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

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

2025 年 4 月 8 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

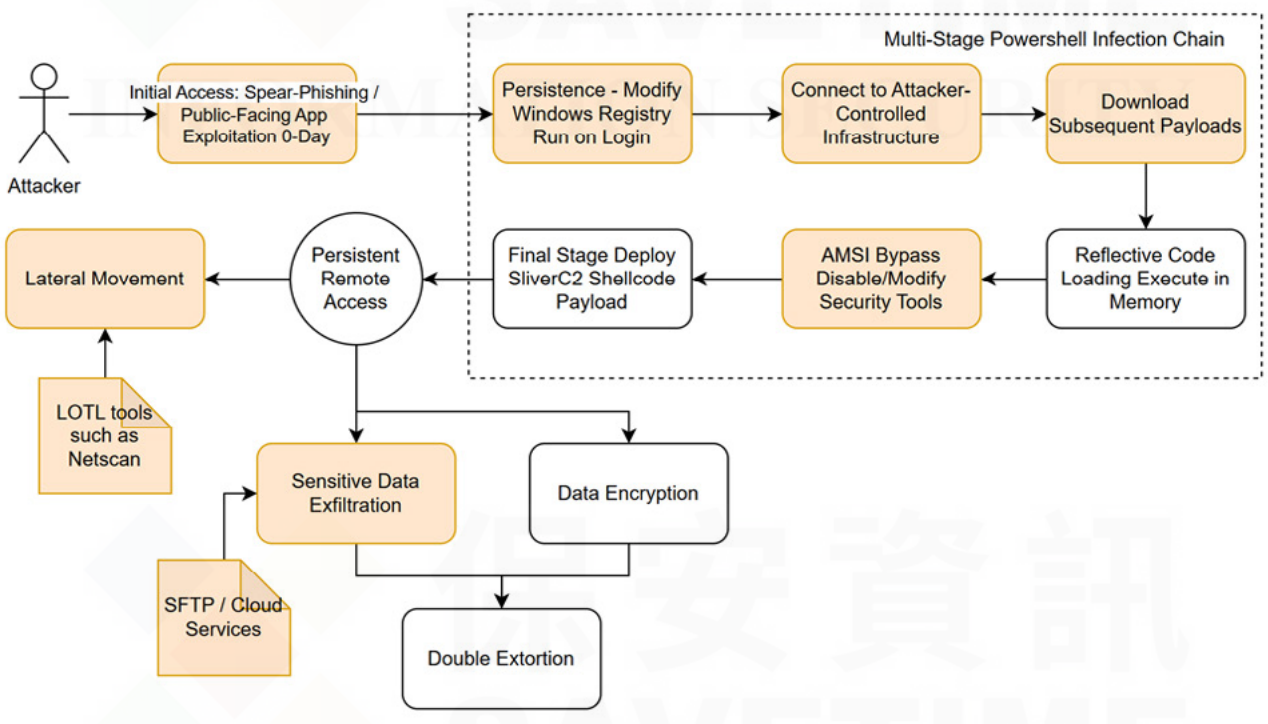
Hellcat：勒索軟體生態圈的後起新秀

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

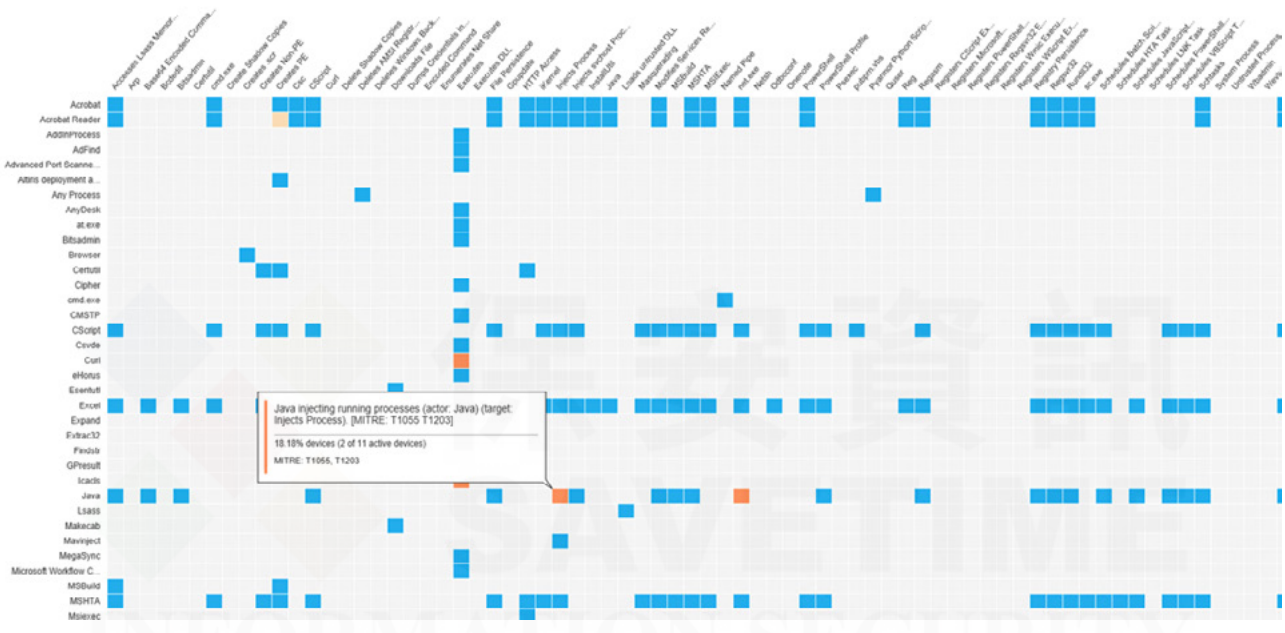
自適應防護(Adaptive Protection)何以成為資安技術的鎂光燈焦點

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。

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**。