保安資訊--本周(台灣時間2025/05/09)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 900 台受保護端點上總共阻止了 5,410 萬次攻擊。這些攻擊中有 83.6% 在感染階段前就被有效阻止：**(2025/05/06)**

- 在**8萬2,500**台端點上，阻止了**2,340**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**7萬6,200**台端點上，阻止了**570**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬3,900**台**Windows**伺服主機上，阻止了**670**萬次攻擊。
- 在**5萬3,700**台端點上，阻止了**220**萬次嘗試掃描伺服器漏洞。
- 在**1萬4,700**台端點上，阻止了**1萬1,000**次嘗試掃描在**CMS**漏洞。
- 在**4萬8,700**台端點上，阻止了**200**萬次嘗試利用的應用程式漏洞。
- 在**9萬5,200**台端點上，阻止了**200**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**67萬2,100**次加密貨幣挖礦攻擊。
- 在**9萬1,100**台端點上，阻止了**640**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**484**台端點上，阻止了**6萬2,100**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 3,600 個受保護端點上阻止了總計 670 萬次攻擊。**(2025/05/06)**

- 使用網頁信譽情資，在 **147.5K** 個端點上阻止 **630** 萬次攻擊。
- 攔截 **17.3K** 個端點上 **268.2K** 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 **94.2K** 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 **285** 個端點上攔截 **3K** 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。

2025/05/08

惡意電子郵件攻擊行動傳播Java版本的遠端存取木馬(RAT)

最近發現有人針對義大利、葡萄牙和西班牙的組織進行惡意電子郵件攻擊。該惡意電子郵件攻擊行動利用西班牙電子郵件服務供應商，試圖使用含 PDF 附件的電子郵件讓其看似合理情況。PDF 被存放在多個公開內容託管網站 (Dropbox、Google Drive 和 Mediafire) 上，透過其下載啟動多階段傳送。有效酬載的檔案是 Java 版的 Ratty 遠端存取木馬 (RAT)。該惡意電子郵件攻擊行動的詳細資訊可在 Fortinet 發佈的報告中查看。

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

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.SuspBeh!gen22
- SONAR.SuspBeh!gen625

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.ASync!g2
- Backdoor.Ratenjay
- Backdoor.Ratenjay!gen2
- Backdoor.Ratenjay!gen3
- MSIL.Trojan!gen2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Maljava
- Trojan.Maljava!gen55
- 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

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。

2025/05/08

LZRD--在真實網路情境裡發現Mirai殭屍網路家族的最新變種

據報導，發現新一波的網路攻擊行動，在真實網路情境裡發現 Mirai 殭屍網路家族的最新變種。該惡意軟體利用兩個影響 GeoVision IoT 裝置的指令注入漏洞--CVE-2024-6047 和 CVE-2024-11120，這兩個漏洞已在去年就被揭露。若被成功開採濫用，攻擊者會嘗試下載並執行以 ARM 為基礎的 Mirai 殭屍網路家族之有效酬載，其中包括被稱為 LZRD 最新變種。此變種被觀察到的功能與許多先前 Mirai 變種一致，目的是執行分散式阻斷服務攻擊 (DDoS：Distributed Denial-of-service Attack)。

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：

- CL.Downloader!gen277
- Downloader
- Linux.Mirai
- Linux.Mirai!g2
- Scr.Malcode!gen107
- Trojan.Gen.NPE
- Trojan.Gen.MBT
- WS.Malware.1
- 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。

2025/05/08

CVE-2025-31324--存在SAP NetWeaver的嚴重等級漏洞

CVE-2025-31324 是最近被揭露一個存在 SAP NetWeaver Visual Composer 的嚴重等級 (CVSS 風險評分：10 滿分) 不受限制的檔案上傳漏洞。如果被成功開採濫用，此漏洞可能會允許未認證的攻擊者上傳任意檔案，導致完全控制目標系統。供應商已在修補的產品版本中修復此漏洞。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，顯示該漏洞在真實網路情境中已遭大肆開採濫用。據觀察，利用此漏洞攻擊是使用惡意的 JSP webshells 在易受攻擊的 SAP NetWeaver 系統上進行。

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

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: Metasploit JSP Payload

- Web Attack: Malicious Java Payload Upload 17
- Web Attack: Malicious Java Payload Upload 19
- Web Attack: Malicious Java Payload Upload 25
- Web Attack: SAP NetWeaver CVE-2025-31324

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。

2025/05/08

CVE-2025-32433--存在Erlang/OTP SSH函式庫身份驗證機制的嚴重等級遠端執行程式碼(RCE)漏洞

CVE-2025-32433 是最近被揭露存在 Erlang/OTP SSH 函式庫身份驗證機制的嚴重等級遠端執行程式碼 (RCE) 漏洞，會影響 Erlang/OTP (是一組用於 Erlang 程式語言的函式庫)。若被成功開採濫用，則未經認證的攻擊者可存取存在該漏洞的 Erlang/OTP SSH 伺服器，並執行任意指令。此漏洞已在新的 OTP-27.3.3、OTP-26.2.5.11 及 OTP-25.3.2.2 版本中完成修補。

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: Erlang/OTP CVE-2025-32433

2025/05/07

拆解Bert勒索軟體～對應到MITRE ATT&CK網路攻擊戰術、技術以及知識庫的完整分類

今年 4 月，有人觀察到一種名為「Bert」全新勒索軟體在真實網路情境出沒，據稱有數個組織成為受害者，包括美國和土耳其的醫療保健行業、科技業和展行銷與活動管理服務等領域的組織。

為了有利於初始攻擊或規避防禦機制來完成整個攻擊鏈的所有環節，攻擊者刻意採用基於 PowerShell 的惡意程式載入器式，試圖停用安全軟體、提權限並載入勒索軟體的有效酬載。

成功入侵後，受害者的電腦檔案會被加密並冠上 .encryptedbybert 副檔名，並存放在存有勒索贖金支付說明文字檔 (.note.txt) 的多個目錄中。

該勒索贖金支付說明文字內容明確表明採用典型的雙重勒索手法，同時檔案加密並威脅不就範就會公開機敏資料。開頭是一段問候語，並告知受害者他們的網路已遭入侵，檔案已被加密。攻擊者聲稱已從受害者網路中滲出重要的資料，暗示除了檔案加密之外，也竊取資料。攻擊者提供透過注重隱私的 Session messenger 與攻擊者聯絡之指示，要求受害者使用所提供的唯一 Session ID。攻擊者的洋蔥網站連結也包含在內。

此威脅經拆解可對應到 MITRE ATT&CK 網路攻擊戰術、技術以及知識庫的完整分類。

- **執行**：使用本機 API(T1106) 和指令與腳本解釋器 (T1059)，特別是 PowerShell(T1059.001)，在暫存目錄中植入 PE 檔案。也利用使用者執行 (T1204) 和工作排程 (T1053.005) 透過使用者互動和自動化任務進行初始執行。
- **常駐與提權**：透過變更登錄檔的啟動機碼／啟動目錄 (T1547.001)、開機自動啟用 Office 應用程式 (T1137) 及 DLL 側載 (T1574.002)，並大量嘗試載入遺失或遭劫持的 DLL。修改系統服務 (T1543.003) 並利用建立或修改系統程序 (T1543)。繞過 UAC(T1548.002)，並透過修改登錄檔來停用安全軟體。
- **防禦規避**：執行混淆和解除混淆 (T1140)、時間錯誤 (T1070.006) 和使用記憶體寫入觀察 (T1497) 逃避沙箱。還會停用 Defender 和 UAC(T1562.001)、在除錯模式下啟動程序，並建立防護頁面以抵抗分析。使用資源回收桶中的隱藏檔案 (T1564.001) 來隱藏贖金通知。
- **程序注入**：使用程序注入 (T1055) 針對一般程序，例如：explorer.exe，協助防禦規避和提權。
- **尋找系統與軟體**：執行登錄檔機碼查詢 (T1012)、擷取作業系統與磁碟區資訊 (T1082)、列舉執行中的程序 (T1057) 以及發現使用者帳戶 (T1087)。偵測虛擬化或沙盒環境 (T1497) 並識別安全軟體是否存在 (T1518.001)。
- **尋找檔案與目錄**：列舉使用者目錄、存取啟動資料夾，以及操作 .ini 檔案 (T1083)。
- **資料暫存**：在潛在資料竊取或暴露之前，在臨時或已知目錄中準備外洩資料 (T1074)。
- **憑證存取**：透過原始輸入方法擷取使用者輸入 (T1056)，並可能針對瀏覽器 cookies 進行會話劫持 (T1539)。
- **橫向移動**：感染共用內容和可執行檔案，包括 .html 檔案 (T1080)，以跨系統或網路共用傳播。
- **命令與控制**：使用應用層通訊協定 (T1071) 與其基礎架構通訊，同時混入合法流量。可能使用 HTTP/S 或其他網頁型態的通訊方法。
- **攻擊者嘗試影響 (控制、中斷、破壞)**：加密檔案以索取贖金 (T1486)，並透過刪除或停用備份和還原功能來抑制系統復原 (T1490)。停止系統服務 (T1489) 以逼迫受害者在最短的時間內乖乖就範。

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。

基於端點偵測與回應(EDR)：

- 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：

- Downloader
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.C

2025/05/07

全新惡意程式載入器：NETXLOADER--深受Agenda勒索軟體駭客集團青睞與重用

在最近一份報告中，分享一個名為 NETXLOADER 全新惡意程式載入器的詳細資訊。此惡意程式載入器與 SmokeLoader 惡意程式載入器搭配，涉入 Agenda 勒索軟體駭客集團所發動的攻擊。與該駭客集團相關活動已在多個國家的多個行業中被觀察到。

NETXLOADER 被該駭客集團用來秘密部署有效酬載，例如：SmokeLoader 和 Agenda 勒索軟體。此惡意程式載入器經高度混淆、基於 .NET 的惡意軟體。混淆被用作一種防禦逃避策略，使其更難被安全研究人員進行逆向工程。此外，NETXLOADER 會解密並直接在記憶體中執行其有效酬載，試圖進一步迴避資安防禦措施的偵測。

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

基於行為偵測技術(SONAR)的防護：

- SONAR.ProcHijack!g55
- 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：

- 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。

2025/05/07

駭客威脅份子利用巴哈甘(Pahalgam)恐怖攻擊事件發動網路惡意攻擊行動

駭客威脅份子利用最近 Pahalgam 攻擊事件的誘餌文件，以印度政府人員為攻擊目標。攻擊者以幾可亂真的官方政府通訊電子郵件誘騙使用者，並附上偽裝的官方簡報或情報報告 PDF 附件。偽裝的惡意文件包含嵌入式巨集，啟用後可部署多階段的惡意軟體有效酬載。惡意軟體會蒐集系統資訊並滲透敏感資料，同時嘗試在政府網路內進行橫向移動。

網路背景知識：印度控制的克什米爾地區，素有「小瑞士」美名的巴哈甘 (Pahalgam)，4月22日發生恐怖攻擊事件，釀成26死、數十傷的悲劇。

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：

- Phish.Pdf
- Scr.Malcode!gen
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE

- Web.Reputation.2
- Web.Reputation.3
- 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
- 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。

2025/05/07

FormBook惡意軟體透過武裝的Word文件檔散佈

最近發現一種攻擊，以含有惡意 MS Word 檔案附件的網路釣魚電子郵件引爆。社交工程在引誘使用者點擊武裝的的附件中扮演重要角色。開啟惡意文件後，會開始執行內嵌的 RTF 檔案，以 PowerShell 發出指令，啟動 FormBook 惡意軟體的多階段記憶體部署。

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-RgPst!g1
- ACM.Rd32-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。

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.Gen.NPE
- 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。

2025/05/07

Balloonfly勒索軟體駭客集團利用零時差漏洞發動網路攻擊

Balloonfly 勒索軟體駭客集團利用零時差漏洞發動網路攻擊

賽門鐵克威脅獵捕團隊最近發現到歸屬於 Balloonfly 勒索軟體駭客集團的網路攻擊活動。這個勒索軟體駭客集團通常負責散佈 Play 勒索軟體。在最近一次攻擊行動中，該勒索軟體駭客集團利用影響 Microsoft Windows Common Log File System Driver (CVE-2025-29824) 的零時差權限升級漏洞。這次針對美國某組織的攻擊，並未造成勒索軟體感染，但卻部署名為 Grixba 的惡意竊密程式，以及其他樣本和駭客工具。

請參閱我們的部落格：索軟體駭客集團發動權限提升的零時差攻擊。

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.Icacls-Lnch!g1
- ACM.Ps-Net!g1
- ACM.Ps-Reg!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：

- Exp.CVE-2025-29824
- Hacktool
- Trojan Horse
- Trojan.Dropper

- 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.AdvMLA!500
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.C

2025/05/07

CVE-2025–34028：存在備份軟體Commvault Command Center的路徑遍歷漏洞

CVE-2025-34028 是存在備份軟體 Commvault Command Center 路徑遍歷漏洞，CVSS 風險評為 10 分的滿分嚴重等級風險。讓遠端攻擊者在未認證的情況下執行任意程式碼。此問題源於端點上一個名為「deployWebpackage.do」，由於沒有過濾可與哪些主機通訊，此端點容易受到預先驗證的伺服器端請求偽造 (SSRF) 漏洞攻擊。此 SSRF 漏洞可透過傳送包含 .JSP 檔案的惡意 ZIP 檔案進一步利用，讓攻擊者可提升權限並執行任意程式碼，最終危害整個 Command Center 環境。

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: Commvault Command Center CVE-2025-34028

2025/05/06

假冒法國公證人的Telegram網路釣魚攻擊行動

賽門鐵克發現一個利用模仿法國官方公證服務的惡意 HTML 進行憑證網路釣魚攻擊行動。它是法國涉及公證行為的法律事務之中央資訊中心。

這些誘餌透過惡意電子郵件以獨立 .html 檔案的形式傳送--直接以附件或連結至託管 HTML 的雲端儲存空間。它們使用類似「Notaire pdf.html」或「NotairedeFrance.html」的檔名，並設計成看起來像安全文件入口網站，提示使用者檢視「ACTE NOTARIAL.pdf」或「Justificatif de paiement.pdf」等檔案。

一旦在本機瀏覽器中開啟，HTML 頁面就會以認證為晃子，提示使用者輸入電子郵件和密碼。在背景，這些憑證透過 Telegram 殭屍 API 使用硬編碼 (寫死在程式碼) 的權杖被擷取和滲出。具體而言：

「Notaire pdf.html」使用：

- Telegram Bot Token: 7018194163:AAH_wm2nj9WYGLu23KY-faD_y8R2iCAOuKY
- Chat ID：8008270064

「NotairedeFrance.html」使用：

- Telegram Bot Token: 6038674513:AAHJl_ru4UCCkHosyVAw-dwAcJ-I6sGlI6M
- Chat ID：5192985270

有些變種在輸入憑證後，會將受害者重導向至合法的 Notaires 頁面，以避免被懷疑。

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：

- Phish.ScrTgHtml!gen1

2025/05/06
防護亮點：賽門鐵克檔案信譽(File Reputation)技術，上星期給客戶帶來哪些效益？

賽門鐵克的檔案信譽服務是我們領先業界防護系統之基石。它會默默地分析雲端中的檔案和入侵指標 (Indicators-of-Compromise，簡稱 IoC)，並在幾分鐘內發佈這些檔案的信譽評等。File Reputation 維護超過 80 億個檔案的信任與惡意軟體評等。它每天分析約 40 億個 IOC 和超過 2,000 萬項新的信譽變更，讓每天有超過 600 萬個新檔案和簽章新增至檔案信譽資料庫。

作為一項雲端服務，Symantec File Reputation 已整合至所有 Symantec 和 Carbon Black 產品中，讓我們的客戶即時受到保護。具有 File Reputation 防護技術的產品包括

- 端點防護產品： SEP/SESE/SESC 等全系列端點防護解決方案
- 網頁閘道產品： WSS Gateway、Cloud SWG
- 電子郵件閘道產品：郵件安全雲端服務 (Email Security.Cloud)、地端自建郵件安全閘道 (SMG)
- 儲存設備：SPE
- Carbon Black 產品，包括：Endpoint standard、EEDR、AppControl

過去一週，賽門鐵克檔案信譽 (File Reputation) 技術為我們的客戶提供以下保護：

惡意軟體攔截

- 有 33 萬台電腦，依賴此技術攔截到 225 萬次的惡意程式。

賽門鐵克每天都會收到數百萬個新檔案和檔案雜湊值的資訊。當檔案被掃描時，掃描程序會交叉檢查我們的 Reputation 系統，查看它是否是已知的惡意軟體。

機器學習 (ML-Machine Learning) 攔截

- 有 2 萬 5 千台電腦，依賴此技術攔截到 9 萬 5 千次的惡意程式。

賽門鐵克檔案信譽支援機器學習演算法，提供信譽給我們領先業界的 ML 分類器，然後將可疑檔案的入侵指標 (Indicators-of-Compromise，簡稱 IoC) 轉換成已確認的惡意軟體。

保護重要系統檔案和裝置驅動程式

- 12 億已識別的關鍵系統檔案資料庫，可確保我們的客戶不受惡意軟體影響，而不會中斷作業

賽門鐵克檔案信譽 (Symantec File Reputation) 可確保賽門鐵克產品不會因誤判而刪除關鍵系統檔案和裝置驅動程式而造成傷害。如今，先進的威脅會利用易受攻擊的裝置驅動程式，因此良好的惡意軟體防護必須能夠分辨遭入侵和乾淨的系統檔案。Symantec Reputation 包括所有主要作業系統 (Windows、Mac、Linux) 上所有已知作業系統檔案和裝置驅動程式的乾淨檔案信譽和簽章者的信譽。

下載鑑識(Download Insight)

- 有 3 萬 2 千台電腦，依賴此技術攔截到 60 萬次的惡意程式。

下載鑑識 (Download Insight) 是一項積極的安全政策，可防止未知 PE 和 MSI 檔案在受保護的機器上執行。當下載新檔案、未簽署、非普遍或以其他方式識別為客戶使用的檔案時，下載鑑識 (Download Insight) 即會啟動。

欲進一步了解下載防護：下載鑑識(Symantec Download Insight) 的詳細資訊，請點擊此處。
欲進一步了解 Symantec Endpoint Protection 如何使用 Symantec Insight 進行檔案相關決策，請點擊此處。

2025/05/05

後生可畏～StealC惡意竊密程式V2版本，功力大增

已觀察到常見的惡意竊密程式 StealC 增強版本。它具有升級控制面板、以 JSON (JavaScript Object Notation) 資料交換格式精簡化的 C&C 通訊協定，以及增加的有效酬載傳送選項，包括 MSI 套件和 PowerShell 腳本。此外，它還引入混淆、API 解析和組態加密方面的優化。新功能包括多顯示器螢幕截圖、整合式的檔案下載器、伺服器端強制憑證，以及可根據地理位置、硬體 ID 和已安裝軟體自訂的有效酬載傳送規則。

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.Dropper

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.Sox5systemz!g2
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500

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。

2025/05/05

全新TerraStealerV2和TerraLogger惡意軟體家族～出世

兩種全新的惡意軟體家族：TerraStealerV2 和 TerraLogger 已被報導出現在真實網路情境上，且與財務動機相關的威脅組織 Golden Chickens 有關連。TerraStealerV2 目的在竊取瀏覽器憑證、加密貨幣錢包資料和瀏覽器擴增功能／外掛資訊，並將竊取資料滲出到 Telegram 和攻擊者操控的命令和控制 (C&C) 伺服器。相較之下，TerraLogger 可作為獨立的鍵盤側錄器運作，但缺乏資料滲透功能。這兩個惡意軟體系列仍在積極開發中，顯示威脅者仍在不斷改進。

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：

- Scr.Heuristic!gen2
- Trojan Horse
- Trojan.Coinminer
- 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!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。

2025/05/04

改良版的Stealerium惡意竊密程式，準備好在報稅季大幹一場

隨著美國報稅季的到來，有人觀察到威脅份子正虎視眈眈，透過釣魚電子郵件散佈改良版的 Stealerium 惡意竊密程式。偽裝成稅務相關文件 (例如：稅單) 的惡意 .LNK 捷徑檔引誘使用者執行 Base64 編碼的 PowerShell 指令碼。這個腳本會從遠端伺服器下載額外的有效酬載，最終傳送 Stealerium 惡意竊密程式。此惡意軟體會擷取敏感資料，例如：瀏覽器憑證、加密貨幣錢包資訊、系統的 metadata 資料，並從 Discord、Steam、NordVPN 和 Telegram 等熱門應用程式洩露資料，在報稅期間對個人和組織造成重大風險。

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-Enc!g1
- ACM.Ps-Http!g2

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.Mallnk!gen13
- Trojan Horse
- Trojan.Gen.MBT
- Web.Reputation.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。

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**。