保安資訊--本周(台灣時間2025/04/11)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 6,100 台受保護端點上總共阻止了 4,870 萬次攻擊。這些攻擊中有 85.9% 在感染階段前就被有效阻止：**(2025/04/07)**

- 在**7萬9,900**台端點上，阻止了**2,070**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**7萬3,700**台端點上，阻止了**540**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬4,500**台**Windows**伺服主機上，阻止了**670**萬次攻擊。
- 在**4萬9,900**台端點上，阻止了**200**萬次嘗試掃描伺服器漏洞。
- 在**1萬4,300**台端點上，阻止了**92萬7,500**次嘗試掃描在**CMS**漏洞。
- 在**4萬3,000**台端點上，阻止了**170**萬次嘗試利用的應用程式漏洞。
- 在**9萬6,300**台端點上，阻止了**220**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**959**台端點上，阻止了**70萬4,400**次加密貨幣挖礦攻擊。
- 在**9萬7,800**台端點上，阻止了**630**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**506**台端點上，阻止了**7萬2,000**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 15 萬 7,500 個受保護端點上阻止了總計 670 萬次攻擊。**(2025/04/07)**

- 使用網頁信譽情資，在 **151.1K** 個端點上阻止 **630** 萬次攻擊。
- 攔截 **17.7K** 個端點上 **280.7K** 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 **5.2K** 個端點上攔截 **121.9K** 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 **150** 個端點上攔截 **1.9K** 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。

2025/04/10

Chaos勒索軟體假冒資安工具軟體瞄準IT人員

Chaos 勒索軟體一直以來都有層出不窮的新變種，大多透過瀏覽網頁時的順道下載的手法以社交工程伎倆來鬆懈受害人的警覺。與透過更複雜精密的攻擊鏈針對大型組織的雙重勒索戰略的攻擊相比，這些攻擊通常要求較少的贖金。

在最近活動中，發現以 ANOMALY 為名的駭客團體或個體戶一直針對資安相關從業人員--應用程式安全 (簡稱 AppSec) 團隊、藍隊、IT 管理員和開發、安全、運營 (DevSecOps) 團隊--使用偽裝成虛假 Acunetix 軟體啟動器的 Chaos 勒索軟體來引誘受害者。Acunetix 是一款商用網路漏洞掃描器，設計用來識別並協助修復網站、網路應用程式和 API 中的安全問題。

一旦執行惡意酬載，檔案就會被加密並冠上四個字元的隨機副檔名。它還會在多個目錄中留下勒索 (贖金支付) 說明文字檔。

勒索 (贖金支付) 說明文字檔警示受害者他們的檔案因執行惡意檔案而被加密，並要求支付等值於 900 美元的加密貨幣以取得解密金鑰。它同時列出常見的加密貨幣的錢包地址--比特幣、以太坊、Solana、Monero、Litecoin 和 Dogecoin，以利贖金的支付。

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：

- Ransom.Sorry

2025/04/10

駭客集團：Sapphire Werewolf正在散播全新的Amethyst Stealer惡意竊密程式

在真實網路情境裡發現散播 Amethyst Stealer 惡意竊密程式最新後繼版本的網路攻擊行動。此行動是由駭客集團：Sapphire Werewolf所發動。惡意軟體以電子郵件附件的壓縮檔形式傳送給受害者。信件偽裝成人力資源部門的備忘錄，並附有顯示給使用者作為誘餌的 .pdf 檔案。Amethyst Stealer 具備從受感染的端點收集和滲出各種敏感資訊的功能，包括憑證、儲存在網頁瀏覽器中的資料、設定檔以及內部磁碟機和可攜式儲存裝置中的檔案。這個惡意軟體的最新後繼版本採用額外的功能來檢查虛擬化環境，並使用 Triple DES 演算法來加密。

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.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。

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!gdn14
- Scr.Malcode!gdn32
- 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

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。

2025/04/10

CVE-2025-31161--存在CrushFTP身份驗證繞過漏洞已在真實網路情境裡遭開採濫用

CVE-2025-31161 是最近被揭露的嚴重等級 (CVSS 風險評分：9.8 分) 身份驗證繞過漏洞，會影響 CrushFTP 檔案傳輸解決方案。如果被成功開採濫用，此漏洞可透過特定的 HTTP 請求，授予未經驗證的攻擊者管理層級存取底層伺服器權限。此漏洞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。據報導，攻擊者利用 MeshAgent 工具開採濫用此漏洞，並部署 TgBot 二進位檔案。原廠已針對此漏洞釋出修補程式版本。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g463

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.9
- Trojan.Gen.MBT

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：

- Web Attack: CrushFTP CVE-2025-31161

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，預設的鎖定政策可保護底層的

UNIX／Windows 伺服器，防止此漏洞，包括防止執行任意指令和限制存取作業系統重要檔案的讀取。

- DCS 政策中的網路規則可設定為限制僅供受信任的用戶端存取 CrushFTP 應用程式。

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。

2025/04/09

Neptune遠端存取木馬(RAT)

Neptune 遠端存取木馬 (RAT) 具有高度模組化以及多功能的特色。此惡意軟體包含提供許多功能的 DLL 外掛程式。其他功能包括但不限於以下幾項：

- 從應用程式、瀏覽器和密碼庫竊取憑證
- 竊取加密貨幣錢包
- 透過反虛擬、修改登錄檔機碼和工作排程的手法來取得持續／常駐能力
- 具有勒索軟體行為

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

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.Neptune
- 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

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。

2025/04/09

以薪酬調整為幌子的網路釣魚行動，濫用常見的PDF文件檔將使用者重導向至AWS S3上代管的網路釣魚網頁

賽門鐵克發現一起全新的網路釣魚行動，該威脅份子濫用常見的 PDF 文件檔將使用者重導向至 AWS S3 上代管的網路釣魚網頁。

此行動由一封惡意電子郵件所引爆--通常使用「Salary Adjustment Notice - Please Review. [random 2-digit number]」--與所謂的薪資調整有關。當使用者開啟附件中的 PDF 文件檔 (Salary_Adjustment.pdf) 時，他們會看到一份設計類似合法 DocuSign 通知的文件。它的版面如同官方正式的樣貌，並指示收件者檢視並簽署一份文件。頁面中央有一個顯眼的「檢視文件」按鈕。該文件不包含實際的合約或薪資資訊，其功能僅為引誘之用。

按一下按鈕就會默默地將使用者重導向到外部連結，濫用 Snipcart 作為重導向程式，然後將使用者導向 AWS S3 上的釣魚網頁。此頁面模仿 Outlook 登入畫面，引誘使用者毫無戒心地輸入憑證。

- 首先出現引誘被害人的畫面：hxxps://em3[.]snipcart[.]com/ls/click?upn=u001. qkQ5iC84jhtf0lXrK2qLtDh5YHQOsNMdlTR6pHwQc3A-2FpOjfYWrTyRh-2F59x9ZhcJMt8vA9-2FTq2EPV68hAtJ43A-3D-3DP1-U_8Ur0dLBv-2BeyMQ3-2BKRkbRloEyflwgy101Og5Vwzf- 2BoYmm1qq67i8aG191QtDyfCXatNzVSPOSReCNniMOGjBEGZoz52WSGjhNijOOgj0lxCMejaB1y5zDRhtNQKL8YJjrDgj6sHu7WrP9O1uBXxkdskPGeo4dPn1i7kOpwWfJgH3vnBfCmcUFb149LNOwP04CEXuahU- 2F-2BKIftpeQHQq46tn2z7uDgJ2rDuzQbMfhfCqJYyhgYtOr0E4p2e4ZGkgVRaHe4S3Qi1SDO-2FOSyPtbwtg-3D-3D
- 釣魚網頁：hxxps[:]//xiomo[.]s3[.]us-east-2[.]amazonaws[.]com/index[.]html

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：

- Scr.DLHeur!gen16

2025/04/09

CVE-2025-1094--存在PostgreSQL的SQL注入漏洞

CVE-2025-1094 是一個最近被揭露的嚴重等級(CVSS 風險評分：8.1) SQL注入漏洞，影響 PostgreSQL，這是一個開放原始碼的關聯式資料庫管理系統 (RDBMS)。若遭成功開採濫用該漏洞，由於 SQL 輸入未經消毒／淨化處理 (sanitization)，可能導致遠端程式碼執行。CVE-2025-1094 漏洞已經證實被利用涉入多重漏洞利用的攻擊鏈中，像是資安業者 BeyondTrust 旗下的遠端支援 (Remote Support，RS) 系統、特權遠端存取 (Privileged Remote Access，PRA) 系統已經被揭露且該原廠也經完成修補的 CVE-2024-12356 嚴重等級漏洞。

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: PostgreSQL CVE-2025-1094

2025/04/09

鎖定烏克蘭UAC-0226網路攻擊行動，以散播GiftedCrook惡意竊密程式為目的

根據烏克蘭電腦緊急應變團隊 (CERT-UA) 最近發佈的安全警示，已偵測到鎖定烏克蘭各軍事和政府單位的新一輪目標式攻擊。這場名為 UAC-0226 的攻擊行動會散佈含有惡意巨集 .xlsm 附件的網路釣魚電子郵件。在目標端點執行後，會感染一個名為 GiftedCrook 的 C/C++ 惡意竊密程式。該攻擊行動還利用 GitHub 儲存庫 PSSW100AVB 的 PowerShell 反向 shell 腳本。GiftedCrook 功能是收集和滲透各種敏感資訊，包括儲存在系統網路瀏覽器中的資料、cookies、驗證資料、瀏覽歷程等。

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：

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
- 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
- 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。

2025/04/09

CVE-2025-29927--存在熱門網站開發框架Next.js的中介軟體授權繞過漏洞

CVE-2025-29927 是最近被揭露嚴重等級漏洞 (CVSS 風險評分:9.1 分)，會影響 Next.js，這是一個開放原始碼的網頁開發 javascript 框架。若遭成功開採濫用該漏洞，攻擊者可透過特定的 HTTP 請求發動授權繞過攻擊，可能導致受保護的內容曝光。已發佈修補程式的 Next.js 版本 12.3.5、13.5.9、14.2.25 及 15.2.3 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: Next.js Middleware CVE-2025-29927

2025/04/09

IT人員請小心！Vidar款惡意竊密程偽裝成IT人員工作中不可或缺的得力助手：Sysinternals

Vidar 惡意竊密程式，自 2018 年起開始活躍。是透過惡意軟體即服務 (Malware-as-a-Service)來散播，攻擊者利用它來竊取敏感資料，例如：儲存在瀏覽器、應用程式和雲端儲存服務中的憑證。其他危害還包括竊取加密貨幣錢包和劫持各種流行應用程式的對話。最近發現到 Vidar 最新變種偽裝成 Microsoft Sysinternals 工具程式包中的工具，其中一些檔案的細節與合法版本完全吻合。

保安建議：下載任何軟體請到原廠網站，不要使用來路不明或搜尋引擎找到連結就毫無戒心地下載使用。

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：

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.Vidar
- 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。

2025/04/08
防護亮點：自適應防護(Adaptive Protection)何以成為資安技術的鎂光燈焦點～以有效瓦解Hellcat勒索軟體為例

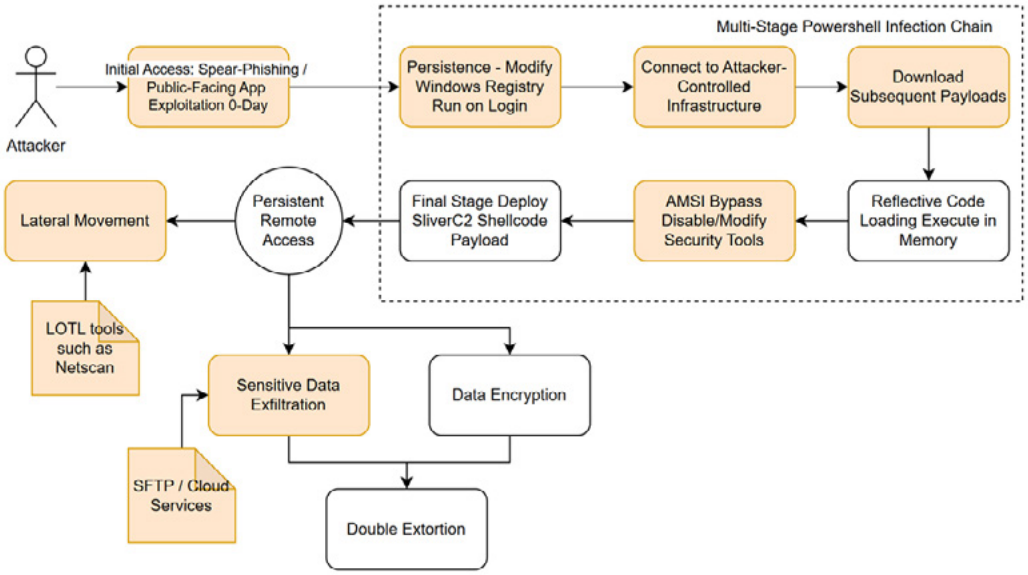
Hellcat：勒索軟體生態圈的後起新秀

網路威脅領域目睹一個新興且特別具侵略性的角色快速崛起：Hellcat 勒索軟體集團。Hellcat 約於 2024 年中崛起，迅速成為嚴重的威脅，並顯示出專門針對政府、教育和能源等關鍵部門的偏好。該組織不僅會加密資料，還會利用心理戰術和先前未知的漏洞，將影響發揮到極致。Hellcat 以「勒索軟體即服務」(RaaS) 的模式運作，透過招募附屬組織來擴大其影響範圍。其核心策略包括雙重勒索、在加密前滲出敏感資料，並威脅若不乖乖就範就公開洩露資料。此外，Hellcat 已顯示有能力利用零時差漏洞 (例如：最近在 Atlassian Jira 發現的漏洞) 來取得初始存取權。他們的目標包括各行各業的多個機構，對全球組織造成嚴重威脅。

拆解 Hellcat 攻擊鏈

發動 Hellcat 勒索軟體的攻擊者利用魚叉式網路釣魚和公開網路伺服器或應用程式來發動攻擊，通常會利用零時差漏洞。在取得初始存取權之後，他們會部署一個多階段的 PowerShell 感染鏈。第一階段透過修改 Windows 註冊表建立持久性／常駐能力，確保惡意指令碼能在使用者登入時執行。然後，這個腳本會連線到攻擊者控制的基礎架構，下載後續的有效酬載。Hellcat 採用反射式程式碼載入，直接在記憶體中執行惡意程式碼，規避安全軟體的偵查。他們也使用 AMSI 繞過技術來停用或修改安全軟體，讓他們的腳本可以恣意的執行。最後階段是透過 shellcode 有效酬載部署 SliverC2(一個命令與控制框架)，允許持續的遠端存取。

為了進行橫向移動和權限升級，Hellcat 利用 Netcat 和 Netscan 等「就地取材」的二進制程式，混入合法的網路活動中。攻擊者在加密系統之前，會利用 SFTP 和雲端服務將敏感資料外洩，並採用雙重勒索策略。



針對 Hellcat 勒索軟體的已知行為，賽門鐵克的自適應防護技術 (Symantec Adaptive Protection) 已發佈下列特徵碼。此外，值得注意的是，隨著 Hellcat 和其他勒索軟體的演進，它們會不斷改變特定的工具和技術，以逃避基於特徵檔比對的安全解決方案。賽門鐵克自適應防護 (Adaptive Protection) 提供強大、全面的攻擊面減緩優勢，可以協助組織在這些進階攻擊的每個階段加強防護。

行　　為	自適應保護特徵碼
使用惡意附件的魚叉式網路釣魚電子郵件，以啟動 PowerShell 感染鏈	ACM.Exl-Ps!g1 ACM.Ppt-Ps!g1 ACM.Word-Ps!g1 ACM.Note-Ps!g1 ACM.Acr-Ps!g1 ACM.Acr32-Ps!g1 ACM.Cscr-Ps!g1 ACM.Wscr-Ps!g1 ACM.Mshta-Ps!g1
PowerShell 執行遠端有效酬載	ACM.Ps-Http!g2
透過使用 Run 或 RunOnce 登錄機碼，讓使用者登入時執行惡意程式	ACM.Ps-Reg!g1 ACM.RegRun-TPs!g1
PowerShell 列舉網路共用	ACM.Ps-NtShEnum!g1
使用 Netscan	ACM.Netscan-Lnch!g1
透過 SFTP 或雲端服務外洩資料	ACM.MegaSync-Lnch!g1 ACM.Restic-Lnch!g1

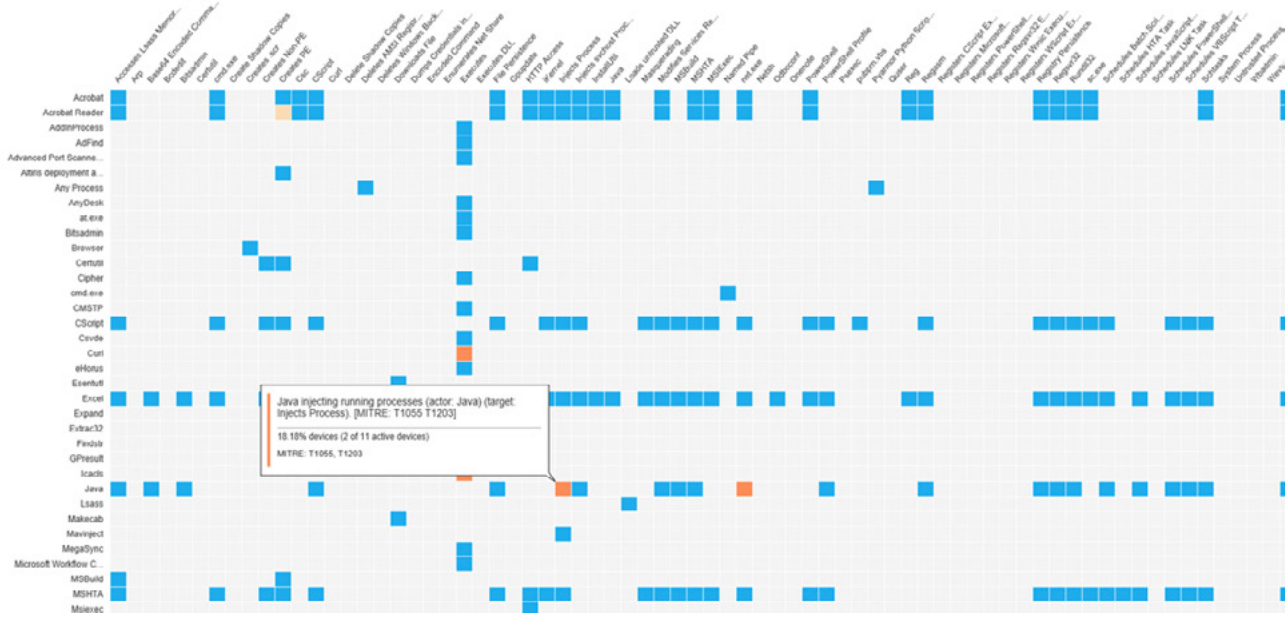
自適應防護(Adaptive Protection)何以成為資安技術的鎂光燈焦點

自適應防護 (Adaptive Protection) 的現有重要指標：

- 追蹤的行為：涵蓋 70 種常用應用程式的 496 種行為
- 受自適應防護技術保護的端點：超過 290 萬個
- 自適應防護政策的「拒絕」模式的效用：平均而言，客戶每次部署會封鎖超過 345 種行為

自適應防護 (Adaptive Protection) 可確保對 Hellcat 以及類似不斷演進和新興的勒索軟體威脅提供強大的防禦，同時維持組織的作業效率。想要立即啟用 Adaptive Protection？請參閱以下連結以了解更多資訊。

自適應防護 (Adaptive Protection) 最近已整合至地端自建型的端點防護管理主控台 (SEPM：Symantec Endpoint Protection Manager)。下面截圖是調適型防護熱圖--顯示 SEPM 主控台上現有自適應防護 (Adaptive Protection) 規則之相對應行為的普及程度。可以安全地攔截零普及程度行為，以強化攻擊面。



請點擊此處，以了解有關如何在組織中透過自適應防護攔截就地取材攻擊 (Living Off the Land：LOTL)。

欲了解啟用賽門鐵克端點安全完整版 (SESC) 上的「自適應防護」透過管理受信任應用程式所執行的潛在風險行為來減少攻擊面，請點擊此處。

2025/04/08

EncryptHub駭客組織利用惡意MSC檔案散播有效酬載

最近一起由 EncryptHub(也稱為Water Gamayun) 駭客組織發起的攻擊行動中，威脅份子利用微軟管理主控台 (MMC) 漏洞 (被歸納為 CVE-2025-26633 漏洞) 檔案執行惡意有效酬載。據趨勢科技研究人員報告，該行動使用 PowerShell 的 MSC EvilTwin 惡意程式載入器，導致受害者在未修補的端點上載入惡意 MSC 檔案。感染鏈會導致部署各種惡意竊密程式的有效酬載，例如：Rhadamathys 或 StealC。

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.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：

- Downloader
- ISB.Exploit!gen13
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Rhadamanthys!g5
- Web.Reputation.1
- 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
- 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。

2025/04/08

利用偽裝的惡意PDF檔案誘騙使用者的HollowQuill網路攻擊行動

HollowQuill 網路攻擊行動，透過經武器化的惡意 PDF 文件檔鎖定全球學術機構和政府機關發動攻擊。此攻擊行動運用社交工程伎倆，將惡意 PDF 文件檔偽裝成研究論文、獎助金申請、誘騙研究邀請函或政府通訊，誘騙毫無戒心的使用者。一旦系統被滲透，多階段感染鏈會從包含 .NET 惡意軟體驅動程式的惡意 RAR 壓縮檔開始觸發。此植入程式會部署多個有效酬載，包括合法的 OneDrive 應用程式、基於 Golang 的 shellcode 惡意程式載入器和誘餌 PDF 檔案。透過利用真實的文件和先進的惡意軟體技術，此威脅行為者的目標是入侵系統，同時滲出敏感資料。

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-FlPst!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：

- 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
- 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。

2025/04/07

Springtail進階持續威脅(APT)駭客組織鎖定韓國政府單位為目標

Springtail(又稱 Kimsuky) 進階持續威脅 (APT) 駭客組織最近針對韓國政府單位進行攻擊。這些攻擊行動利用以政府為主題的訊息 (一個是稅務相關的訊息，另一個則是關於性犯罪者主題的政策)，以惡意垃圾郵件附件的方式散佈惡意 .LNK 捷徑檔。

惡意 .LNK 捷徑檔用作下載惡意的 HTA，執行後會繼續攻擊。下載其他元件包括 ZIP 壓縮檔，其中包含更多編碼檔案形式的惡意內容，以及 VBS 和 PowerShell 腳本。攻擊最終目標包括資料竊取／滲透和鍵盤記錄等。

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.Mshta-Cmd!g1
- ACM.Mshta-Ps!g1
- ACM.Mshta-RgPst!g1
- ACM.Ps-Mshta!g1

- 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：

- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Malscript
- VBS.Downloader.Trojan

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。

2025/04/06

從網路釣魚到LINE詐騙：樂天證券的客戶處於危險之中

在過去幾個星期，網路釣客鎖定樂天證券客戶發起一波波的網路釣魚行動，企圖竊取他們的憑證--以下有更詳盡的資訊。

在最新一輪攻擊中，網路釣客利用社交工程伎倆發動投資詐騙。它以一封惡意電子郵件 (主旨：【緊急・重要】楽天証券による注意喚起あり) 為引爆點，內容是關於透過 LINE 提供免費投資指南優惠。

如果使用者被成功誘騙點擊釣魚電子郵件中提供的連結，就會轉到一個網頁，敦促他們新增一個 LINE 帳戶，以換取「禮物」和參加有關增加退休資產的免費研討會。該網站宣稱可提供有關使用 NISA、選擇股票和提早退休的建議。該網站謊稱樂天證券的執行長透過 LINE 宣傳這個騙局。該訊息利用使用者對財務的疑慮，迫使他們投資並加入所謂的投資社群。

威脅份子已為此惡意行動製作許多網域。這些網域名稱遵循共同的格式：「www[.][<5 – 8 lowercase letters>].[cn或com.cn]」。這與動態網域演算法 (DGA-Domain Generation Algorithm) 或大量註冊的基礎設施相符，其目的在於快速輪換和短期使用。

- hxxps[:]//www[.]zgmljq[.]cn
- hxxps[:]//www[.]hrbyanyi[.]cn
- hxxps[:]//www[.]kokwvr[.]cn
- hxxps[:]//www[.]okbko[.]cn

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 Horse
- Trojan.Gen.MBT
- Trojan.Malscript
- VBS.Downloader.Trojan

2025/04/06

假冒台灣物流公司發出的電郵，ModiLoader惡意程式載入器利用.SCR檔案散播

惡意軟體濫用 Windows 螢幕保護程式檔案格式 (.scr) 已有一段時間。雖然這些檔案看似無害，但其本質上是具有不同檔案副檔名的可執行程式之腳本 Script 檔案。一旦被執行，這些檔案可執行一般可執行程式所能執行的任何動作，例如：安裝惡意程式載入器、後門程式、鍵盤側錄程式或勒索軟體。時至今日，這些檔案仍在攻擊鏈中被大量使用。

在最近一個案例中，賽門鐵克觀察到一起正在進行中的網路攻擊行動，攻擊者假冒一家知名的台灣貨運代理和物流公司，該公司處理亞洲和其他地區的國際航運和海關協調。

- 電子郵件主旨：//AMD ISF + AMD BL DRAFT// 聯盛-裝船通知單-4/7 結關 KAO TO ATLANTA, GA VIA NYC CFS【友鋮】SO.N023
- 目標行業：工業機械製造、出版、廣播、汽車製造、電子、膠黏產品製造、綜合企業(汽車、航太)、衛浴用品零售、研磨產品製造、主題樂園
- 目標國家：日本、英國、瑞典、美國、香港、台灣、泰國、馬來西亞

這封以中文撰寫的電子郵件是虛構的物流更新，通知收件者有一批貨物預定於 4 月 7 日從高雄經紐約到亞特蘭大通關。它要求核實貨運訂單，並要求提供隨附文件，例如：ISF、裝箱單和發票。

該電子郵件附有一個名為「景大 台北港 ISF(032525)-invoice# JN-032525C-KAO TO ATLANTA, GA VIA NYC CFS【友鋮】SO.N023.xlsx.rar」的惡意檔案，其中包含一個惡意的 .SCR 腳本檔案。當被執行時，受害者會在不知情的情況下在他們的機器上部署 ModiLoader--一個 Delphi 類型的惡意程式載入器。

此惡意程式載入器已存在一段時間，多年來已觀察到它部署大量的惡意竊密程式和遠端存取木馬程式。最近，它開始載入 Remcos、Agent Tesla、MassLogger、AsyncRAT、Formbook 等惡意程式家族。

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。

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.MBT
- Scr.Malcode!gen19

基於機器學習的防禦技術：

- Heur.AdvML.B

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**。