保安資訊--本周(台灣時間2025/07/25)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 1,500 台受保護端點上總共阻止了 4,930 萬次攻擊。這些攻擊中有 81.5% 在感染階段前就被有效阻止：**(2025/07/21)**

- 在**7萬6,200**台端點上，阻止了**2,000**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**7萬600**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**2萬2,100**台**Windows**伺服主機上，阻止了**600**萬次攻擊。
- 在**4萬7,200**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1萬2,500**台端點上，阻止了**83萬3,800**次嘗試掃描在**CMS**漏洞。
- 在**4萬1,400**台端點上，阻止了**180**萬次嘗試利用的應用程式漏洞。
- 在**6萬600**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**73萬5,700**次加密貨幣挖礦攻擊。
- 在**10萬4,600**台端點上，阻止了**840**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**418**台端點上，阻止了**7萬2,700**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 3,700 個受保護端點上阻止了總計 1,260 萬次攻擊。**(2025/07/21)**

- 使用網頁信譽情資，在 **273.7K** 個端點上阻止 **12M** 次攻擊。
- 攔截 **27.4K** 個端點上 **378.7K** 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 **7.1K** 個端點上攔截 **172.6K** 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 **385** 個端點上攔截 **17.2K** 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。

2025/07/24

全新Chaos勒索軟體即服務集團以激進的手段現身

一個新發現的勒索軟體即服務 (ransomware-as-a-service) 勒索軟體集團：Chaos 已迅速壯大，主要在美國發動雙重勒索攻擊，另外在英國、印度和紐西蘭也有受害者。Cisco Talos 根據重疊的手法和工具，將該組織與前 BlackSuit(Royal) 營運商聯結起來。Chaos 採用語音網路釣魚進行初始存取，濫用遠端管理工具進行持續存取，並使用快速、選擇性的加密方法來癱瘓網路。該組織避開金磚國家 (BRICS)／獨立國協 (CIS) 等目標，並設置資料洩漏網站，向未付款的受害者施壓，勒索高達 300,000 美元的贖金。儘管名稱如此，這個 Chaos 勒索軟體集團與早期的 Chaos 勒索軟體毫無關係，故意製造混亂以阻礙偵測和歸屬判定。

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.B

2025/07/24

惡意的韓語文字處理器文件檔，傳播RokRAT惡意軟體

一改以往的散佈方式，RokRAT 惡意軟體最近透過韓語文字處理器文件 (.hwp)，而非之前觀察到的惡意 .LNK 捷徑檔散佈。HWP 文件包含一個合法的可執行檔和一個惡意的 DLL，負責初始有效酬載的執行。執行時，可執行檔會側載 DLL，並嘗試從內容託管商 (Dropbox) 下載影像檔案。在此範例中，影像檔案包含負責將 RokRAT 直接載入記憶體的 shellcode。一旦成功入侵，攻擊者便可控制系統，進而實現資料外洩或遠端程式碼執行等行為。

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
- WS.Malware.1
- 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。

2025/07/24

中國進階持續威脅(APT)駭客集團加劇對台灣半導體產業的攻擊

台灣半導體產業已成為由三個不同的中國國家支持的威脅團體所策劃的一系列精密魚叉式網路釣魚活動的主要目標：UNK_FistBump、UNK_DropPitch 和 UNK_SparkyCarp。這些威脅團體的目標是滲透整個半導體供應鏈中的組織，包括製造、設計、測試、設備供應商，甚至是專門從事該產業的財務分析師。他們採用以人才招募為主題的網路釣魚策略，發送偽造的工作申請要求電子郵件。這些電子郵件包含偽裝成 PDF 履歷的惡意 .LNK 捷徑檔。

檔案開啟後，會啟動多階段的攻擊程序，以部署 Cobalt Strike 或自訂的 C-based 後門 Voldemort。為了轉移懷疑，受害者會同時看到一份誘餌文件。另外，有些網路釣魚電子郵件包含 PDF 文件的連結，在存取時會下載包含惡意 DLL 的 ZIP 檔案。該 DLL 隨後會透過 DLL 側載執行，使其能以名為 HealthKick 的後門運作。攻擊者透過社交工程手法取得存取權限，或濫用漏洞竊取資料，以進行日後針對其他政府單位和重要基礎設施進行網路間諜行動。

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.Ps-Http!g2
- ACM.Ps-Wscr!g1
- ACM.Ps-Rd32!g1
- ACM.Rd32-Schtsk!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.Cryptlk.AN!g2

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
- Hacktool.Flooder
- Scr.Malcode!gen*
- Scr.Mallnk!gen*
- Scr.xSense!gen*
- Trojan Horse;
- 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.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。

2025/07/23

UNG0002威脅組織近期所涉入的的惡意活動

一個被稱為「Operation AmberMist」的全新惡意活動群組被歸屬於名為 UNG0002 的威脅組織。攻擊者集中攻擊各行各業的受害者，並散佈各種有效酬載，包括 Shadow RAT、Blister DLL Implant 和 INET RAT。多階段攻擊鏈利用惡意 .LNK 捷徑檔、VBScript 以及 PowerShell 指令碼檔案，特別針對東南亞地區進行攻擊。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!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。

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：

- Downloader
- Scr.Mallnk!gen3
- Scr.xSense!gen1
- Scr.xSense!gen10
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Mallnk
- Web.Reputation.1
- Web.Reputation.2
- WS.Malware.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!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。

2025/07/23

由Seedworm進階持續威脅(APT)駭客集團散佈的DCHSpy惡意軟體

據報導，一個散佈行動 DCHSpy 監控惡意軟體的全新網路攻擊行動，已在真實網路情境上展開。此網路攻擊行動是由 Seedworm 進階持續威脅 (APT) 駭客集團 (也稱為 MuddyWater) 所為。DCHSpy 具備從受攻擊裝置收集和滲出各種資料的功能，包括：儲存的聯絡人、簡訊內容、本機檔案、通話記錄、WhatsApp Messenger 資料等。該惡意軟體還具有其他功能，允許攻擊者使用裝置內建的相機和麥克風拍攝照片或錄製音訊。Seedworm會將惡意的二進位檔案偽裝成不同名稱之 VPN 應用程式 (例如：Earth VPN、Hide VPN、Comodo VPN 或 Starlink VPN)，散播給不知情的使用者。

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。

- AdLibrary:Generisk
- 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。

2025/07/23

Greedy Sponge威脅組織向墨西哥組織散佈AllaKore RAT和SystemBC惡意軟體

據報導，一個名為「Greedy Sponge」的以財務為動機的威脅組織發動一項新的攻擊行動，向墨西哥組織散佈 AllaKore RAT 和 SystemBC 惡意軟體。為了部署這些惡意有效酬載，攻擊者利用被執入後門的微軟軟體安裝檔 (.MSI)，內含 .NET 類型的惡意下載程式。攻擊者可利用散佈的有效酬載執行各式各樣的惡意活動，包括鍵盤側錄、資訊竊取、遠端控制受攻擊的端點或任意檔案操作等等。

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.Untrst-RunSys!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。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.ASync
- Downloader
- Infostealer.Bancos
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- 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
- 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：

- Audit: Bad Reputation Application Activity
- System Infected: Trojan.Backdoor Activity 638
- URL Reputation: 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。

2025/07/23

新版ACR Stealer惡意竊密程式，具有更新防禦規避偵測伎倆的功能

ACR Stealer 惡意竊密程式是採用 C++ 撰寫的惡意竊密程式家族，去年出現在網路威脅生態圈。據報導，在真實網路情境裡，已有新的網路攻擊行動散佈此惡意軟體。傳播中的惡意竊密程式在偵測和鑑識分析迴避方面進行多次更新。其中一種使用的技術是 Heaven's Gate，它允許攻擊者從看似無害的 32 位元程序中呼叫惡意的 64 位元程式碼。在功能方面，新版的 ACR Stealer 與舊版並無差異，目標是收集和滲出各種敏感資料，包括系統資訊、憑證、瀏覽器 cookies、第三方應用程式的設定檔、加密貨幣錢包等。

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.Untrst-RunSys!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.Gen.2
- Trojan.Gen.MBT
- 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

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
- URL Reputation: 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。

2025/07/22

防護亮點：有效應對防禦規避的攻擊手法，Carbon Black EDR(端點偵測與回應)神通廣大

現代網路安全解決方案是利用先進、多層次的技術來對抗不斷演變的威脅。然而，攻擊方會不斷改良其技術以混入企業環境，利用看似合法的行為來逃避偵測。2025 年 6 月，VMware Carbon Black EDR(端點偵測與回應) 偵測到採用防禦規避的網路攻擊行動激增，讓客戶能夠迅速回應並降低威脅。本公告重點介紹所觀察到的趨勢和駭客所使用的技倆，以及 Carbon Black 如何協助瓦解這些趨勢和技倆。

Carbon Black EDR(端點偵測與回應)

Carbon Black EDR(端點偵測與回應) 透過雲端原生平台提供進階的端點偵測與回應功能，該平台整合行為分析與端點活動的可視性。它使用單一輕量級代理程式和統一主控台簡化防護和回應。

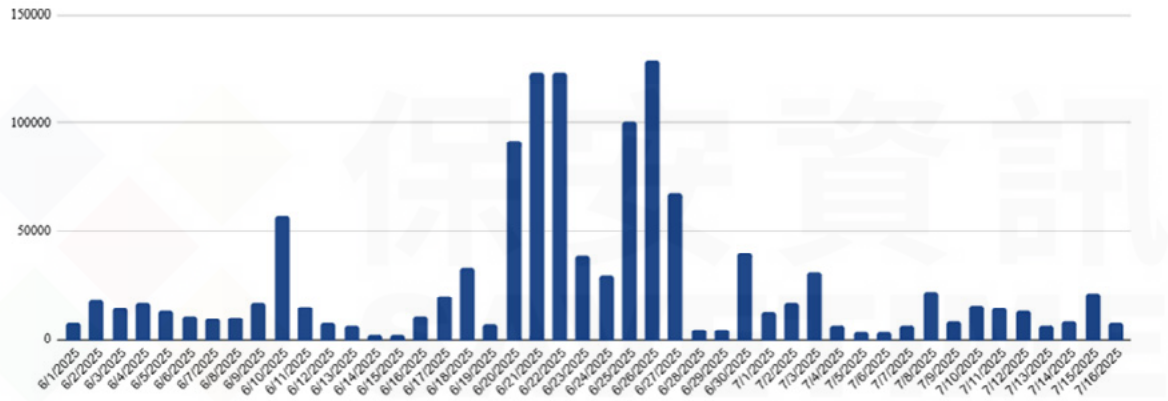
主要功能包括

- 阻止已知和未知的惡意軟體、勒索軟體和就地取材 (LotL) 攻擊
- 運用檔案信譽、啟發式技術、機器學習和行為模型
- 提供開箱即用的防禦政策與客製化選項
- 提供攻擊鏈的完整可見性，以便進行快速調查
- 啟用遠端 shell 存取功能以進行即時回應
- 利用監視清單(Watchlists)進行持續的威脅攔截與警示

偵測到的趨勢

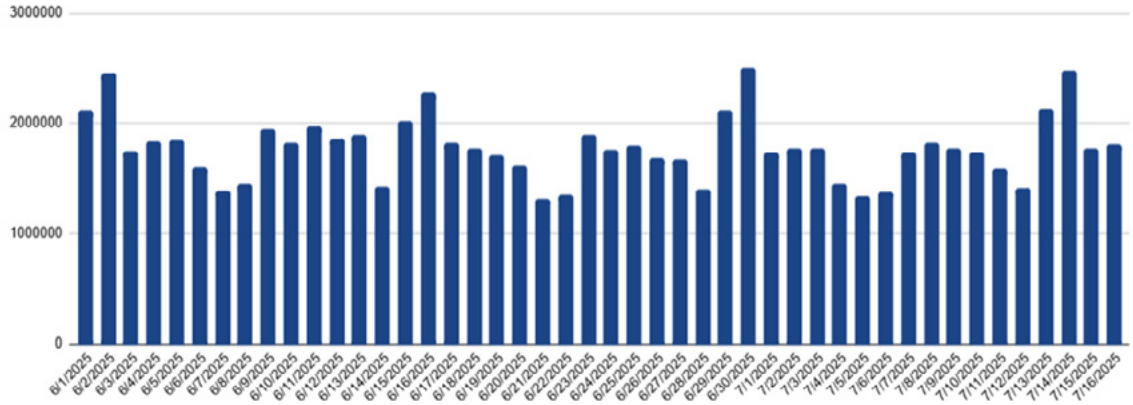
兩組不同的資料集顯示 Carbon Black 在 6 月和 7 月初對防禦規避活動的涵蓋情況。在 2025 年 6 月 18 日至 26 日期間，警報數量激增，最高峰時每天超過 120,000 次。這些警報代表即時偵測到主動規避嘗試，例如：DLL 側載和就地取材 (LOLBin) 工具的濫用。。

防禦規避嘗試的警示



在這段期間內，監視清單 (Watchlists) 每天標記 150 萬至 250 萬個潛在的防禦規避行為。這些警示是由主動的威脅獵捕 (threat hunting) 查詢所產生，且有助發現可能會避開自動化偵測的隱匿行為。

監視清單(Watchlists)顯示的防禦規避的警報



觀察到的常見防禦規避技術

威脅發動者利用各種 MITRE ATT&CK 對應的攻擊手法來避免被偵測並維持持久性。其中許多手法被 Carbon Black EDR(端點偵測與回應) 透過即時警示和持續的監視清單 (Watchlists) 查詢偵測到。以下是觀察到一些最普遍的攻擊手法。

- DLL 側載 (T1574.001)：攻擊者濫用合法的可執行檔來載入惡意的 DLL。這通常是透過搜尋順序劫持或將可信任的應用程式與攻擊者製作的 DLL 綁定在一起來達成。此技術常用於持久性、提權及防禦規避。
- 不尋常的 DLL 執行 (T1218.011、T1218.010)：rundll32.exe 和 regsvr32.exe 等公用程式被用來從意外路徑載入 DLL 或使用非標準擴充檔，通常會偽裝成合法的系統行為，以繞過啟發式偵測。
- 常用的合法工具 (LOLBins) 被改名 (T1036.003)：內建的 Windows 工具 (例如：powershell.exe、cmd.exe) 被改名，以掩蓋其真正目的。這些被改名的二進位檔隨後被用於隱蔽執行、橫向移動、提權和遠端指令執行，同時根據檔案名稱或雜湊值逃避偵測。
- 系統二進位代理執行 (T1218)：攻擊者利用可信任的 Windows 二進位檔 (例如：mshta.exe、regsvr32.exe) 來執行惡意的有效負載，並採用代理執行策略。此技術常用於繞過應用程式控制及安全政策。
- 篡改安全工具 (T1562.001、T1112)：攻擊者使用多種手法以削弱資安防護機制，包括終止 AV／EDR 程序、修改或刪除登錄檔機碼，以及停用更新機制以防止部署新憑證或修補程式。

Carbon Black 偵測到多個威脅組織和惡意軟體家族採用這些防禦規避手法。

勒索軟體家族

- LockBit
- BlackBasta
- Hive
- BlackCat
- Kofurlak
- RansomHub

木馬／後門程式家族

- Emotet
- IcedID
- Pikabot
- ShadowPad
- Mocha Manakin（基於 NodeJS）

多層次防禦技術

Carbon Black EDR 多層次防禦技術結合即時行為分析與透過監視清單 (Watchlists) 進行的持續威脅攔截，可針對進階的防禦規避技術提供可視性與可操作性。6 月份警報的急劇增加突顯威脅發動者的敏捷性，以及持續監控和主動偵測的必要性。隨著威脅份子的演變，組織必須持續利用 Carbon Black EDR 等工具，不僅是為了防護，也是為了洞察、回應和調適。

欲瞭解有關 Symantec 端點偵測與回應 (EDR) 最新簡報檔，請點擊此處。
欲深入瞭解更多有關賽門鐵克郵件安全雲端服務(Email Security.Cloud)的郵件威脅偵測和回應(ETDR)功能，請點擊此處。

2025/07/21

新一波綁架騙局：「職業殺手」用暴力攻擊恐嚇來騙取Litecoin(萊特幣)

最近賽門鐵克發現綁架騙局電子郵件的主題突然發生變化。一般而言，這些電子郵件會使用威脅性的語言向收件者勒索金錢。詐騙者似乎啟動新的綁架騙局活動，以「職業殺手」的身份提供毀壞財產或傷害等服務。收件人會收到該信件的原因是曾經求愛被拒或職場競爭的投訴，而「職業殺手」的任務是向受害者潑硫酸。「職業殺手」還會提供一個反提議，以花錢消災來避免潑酸。受害者可以將 2000 美元以 Litecoin(LTC) 加密貨幣的形式轉帳至電子郵件中提供的 LTC 位址。這種新方法旨在利用恐懼和個人弱點，同時利用加密貨幣的匿名性。

電子郵件標頭：

- Subject: PROPOSAL
- From: "First name Last name" <偽造的寄件者郵件帳號>

網路知識：Litecoin 是一個點對點的網際網路數位貨幣，它提供全球每一個人快速且零成本的付款機制。Litecoin 是一個開放原始碼的全球支付網路並建立在完整的中心化機制上，排除了任何中央機構。由數學確保網路的安全並使得個人完全掌控自身的財務。Litecoin 特點在於更快的傳輸與認證時間，並增進儲存效能領先其他已數學為基礎的數位貨幣。擁有大量的產業支撐交易量跟流動性，Litecoin 已經證明是 Bitcoin 的商業交易互補媒介。

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)。

2025/07/21

CVE-2025-53770--存在SharePoint的嚴重等級零日漏洞，在真實網路情境上已遭開採濫用

微軟已修補存在 SharePoint 的嚴重等級零日漏洞，因為有報導指出該漏洞已被廣泛開採濫用。此漏洞 (CVE-2025-53770) 稱為 ToolShell，會影響內部部署的 SharePoint 伺服器，讓攻擊者在未認證情況下存取受影響的伺服器，進而遠端執行程式碼並存取所有內容和檔案系統。這個新的零時差漏洞是最近修補過的漏洞 CVE-2025-49704 的衍生漏洞，CVE-2025-49704 已於 2025 年 7 月修補過。此漏洞已被加入 CISA 已知漏洞 (KEV) 目錄中。

請參閱我們的部落格：ToolShell：嚴重的 SharePoint 零日漏洞已遭到廣泛攻擊。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.NPE

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: Microsoft SharePoint CVE-2025-49704

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，內建對微軟 IIS 的預設強化可針對此漏洞提供零時差防護，防止在此情況下被部署和執行 webshells。
- 透過 DCS 在 SharePoint 伺服器上的佈署 default windows hardened policy 的網路規則可阻止連線至網際網路，進而減少攻擊面。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

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。

2025/07/18

Scanception：複雜的QR Code網路釣魚攻擊行動

有人觀察到一起被稱為 Scanception 的網路釣魚攻擊行動，目標是醫療保健、金融等重要領域的組織。此攻擊的引爆點是含有 PDF 附件的網路釣魚電子郵件，這些附件看似合法，但內含 QR Code。當掃描該 QR Code 時會將使用者重導向到偽造的 Microsoft 365 登入頁面，讓攻擊者能夠擷取憑證。該攻擊行動採用中間人攻擊 (AiTM) 技術繞過多因素驗證 (MFA)，並使用 AES 加密通道安全地滲出竊取的資料。為了進一步逃避偵測，攻擊者利用 Google 和 Bing 等可信賴的代理服務來掩飾與 C&C 基礎架構的通訊。

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：

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：

- Phish.Pdf
- Scr.HeurQR!gen1
- Web.Reputation.1
- 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。

2025/07/18
SquidLoader惡意程式載入器，以金融機構為目標

據報導，一個利用 SquidLoader 惡意程式載入器進行惡意有效酬載傳送的新攻擊行動以香港、新加坡、中國和澳洲的金融機構為目標。攻擊鏈透過偽裝成發票相關信件的目標性惡意垃圾郵件發起。這些電子郵件包含 .RAR 壓縮檔，一經解壓後便會為受害者注入惡意 Windows 平台上的 PE(Portable Executable) 類型檔案，導致目標端點感染 Squidloader。在報告攻擊行動中部署的最終有效酬載是滲透測試工具 Cobalt Strike 的信標(Beacon)，攻擊者可能用於遠端存取和控制。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- 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：

- Infostealer
- 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

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。

2025/07/18
KawaLocker勒索軟體

KawaLocker(也稱為 KAWA4096) 是最近在真實網路情境上發現的全新勒索軟體。該惡意軟體會加密使用者資料，並冠上隨機副檔名。勒索 (贖金支付通知) 是以一個名為「!!Restore-My-file-Kavva.txt」的文字檔形式注入，受害者被要求透過 Tox 這種端到端加密及對等網路的即時通訊 (Tox messenger) 與攻擊者聯繫以獲得進一步指示。KawaLocker 具備透過 Windows Management

Instrumentation(WMI) 刪除本機備份和磁碟區陰影複本的能力。此勒索軟體變種背後的威脅份子還擁有一個資料洩漏網站，其設計與 Akira 勒索軟體駭客集團所使用的網站非常相似。

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：

- AGR.Terminate!g2
- SONAR.RansomPlay!gen1
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g193
- SONAR.SuspLaunch!g253
- SONAR.SuspLaunch!gen4
- 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：

- Ransom.KawaLocker
- Trojan Horse
- 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!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。

2025/07/18

Matanbuchus惡意軟體載入器推出最新版本V3.0

在真實網路情境上已發現到 Matanbuchus 惡意軟體載入器推出最新版本V3.0。最近攻擊主要是利用 Microsoft Teams 的外部呼叫功能，攻擊者冒充 IT 支援人員，誘騙受害者執行偽裝成 Notepad++ 更新程式的惡意 PowerShell 腳本。一旦進入系統，Matanbuchus 3.0 會使用先進的隱匿技術，例如：記憶體內混淆和加密，以逃避偵測，並支援多種有效酬載類型，包括 EXE、DLL 和 shellcode。它可以收集系統資訊、監視執行中的程序和偵測安全工具，同時採用排程任務和程序空洞化等持久性／常駐方法，即使在重新開機後也能繼續維持存取權限。

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

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

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**。