保安資訊--本周(台灣時間2025/08/01)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 33 萬 2,600 台受保護端點上總共阻止了 5,990 萬次攻擊。這些攻擊中有 85.3% 在感染階段前就被有效阻止：**(2025/07/28)**

- 在**8萬6,500**台端點上，阻止了**2,500**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**6萬9,500**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**2萬1,400**台**Windows**伺服主機上，阻止了**550**萬次攻擊。
- 在**5萬6,900**台端點上，阻止了**210**萬次嘗試掃描伺服器漏洞。
- 在**2萬4,000**台端點上，阻止了**160**萬次嘗試掃描在**CMS**漏洞。
- 在**5萬2,600**台端點上，阻止了**240**萬次嘗試利用的應用程式漏洞。
- 在**6萬1,600**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**1,200**台端點上，阻止了**66萬6,200**次加密貨幣挖礦攻擊。
- 在**9萬9,400**台端點上，阻止了**820**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**493**台端點上，阻止了**7萬6,200**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 500 個受保護端點上阻止了總計 1,250 萬次攻擊。**(2025/07/28)**

- 使用網頁信譽情資，在 **270.1K** 個端點上阻止 **11.9M** 次攻擊。
- 攔截 **27.6K** 個端點上 **427.5K** 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 **7K** 個端點上攔截 **190.9K** 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 **447** 個端點上攔截 **9.6K** 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。

2025/07/31

CVE-2025-6558--存在Google Chromium與ANGLE和GPU元件在處理未經驗證輸入時的驗證不足有關之漏洞

CVE-2025-6558 是最近揭露的不當輸入驗證漏洞，會影響 Google Chromium ANGLE(Almost Native Graphics Layer Engine 的縮寫) 和 GPU 元件。此漏洞源自於未信任輸入的驗證不足，一旦被開採濫用，遠端攻擊者可能會透過製作的 HTML 頁面執行沙箱逃脫。此漏洞已在上星期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，顯示該漏洞在真實網路情境中已遭大肆開採濫用。

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，預設會保護作業系統，防止透過特權服務漏洞的 RCE 以及關鍵檔案／資源的篡改。
- DCS IPS 政策中的 Google Chrome 自訂沙箱，可以控制哪些程式可以在此沙箱中執行。它也可以控制哪些資源可以被寫入或讀取。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2025/07/31

0bj3ctivityStealer惡意竊密軟體涉入的全球產業攻擊行動，採用圖片隱寫技術和就地取材攻擊手法

最近觀察到有人透過魚叉式網路釣魚電子郵件部署 .NET 型態的 0bj3ctivityStealer 惡意竊密軟體，該電子郵件包含指向 Mediafire 託管的 JavaScript 連結。這個腳本會從 Archive.org 圖片下載一個隱藏的惡意程式載入器式，利用程序空洞化方式注入最終的有效酬載。惡意程式會執行反分析檢查以逃避偵測，然後擷取敏感資料，包括瀏覽器憑證、即時通訊軟體的檔案、電子郵件用戶端憑證和加密貨幣錢包資料。外洩會透過 Telegram 機器人進行，並以 SMTP 作為備份通道。此攻擊行動以美國、德國和蒙特內哥羅的政府和製造業為目標，使用隱寫技術和就地取材 (LotL) 來逃避標準偵測機制。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Base64!g1
- ACM.Ps-Wscr!g1
- ACM.Untrst-RunSys!g1
- ACM.Wscr-Ps!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!gen1
- SONAR.Powershell!g85
- 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：

- Hacktool
- ISB.Downloader!gen48
- Phish.ScptML.L
- Scr.xSense!gen3
- 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.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: PowerShell Process Accessing Archive.org

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。

2025/07/31

CVE-2025-2775、CVE-2025-2776同時存在IT管理系統：SysAid地端自建版本的XXE漏洞

CVE-2025-2775 和 CVE-2025-2776 是兩個影響 IT 管理系統：SysAid 地端自建版本的 XML External Entity(XXE) 漏洞。如果成功被開採濫用，這些漏洞可能允許管理員帳戶被劫持並執行檔案讀取的基本操作。這兩個漏洞已在上星期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，顯示該漏洞在真實網路情境中已遭大肆開採濫用。

網路知識：XML external entity injection 也就是 XXE，可以透過惡意的請求查看伺服器之敏感資料，若可以搭配伺服器請求偽造 (SSRF) 攻擊，就可以從 XXE 到進階攻擊內部網路。許多網站透過 XML 格式的檔案進行傳輸，而後端所使用的函式庫或後端程式邏輯，針對 XML 處理的解析器預設開啟許多危險的功能，若沒有進行關閉或是限制，可能就會造成 XXE 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：

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: Malicious XML External Entity Payload Upload
- Web Attack: XML External Entity Attack

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，針對 SysAid 地端自建版本的自訂沙箱具有強化規則，可防止執行任意指令、資料或網路滲透，並可防止特定漏洞的被開採濫用。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2025/07/31

XWorm 6.0版本已出現在真實網路情境裡

惡名昭彰的 XWorm 惡意軟體 6.0 版已經在真實網路情境裡被發現。該惡意軟體具有更強的反分析和持久性功能。XWorm 6.0 版本在最初攻擊階段利用 VBScript 類型的惡意植入器，很可能是透過社交工程手法傳送。為了避免被偵測到，惡意軟體有能力使用 clr.dll 二進位檔的記憶體修補程式來繞過 Windows 反惡意軟體掃描介面工具 (AMSI：Antimalware Scan Interface)。XWorm 還附有預先已寫在程式碼內的命令與控制 (C&C) 伺服器位址。

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-RgPst!g1
- ACM.Ps-Wscr!g1
- ACM.Wscr-CNPE!g1
- ACM.Wscr-Ps!g1
- ACM.Wscr-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：

- ISB.Downloader!gen52
- ISB.Downloader!gen56
- MSIL.XWorm!gen2
- Scr.Malcode!gdn14
- Scr.Malcode!gdn20
- Scr.Malcode!gen120
- Scr.xSense!gen1
- Scr.xSense!gen3
- Web.Reputation.1
- Web.Reputation.3
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- 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。

2025/07/31

ArmouryLoader惡意程式載入器

ArmouryLoader 是去年首次出現在真實網路情境裡的惡意程式載入器，已知可用於傳送 CoffeeLoader 或 SmokeLoader 等附加有效酬載。此惡意軟體劫持華碩 Armoury Crate 系統管理軟體的匯出功能，將自身載入有漏洞的系統。ArmouryLoader 執行排程任務以確保常駐能力，並利用先進的程式碼混淆與反 EDR 功能來躲避偵測。

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

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
- 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!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。

2025/07/31

CVE-2025-27210--存在NodeJS的路徑遍歷漏洞

CVE-2025-27210 是最近被揭露的路徑遍歷漏洞，會影響 NodeJS。NodeJS 是開放原始碼、跨平台的 JavaScript 執行環境。此漏洞會影響如 CON、PRN 及 AUX 等 Windows 的預留裝置名稱，該漏洞是由於 Node.js 先前漏洞 CVE-2025-23084 的修補程式不完整所導致。若成功開採濫用此漏洞，攻擊者可能未經授權存取敏感檔案及機密資料。Node.js 團隊已在受影響的版本中發佈修補程式，以解決此漏洞。

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: NodeJS CVE-2025-27210

2025/07/31

LockBit勒索軟體的深入探討

在最近一份報告中，賽門鐵克與 Carbon Black 威脅獵捕團隊分析 LockBit 勒索軟體最近的活動。部署 LockBit 勒索軟體的攻擊者持續進化其戰術、技巧和程序 (TTPs)，以逃避偵測並將其影響力最大化。在他們複雜的武器庫中，有兩種技術因能有效隱藏惡意活動且脫穎而出：DLL sideloading 和 masquerading。

請參閱我們的部落格：揭開 LockBit 的真面目：深入探討 DLL 側載和偽裝技倆。

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.Psxec-Lnch!g1
- ACM.Psxsv-Net!g1
- ACM.Psxsv-Quser!g1
- ACM.Psxsv-Untrst!g1
- ACM.Untrst-RLsass!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.RansomGen!gen4
- SONAR.Ransomware!g1
- SONAR.Ransomware!g3
- SONAR.SuspLaunch!g559

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：

- PUA.Gen.2
- Ransom.Blackmatter!gm1
- Ransom.LockBit
- Trojan Horse

- Trojan.Gen.9
- 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
- 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: TeamViewer Remote Access Activity
- Audit: TeamViewer Remote Access Activity 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。

2025/07/30

安卓手機／行動裝置平台出現全新RedHook木馬程式

據報導，安卓手機／行動裝置平台出現全新 RedHook 木馬程式，目前已出現在對越南使用者的攻擊。此惡意軟體透過釣魚網站散佈，釣魚網站假冒合法的越南機構組織，例如：銀行和金融機構，誘騙使用者下載惡意 .APK 的 APP 安裝檔，惡意 APK 託管在暴露的 AWS S3 儲存貯體上。安裝後，RedHook 會濫用存取服務和覆蓋權限來竊取敏感資訊，包括登入憑證、簡訊資料和螢幕內容。它透過 WebSocket 與其命令與控制 (C&C) 伺服器通訊，並支援超過 30 種遠端命令，讓攻擊者能完全遠端控制裝置。

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
- AppRisk: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。

2025/07/30

SHUYAL惡意竊密軟體～還能停用Windows工作管理員的功能

最近發現惡意竊密軟體：SHUYAL 能夠擷取許多敏感資料，包括系統組態、使用者憑證、剪貼簿內容、螢幕截圖、系統瀏覽器資料和 Discord 認證識別碼。這些資訊隨後會透過 Telegram 機器人外流。惡意軟體還會透過登錄檔機碼的竄改來停用 Windows 工作管理員的功能。

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：

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.Dropper
- SONAR.Stealer!gen1
- SONAR.SuspBeh.C!gen5
- SONAR.SuspBeh.C!gen18
- SONAR.SuspDrop!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
- 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.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: 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。

2025/07/30

Oyster後門程式

Oyster 後門程式 (也稱為 Broomstick) 已在最近被回報的惡意廣告散播行動中被大肆傳送。攻擊者利用購買或操弄關鍵字排名的 SEO(搜尋引擎優化) 中毒手法，來提升其廣告託播在搜尋結果中的排名，並將毫無戒心的受害者引導至惡意網站，此惡意網站上架知名合法的應用程式 (如 PuTTy、KeyPass 或 WinSCP) 並加料特洛伊木馬安裝程式版本。後門一經執行，攻擊者便可收集系統資訊、執行任意指令、下載及執行後續的有效酬載等。

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-Schtsk!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.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。

2025/07/30

Soco404--全新加密劫持／惡意加密挖礦行動

據報導，一個被稱為 Soco404 的全新加密劫持／惡意加密挖礦行動已在真實網路情境上出現。此行動針對 Linux 和 Windows 系統，攻擊者將部署惡意二進位檔偽裝成合法的系統程序。在初始攻擊階段，威脅者開採濫用各種漏洞，包括存在 Apache Tomcat、Apache Struts 和 Atlassian Confluence 伺服器的漏洞，以及 PostgresSQL 的錯誤配置。

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-Sc!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.MalTraffic!gen1
- SONAR.SuspBeh!gen609
- SONAR.SuspDriver!gen1
- SONAR.SuspStart!gen6
- SONAR.SuspStart!gen9
- 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：

- PUA.Gen.2
- Trojan Horse
- Trojan.Coinminer
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- 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

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：

- System Infected: Coinminer Activity 5
- System Infected: Miner.Bitcoinminer Activity 8
- System Infected: Miner.BitcoinMiner Activity 11
- System Infected: Miner.Bitcoinminer Activity 16
- System Infected: Miner.Bitcoinminer Activity 27
- Web Attack: Apache Tomcat CVE-2025-24813

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。

2025/07/30

假冒Trip.com忠誠度計畫／獎勵計畫的新一波網路釣魚行動

賽門鐵克偵測到針對日本使用者的網路釣魚行動，該網路釣魚行動使用偽造的 Trip.com 電子郵件。Trip.com 是一家線上旅行社，提供機票、火車票、租車、旅遊、酒店等預訂平台。這些釣魚電子郵件的主旨是：會員特典変更のお知らせ -> (翻譯為：「會員權益異動通知」)

詐騙者利用大受歡迎的 Trip.com 點數計畫--讓客戶從旅遊預訂中賺取點數的忠誠度功能，精心製作詐騙性電子郵件。這些訊息通常會強調會員權益異動公告，目的是誘騙使用者按下釣魚連結並交出憑證。

網路知識：Trip.com 是攜程集團旗下的一家在線旅行社，其總部位於新加坡。Trip.com 提供機票、酒店、火車票、租車、機場接送、旅遊和景點門票的預訂服務。Trip.com 於 2017 年 10 月被攜程集團收購。

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。

2025/07/30

Raven惡意竊密程式

據報導，一個以 Delphi 和 C++ 寫成的惡意竊密程式，被稱為 Raven 。該惡意軟體利用記憶體內的 DLL 注入來避免偵測，並收集敏感資料，例如：瀏覽器憑證、加密錢包、系統資訊、VPN 用戶端等。它使用 Telegram 的 Bot API 將被盜取的資料打包成 .ZIP 壓縮檔，直接傳送到攻擊者的 Telegram 聊天室。此手法可讓惡意軟體隱蔽地混入正常的 HTTPS 流量至 Telegram API 而難以被發現。

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 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.B
- 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。

2025/07/30

Epsilon Red勒索軟體透過假冒的驗證頁面傳播

據報導，有威脅份子利用偽造的 ClickFix 式驗證網頁，誘騙使用者下載惡意 .HTA 檔案。這些頁面偽裝成可信任的線上平台，利用社交工程伎倆說服使用者執行有效酬載。一旦觸發，腳本就會在背景中默默下載並執行 Epsilon Red 勒索軟體，同時顯示假冒的確認訊息以掩蓋活動。Epsilon Red 是一種已知勒索軟體類型，它使用 PowerShell 和排程任務來進行持久化和檔案加密。

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，圖靈驗證等名義為誘餌，幾可亂真網頁或文件外觀，誘導使用者執行惡意指令。要求使用者點選特定按鈕，然後依照指示以快速鍵開啟執行視窗、貼上等操作來「修正」問題，但實際上，這麼做是將剛才暗中複製的惡意命令貼上並執行，使得駭客得以對受害電腦上下其手。

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

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh!gen678
- SONAR.SuspLaunch!g483

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.Cobalt
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

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

2025/07/29

防護亮點：手機行動裝置上的威脅形勢不斷進化，磨刀霍霍向加密貨幣使用者

隨著加密貨幣市場創下歷史新高，特別針對加密貨幣愛好者和使用者的手機行動裝置上的威脅也大幅增加。詐騙者以各種不同的方式利用人們對數位資產日益增加的興趣。威脅方式可能從簡單的簡訊網路釣魚攻擊 (誘騙使用者洩露機密資料) 到惡意 APP(專門竊取私密金鑰和加密錢包憑證)。

過去這幾年來，攻擊者越來越專注於手機行動裝置，將其視為取得使用者所持加密貨幣的最便捷途徑之一。本公告概述最近一些手機行動裝置威脅的趨勢，以及攻擊者針對行動加密貨幣使用者所採用的技倆。

簡訊網路釣魚攻擊又稱為 Smishing

簡訊網路釣魚攻擊，是指網路犯罪份子利用簡訊服務的文字訊息誘騙手機使用者透露敏感資訊。簡訊網路釣魚攻擊也可能引誘使用者點擊惡意連結，進而導致任意有效酬載的執行。在

加密貨幣的世界中，簡訊網路釣魚攻擊已經成為針對加密貨幣使用者最熱門的技倆之一，這主要是由於行動裝置在日常生活中的廣泛使用。在所觀察到的網路釣魚詐騙中，攻擊者通常會冒充合法加密貨幣平台的知名品牌，目的是讓受害者相信訊息的真實性，進而損害他們的加密貨幣資金。

山寨加密貨幣錢包和挖礦 APP

另一種常見導致加密貨幣資產受損的手法是散佈冒充合法供應商的偽造加密貨幣交易所、錢包或挖礦 APP。這些惡意 APP 透過各種途徑，包括直接網路釣魚、第三方 APP 商店、社交媒體上的貼文／廣告或偽裝成合法服務的詐欺網站／儲存庫，傳播給加密貨幣使用者。在行動裝置上安裝後，攻擊者會透過鍵盤側錄技術或冒充受害者熟悉的合法加密貨幣錢包 APP，從特定加密貨幣錢包中竊取憑證。

Crypto-Clipping 惡意軟體

此手機行動裝置上的惡意軟體稱為 Crypto-Clipper，具有截取剪貼簿資料的功能，主要針對加密貨幣的錢包地址。在偵測到使用者複製加密貨幣錢包地址進行交易的活動後，惡意軟體會將其取代為攻擊者控制的地址。在成功取代加密貨幣錢包地址後，加密貨幣會直接轉移到攻擊者的錢包，造成受害者的財務損失。此類惡意軟體通常透過從非官方來源下載、特洛伊木馬或其他假冒的 APP 所散佈。

使用 OCR(光學字元辨識) 技術從影像中擷取資料

行動威脅領域最近一項發展，是惡意應用程式能夠在光學字元識別 (OCR) 技術的協助下，竊取加密貨幣資訊。最近幾種利用 OCR 竊取加密貨幣相關資訊的惡意軟體有 SpyAgent、SparkCat 以及新發現的 SparkKitty。這些惡意軟體變種能夠掃描本機裝置儲存區和雲端儲存庫中的加密貨幣資訊。涵蓋加密錢包憑證、私鑰、恢復短語 (recovery phrase)，甚至是以影像檔儲存的財務文件。一旦有找到，惡意軟體就會運用 OCR 技術從影像檔案中擷取敏感資訊，隨後將其傳送到威脅份子所控制的伺服器。

加密錢包種子短語(seed phrase)的收集成為重點

種子短語 (seed phrase，也稱為恢復短語 (recovery phrase) 或助記詞 (Mnemonic phrase))，助記詞是一組 12、15、18、21 或 24 個單詞 (符合 BIP39 標準)，用來生成私鑰。它是私鑰的可讀形式，方便人類記憶與備份。助記詞可以恢復錢包內的所有私鑰，因此必須妥善保管，不可洩漏。當加密貨幣錢包遺失或無法在之前使用的行動裝置上存取時，種子短語對於復原加密貨幣錢包非常重要。種子短語實際上被視為主備份金鑰，允許完全恢復加密貨幣錢包的存取權。因此，它也需要額外的保護步驟，以隨時保持安全性，例如：建議使用物理離線儲存。但實際上，加密貨幣使用者通常會將種子短語儲存為本機磁碟機上的影像。無論是透過竊取資訊的惡意軟體、社交工程或其他途徑而言，這種高風險的行為大大增加竊取的威脅。Crocodilus 是最近專門針對收集和滲透錢包種子短語的惡意 APP 家族之一。

正在發展的 SIM 卡挾持攻擊／SIM卡交換攻擊 (Sim Swapping) 趨勢

SIM 卡挾持攻擊或稱 SIM 卡交換攻擊 (Sim Swapping) 是一種網路攻擊，威脅者在未經授權的情況下取得受害者電話號碼的控制權。這可以透過誘騙行動電話服務供應商將受害者的電話號碼移植到攻擊者控制的 SIM 卡上來實現。對大多數加密貨幣使用者而言，簡訊傳送的 2FA(雙因

素驗證) 是存取加密貨幣交易所和錢包的主要安全機制。當攻擊者取得受害者電話號碼的控制權時，他們可以截取時效性高的 2FA 驗證碼，並取得存取持有其加密資產的錢包之權限。

預載 APP 的危險

正如今年早些時候媒體所報導，未經核准的製造商在低階智慧手機上，預載的惡意 APP 對手機行動裝置上之加密貨幣用戶構成另一個重大威脅。這些裝置經常模仿受歡迎的智慧型手機品牌，甚至採用相似的裝置名稱。例如：最近披露的事件包含模仿流行 WhatsApp 和 Telegram 訊息聊天工具的惡意 APP，一般使用者在購買新手機時很可能不會質疑這些 APP 的存在。交付的惡意軟體能夠竊取敏感的使用者資料，並更改聊天對話中分享的加密貨幣位址。

對照 MITRE ATT&CK 策略和技術知識庫的攻擊鏈

威脅份子利用各種 MITRE ATT&CK 對應的攻擊手法，針對行動加密貨幣使用者進行攻擊，以獲取財務利益，其中一些技術包括：

- 初始存取：應用程式版本控制：T1661--駭客可能會推送更新給先前正常的應用程式，以加入惡意程式碼。
- 初始存取：驅動式惡意入侵：T1456--攻擊者可能會透過使用者在正常瀏覽過程中所瀏覽的網站來存取系統。
- 初始存取：網路釣魚：T1660--攻擊者可能發送惡意內容給使用者，以存取他們的行動裝置。
- 初始存取：SIM 卡交換：T1451--攻擊者可能透過將受害者的電話號碼轉移或交換給他們控制的 SIM 卡及行動裝置，以取得行動裝置的存取權。
- 初始存取：供應鏈入侵：T1474--為了入侵資料或系統，攻擊者可能會在最終消費者收到產品之前，篡改產品或產品交付機制。
- 收集：剪貼簿資料：T1414--惡意使用者可能會濫用剪貼簿管理程式 API，以取得複製到裝置剪貼簿的敏感資訊。
- 收集：輸入擷取：鍵盤記錄 T1417.001--惡意份子可能會記錄使用者的按鍵動作，以便在使用者輸入憑證或其他資訊時擷取這些資訊。
- 收集：螢幕截取 T1513--攻擊者可能使用截取螢幕來收集目標裝置的其他資訊，例如：在前台執行的應用程式、使用者資料、憑證或其他敏感資訊。
- 滲透：透過 C2 頻道滲透：T1646--攻擊者可能透過現有的指揮與控制通道滲透資料，進而竊取資料。
- 影響：資料操控：傳輸資料竄改：T1641.001 T1641.001--為了操控外部結果或隱藏活動，攻擊者可能會更改傳送至儲存庫或其他系統的資料。舉例：Clipper 惡意軟體活動。

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：

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.1
- 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。

欲了解有關賽門鐵克的重要主機防護系統：Data Center Security(DCS) 更多資訊，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。

2025/07/29

威脅組織Dropping Elephant對土耳其導彈系統製造商發動攻擊行動

威脅組織 Dropping Elephant(也稱為 Chinastrats 或 Patchwork) 一直專門針對土耳其一家精準導彈系統製造商。攻擊鏈是透過高度針對性的魚叉式網路釣魚電子郵件啟動，運用社交工程策略，將惡意 .LNK 捷徑檔偽裝成會議邀請函，特別針對無人機系統感興趣的個人。.LNK 檔案執行後，會觸發複雜的五階段感染程序。此過程會利用 PowerShell 從遭入侵的網域下載惡意軟體。Dropping Elephant 利用 VLC 多媒體播放器和 Microsoft 工作排程等合法程式作為攻擊鏈的一部分。透過使用 DLL 側載技術，他們能有效繞過一般的安全措施，將惡意程式碼深入嵌入受攻擊的系統中，以取得存取權限、執行指令及滲透資料。

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-Rd32!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：

- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- 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

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

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。

2025/07/29

威脅份子偽造日本新幹線的線上預訂服務以竊取註冊會員的憑證

賽門鐵克發現新一波的網路釣魚攻擊，冒充日本新幹線的訂位服務，以竊取註冊會員的憑證。在這一波攻擊中，釣魚電子郵件偽裝成要求立即更正和確認註冊電子郵件位址的通知。收件人會被告知，如果不這樣做，可能會導致服務中斷。電子郵件內容簡短，鼓勵收件人點選釣魚網址 (URL)。一旦點擊，受害者就會遇到專門用於收集憑證的網頁。

- 電子郵件主旨：【EX予約】メールアドレスの確認
- 翻譯的電子郵件主旨：[EX 預約] 確認您的電子郵件位址

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。

2025/07/29

Koske：Linux平台出現的全新惡意軟體，透過貓熊(Pandas)圖片傳播

安全研究人員發現一種新的 Linux 惡意軟體 Koske，據觀察該惡意軟體是透過貓熊 (Pandas) 圖片散佈。Koske 疑似由人工智慧 (AI) 產生，是一個 Linux 平台上的模組化惡意軟體，可能會以 rootkit 或用來執行不同功能的 shell script 形式出現，例如：下載惡意挖礦程式。這些有效酬載已被發現到附加在貓熊 (Pandas) 圖片中，然後直接在記憶體中執行，試圖繞過預防性的安全措施。

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：

- Hacktool.Rootkit
- PUA.Gen.2
- Trojan Horse
- Trojan.Gen.NPE

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。

2025/07/28

SarangTrap敲詐勒索行動～安裝APP務必提高警覺

據報導，一種名為 SarangTrap 的 Android APP 敲詐勒索行動，假冒約會或社交網路 APP，以該使用者為目標。此敲詐勒索行動利用誘人的邀請碼和令人信服的使用者介面，對受害者進行情緒操縱，然後要求過高的權限，以存取連絡人、照片、簡訊、裝置識別資料等。一旦安裝，這些 APP 會悄悄地滲出個人資料，攻擊者會利用這些資料威脅受害者，或在非法平台上濫用竊取來的內容賺錢。

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。

2025/07/28

Gunra勒索軟體～源於Conti勒索軟體程式碼的強化版

2025 年 4 月中旬首次發現到一種名為 Gunra 的全新勒索軟體，是源於已洩露的 Conti 勒索軟體程式碼為基礎，並加以強化，目的在增加社交工程壓力並加速勒索談判。它使用強大的加密演算法 (RSA 和 ChaCha20)，並根據受害者的 CPU 核心數調整任務數量，以最佳化檔案加密速度。一旦執行，Gunra 會為被加密的檔案冠上 .ENCRT 副檔名，並避開資源回收桶和可執行檔案等系統關鍵位置，刪除磁碟區陰影複本，並注入名為「R3ADM3.txt」的勒索贖金支付通知，內容指示受害者存取攻擊者的暗網入口網站，並支付解密費用。

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：

自適應防護技術(包含於SESC)：

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

基於行為偵測技術(SONAR)的防護：

- SONAR.Cryptlck!g171
- SONAR.Ransom!gen56
- SONAR.SuspLaunch!g193

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.Cobalt
- Ransom.Gen
- 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

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。

2025/07/28

UNG0901網路間諜行動利用EAGLET後門攻擊VASO(俄羅斯的沃羅涅日飛機製造股份公司)

一起網路間諜行動一直以俄羅斯的航太與國防產業為目標，目的在透過名為 EAGLET 的後門將敏感資料外洩。負責此次行動的威脅團體被認定為 UNG0901。此行動主要針對 Voronezh Aircraft Production Association(VASO：俄羅斯的沃羅涅日飛機製造股份公司) 的員工，VASO 是俄羅斯飛機製造的重要企業。攻擊者利用對俄羅斯物流作業非常重要的「運輸託運單」文件作為誘餌。

此攻擊通常會以魚叉式網路釣魚電子郵件開始，其設計會模仿合法的貨物遞送通知。這些電子郵件包含一個 ZIP 壓縮檔，內含 Windows 捷徑 (LNK) 檔案。執行時，此 LNK 檔案會利用

PowerShell 顯示一個看似無害的誘餌文件，將 EAGLET DLL 悄悄植入受害者的系統。簡而言之，該攻擊行動利用惡意 LNK 檔案和自訂 DLL 植入程式 (代號 EAGLET) 來取得存取權限、執行指令和滲透資料。

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-Rd32!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLoad!g49

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
- CL.Downloader!gen241
- Scr.Heuristic!gen20
- Scr.Mallnk!gen10
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- 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
- 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。

2025/07/28

EdskManager遠端存取木馬(RAT)

EdskManager 遠端存取木馬 (RAT) 已被發現涉入多階段感染鏈的網路攻擊，從偽裝成合法軟體的惡意程式載入器開始。它會擷取加密的 .edskv 設定檔，在記憶體中解密並使用 zlib 壓縮的 socket 流量與 C&C 伺服器通訊，同時也會使用備援網域來確保連線的穩定。其主要功能是 HVNC，可透過隱藏視窗實現隱形遠端控制。惡意軟體透過工作排程和修改登錄檔機碼來取得常駐能力，同時使用記憶體混淆、API 掛鉤和偵錯程式偵測等規避伎倆，使其成為隱匿的長期威脅。

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：

- Downloader.Upatre
- 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.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
- 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。

2025/07/28

LameHug惡意軟體支援LLM(大型語言模型)的指令生成功能

據報導，一種被稱為 LameHug 的全新 Python 類型惡意軟體利用 LLM(大型語言模型) 在受感染的端點上產生指令。LameHug 透過 Hugging Face API 使用開源 LLM Qwen 2.5-Coder-32B-Instruct 來根據靜態描述產生可執行程式碼或任意 shell 指令。最近觀察到此惡意軟體系列的散佈，屬於 Swallowtail 威脅組織 (也稱為 APT28 或 UAC-0001)。此惡意攻擊行動著重於偵察與資訊竊取活動。

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：

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：

- Infostealer
- 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。

2025/07/28

Ghost Crypt在加密目標攻擊中提供PureRAT

2025 年 5 月，有人觀察到網路釣魚行動透過稱為 Ghost Crypt 的新型加密器傳送 PureRAT。惡意 PDF 連結至 Zoho WorkDrive ZIP 檔案，其中包含偽裝的可執行檔和 DLL。一旦被執行，Ghost Crypt 就會側載 DLL，DLL 會解密並使用程序催眠將 PureRAT 注入 csc.exe。此惡意軟體以 Chromium 瀏覽器和桌面應用程式中的加密錢包為目標，透過修改登錄檔機碼來取得常駐能力，並防止系統休眠以保持不被偵測。

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：

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.Dromedan
- Scr.Malcode!gdn32
- Trojan Horse
- Trojan.Gen.MBT
- W32.Faedevour!inf
- W32.Fixflo.B!inf
- W32.Wabot
- 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.B

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**。