保安資訊--本周(台灣時間2025/03/28)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 4,200 台受保護端點上總共阻止了 4,480 萬次攻擊。這些攻擊中有 82.5% 在感染階段前就被有效阻止：**(2025/03/24)**

- 在**7萬9,000**台端點上，阻止了**1,710**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**7萬8,400**台端點上，阻止了**640**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬4,000**台**Windows**伺服主機上，阻止了**590**萬次攻擊。
- 在**4萬9,500**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1萬1,900**台端點上，阻止了**92萬9,200**次嘗試掃描在**CMS**漏洞。
- 在**4萬3,800**台端點上，阻止了**170**萬次嘗試利用的應用程式漏洞。
- 在**10萬8,200**台端點上，阻止了**240**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,700**台端點上，阻止了**78萬1,100**次加密貨幣挖礦攻擊。
- 在**11萬400**台端點上，阻止了**720**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**555**台端點上，阻止了**7萬9,800**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 17 萬 2,100 個受保護端點上阻止了總計 730 萬次攻擊。**(2025/03/24)**

- 使用網頁信譽情資，在 **165.2K** 個端點上阻止 **700** 萬次攻擊。
- 攔截 **19.5K** 個端點上 **269.2K** 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 **5.7K** 個端點上攔截 **109.7K** 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 **186** 個端點上攔截 **2.9K** 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。

2025/03/28

Remcos惡意後門程式涉入Shuckworm進階持續威脅(APT)駭客集團的最新網路攻擊行動

來自 Cisco Talos 研究人員報告，揭露一項全新的惡意網路行動，主使者是 Shuckworm 進階持續威脅 (APT) 駭客集團 (又名Gamaredon)。根據這份報告，攻擊者正在瞄準烏克蘭人民，使用惡意的 .LNK 捷徑檔和 PowerShell 下載器，在感染他們之前先投放 Remcos 惡意後門程式的有效酬載。該行動利用與戰爭相關主題的網路釣魚電子郵件。這些電子郵件夾帶惡意的 .zip 壓縮檔案附件，內含有惡意的 .LNK 捷徑檔。Remcos 是一種眾所周知且被大肆濫用的熱門遠端存取木馬 (RAT)，攻擊者常用它進行遠端控制、資料收集、命令執行、服務和程序管理，以及下載／執行額外任意有效酬載的能力。

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：

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.Malcode!gen
- Scr.Mallnk!gen6
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- Trojan.Mallnk
- Trojan.Mallnk!g4
- Web.Reputation.1
- Web.Reputation.2
- WS.Malware.1
- WS.SecurityRisk.4

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。

2025/03/28

鎖定阿根塔銀行(Argenta Bank)客戶的網路釣魚郵件攻擊

阿根塔 (Argenta) 是一家總部位於比利時的銀行，同時也在荷蘭和盧森堡營運。最近，賽門鐵克發現到新一波的網路釣魚攻擊，偽裝成阿根塔的銀行服務，發送虛假的帳戶通知。郵件內容簡短，鼓勵收件人點擊並啟動一個安全更新，以提供額外的保護層以抵禦威脅。點擊郵件中的連結會將收件人重定向到一個偽造的阿根塔銀行 (Argenta Bank) 登錄頁面，旨在竊取憑據。一旦帳戶遭入侵／接管，攻擊者就可以存取受害者的該銀行帳戶。

郵件標頭：

- Beveiligingscontrole: Bevestig uw accountgegevens
- 翻譯：安全檢查：確認您的銀行帳號明細

郵件標頭：

- Beveiligingscontrole: Bevestig uw accountgegevens
- 翻譯：安全檢查：確認您的銀行帳號明細

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。

2025/03/28

RALord～全新勒索軟體

RALord 是在真實網路情境中發現以 Rust 撰寫的全新勒索軟體。該勒索軟體會加密使用者資料，並冠上「.RALord」副檔名。隨附的勒索 (贖金支付) 說明文件檔建議受害者透過 qTox 加密聊天室聯絡攻擊者以取得進一步指示。此勒索變種背後的主使者還威脅受害者，如果不乖乖就範付贖金，就會透過公開洩露頁面釋放被竊取的資料。

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：

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
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!500
- Heur.AdvML.C

2025/03/27

VIPKeyLogger鍵盤側錄惡意軟體涉入日本境內的企業網路攻擊

VIPKeyLogger 是一種隱秘的鍵盤側錄惡意軟體，已經有兩起鎖定日本組織和在日本設有當地辦事處國際公司的兩次網路釣魚行動中被發現到。該惡意軟體可以擷取使用者輸入，包括憑證，全球的駭客集團和個人利用它進行間諜活動、憑證盜竊和欺詐，使用以商業為主題的網路釣魚電子郵件來誘騙受害者。

第一起網路攻擊行動：

攻擊者冒充一家專門從事振動測試系統的日本公司，宣稱是接續處理 2019 年的一份報價。郵件禮貌且專業，請求確認價格，並附上惡意採購訂單。

- 主旨：価格と期限情報(ref:0467) 【注文書】WP2501001152 WP2501001153
- 附件：(ref0467) 【注文書】sales Agreement WP2501001152 WP2501001153.7z
- 攻擊鏈：郵件 > 7z 壓縮檔 > PEEXE (32-bit .NET)

第二起網路攻擊行動：

第二起網路攻擊行動假冒一家專門從事工業管道材料的日本公司。電子郵件請求報價，顯得專業，並包含聯繫資訊和辦公位址。

- 主旨：見積依頼 関電プラント向け
- 附件：見積依頼_関電プラント向け_pdf.r00
- 攻擊鏈：郵件 > r00 壓縮檔 > PEEXE (32-bit .NET)

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.ProcHijack!g55

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.Malcode!gdn32

基於機器學習的防禦技術：

- Heur.AdvML.B

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: Untrusted Telegram API Connection

2025/03/27

Android平台上的惡意軟體：PJobRAT

來自 Sophos 研究人員發現一個 Android 平台上的惡意軟體：PJobRAT 的散播行動。該行動主要針對台灣的手機用戶，目的是蒐集和滲出敏感資料，包括簡訊內容、聯絡人名單，以及儲存在遭入侵裝置上的文件和媒體檔案。PJobRAT 被偽裝成合法的訊息應用程式散佈。惡意程式使用 FCM(Firebase Cloud Messaging) 跨平台訊息解決方案進行 C&C 通訊，並使用 HTTP 通訊協定外洩竊取的資料。

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：

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

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。

2025/03/27

CVE-2025-24799--存在熱門的開源IT服務管理(ITSM)軟體套件：GLPI的SQL注入漏洞

CVE-2025-24799 是一個最近發現的 SQL 注入漏洞，會影響 GLPI，這是一個熱門的開源 IT 服務管理 (ITSM) 軟體套件。如果遭成功開採濫用，此漏洞可能會讓未認證的遠端攻擊者成功進行 SQL 資料庫注入，進而透過遭攻擊的機器執行遠端程式碼。此漏洞已在 10.0.18 版本的產品中完成修補。

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: GLPI CVE-2025-24799

2025/03/27

CVE-2025-24799--存在Apache Camel中的Bypass(略過權限檢查)/注入漏洞

CVE-2025-29891 是最近發現的第二個影響 Apache Camel Bypass(略過權限檢查)／注入漏洞，Apache Camel 是一個熱門的開源整合框架。若成功開採濫用此漏洞，遠端攻擊者可在傳送至 Camel 應用程式的 HTTP 請求中注入任意參數。此漏洞與先前揭露的 CVE-2025-27636 有關，會影響任意 HTTP 標頭的注入。修補此漏洞的 Apache Camel 版本已經由產品供應商推出。

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：

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: Apache Camel CVE-2025-29891

2025/03/27

macOS平台出現採用Go語言撰寫ReaderUpdate惡意軟體載入器的後繼新變種

在真實網路情境上發現 macOS 平台出現採用 Go 語言撰寫的 ReaderUpdate 惡意軟體後繼新變種。此惡意軟體家族早先是採用 Crystal、Nim 和 Rust 程式語言。該惡意軟體已知會透過第三方軟體下載網站及特洛伊木馬應用程式散佈。ReaderUpdate 惡意程式載入器具有從其操作者擷取並

執行遠端指令的功能，這包括傳送額外的任意有效酬載，例如：廣告軟體或惡意軟體。

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：

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：

- OSX.Trojan.Gen
- OSX.Trojan.Gen.2
- 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。

2025/03/26

鎖定Rakuten Securities(樂天證券)客戶的網路釣魚事件激增

最近幾週，鎖定日本最大、最知名的線上經紀公司之一 Rakuten Securities(楽天証券) 客戶的網路釣魚行動越來越多。該公司提供多元的投資服務，包括股票、ETF、共同基金、期貨、期權、外匯交易和 NISA(日本稅務優惠投資帳戶)。

這些活行動幕後的攻擊者在 .cn 頂級網域名稱下產生了量隨機化的子網域，全部模仿樂天證券。在最新攻擊活動中，這些網域名稱遵循五個字元的字母數字字串，其次是 /rakusec(例如 ：yuowy[.]cn/rakusec) 的模式。此行動中使用的網路釣魚電子郵件主旨「以降のオンラインサービスログイン時の確認畫面表示について【楽天証券】」、目的在引誘收件人，使其相信該訊息是來自樂天證券的合法安全通知。

根據報導，攻擊者在成功竊取憑證後，在某些情況下會試圖清算受害者的投資組合，並大量購買中國股票。

樂天證券用戶應提高警惕，點擊之前應驗證所有郵件和連結。強烈建議提款和登入時啟用簡訊認證，以確保多一層保護。

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。

2025/03/26
全新Android惡意軟體導入.NET MAUI框架來逃避偵測

一個利用 .NET MAUI 框架的全新 Android 惡意軟體在真實網路情境上被發現。.NET MAUI 是用來以 C# 和 XAML 建立原生桌面和行動應用程式的一個跨平台框架。散佈的惡意二進位檔被假裝成合法的應用程式，例如：銀行、約會或社交網路應用程式。部署的惡意軟體主要針對收集和滲透敏感的使用者資料，包括個人和財務資訊等。

網路知識：.NET 多平臺應用程式 UI(.NET MAUI) 是使用 C# 和 XAML 建立原生行動和桌面應用程式的跨平台架構。使用 .NET MAUI，您可以從單一共享程式代碼基底開發可在 Android、iOS、macOS 和 Windows 上執行的應用程式。

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：

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。

2025/03/26
PlayBoy Locker勒索軟體

PlayBoy Locker 是去年 9 月被發現的全新勒索軟體，最初以勒索軟體即服務 (Ransomware-as-a-Service-RaaS) 的形式散佈。該勒索軟體平台提供多種作業系統的支援，包括 Windows、NAS 和 ESXi 作業系統。11 月稍後有報導指出 Playboy Locker 勒索軟體的完整原始碼被提供出售，可能使其被其他威脅份子取得。PlayBoy Locker 會加密使用者資料，並在冠上 .PLBOY 副檔名。該惡意軟體還能刪除受感染端點上的磁碟區陰影複本。所觀察到的勒索(贖金支付)說明是以一個檔名為「INSTRUCTIONS.txt」文字檔形式被注入，攻擊者建議受害者就贖金要求和進一步指示與他們聯絡。

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

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
- 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

2025/03/26

CVE-2025-24813--存在Apache Tomcat嚴重等級的遠端程式碼執行(RCE)漏洞

安全研究人員觀察到 CVE-2025-24813 的漏洞已遭大肆開採濫用，這是存在 Apache Tomcat 一個嚴重等級的遠端程式碼執行 (RCE) 漏洞，Apache Tomcat 是 Java 應用程式的開放原始碼伺服器容器和網頁伺服器。此漏洞是由路徑等價 (path equivalence) 問題所引起，攻擊者可繞過安全限制並遠端執行任意程式碼。攻擊者可利用以 HTTP PUT 處理檔案上傳、NTFS junction exploitation 及惡意反序列化來獲得持久性及提升權限。此漏洞對在企業和雲端環境中使用 Apache Tomcat 主機 Web 應用程式的組織造成嚴重風險。

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: Apache Tomcat CVE-2025-24813

2025/03/26

針對美國和歐洲國家的Dragon勒索軟體即服務駭客集團

Dragon 勒索軟體即服務駭客集團是 2024 年 7 月浮上檯面的駭客集團，主要針對美國、以色列、英國、法國和德國的組織。該駭客集團利用 Web 應用程式漏洞、暴力攻擊和竊取憑證作為其主要攻擊媒介，並使用兩種勒索軟體家族：一種以 Windows 為重點的加密程式，很可能是 StormCry 修正版；另一種是 PHP webshell，可提供後門功能和持久性勒索軟體功能。

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.RansomPlay!gen1

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!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。

2025/03/26

在最近的惡意垃圾郵件散播行動中發現到全新JS惡意程式下載程式

賽門鐵克發現新一起惡意電子郵件行動，以附件形式傳送 JavaScript 的惡意下載程式。JS 惡意下載程式會以不同的檔名透過不同主旨的電子郵件傳送。JS 被執行時會啟動 PowerShell 指令碼下載、解碼並將鍵盤記錄程式有效酬載注入名為 MSBuild.exe 的新程序。此鍵盤記錄程式使用 Telegram 作為其 C&C。可能的電子郵件特徵包括下列內容：

主旨：

- NEW Contract & PI
- Remittance Slip Attached

附件：

- NEWContractPI.js
- PaymentSwiftCopy.js

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-Wscr!g1
- ACM.Wscr-Ps!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：

- ISB.Downloader!gen48
- Web.Reputation.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: Suspicious Process Accessing Lets Encrypt Certified Site
- 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。

2025/03/25

Funnelweb駭客組織發動以「Operation FishMedley」為名的目標式攻擊行動

受中國支持的進階持續性 (APT) 威脅組織 Funnelweb(又名 Aquatic Panda、Earth Lusca、FishMonger) 發動一場名為「Operation FishMedley」的大規模行動。此行動針對許多國家的政府、非政府組織和智庫等機構。在這次行動中，利用了先前與此組織相關的各種植入程式，以及其他由中國支持 APT 所使用的植入程式。這些植入程式包括 RPipeCommander (反向shell)、ShadowPad (模組化後門)、SodaMaster (dll 側載後門) 和 Spyder (模組化後門) 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

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.Trojan
- Trojan Horse
- WS.Malware.2

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。

2025/03/25

防護亮點：賽門鐵克端點安全行動版，有效防護暗藏在行動APP中的惡意OCR資料滲透

最近安全研究發現，Google Play 和 iOS App Store 上有超過 20 個 APP 有暗藏惡意 OCR 的技倆來擷取和滲透敏感資料，稱為「SparkCat」。這些 APP 會掃描本機和雲端儲存，針對加密金鑰、密碼和財務文件，然後將資料傳送至 AWS 控制的伺服器。

iOS 惡意軟體：複雜的威脅

我們的主要焦點是 iOS，因為它對企業安全有影響。這些 APP 內的惡意框架：

- 當使用者開啟支援視窗時被啟動，允許檔案存取。
- 使用 OCR 掃描檔案，尋找敏感關鍵字，包括加密復原金鑰。
- 將識別出的檔案滲透到由 C&C 基礎架構控制的 Amazon 主機伺服器。

值得注意的是，並非所有的 APP 版本都會受到影響，這顯示是一種供應鏈攻擊，在開發過程中的某個階段被注入惡意程式碼。

為何這項研究引人注目

- 大規模迴避--惡意軟體繞過 Apple 安全審查，在 App Store 上維持一年以上未被偵測到。
- 隱身伎倆--攻擊者利用合法的網路服務來逃避偵測。
- AI 驅動的滲透--機器學習在擷取和傳輸敏感資料的過程中扮演重要角色，顯示行動威脅的複雜性達到新的水準。
- 超越靜態偵測--傳統安全工具無法偵測到這些威脅，突顯出行為驅動安全方法的必要性。

賽門鐵克如何保護客戶

儘管惡意軟體採取隱蔽方式，賽門鐵克的行動威脅防禦 (MTD) 仍能及早識別並降低威脅：

- 網路完整性政策使用 WebPulse 網頁信譽分析將 C&C 伺服器標示為可疑。
- 不需要的 APP 政策會偵測到試圖滲透敏感資料受感染版本應用程式。
- 以行為為基礎的偵測識別出靜態簽章以外的風險，在公開披露之前標記高風險活動。

有趣的是，在這些行為被大肆報導之前，我們的系統已經在其他應用程式中發現這些行為，最早可追溯至 2024 年 1 月。我們也標記原始研究未涵蓋的受感染應用程式之風險行為，包括攻擊者 AWS 存取金鑰 ID 及嵌入惡意函式庫和框架的秘密金鑰。

持續的風險需要不間斷防護機制

這些應用程式在 iOS App Store 上仍然活躍，如此增加供應鏈攻擊的可能性。然而，開發人員必須整合惡意框架--直接或透過 Xcode 等特洛伊木馬工具。這表示單靠靜態偵測並不足夠；必須動態分析每個應用程式版本的高風險行為。

關鍵要點：僅靠 App Store 的自我審核機制是不夠安全

企業的行動保護需要主動、動態的安全性來防止資料遺失。當威脅的複雜程度和規模持續演進時，僅依賴 Apple 或 Google 的自我審核機制是不夠安全。

賽門鐵克的端點安全企業版 (SESE)／端點安全完整版(SESC)內含防護 IOS／Android 的最先進防護技術，請點擊此處瀏覽更完整的資訊。

2025/03/25
CVE-2025–26319--存在Flowise的預先授權(Pre-Auth)任意檔案上傳漏洞

CVE-2025-26319 是最近被揭露存在 Flowise 的預先授權 (Pre-Auth) 任意檔案上傳漏洞。Flowise 是開發人員建立自訂 LLM(Large Language Model) 編排流程和 AI 代理的流行開放原始碼工具。如果遭成功開採濫用，可能允許未驗證攻擊者取得受影響伺服器的遠端控制權，並允許他們上傳惡意檔案、指令碼、組態檔案、SSH 金鑰等。

網路知識：Flowise 是基於 LangChain 的低代碼 (這使得即使沒有程式設計背景的用戶，也能輕鬆設計並部署自己的 AI 應用程序)。AI 工作流構建工具。LangChain 是一個專為多步驟 AI 任務設計的框架，而 Flowise 將其功能擴展為可視化的工具，讓開發者可以通過拖放方式輕鬆設計工作流。無論是個人開發者還是企業團隊，Flowise 都可以幫助他們快速構建複雜的 AI 解決方案，例如：聊天機器人、智能問答系統、內容生成工具以及自動化數據處理應用。

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：

- Attack: Flowise Pre-Auth Arbitrary File Upload CVE-2025-26319

2025/03/25
FogDoor惡意後門散播行動

據報導，一起針對波蘭語系求職開發人員的全新攻擊行動，傳送被稱為 FogDoor 的全新惡意後門程式。攻擊者以假冒的招聘測試引誘受害者下載包含惡意 .lnk 捷徑檔的 .iso 檔。經執行的 .lnk 檔會呼叫 PowerShell 指令碼來安裝惡意軟體的有效酬載。部署的後門允許威脅攻擊者從受感染的端點執行遠端命令執行和資料收集。FogDoor 利用稱為固定情報解析器 (DDR-Dead Drop Resolver) 的技術，將合法網站 (例如：社交媒體檔案) 用作中介 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.Mshta-Http!g1
- ACM.Mshta-Ps!g1
- ACM.Ps-Http!g2
- ACM.Ps-Mshta!g1
- 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：

- Scr.Lemonduck!gen1
- Scr.Malcode!gen43
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE.C
- Web.Reputation.1
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- 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
- Audit: PowerShell Process Accessing Github

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。

2025/03/25

CVE-2024-56346 & CVE-2024-56347--近期IBM AIX作業系統漏洞～DCS可以有效防護漏洞利用攻擊

CVE-2024-56346 及 CVE-2024-56347 是兩個最近公佈影響 IBM AIX 作業系統的嚴重漏洞 (CVSS 風險評分：10.0 及 9.6)。若遭開採濫用，遠端攻擊者可透過不當的程序控制執行任意指令。根據 IBM 最近安全公告，CVE-2024-56346 會影響 AIX 的 nimesis Network Installation Management (NIM) master 服務，而 CVE-2024-56347 則與 AIX 的 nimsh 服務 SSL／TLS 保護機制有關。這兩個漏洞都已在發佈的產品修補程式中解決。

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 預設強化政策可為底層作業系統 (IBM AIX) 提供零時差保護，防止 CVE-2024-56346 和 CVE-2024-56347 攻擊。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2025/03/24

SVCStealer惡意軟體

SVCStealer 是一款新型的基於 C++ 的惡意竊密軟體，已經出現在真實網路情境。該惡意竊密軟體從感染的終端收集各種敏感資訊，例如：系統資訊、憑據、加密貨幣錢包、瀏覽器中存儲的資料、螢幕截圖、與熱門通訊應用程式 (Discord、Tox、Telegram) 或 VPN 應用程式有關的資料等。收集到的資訊被壓縮成 .zip 檔案，並外傳到遭攻擊者控制的 C&C 伺服器上。

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-RLsass!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.MalTraffic!gen1
- SONAR.Stealer!gen1
- 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
- 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: Bad Reputation Process Request 4
- 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。

2025/03/21

Albabat勒索軟體的最新變種可以攻擊更多種作業系統

根據趨勢科技的最新報告，Albabat 勒索軟體最新變種已提供更多種作業系統的支援。Albabat 勒索軟體家族種還在積極發展中，並將 Linux 和 macOS 平台納入鎖定的攻擊目標。該勒索軟體會加密遭感染端點上的檔案，但位於特定系統相關資料夾中的檔案除外。該惡意軟體還具有停用各種系統、偵錯或虛擬機器相關程序的功能。據報告，最新的 Albabat 變種利用 GitHub REST API 進行組態資料擷取。

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-Http!g2
- ACM.Ps-Net!g1
- ACM.Ps-Reg!g1
- ACM.Ps-Sc!g1
- ACM.Ps-Wbadmin!g1
- ACM.Untrst-Bcdedit!g1
- ACM.Untrst-RunSys!g1
- ACM.Untrst-Wbadmin!g1
- ACM.Vss-DlShcp!g1
- ACM.Wbadmin-DlBckp!g1
- ACM.Wmic-DlShcp!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!gen1
- SONAR.SuspLaunch!gen4
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g193
- SONAR.SuspLaunch!g195
- SONAR.SuspLaunch!g250
- SONAR.SuspLaunch!g253
- 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：

- Ransom.Albabat
- Trojan.Gen.MBT
- 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.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
- Audit: Github Cloud Service Connect Attempt
- System Infected: Bad Reputation Application Connecting to Cloud Storage

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。

2025/03/21

鎖定Pocket Card會員的新型網路釣魚行動

賽門鐵克偵測到鎖定日本民眾的網路釣魚行動，該行動使用偽造的 Pocket Card 通知電子郵件。這些電子郵件的主旨是

- レジットカードのポケットカード會員専用ネットサービスからのお知ら

(翻譯：「信用卡口袋卡會員線上服務通知」) 詐騙者利用大家熟悉的「身分驗證服務 (3D Secure)」程序，這是用來確保客戶帳戶安全的附加驗證服務。它讓電子郵件看起來合法且與使用者相關。點擊電子郵件中的註冊連結會將使用者重導向到偽造的 Pocket Card 登入頁面，目的是竊取憑證。一旦入侵，攻擊者就可以存取受害者的 Pocket Card 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。

2025/03/21

VanHelsing勒索軟體

VanHelsing 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 .vanhelsing 或 .vanlocker 副檔名。VanHelsing 會以檔名「README.txt」的文字檔形式注入勒索 (贖金支付) 說明，而且還能夠修改桌面背景。該勒索軟體具有刪除受感染端點上的磁碟陰影複本功能。此惡意軟體背後的主使者採用雙重勒索策略，威脅受害者若不配合支付贖金，就會公開揭露竊取的資料。

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：

自適應防護技術(包含於SESC)：

- ACM.Untrst-RunSys!g1
- ACM.Wmic-DlShcp!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Ransom!gen14
- SONAR.RansomGen!gen3
- SONAR.RansomPlay!gen1
- SONAR.Ransomware!g16
- SONAR.SuspLaunch!g193
- 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.Gen
- WS.Malware.1
- WS.SecurityRisk.3

基於機器學習的防禦技術：

- Heur.AdvML.A!500
- 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：

- Heur.AdvML.A!500
- Heur.AdvML.C

2025/03/21

使用「ClickFix」社交工程技倆，冒充旅遊預訂網站的行動

一起冒充 Booking.com 的網路釣魚行動已被揭露，鎖定亞洲、北美、大洋洲和歐洲的酒飯店業，大肆傳播竊取憑證的惡意軟體。攻擊者發送偽造的電子郵件，冒充線上旅行社。郵件內容各異，不外乎負面客戶評價、潛在客戶的請求、線上促銷機會、帳戶驗證等主題，但在郵件正本或 PDF 附件中包含一個網址。點擊該連結會被引導到顯示偽造的驗證碼的網頁，背景微妙地設計成模仿合法的 Booking.com 頁面。這個偽造的驗證碼是網頁利用 ClickFix 社交工程技倆下載惡意籌載的地方。

保安補充：ClickFix 攻擊是一種複雜的社交工程伎倆，利用真實性的外觀來操縱用戶執行惡意腳本。自 2024 年初首次被定義以來，已經成為惡意軟體散佈行動的主流手法，利用遭入侵或偽造網站、惡意分發基礎設施和電子郵件釣魚。

網路知識：Booking.com 是世界最大的旅遊電子商務公司之一，主要提供全球住宿預訂的服務，是美國上市公司 Booking Holdings 的旗下品牌之一。

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

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：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- 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。

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**。