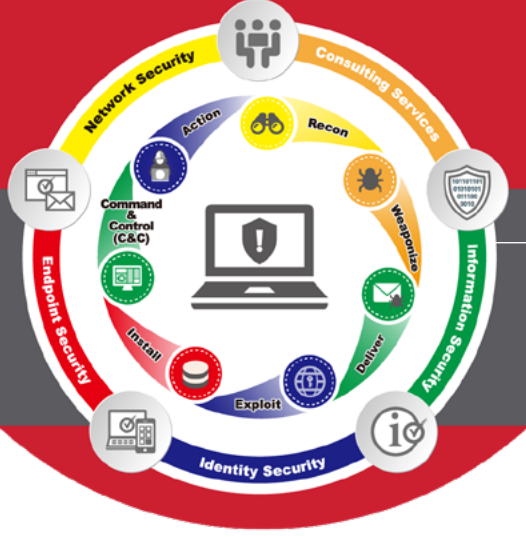




DarkSword--漏洞利用套件 針對iOS行動用戶的攻擊

2026 年 5 月 4 日發布



點擊此處可獲取--最完整的賽門鐵克解決方案資訊

DarkSword 是一款透過 Safari 瀏覽器堆疊發送的完整攻擊鏈式漏洞利用套件，其主要目標為 iOS。該鏈式攻擊結合 WebKit／JavaScriptCore、ANGLE、dyld 以及 XNU 核心中的六項漏洞，僅需透過單一惡意網頁即可實現遠端程式碼執行並部署到記憶體內植入程式。使用者只需造訪該網頁，無需進行任何其他動作就會被感染攻擊。

相關活動自 2025 年 11 月起即被追蹤，並於 2026 年 3 月 18 日至 19 日由 iVerify、Google Cloud Threat Intelligence(Mandiant) 及 Lookout 對外公開披露。Apple 已透過一系列更新修補六個版本的元件漏洞——iOS 18.7.2 / 26.1、18.7.3 / 26.2 及 26.3——並於 2026 年 3 月 24 日透過 iOS/iPadOS 18.7.7 將修補程式回溯至舊版裝置，且於 2026 年 4 月 2 日發布後續安全公告，涵蓋更多裝置型號。根據文件記載，該完整攻擊鏈對運行 iOS 18.4 至 18.7.2 的裝置能有效攻擊。運行 18.7.3 至 18.7.6 版本的裝置僅獲得部分修補：兩個初始遠端執行 (RCE) 漏洞 (CVE) 已修復，但 dyld 緩解措施繞過漏洞 (CVE-2026-20700) 直至 18.7.7 版本才有回溯修補，因此在裝置更新前，該漏洞仍可與任何未來的初始存取向量連鎖利用。

部分修補與全面修補之間的這段空窗期至關重要，因為該套件已不再僅存於其原始操作者手中。相關攻擊行動已被歸因於至少三個不同的群體——兩家商業監控供應商及一個涉嫌從事間諜活動的俄羅斯組織——據報其攻擊目標遍及沙烏地阿拉伯、土耳其、馬來西亞及烏克蘭。隨著 2026 年初漏洞利用資料的部分外洩，Proofpoint 指出這些資料已被用於更廣泛的釣魚攻擊行動，這降低了以牟利為動機及伺機而動的攻擊者門檻。

該攻擊鏈最初由 iVerify 記錄，其描述一個基於 JavaScript 的端點到端點漏洞利用框架，其中分階段腳本會載入特定版本的模組，從 Safari 渲染器中的初始遠端程式碼執行開始，歷經兩次沙箱逃逸及一次核心權限提升，最終部署於記憶體內植入程式。Google Cloud Threat Intelligence (Mandiant) 與 Lookout 隨後的分析證實了這些發現，並進一步延伸了歸因討論。「DarkSword」這個名稱源自受感染裝置上 mediaplaybackd 進程的統一日誌輸出中觀察到的標記字串，包括 [DarkSword-WIFI-DUMP]、[CHAIN] 及 [MAIN]。

攻擊者透過三種在實際環境中觀察到的傳播機制感染給受害者：

- 水坑攻擊
- 釣魚電子郵件
- 簡訊與通訊平台

傳播機制的選擇通常取決於攻擊者。Google Cloud 威脅情報追蹤到三個運行 DarkSword 的群組，每個群組都與不同的植入程式家族相關聯：

- PARS Defense -- 一家土耳其商業監控供應商，曾被觀察到針對土耳其 (2025 年 11 月) 及馬來西亞 (2026 年 1 月) 的目標部署 GHOSTSABER 植入程式。「PARS Defense」是 GCTI 歸因報告中提及的名稱，請勿與本報告以外任何名稱相似的實體混淆。
- UNC6353 -- A suspected Russian espionage cluster observed using watering-hole compromises against Ukrainian targets between December 2025 and March 2026 to deliver the GHOSTBLADE implant. UNC6353 was previously observed using the Coruna exploit kit in summer 2025.
- UNC6353 -- 一個疑似俄羅斯間諜活動的群組，據觀察於 2025 年 12 月至 2026 年 3 月期間，針對烏克蘭目標利用「水坑攻擊」手法，植入 GHOSTBLADE 後門程式。此前曾於 2025 年夏季觀察到 UNC6353 使用 Coruna 漏洞利用套件。

這三個群組的底層鏈路皆相同。它結合了六項 CVE，涵蓋 Safari 渲染器、WebContent 沙箱、GPU 進程以及 XNU 核心，而變體的選擇則取決於受害者的 iOS 版本。

CVE	元件	在鏈中的角色	已修正的版本
CVE-2025-31277	JavaScriptCore (JIT、正規表達式類型混淆)	Safari WebContent 中的初始 RCE 漏洞，iOS 18.4 – 18.5	iOS 18.6
CVE-2025-43529	JavaScriptCore (DFG JIT 釋放後使用漏洞)	Safari WebContent 中的初始 RCE 漏洞，iOS 18.6 – 18.7.2	iOS 18.7.3, 26.2
CVE-2026-20700	dyld (用於偽造 PAC 簽署指標的可信路徑唯讀原始元件)	將緩解措施繞過與初始遠端程式碼執行 (RCE) 結合，以突破使用者模式的程序存取控制 (PAC)，並實現 ROP 風格的控制流程	iOS 26.3 (back-ported to 18.7.7)
CVE-2025-14174	ANGLE / WebGL	WebContent → GPU 程序沙箱逃逸	iOS 18.7.3, 26.2
CVE-2025-43510	AppleM2ScalerCSCDriver (寫入時複製)		
	GPU → mediaplaybackd 沙箱逃逸	iOS 18.7.2, 26.1	
CVE-2025-43520	XNU 核心 (VFS 競態條件)	核心特權提升	iOS 18.7.2, 26.1

當 Safari 遇到惡意渲染的 iframe 時，攻擊流程便開始執行。最初的 JavaScriptCore 遠端執行 (RCE) 漏洞會與 dyld PAC 繞過技術串聯，藉此在 WebContent 沙箱內執行 shellcode。隨後利用 ANGLE 漏洞向 GPU 進程進行槓桿攻擊，再透過 AppleM2ScalerCSCDriver 漏洞從 GPU 進程轉移至 mediaplaybackd。附加於 mediaplaybackd 而非直接進入核心，給這個攻擊鏈提供了一個使用者層級的灘頭堡，擁有比 GPU 沙盒更廣泛的 IOKit 和 IOSurface 操作權限，而植入程式的記錄與資料準備程式正是從此進程中執行——這與該進程統一日誌輸出中觀察到的 [DarkSword-*] 字串一致。最後階段是 XNU VFS 競態條件，可提供核心讀寫權限，植入程式利用此權限將磁碟上的痕跡刪除，並將竊取資料的例程完全在記憶體中執行。

據此觀察，GHOSTKNIFE、GHOSTSABER 及 GHOSTBLADE 系列植入程式在將資料外洩前，會先將以下資料暫存於 /private/var/tmp/ 目錄下：

- 密鑰項目與金鑰包資料。綁定至 Secure Enclave 硬體金鑰的項目無法在裝置外解密；該植入程式會預先載入加密的金鑰包與封裝的密鑰資料區塊以供離線分析，並僅在裝置上即時解密那些在用戶通過驗證時可存取的項目。
- 訊息、聊天應用程式資料庫及照片
- 位置記錄與通話元資料
- Safari 瀏覽記錄與會話 Cookie
- Wi-Fi 憑證
- 裝置上快取的 iCloud 資料
- 加密金鑰資料及加密貨幣錢包檔案（若存在）

尤其是瀏覽相關的遺留資料，其影響範圍遠超出裝置本身：如果從遭入侵的裝置中提取會話 Cookie 和憑證，即使在強制實施多重驗證的情況下，仍可能導致帳戶遭竊取，這取決於受影響服務的會話綁定政策。

DarkSword 展現了 2026 年行動裝置漏洞利用套件的運作現況：僅需瀏覽單一網頁即可完全控制裝置，攻擊鏈橫跨整個客戶端堆疊（從 JIT 到 XNU），而漏洞利用資料的部分外洩，已使該套件脫離原始操作者的掌控。分階段的修補程序也導致可觀數量的裝置處於部分修補狀態——雖已針對 iOS 18.7.3 版本的初始遠端執行漏洞（RCE）進行封堵，但在 2026 年 3 月 24 日 18.7.7 版本回溯修補前，仍持續暴露於 dyld 繞過漏洞之下。對防禦者而言，實用的控制手段包括加快修補速度、在網路層阻斷與 C2 基礎設施的連線，以及基於系統狀態的條件性存取；由於受限於 iOS 沙盒模型，裝置端的偵測不應作為主要防禦手段。

賽門鐵克與博通的產品針對與 DarkSword 相關的活動提供以下防護：

- 網站與網址信譽 (WebPulse、Global Intelligence Network)。無論連結是透過電子郵件、簡訊、聊天軟體或行事曆邀請傳送而來，已知的 DarkSword 傳遞及指揮控制基礎架構皆會在全球信譽系統中被評級為惡意並封鎖。
- 賽門鐵克端點防護行動版 (SEP Mobile)。當作業系統暴露越獄、完整性及狀態異常時，系統會標記這些異常，並回報已安裝的 iOS 版本以執行合規性管控。由於 iOS 沙盒限制，裝置上的代理程式可取得的遙測資料是有限的；因此偵測機制仰賴作業系統有揭露的訊號、網路層信譽及裝置狀態，而非檢查其他程序的記憶體內容。
- 作業系統更新合規性。SEP Mobile 政策可阻擋運行未修補 iOS 版本的裝置存取企業資源，從而加速針對已知遭利用漏洞的修補進度。
- Symantec Email Security.cloud。在閘道處會直接攔截附帶 DarkSword 誘餌的釣魚訊息，包括被 WebPulse 評定為惡意的連結。
- MDM/UEM 整合。條件式存取政策可利用 SEP Mobile 的狀態訊號，防止不符合規性的裝置存取敏感應用程式與資料。

參考資料：

- 深入解析 DarkSword：一款新的 iOS 漏洞利用套件 — iVerify
- DarkSword 漏洞利用HUB — iVerify
- DarkSword 的擴散：多方威脅行為者利用 iOS 漏洞鏈 — Google Cloud 威脅情報 (Mandiant)
- 利用 DarkSword 的攻擊者威脅 iOS 用戶 — Lookout
- Apple 將 DarkSword 修補程式擴展至 iOS 18.7.7 — Malwarebytes
- DarkSword 攻擊現正透過釣魚電子郵件鎖定存在漏洞的 iPhone — PCMag

原廠網址：https://www.broadcom.com/support/security-center/protection-bulletin/protection-highlight-darksword-ios-exploit-kit-targeting-mobile-users
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。

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, 以及基於比原廠更熟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, 把我們當成可信賴的資安建議者, 可以提供良好諮詢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。