保安資訊--本周(台灣時間2025/03/21)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 38 萬 1,300 台受保護端點上總共阻止了 4,000 萬次攻擊。這些攻擊中有 80.8% 在感染階段前就被有效阻止：**(2025/03/18)**

- 在**7萬7,800**台端點上，阻止了**1,310萬**次嘗試掃描**Web**伺服器的漏洞。
- 在**8萬2,300**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**2萬4,900**台**Windows**伺服主機上，阻止了**540萬**次攻擊。
- 在**4萬7,800**台端點上，阻止了**160萬**次嘗試掃描伺服器漏洞。
- 在**9萬8,000**台端點上，阻止了**62萬9,400**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**10萬7,900**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**1,300**台端點上，阻止了**83萬700**次加密貨幣挖礦攻擊。
- 在**11萬1,000**台端點上，阻止了**690萬**台次向惡意軟體**C&C**連線的嘗試。
- 在**542**台端點上，阻止了**8萬700**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。**(2025/03/18)**

- 使用網頁信譽情資，在 **159.6K** 個端點上阻止 **710** 萬次攻擊。
- 攔截 **19.6K** 個端點上 **280.9K** 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 **5.6K** 個端點上攔截 **98.5K** 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 **169** 個端點上攔截 **3.1K** 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。

2025/03/20

台灣小心～最近針對台灣機構組織由UAT-5918 APT駭客集團發動的惡意活動

來自 Cisco Talos 研究人員報告一場針對台灣機構組織的長期攻擊活動，並將其歸屬於 UAT-5918 APT 駭客集團。據了解，攻擊者通常透過漏洞利用取得目標環境的存取權。此威脅份子利用各種 web shell、開放源碼工具、網路監控工具、憑證竊取器等。根據已公佈的報告，UAT-5918 集團所進行的行動與其他幾個威脅份子 (例如：Volt Typhoon、Flax Typhoon、Earth Estries 和 Dalbit) 所採用的戰略、手段、流程 (TTPs) 有一定的相似性。

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.SuspLaunch!g445
- SONAR.TCP!gen1
- 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：

- Hacktool
- Infostealer
- Trojan Horse
- 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

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。

2025/03/20

DarkCrystal遠端存取木馬程式在UAC-0200惡意行動中被大肆散佈

根據烏克蘭電腦緊急應變小組 (CERT-UA) 最近發佈的警報，烏克蘭已偵測到新一輪針對國防部門的攻擊。這個被稱為 UAC-0200 的攻擊行動透過 Signal messenger 散發惡意訊息，導致受害者執行 DarkTortilla 惡意軟體載入器，進而解密並執行 DarkCrystal RAT (也稱為 DCRat) 的有效酬載。DarkCrystal RAT 是一種知名的模組化遠端存取木馬程式，其功能包括執行指令、遠端控制和資料滲出等。

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-Wscr!g1
- ACM.Untrst-RunSys!g1
- ACM.Wscr-Cmd!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh.C!gen18
- 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：

- Backdoor.DCRat
- ISB.Malscript!gen25
- Scr.Malcode!gdn32
- Scr.Malscript!gen4
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE.C
- 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：

- System Infected: Trojan.Backdoor Activity 721
- 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。

2025/03/20

RansomHub勒索軟體聯盟部署的自訂Betruger後門

博通公司旗下的賽門鐵克威脅獵手團隊觀察到一個可與 RansomHub 勒索軟體聯盟有關聯的自訂後門活動。RansomHub 是一種勒索軟體即服務 (Ransomware-as-a-Service) 產品，而這個後門被命名為 Betruger。這是一個多功能後門，似乎是專為執行勒索軟體攻擊而開發。Betruger 結合勒索軟體攻擊時通常會使用的多種工具功能。相信這是為了在攻擊過程中減少所需不同工具的數量，以減少攻擊的足跡。部分功能包括：

- 擷取螢幕截圖
- 竊取憑證
- 按鍵紀錄
- 網路掃描
- 權限升級

我們的部落格文章有更深入的說明：RansomHub：攻擊者利用新的自訂後門。

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.Ps-SvcReg!g1
- ACM.Rcln-Lnch!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：

- Backdoor.Betruger
- Backdoor.Cobalt
- Backdoor.Trojan
- Backdoor.SystemBC
- Hacktool
- Ransom.Ransomhub!g1
- Trojan.Dropper
- Trojan.Gen.2
- Trojan.Gen.MBT
- 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
- 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。

2025/03/19

全新隱匿式惡意軟體行動利用JPEG檔案來散佈惡意竊密程式

一個全新的隱藏式惡意軟體攻擊行動已被發現，它利用 JPEG 圖檔散佈各種惡意竊密程式。此攻擊會先引誘使用者下載經混淆的 JPEG 檔案，其中包含隱藏的惡意腳本和可執行程式。一旦被執行，這些腳本就會從瀏覽器、電子郵件用戶端和 FTP 應用程式中擷取敏感憑證和資料。惡意軟體隨後會觸發一連串事件，下載額外的有效酬載，包括可自訂的惡意竊密程式，例如：Vidar、Raccoon 和 Redline。

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-Wscr!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。

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：

- CL.Downloader!aat171
- ISB.Downloader!gen80
- ISB.Heuristic!gen5
- ISB.Houdini!gen6
- Scr.Malcode!gen
- Hacktool
- Trojan Horse
- Trojan.Malimg

基於機器學習的防禦技術：

- 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。

2025/03/19

濫用假冒的圖靈(CAPTCHA)驗證機制引誘受害者執行惡意指令來散播rootkit

又有一起假冒圖靈 (CAPTCHA) 驗證機制的網路攻擊行動正在氾濫，導致 rootkits 被部署到毫無戒心的受害者電腦上。此攻擊透過假冒熱門軟體工具和網站的假冒驗證碼散佈，驗證碼使用 curl 將惡意的 Powershell 指令複製到使用者剪貼簿，並提供如何執行指令以證明他們是真人而非機器人。實際上，這個腳本會部署一個 .BAT 檔案，在受害者的電腦上安裝 rootkit。

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

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh!gen6
- SONAR.SuspBeh!gen752
- SONAR.SuspBeh!gen93
- SONAR.SuspDataRun

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.Suspexec!gen152
- CL.Suspexec!gen52
- Scr.Malcode!gdn14
- Scr.Malcode!gdn20
- Scr.XSNet!sr1
- Trojan.Gen.MBT
- Trojan.Gen.NPE.C
- Trojan.Remcos
- 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
- 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。

2025/03/19

CVE-2024-27564--去年公布的ChatGPT附加元件SSRF漏洞，出現實際的攻擊行動

有新的報告指出，威脅份子正大肆濫用較舊的伺服器端請求偽造 (SSRF) 漏洞 (CVE-2024-27564)，影響 OpenAI 的 ChatGPT。此漏洞存在於 ChatGPT Commit f9f4bbc，這是一個開放原始碼 GitHub 上的 PHP 專案。若成功開採濫用該漏洞，攻擊者可將製作的網址 (URL) 注入輸入參數，迫使應用程式進行任意請求。據報導，此漏洞的嘗試攻擊目標為美國的政府機構。

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: ChatGPT commit f9f4bbc SSRF CVE-2024-27564

2025/03/19

NailaoLocker勒索軟體

NailaoLocker 是去年在針對歐洲多個醫療機構攻擊行動中散佈的勒索軟體。發動攻擊的主使者，在攻擊的初始階段濫用先前已揭露存在 Check Point 安全閘道漏洞 CVE-2024-24919。勒索軟體有效酬載被解密，並利用 NailaoLoader 這支惡意軟體下載器的幫助下載到記憶體。成功感染後，NailaoLocker 會加密用戶資料，並冠上「.locked 」副檔名。勒索 (贖金支付) 說明檔案是以 .html 檔案的形式注入，建議受害者聯絡攻擊者以取得進一步指示。拆解其攻擊鏈發現，攻擊者也向受害者傳送 ShadowPad 和 PlugX 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：

基於行為偵測技術(SONAR)的防護：

- SONAR.RansomNailo!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：

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

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：

- Web Attack: CheckPoint Gateway Information Disclosure CVE-2024-24919

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。

2025/03/19

AnubisBackdoor：與Coreid APT駭客集團有關的全新Python惡意軟體

一個被稱為 AnubisBackdoor 相對較新的後門惡意軟體，在真實網路情境上被發現。這個以 Python 程式語言撰寫的後門惡意軟體是由 Savage Ladybug 駭客集團所開發，據報導該駭客集團與惡名昭彰的 Coreid(aka Fin7) APT 駭客集團有關聯。該惡意軟體的設計目的是授予遠端存取權、執行命令，以及進行資料外洩，同時避開大多數防毒軟體的偵測。初期 Anubis 惡意軟體以針對 Android 裝置的銀行特洛伊木馬功能而聞名，而 AnubisBackdoor 則不同，它是專為其他平台的遠端指令執行和系統入侵而設計。

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：

- Backdoor.Trojan
- Trojan Horse

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。

2025/03/19

CVE-2025-27636--存在較舊版本Apache Camel的訊息標頭插入漏洞

CVE-2025-27636 是一個最近發現的繞過／插入攻擊弱點，會影響 Apache Camel，這是一個熱門的開源整合框架。該漏洞若成功被開採濫用，遠端攻擊者可向請求注入任意標頭，進而執行 Camel 的語法。產品供應商已發佈修補此漏洞的 Apache Camel 版本。

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-2025-27636

2025/03/19

StilachiRAT惡意軟體

StilachiRAT 是微軟研究人員最近發現一種全新的遠端存取木馬。該惡意軟體具有廣泛的遠端控制和資訊竊取功能。它會收集受感染裝置的相關資訊、憑證、剪貼簿資料，並針對超過 20 種不同加密貨幣錢包的 Google Chrome 擴充套件進行資料滲出。StilachiRAT 採用多種反分析和迴避技術，包括事件日誌刪除、登錄檔機碼篡改、沙箱迴避行為等。該惡意軟體還支援 RDP 對話監控，並執行從攻擊者控制的 C&C 伺服器接收的指令。

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：

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
- WS.Malware.2

基於機器學習的防禦技術：

- 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。

2025/03/18
防護亮點：Carbon Black Endpoint Standard有效阻擋勒索軟體

現今檯面上數百家爭鳴之勒索軟體家族是一個蓬勃發展的威脅生態。不單單只是對檔案加密之外，源於相同勒索軟體家族的後繼新變種也各出奇招，出現越來越多的新變種並整合無檔案的威脅技術。數十年來，駭客勒索軟體隨著時間推進與新技術發展而變得越來越複雜，因此對網路安全專家造成嚴峻的挑戰。在 2025 年 1 月，我們發現勒索軟體攻擊激增，但 Carbon Black Endpoint Standard 成功阻擋這些攻擊。在所有情況下，客戶都能避免檔案被加密。

Carbon Black Endpoint Standard

Carbon Black Endpoint Standard 透過整合代理程式的統一平台提供端點防護，並運用行為分析來強化偵測、預防及對應網路攻擊。Carbon Black Endpoint Standard 透過單一代理程式和主控台簡化端點安全功能，提供更快、更有效的修復功能，並提供端點上執行程序的高能見度和詳細的情境脈絡。

- 阻止已知和未知的惡意軟體、勒索軟體和外來攻擊
- 採用多重防護層，包括檔案信譽和啟發式、機器學習和行為模型
- 開箱即用且能依環境自訂的防禦政策
- 整個攻擊鏈的可見性，以便調查
- 可遠端 shell 進入端點以立即採取行動
- 單一代理程式與主控台的雲端原生平台

熱門的勒索軟體家族

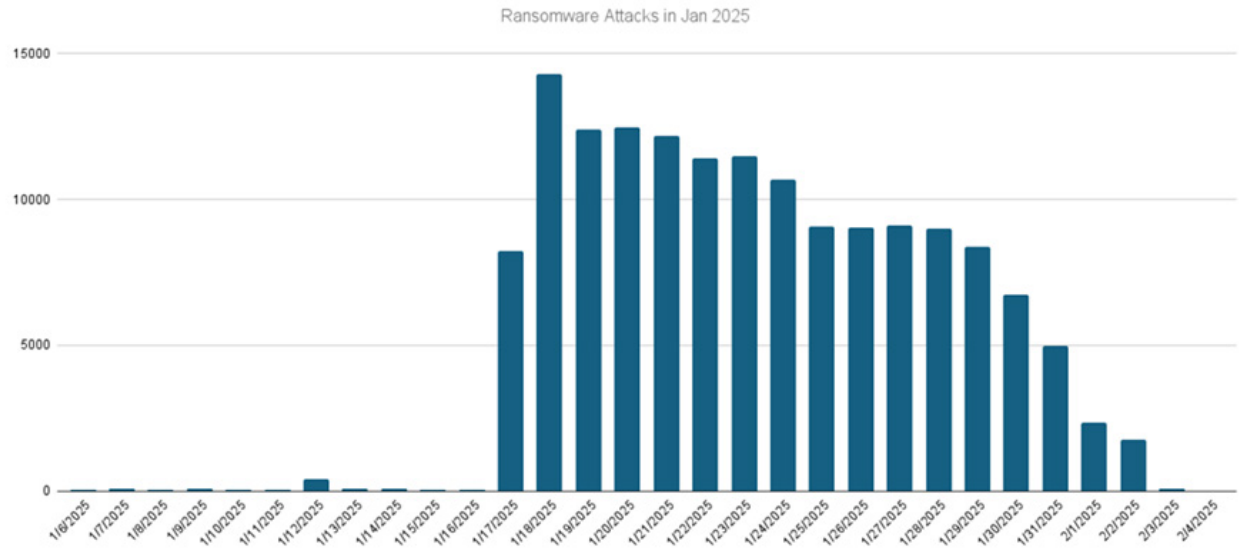
以下勒索軟體家族是涉入 2025 年 1 月網路攻擊的主要威脅者。

- **Cactus**：是採用雙重勒索手法的勒索軟體體，會加密受害者的資料，如果受害者拒絕支付贖金，還會洩露資料。它通常利用虛擬私人網路 (VPN) 軟體的漏洞來取得初始存取權。一旦完成加密和檔案滲出，惡意軟體就會在使用者的電腦上張貼勒索 (贖金支付) 通知。
- **RansomHub**：使用多種演算法組合來加密使用者資料，然後要脅贖金以還原檔案。如果受害者拒絕支付，攻擊者會威脅要出售或公佈竊取的資訊。它還具有透過網路傳播的能力。與其他勒索軟體一樣，它會刪除磁碟區陰影複本並停用 Windows 自動啟動修復功能，以確保資料無法輕易還原。
- **Blacksuit**：利用多種初始存取媒介，包括網路釣魚活動、RDP 漏洞利用。它會加密和滲出受害者的資料，並洩露那些不乖乖就範付贖金的受害者資料。惡意軟體的功能包括停止與虛擬機器環境相關的程序、停止特定的 Windows 服務，以及刪除受攻擊系統的磁碟區陰影複本。

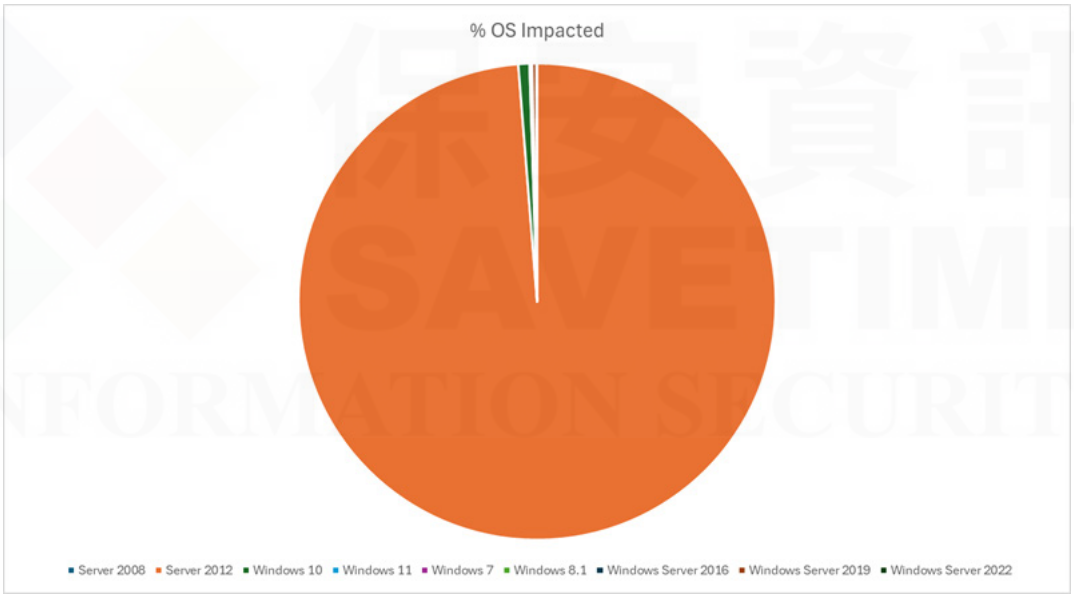
拆解其攻擊鏈發現其在加密檔案之前，有許多前置的變動系統設定的作業：

- 使用 vssadmin.exe／wmic.exe 刪除陰影複本
- 使用 bcdedit.exe 竄改開機設定以停用復原功能
- 使用排程任務來持續執行和提升權限
- 使用 msiexec.exe 透過軟體 GUID 卸載常見的防毒軟體

下圖為 2025 年 1 月的資料，顯示 Carbon Black Endpoint Standard 所阻擋的勒索軟體攻擊。



下圖顯示勒索軟體所針對的作業系統版本。98% 的攻擊以 Win Server 2012 為目標。



欲了解更多關於 Carbon Black Endpoint 的資訊，請點擊此處。

2025/03/18

發現基於JPHP的全新惡意軟體下載器

最近觀察到一個使用 JPHP 編譯的新型惡意軟體下載器。JPHP 是一種直譯 (Interpreter)，可讓 PHP 腳本在 Java 虛擬機器中執行。此惡意軟體原本以 ZIP 檔案傳送，並利用 Telegram 進行 C&C 通訊。潛在的下載有效酬載包括資訊竊取程式，例如：Danabot。

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.Maljava!g6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Trojan.Gen.MBT
- Trojan.Maljava
- WS.Malware.1

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。

2025/03/18

VenomRat惡意軟體行動使用VHD檔案進行資料外洩

在真實網路情境上發現到 VenomRat 惡意軟體涉入的攻擊行動中，有使用到 VHD 檔案。此攻擊的導火線是由一封釣魚電子郵件所觸發，其中包含一個偽裝成採購訂單的壓縮檔附件來引誘使用者。壓縮檔內有一個 .vhd 檔案，開啟時會掛載為硬碟。VHD 映像包含一個經過嚴重混淆的批次腳本，可透過 PowerShell 執行惡意動作。腳本會將受害者的敏感資料滲透到攻擊者操控的 C&C 伺服器，而 C&C 伺服器則託管在合法平台 Pastebin 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.Ps-Base64!g1
- ACM.Ps-Wscr!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。

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：

- CL.Downloader!aat1
- Downloader
- Scr.Malcode!gen
- Trojan Horse

- Trojan.Gen.2
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.B!100

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。

2025/03/18

macOS平台的惡意軟體：XCSSET出現最新變種

根據最近的報導，微軟的研究人員發現 MacOS 平台上模組化惡意軟體 XCSSET 的全新變種。XCSSET 於 2020 年首次被發現，是一種精密的模組化惡意軟體，已知會透過感染 Apple Xcode projects 來攻擊使用者。

CSSET 最新變種導入增強的混淆技術、優化持久性機制和翻新感染策略，同時保留其原有的功能，即從數位錢包、聊天應用程式、網頁瀏覽器、合法 Notes 應用程式的資料中竊取敏感資訊，以及滲出系統資訊和檔案。

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：

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。

檔案型(基於回應式樣本的病毒定義檔)防護：

- OSX.Trojan.Gen
- OSX.Xcsset
- 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。

2025/03/17

Sobolan惡意軟體涉入新一波的網路攻擊行動

網路駭客利用已遭入侵的互動式運算環境 (例如：Jupyter Notebooks) 來發動多階段 Sobolan的惡意軟體攻擊。初始攻擊，攻擊發動者濫用配置不當，透過未經認證的 JupyterLab 實例來取得初始存取權。攻擊者從遠端伺服器下載壓縮檔案，一旦執行，便可部署多個惡意工具組和惡意挖礦程式。

網路上的知識：Jupyter Notebook 是一個開源的網頁應用，它允許用戶建立和分享包含即時程式碼、數學方程、可視化和解釋性文本的文件檔。這個平台適合做實驗、數據分析，而且還支持多種程式語言，例如：Python、R 和 Julia。

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：

- PUA.Gen.2
- Trojan.Gen.MBT
- WS.SecurityRisk.3
- 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。

2025/03/14

OctoV2手機／行動裝置惡意程式以假冒的DeepSeek AI的APP大肆散佈

最近，在 Android 平台上的 OctoV2 銀行惡意程式的最新變種假冒 DeepSeek AI 手機應用程式 (APP) 大肆散佈。DeepSeek 是一款最近發布的人工智慧聊天機器人，與已知的 ChatGPT 非常相似。惡意 OctoV2 二進位檔從偽裝成 DeepSeek AI 入口網站的釣魚網站散佈。部署的惡意軟體使用 DGA(網域生成演算法) 進行 C&C 通訊，並執行從攻擊者接收的指令。

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：

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。

2025/03/14

SuperBlack--源於Lockbit勒索軟體的最新變種

SuperBlack 是源於被洩露的 Lockbit 勒索軟體之最新變種。根據報導，最近觀察到此惡意軟體涉入的威脅行動與被稱為 Mora_001 的威脅攻擊者 (可能與 Lockbit 有所關聯)。據報導，攻擊者在攻擊的初始階段會濫用 Fortinet Firewall 的已知漏洞 (CVE-2024-55591 和 CVE-2025-24472)。在部署勒索軟體二進位檔的同時，攻擊者也會執行曾經涉入 BrainCipher 勒索軟體的舊式攻擊行動中的 Wiper 元件。

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.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.UACBypass!gen30

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.Blackmatter!gm1
- Ransom.Gen
- Ransom.Lockbit!g6
- 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

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。

2025/03/14
LithiumWare勒索軟體

LithiumWare 是在真實網路情境中發現到的全新勒索軟體。該惡意軟體會加密檔案，並冠上四個字元的隨機副檔名。LithiumWare 會在啟動資料夾中添加開機啟動應用，並透過修改 Windows 登錄檔 (Registry) 來設定每次系統啟動時的排程執行，以確保其在受感染端點上的持久性／常駐能力。成功加密檔案後，勒索軟體會在每個加密資料夾中注入勒索 (贖金支付) 說明。它還會變更受感染電腦的桌面背景。LithiumWare 還具有刪除備份和卷冊陰影副本的額外功能。

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-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh.C!gen18
- SONAR.SuspDrop!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.HiddenTear!g1
- Ransom.Sorry
- WS.Malware.1

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

2025/03/14
Vedalia駭客組織與Android生態的全新KoSpy間諜軟體有關聯

KoSpy 是最近新發現的 Android 生態系間諜軟體，與北韓進階持續威脅 (APT) 駭客組織--Vedalia(也稱為 APT37 ScarCruft) 有關聯。該間諜軟體被觀察到偽裝成許多公用程式來誘騙受害者。以下僅列出 KoSpy 的部分功能：

- 收集簡訊內容或通話記錄
- 下載附加外掛程式以增強功能
- 擷取螢幕截圖

- 按鍵側錄
- 錄製音訊或視訊

據了解，Vedalia 駭客組織主要以韓國為目標，但也活躍於亞洲、歐洲和中東的其他國家。

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。

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**。