保安資訊--本周(台灣時間2025/05/16)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 34 萬 1,600 台受保護端點上總共阻止了 5,000 萬次攻擊。這些攻擊中有 83.3% 在感染階段前就被有效阻止：**(2025/05/12)**

- 在**8萬5,400**台端點上，阻止了**2,060**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**8萬2,600**台端點上，阻止了**630**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬3,100**台**Windows**伺服主機上，阻止了**660**萬次攻擊。
- 在**5萬2,100**台端點上，阻止了**180**萬次嘗試掃描伺服器漏洞。
- 在**1萬1,100**台端點上，阻止了**76萬2,100**次嘗試掃描在**CMS**漏洞。
- 在**5萬2,700**台端點上，阻止了**190**萬次嘗試利用的應用程式漏洞。
- 在**8萬7,000**台端點上，阻止了**170**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**63萬9,400**次加密貨幣挖礦攻擊。
- 在**10萬700**台端點上，阻止了**760**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**557**台端點上，阻止了**6萬7,900**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 300 個受保護端點上阻止了總計 750 萬次攻擊。**(2025/05/12)**

- 使用網頁信譽情資，在 **163.8K** 個端點上阻止 **710** 萬次攻擊。
- 攔截 **18.7K** 個端點上 **254.3K** 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 **84.4K** 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 **230** 個端點上攔截 **4.6K** 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。

2025/05/16

在無檔案類型攻擊鏈中隱匿式的Shellcode惡意程式載入器執行Remcos遠端存取木馬(RAT)

已經觀察到一個複雜的無檔案惡意軟體攻擊行動，利用 PowerShell 來部署 Remcos 遠端存取木馬 (RAT)。此攻擊從嵌入 ZIP 檔案的惡意 .LNK 捷徑檔案開始，通常會偽裝成 Office 文件。這些檔案透過 mshta.exe 觸發混淆的 VBScript，導致 PowerShell 腳本在記憶體中執行。此指令碼會重建並執行 shellcode，最終載入 Remcos RAT。一旦完成部署，Remcos 即可讓攻擊者完全控制系統，並支援鍵盤側錄、螢幕擷取和憑證竊取等功能。它採用先進的迴避技術，包括程序空洞化和繞過使用者帳戶控制 (UAC)，並透過 TLS 加密通道與其命令與控制基礎架構通訊，以避免偵測。

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.Mshta-CNPE!g1
- ACM.Mshta-Http!g1
- ACM.Mshta-Ps!g1
- 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。

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen11
- CL.Downloader!gen203
- ISB.Downloader!gen77
- ISB.Downloader!gen81
- ISB.Downloader!gen205
- ISB.Downloader!gen221
- PUA.Gen.2
- Trojan.Gen.MBT
- Trojan.Remcos
- Web.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。

2025/05/15

駭客組織：Earth Ammit，發動網路間諜滲透行動

駭客組織：Earth Ammit，在中亞、東南亞和東歐發起兩起不同的網路間諜滲透行動 (分別稱為 VENOM 和 TIDRONE)。這些行動策略性地針對政府部門和關鍵基礎設施，例如：軟體服務供應商和上游供應商，跨越數個關鍵領域，包括重工業、媒體、科技、醫療保健和軍事。VENOM 和 TIDRONE 攻擊活動都使用自訂的工具和隱匿式感染攻擊鏈。供應鏈攻擊透過受害者信任的管道，將惡意程式碼注入或更新替換，散佈到終端使用者，試圖滲透高價值的目標受害者。

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：

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.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。

2025/05/15

TransferLoader惡意軟體載入器～分工越來越細的威脅產業鏈

TransferLoader 是一款新發現的惡意軟體載入器，自 2025 年 2 月開始活躍，由三個元件組成：下載器、後門程式和後門載入器。它使用先進的迴避技術，例如：反偵錯、運行環境以字串解密和插入垃圾程式碼，以避免偵測並增加逆向工程的複雜性。下載器透過 HTTPS 擷取有效酬載、解密並執行，然後開啟誘餌 PDF 檔案以掩蓋惡意活動。該後門支援指令碼執行、檔案操作和組態更新，同時利用分散式 InterPlanetary File System (IPFS) 進行彈性指令與控制 (C&C) 通訊。載入器模組使用加密的命名管道進行安全通訊，並透過 COM 劫持和修改登錄檔機碼來取得常駐／持久性。TransferLoader 與 Morpheus 勒索軟體的攻擊有關連，包括對一家美國律師事務所的攻擊。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Untrst-RunSys!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- 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
- Heur.AdvML.A!300

- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.C
- Heur.AdvML.D

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。

2025/05/15

DarkCloud惡意軟體新變種涉入的目標性攻擊，利用視窗程式自動化AutoIt的功能進行混淆

根據 Palo Alto Networks Unit 42 發表的報告，已觀察到 DarkCloud Stealer 惡意竊密軟體的全新變種，主要針對全球各地的政府組織。此攻擊通常以含有 RAR 壓縮檔或 PDF 的釣魚電子郵件引爆，提示受害者下載偽裝成軟體更新的惡意壓縮檔。此檔案包含一個 AutoIt 編譯的可執行檔，可重建並執行 DarkCloud Stealer 的最終有效酬載。此惡意軟體具備反虛擬 (Anti-VM)／虛擬感知功能，其設計目的在於竊取敏感資料，包括瀏覽器憑證、電子郵件密碼和 FTP 登入，同時建立命令與控制 (C&C) 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：

自適應防護技術(包含於SESC)：

- ACM.Untrst-FlPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Stealer!gen1
- SONAR.Stealer!gen2
- SONAR.SuspInject!gen5
- SONAR.SuspLaunch!g529
- SONAR.SuspLaunch!g532

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.Malautoit!g7

- Trojan.Pidief
- 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。

2025/05/14

Chihuahua惡意竊密軟體

Chihuahua 是一個全新 .NET 類型的惡意竊密軟體，透過多階段的攻擊行動散佈。攻擊者利用 Google Drive 雲端硬碟上的惡意文件和惡意 PowerShell 指令碼來引爆感染鏈。最後有效酬載--Chihuahua 惡意竊密軟體是從 OneDrive 雲端硬碟所傳送，其功能是從遭入侵的端點收集和滲透各種敏感資料，包括系統資訊、儲存在系統網頁瀏覽器中的資料、加密貨幣錢包資訊等。收集完成後，資料會加密、壓縮並上傳至攻擊者控制的遠端伺服器。在此操作之後，惡意竊密軟體會執行抹除程序，清除機器上所有進行惡意操作的痕跡。

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.Stealer!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：

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

2025/05/14

PupkinStealer：.NET的惡意竊密軟體

PupkinStealer 是一款 .NET 的惡意軟體，已被觀察到透過包含惡意附件或連結的釣魚電子郵件散佈。此惡意軟體以 Windows 使用者為目標，能夠從 Chromium 核心的瀏覽器、Telegram、Discord、電子郵件用戶端、剪貼簿內容等竊取敏感資料。竊取的資料會壓縮成 ZIP 檔案，並使用 Telegram Bot API 外洩。

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.MalTraffic!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.2
- 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

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: Untrusted Telegram API Connection
- System Infected: Trojan.Backdoor Activity 564
- System Infected: Trojan.Backdoor Activity 654

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。

2025/05/13
防護亮點：賽門鐵克雲端沙箱防護與洞察力

面臨的挑戰

威脅份子不斷發展和精進其戰術、技巧和程序 (TTPs) 以利入侵目標並取得存取權限。這需要找出弱點，並從其他入侵成功的案例中學習，包括一些不常見的全新 TTPs，這些 TTPs 尚未受到完善的防護，或者以前所未見的掩護手法，突破現有防護機制的極限。

對抗惡意行為者的挑戰一直在於偵測、預防，甚至補救措施的成本和潛在風險與惡意軟體的開發和傳播相比，呈現出不對稱的戰爭。越來越多威脅所涉入的攻擊鏈中，日益濫用可信賴的工具和驅動程式，因此必須針對這些 TTPs 擬定詳細的訓練計劃以識別這些威脅、發現任何新技術，並揭露其內部結構，以便在這場戰役中取得優勢。

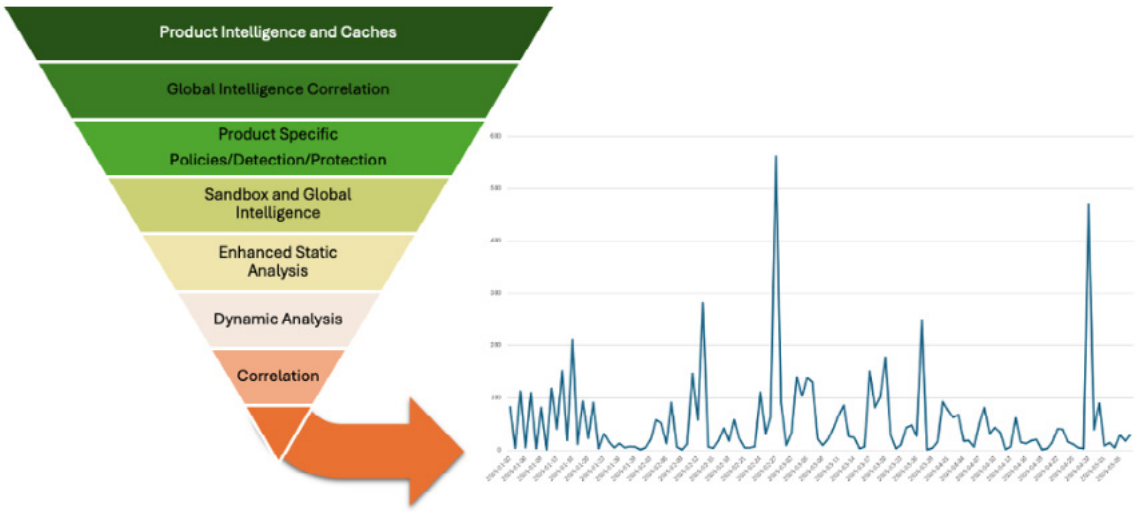
賽門鐵克雲端沙箱

賽門鐵克雲端沙箱能夠正面迎接挑戰，每天識別全新的威脅，為我們的客戶提供保護，並產生情報回饋至賽門鐵克全球情報資料庫，即使這些新技術正在威脅環境中散佈，也能有效瓦解它們。

賽門鐵克雲端沙箱不斷偵測到腳本類型的惡意軟體下載器、安裝程式和惡意竊密程式，當這些威脅使用新技術將惡意程式拆分到遠端有效酬載或隱藏在灰色地帶時，往往會造成偵測上的挑戰。GuLoader 和 MintsLoader 就是賽門鐵克雲端沙箱偵測到此類持續威脅的例子。由於賽門鐵克雲端沙箱採用多種引擎偵測技術會在威脅演變之前不斷發展，因此可持續保護系統。

在賽門鐵克雲端沙箱平台中，所有偵測與分析的引擎都被賦予充裕資源來進行游刃有餘之分析，此為不攔截的分析，得以讓惡意軟體盡可能展現其完整的面向，並讓沙箱內外的各種觀察家接收回饋，從惡意軟體與已知行為的落差以及威脅防禦措施的表現上獲取價值。賽門鐵克雲端沙箱中偵測數量的激增通常表示威脅份子正在引進新的技術或方法，這同時可讓所有賽門鐵克解決方案能共享威脅防護的量能。

電子郵件偵測在沙箱中的偵測技術達到高峰

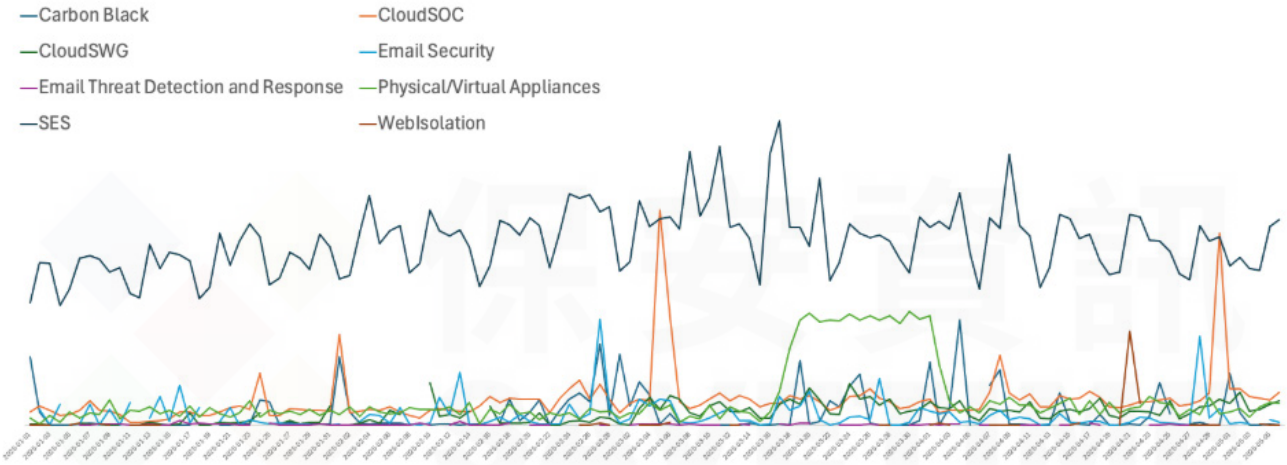


威脅情報--真正的寶藏

賽門鐵克雲端沙箱也可作為生成中介資料／詮釋資料 (metadata) 的來源，協助調查並提供有關威脅的強化資訊。某些賽門鐵克產品包含自動化功能，可將已知的惡意軟體和可疑樣本提交至賽門鐵克雲端沙箱，以蒐集額外的檔案相關資訊，SOC 或自動化系統可利用這些資訊進行威脅追蹤、分析或事件回應。賽門鐵克雲端沙箱透過與所有賽門鐵克產品的整合，提供跨網頁、電子郵件和端點等各種情境的威脅情報，並由多個內部工作流程加以運用，以強化威脅分析和回應程序，因此具有獨特的優勢。

下圖顯示賽門鐵克雲端沙箱提供給各個解決方案的偵測趨勢，因為產品的需求、涉及的威脅以及觀察到的可疑流量會隨著時間改變。

下列解決方案都會將惡意軟體提交至沙箱進行偵測／報告而讓彼此都能增強防護能力



被沙箱偵測為全新威脅的情報，將隨即提供給威脅回應團隊納入為已知的威脅資料庫，同樣威脅就不會再傳送到沙箱來重複偵測，這讓沙箱的處理能力永遠都保持餘裕，能以最快回應時間來偵測與回應前所未見的新威脅。

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。
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。
欲深入瞭解更多有關賽門鐵克郵件安全雲端安全服務(Email Security.Cloud)的電子郵件掃描順序，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。
欲深入瞭解更多有關賽門鐵克端點安全完整版(SESC)的端點偵測和回應(EDR)功能，請點擊此處。

2025/05/12

BTMOB遠端存取木馬(RAT)重出江湖

根據最近的報導，BTMOB 遠端存取木馬 (RAT) 重出江湖，現在目標是模仿支付寶 (Alipay) APP 的介面來竊取個人密碼。它透過偽裝成熱門服務的釣魚網站進行傳播，並使用假冒 APP 來引誘受害者。一旦安裝在 Android 裝置上，它會利用存取權限和覆蓋螢幕畫面來擷取敏感輸入，例如：鎖定螢幕密碼和付款憑證。

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。

- 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。

2025/05/12

免費的永遠最貴～Noodlophile惡意竊密程式以免費AI工具為幌子，暗地裡偷竊寶貴的資訊

最近，Noodlophile 惡意竊密程式以 AI 影片產生器為幌子來發動散佈行動。攻擊者透過社交媒體平台宣傳他們的虛假 AI 平台。使用者首先會被引誘上傳照片或影片來讓 AI 協助自動生成所期望的影片，然後會收到所謂製作完成的下載連結。受害者反而會收到偽裝成影片 .mp4 檔案的惡意籌載之安裝程式。Noodlophile 惡意竊密程式是以惡意軟體即服務 (MaaS) 的形式提供。該有效酬載具有從遭入侵的端點竊取多元資訊的功能，包括憑證、cookie、瀏覽器資料、第三方應用程式權杖等。收集到的資料會在 Telegram API 協助下滲出給攻擊者。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Ps-Reg!g1
- ACM.Ps-RgPst!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：

- Infostealer
- 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

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

2025/05/12

Astryrean Stealer惡意竊密程式

Astryrean 惡意竊密程式是最近在真實網路情境新發現 Python 型態的惡意竊密程式。該惡意軟體目標是收集和滲出多種機密或敏感資訊，包括：遭入侵系統的系統資訊、儲存在系統網頁瀏覽器中的資料、Discord Token (建立帳戶時產生的 Discord 使用者名稱和密碼的加密) 或螢幕截圖等。Astryrean Stealer 還能夠偵測虛擬化環境，並檢查受感染系統上是否存在惡意程式除錯器 (debuggers)。惡意程式碼目前透過 Github 檔案分享平台散佈，並宣稱其僅用於教育與研究目的。

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：

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：

- Infostealer
- WS.Malware.1

2025/05/12

駭客組織：Venom Spider 的攻擊行動，利用「More_eggs」多功能後門程式

在最近一次攻擊行動中，被稱為「Venom Spider* 毒蜘蛛」的駭客組織一直鎖定企業人資經理和招募人員為目標，使用複雜的魚叉式網路釣魚計劃，利用這些用戶打開電子郵件附件或點擊鏈接審閱應徵者簡歷的需求。攻擊者冒充求職者，使用虛假履歷直接發送電子郵件申請真實工作。電子郵件包含一個連結，讓受害者下載假冒的求職者履歷。該連結連接到一個外部網站，其中包含一個驗證碼框，提示受害者點擊以通過驗證碼。這會讓受害者相信這是應徵者的履歷，但實際上是一個惡意檔案，下載後就會被植入一個名為 More_eggs 的多功能後門程式。此後門可被用於廣泛的惡意活動，因為它會收集受感染系統的資訊，並將其傳送至遠端伺服器，供「Venom Spider* 毒蜘蛛」駭客組織進一步處理。

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-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：

- ISB.Downloader!gen314
- Trojan Horse
- Web.Reputation.1
- Web.Reputation.3
- WS.Malware.2
- 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。

2025/05/09

Earth Kasha威脅份子在最近的網路攻擊行動中以台灣和日本為目標

趨勢科技研究人員最近回報，Earth Kasha 威脅組織持續以台灣和日本的使用者為攻擊目標。攻擊者利用內嵌巨集功能的 EXCEL 檔案來掩護稱為 RoamingMouse 惡意軟體植入器的感染。該攻擊鏈的後續階段也會使用 ANELLDR 惡意軟體載入器、Anel 後門的全新變種、SharpHide 工具以及第二階段 NoopDoor 後門。該攻擊行動被認為主要是針對潛在受害者的間諜活動，以及從受攻擊的端點竊取資訊。

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。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT

- Trojan.Gen.NPE
- 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。

2025/05/09

在針對巴西的惡意攻擊行動中部署遠端監控與管理(RMM)工具

Cisco Talos 研究人員報告一項針對巴西使用者的全新惡意網路攻擊行動。攻擊者利用各種商用遠端監控與管理 (RMM:Remote Monitoring and Management) 工具，例如：PDQ Connect 和 N-able 遠端存取軟體。攻擊鏈透過惡意垃圾郵件引爆，將受害者導向下載託管在 Dropbox 檔案共用上的惡意安裝程式。安裝該 RMM 工具後，攻擊者便可遠端存取受攻擊的端點。以這種方式取得的存取權／憑證，可被涉入惡意攻擊行動的初始入侵管道掮客或稱初始存取掮客 (Initial Access Broker：IAB) 出售給其他威脅份子。

網路知識：初始入侵管道掮客或稱初始存取掮客（Initial Access Broker:IAB），就是專門收集可存取特定組織的帳密資料的角色，可以想像為專門竊取大門鎖匙賣給小偷的人，如果重要的IT基礎架構的帳密被竊且轉賣給駭客，就如同門戶大開完全沒有門禁，任何的防護措施也都沒用。

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：

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。

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
- Web.Reputation.3
- 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。

2025/05/09

Mamona勒索軟體

Mamona 勒索軟體是在商品化勒索軟體商圈中新上架的新威脅，它完全是離線運作，沒有外部通訊或資料外洩。該惡意軟體使用自訂的加密規則來加密使用者檔案，並冠上 .HAes 副檔名。它採用混淆技術，例如：使用 ping 進行時間延遲，以避免被偵測到。儘管勒索 (贖金支付) 說明通知，宣稱資料會被竊取，但實際上並沒有資料外洩。已有功能性解密工具可讓受害者復原檔案。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.RansomPlay!gen1
- SONAR.Ransomware!g16

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。

- 賽門鐵克 EDR 能夠監控和標記該威脅攻擊者的策略、技術和程序 (Tactics、Techniques、Procedures，TTPs)。
- 賽門鐵克新增了特定惡意軟體的威脅搜尋查詢，客戶可以在 iCDM 控制台上觸發這些查詢。有關這些查詢的更多資訊，請參閱此鏈接：https://github.com/Symantec/threathunters/tree/main/Trojan/IcedID
- 賽門鐵克的端點偵測與回應 (EDR) 最新簡報檔，請點擊此處。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Gen
- Trojan Horse
- Trojan.Gen.MBT

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。

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**。