



保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

名為圖片，實非圖片——阻擋以 SVG 為載體的攻擊

2026 年 9 月 24 日發布



點擊此處可獲取 **最完整的賽門鐵克解決方案資訊**

多個攻擊者已將第一階段轉移到圖片檔案，其中偏好使用的格式之一是 SVG，因為電子郵件政策光憑副檔名就視之為無害。然而 SVG 由 XML 而非像素構成，瀏覽器會剖析並執行它。單一檔案即可夾帶 <script>、繪製逼真的全螢幕登入頁面，並通過那些為可執行檔與壓縮檔設計的過濾機制。這樣的組合，使 SVG 躋身最常見的三大惡意附件類型之列。我們自身的遙測資料顯示，該格式在 2026 年上半年趨於沉寂，8 月卻急遽回升。本防護亮點說明此格式為何成為趨勢、我們在實務中的觀察，以及賽門鐵克如何結合檔案、機器學習、電子郵件與網頁防護，沿著攻擊鏈一路阻斷，直到最終目的地。

為什麼是 SVG？為什麼是現在？

可攜式執行檔 (Portable Executable, PE) 是 Windows 編譯後二進位檔案的格式，包括 .exe、.dll 與 .sys；Non-PE 則涵蓋其餘所有格式，例如 .pdf、.docx、.vbs、.js、.html 與 .svg。這項區分決定了檔案會走哪一條檢查路徑。附件政策通常是圍繞編譯後的可執行檔、含巨集的文件與獨立腳本而建立的。

腳本副檔名正好說明這一點：.js、.vbs、.hta 與 .ps1 都在主要郵件平台的預設封鎖附件清單上，.svg 卻不在其中。Microsoft 於 2025 年底縮小了相鄰的缺口，Outlook 不再轉譯內嵌 SVG，但 SVG 若以一般附件形式寄送，仍可送達並在瀏覽器中開啟。這與本系列腳本優先攻擊的防護亮點所述的是同一波遷移，只是又往前推進了一步：攻擊者先把第一階段從 PE 移到腳本，如今 SVG 則把酬載包裝在一個連腳本都不像的東西裡。

此格式會如此容易被武器化，關鍵就在於它是 XML：瀏覽器會剖析並執行它，而不是將它當作點陣圖解碼。它原生即可夾帶 <script>，附件只要連按兩下，就能以本機頁面的形式執行。若改以 引用，它則不會執行，這也正是每個誘餌都要催促使用者開啟檔案的原因。

這個執行環境有三種常見用法。其一，以 position:fixed 設為視窗大小的根元素，再搭配可容納任意 HTML 的 <foreignObject>，繪製出逼真的登入表單或文件檢視器。其二，以 Blob 在瀏覽器記憶體中重組壓縮檔，再以下載形式交給使用者；這與 HTML 附件中長期可見的走私技術如出一轍，只是改由看似圖片的檔案來承載。其三，腳本什麼也不做，只負責導向，把受害者送往外部基礎架構。無論是哪一種，釣魚頁面、重組後的壓縮檔或導向行為，全都藏在檔案內部，因此郵件本文根本不必帶有網址，闖道也就無從在投遞前進行信譽檢查。

這一切的底層存在一道落差：政策把 .svg 歸類為圖片，瀏覽器卻把它當作文件來執行。攻擊行動還更進一步，在 SVG 附件上宣告 text/plain，以規避依內容類型進行的路由，但連按兩下時，檔案仍會交給瀏覽器。混淆手法甚至不是必要條件：有些樣本只有一行純文字導向指令，沒有編碼、沒有誘餌、沒有垃圾填充，既無從讓分類器推論，也沒有任何內容需要解除混淆。

2025 至 2026 年的公開報告，對 SVG 攻擊的規模與成長給出一致的描述：

- Microsoft 觀察到一場為期三天的 SVG 攻擊行動 (2026 年 2 月 23 日至 25 日)，向 23 個國家、逾 53,000 個組織投遞了 120 萬封郵件。該行動先設下 CAPTCHA 驗證關卡，再導向偽造的登入頁面。
- Hoxhunt 回報，惡意 SVG 附件較去年同期成長約 50 倍，約佔所有惡意附件的 5%，並躋身附件類型前三名，領先 .docx 與 .eml。
- KnowBe4 指出，以 SVG 檔案隱藏釣魚酬載的情形另有 245% 的成長。
- Kaseya 旗下的 INKY 回報，商品化攻擊的量能持續不墜，其中一項以語音信箱為主題的攻擊行動，在 2026 年 6 月至 8 月間，於 5,500 個組織累計約 26,500 筆偵測。

攻擊者也已將建置過程商品化。走私產生器會為每個樣本產生垃圾元素、隨機化識別碼與多層編碼，使輸出結構相同、位元組卻各不相同。在這種條件下，雜湊與字串特徵碼的效能下滑，機器學習則佔上風。

攻擊行動的作案手法

我們觀察到的每條 SVG 攻擊鏈，都符合同一套骨架。無論目標是竊取密碼還是投放惡意軟體，前幾個階段都相同，因此在鏈條後段出現任何行為之前，附件本身就是偵測的重要依據。執行階段的樣態涵蓋各種情形：腳本可能層層混淆，也可能只有一行沒有任何內容可解開的純文字導向指令。

有兩個階段會變動。關卡 (S3g) 可利用 CAPTCHA、地理圍欄、User-Agent 或作業系統檢查，對任何看起來不像預定受害者的對象提供誘餌內容。這種做法往往擊敗的是分析而非偵測：被記錄為「無法解析」的端點，經常確實存在，只是拒絕提供內容。腳本階段載入器 (stager, S5) 可能深入兩、三層跳轉、被完全略過，或直接取代編譯後的載入器 (loader)。攻擊鏈也是在這一步首次進入端點遙測的可見範圍，因為每一次跳轉都是一次 LOLBin 執行。

How an SVG chain unfolds

Both branches share the first four stages. Only the tail differs.

