的 IPS 引擎

透過將 JA3 指紋識別功能整合至賽門鐵克的端點 IPS 引擎，賽門鐵克安全回應現在可以更有效地：

- 識別使用已知框架的惡意行為者：許多惡意軟體系列和攻擊套件持續使用特定的 TLS／SSL 配置。JA3 可讓 IPS 引擎識別這些模式，即使惡意軟體試圖混淆其程式碼。
- 偵測未知威脅：即使前所未見的特定的惡意軟體，只要它使用與惡意活動相關的 TLS／SSL 配置，IPS 引擎就能將其標示為可疑。
- 減少誤判及漏報：JA3 提供更精確的偵測方法，大幅提升警示的真實度。高精確度可減少誤報 (偽陽性、錯殺率)，同時消除流量偵測中的漏報 (偽陰性、漏網之魚)。

對您的組織的效益

使用 JA3 指紋技術強化賽門鐵克的端點威脅防護，可為您的組織帶來多項好處：

- 主動式防護：在執行前階段偵測並阻擋更多威脅。
- 改善安全態勢：針對複雜的攻擊加強端點防禦。
- 降低風險：將惡意軟體感染的影響降至最低。。

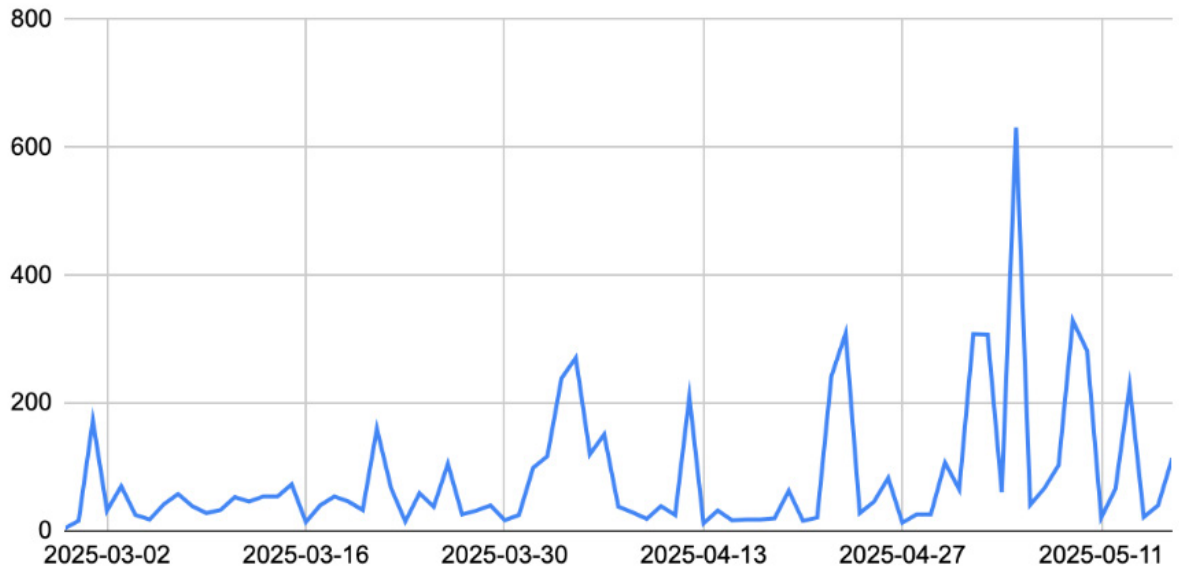
賽門鐵克優勢：由賽門鐵克安全機制應變中心 (Symantec Security Respons) 提供支援

值得注意，賽門鐵克防護技術的威力在於全球賽門鐵克安全機制應變中心團隊的監控與分析。IPS 引擎會根據指紋識別潛在威脅，而我們的專家則會根據最新的威脅情報持續監控和精進這些識別碼，確保端點受到最新威脅的保護。

可用於賽門鐵克雲端沙箱

JA3 指紋識別功能尚未在賽門鐵克產品中可直接設定或報告。不過，賽門鐵克雲端沙箱 (Symantec Cloud Sandbox) 提供此增強的威脅偵測功能。賽門鐵克雲端沙箱是一項後端服務，多項賽門鐵克產品利用這項服務來防禦前所未見新的、進階的、不斷演進的和目標性的攻擊。JA3 指紋偵測方法已證明可有效對抗 Dridex 惡意軟體和 Remcos 遠端存取特洛伊木馬等威脅。報告的偵測趨勢顯示，此功能可補足雲端沙箱的其他技術，增強其日常效能。

賽門鐵克雲端沙箱：基於 JA3 的 IPS 檢測事件



賽門鐵克堅定不移的承諾

在賽門鐵克 IPS 引擎中整合 JA3 指紋識別技術，代表我們在偵測和封鎖迴偵測手法威脅的能力上，向前邁進一大步。透過專注於 TLS／SSL 交握的基本特徵，我們可以識別惡意的行為者和模式，否則可能會被忽略。這項增強功能進一步鞏固賽門鐵克為客戶提供全面、主動安全解決方案的承諾。

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。
讓網路威脅未攻先破－－賽門鐵克的 IPS 入侵預防技術
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。

2025/05/20

Bumblebee惡意程式載入器，附身在熱門工具軟體的安裝程式被大肆傳播

最近發現熱門的第三方 IT 管理工具：RVTools 應用程式的安裝套件被植入 Bumblebee 惡意程式載入器的動態連結程式庫 (DLL)。RVTools 是免費公用程式，可收集並顯示 VMware 環境中與虛擬機器相關的大量資訊。該木馬化安裝程式在被取代之前，曾短暫以官方下載的方式被代管。惡意的 Bumblebee dll 會嘗試連線到各種看似隨機的 .life 網域，以執行下一階段的攻擊。

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.Bumblebee
- 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。

2025/05/19

俄烏衝突也能成為假冒幣安(Binance)加密貨幣交易所網路釣魚的素材

幣安 (Binance) 是全球主要的加密貨幣交易所之一，允許使用者購買、出售和交易各種數位資產，包括比特幣、以太坊和另類非比特幣 (Altcoins)。最近，賽門鐵克觀察到假冒 Binance 服務的網路釣魚活動，並誘使使用者開啟偽造的通知郵件。電子郵件正文內容提到，使用者需要將任何外部錢包 (如果有) 連結並更新至 Binance 帳戶，以此作為一種保護。釣魚郵件的內容指出，正在進行的俄羅斯--烏克蘭衝突是嚴重影響加密貨幣市場的因素之一。正文內容也提到最近的資料外洩事件。用戶會收到一個偽裝成「連接錢包」連結的釣魚網址連結--企圖引誘用戶打開並點擊旨在竊取憑證的釣魚網址連結。

電子郵件標頭(mail header)：

- 電子郵件主旨：【Binance】連結您的外部錢包，保護您的資產。
- 電子郵件寄件者：「Binance」<經偽造的郵件地址>

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。

Symantec
A Division of Broadcom

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。

保安資訊
KEEPSAFE
INFORMATION SECURITY

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**。