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

「調適型防護：Adaptive Protection」如何幫助資安團隊阻止不斷變化的威脅

2024 年 3 月 26 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

身為首席資安長 (CISO) 或安全營運中心 (SOC) 的成員，威脅形勢不斷帶來新的挑戰，其中「勒索軟體攻擊」和「就地取材」的戰術尤其普遍且更具破壞性。這些威脅通常會利用企業內部的合法工具和流程，使其難以在不中斷基本業務運作的情況下被發現和緩解。

賽門鐵克的「調適型防護」功能為此難題提供重要的解決方案。它讓客戶監控並阻止企業內發生的一般應用程式行為，同時透過自動白名單允許合法的使用案例。它使企業能夠主動防禦勒索軟體和其他惡意活動，同時最大限度地減少對日常營運的干擾。

分析最近的安全事件可以發現一個令人擔憂的趨勢，即 AlphaV、Lockbit 和 Play Ransomware 等駭客組織利用各種通用的應用程式之行為來實施惡意活動。利用 Screenconnect、PsExec 和 VssAdmin 等工具進行未經授權的系統存取、網路內橫向移動和系統操控。同樣的，他們也利用 7Zip 隱藏惡意有效酬載，利用 AnyDesk 進行未經授權的系統存取，進而實現資料滲出和惡意軟體部署。此外，攻擊者還利用 PowerShell、PsExec 和 WinRAR 來執行指令、部署惡意軟體、提權、混淆有效酬載或資料洩漏。

為了說明客戶如何使用我們的「調適型防護」功能，請參考 2023 年 9 月這份範例。某客戶已經將 126 種行為設置為拒絕，並希望進一步加強其安全態勢。他們採取的步驟如下：

1. 利用 Adaptive Protection 的熱圖，可深入評估環境中的軟體或工具的行為洞察力。
2. 確定了一組處於監控模式且未在公司使用的行為。具體方法是識別熱圖頁面上的深藍色（零發生率）項目。
3. 使用威脅分類按鈕過濾來識別任何非深藍色但被視為 「拒絕」的風險行為。
4. 檢查系統生成的例外情況，將正常業務操作行為列入白名單。
5. 更新「調適型防護」政策，在 「拒絕」模式中新增新行為。

雖然並非所有基於「調適型防護」的特徵都被切換為拒絕，但該客戶選擇為他們提供額外的保護，以抵禦一次 Lockbit 著名勒索軟體組織的攻擊。以下是賽門鐵克截至 2024 年 1 月 19 日「調適型防護」軟體監控到 「就地取材-Living off the Land 」攻擊的細項：

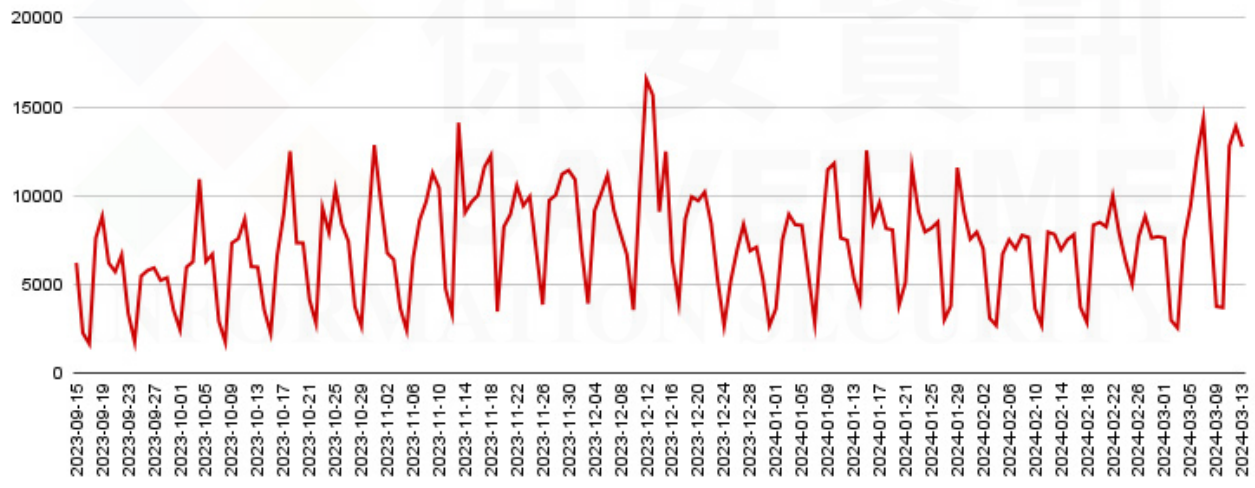
- 未受信任的程序修改登錄檔上的自動執行的機碼註 (autorun)
- 未受信任的程序修改工作排程
- 透過 Netsh 停用安全性設定
- 轉存作業系統憑證
- 使用 Netscan 收集環境資訊
- 使用 Psexec 執行程式碼
- 使用 rclone 將資料移出網路
- 以 Powershell 建立可執行檔
- 使用 Bcdedit 停用還原
- 以 Powershell 呼叫 VSSAdmin 刪除備份
- 以 Powershell 呼叫 WBadmin 刪除備份
- 以 Fsutil 刪除勒索軟體可執行檔的痕跡
- 以 Powershell 下載有效酬載

此類攻擊利用許多系統工具來執行各種任務，從程式碼執行到清除惡意軟體存在的痕跡。有人看到這個清單後可能會認為，他們可以在自己的環境中為所有這些行為開啟拒絕功能--這很好！但是，每個客戶的需求都不盡相同，而「調適型防護」可以量琛打造更靈活地確保最大程度的安全性，同時將干擾降到最低。

總之，「調適型防護」在客戶中的使用證明它的有效性和廣泛應用。

- 469 種行為可設置為拒絕模式。
- 平均每個客戶有 338 種行為被設置為拒絕模式。
- 目前有 150 多萬台機器受到該功能的保護。
- 因此，每天大約有 8,000 個行為被阻止。。

「調適型防護」每天攔截的「就地取材」攻擊數量



雖然被攔截的行為數量看似不多，但關鍵是要認識到這些行為與標準或正常的工具有關而非惡意軟體。傳統的安全技術可能無法發現這些活動，但如果不加以妥善管理，它們有可能造成重大損失。這凸顯了「調適型防護」在識別和緩解濫用日常工具的威脅方面的重要性，進而確保環境更加安全。

欲深入瞭解更多有關賽門鐵克端點安全完整版(SESC)的詳細資訊--Symantec Endpoint Security Complete，請點擊此處。
欲深入瞭解更多有關賽門鐵克「調適型防護」功能的更多資訊，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 年起就全心全力於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環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。保安資訊連絡電話：**0800-381-500**。