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

賽門鐵克EDR，有效應對日益增多的安全軟體殺手工具(AV/EDR Killers)

2024 年 12 月 17 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

駭客瞄準含有漏洞的的系統驅動程式

資安防護軟體可防止敵人執行惡意動作來達成他們的目標。但現在，攻擊者無所不用其極地妨礙資安防禦機制，通常是採取濫用含有漏洞的驅動程式來取得核心層級 (kernel level) 的存取權限。攻擊者在系統中植入含有漏洞的易受攻擊的驅動程式，然後利用它來移除或停用資安防護軟體，以便在不被中斷或被偵測到的情況下進行惡意動作。越來越多浮上檯面的開放原始碼工具都是利用這樣的技術，導致人們對其使用和影響的意識提高。

這種威脅態勢也突顯出這類工具日益老練狡猾，從勒索軟體調查中獲得的證據顯示，濫用常用應用程式中已經被公開揭露的已知漏洞，是目前嘗試滲透客戶環境的勒索軟體攻擊的主要媒介。勒索軟體攻擊者部署的工具數量持續增加，利用「自帶含有漏洞的驅動程式」(bring-your-own-vulnerable-driver，簡稱 BYOVD) 伎倆的工具目前在駭客圈廣受歡迎。

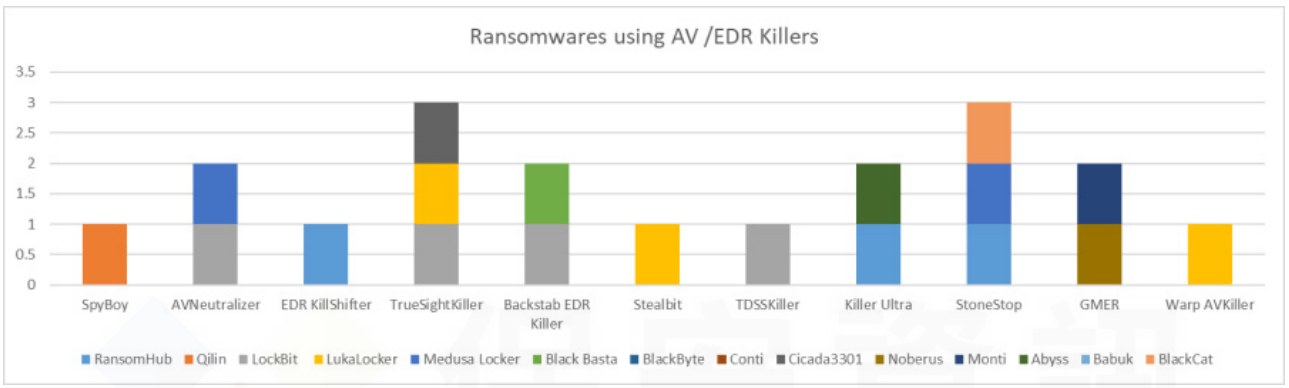
使用安全軟體殺手工具(AV／EDR Killers)癱瘓防禦能力的案例激增

威脅者濫用 BYOVD 攻擊技術，部署合法簽署且可成功載入 Windows 系統的驅動程式。這些易受攻擊的驅動程式賦予攻擊者從特權位置在核心情境中執行攻擊者提供程式碼的能力。

以下是常見的安全軟體殺手工具 (AV／EDR Killers)：

- AV-Neutralizer／AUKill：此工具濫用老舊版本的 Process Explorer 驅動程式。
- EDR KillShifter：此工具會執行自備脆弱驅動程式 (BYOVD) 攻擊。
- Terminator EDR Killer (SpyBoy) and Killer Ultra：這些工具開採濫用 CVE-2024-1853 漏洞，透過使用易受攻擊的 Zemana AntiLogger 驅動程式來停用目標系統上的安全解決方案。
- TDSSKiller：這是卡巴斯基的合法工具，用於嘗試停用目標系統上的端點偵測與回應 (EDR)服務。
- StoneStop：此工具使用惡意的 PoorTry 核心模式的 Windows 驅動程式。
- StealBit：與勒索軟體攻擊鏈相關的自訂資料外洩工具。
- GMER：這是一款相對較舊的 rootkit 掃描程式，駭客可利用它來停用執行緒。
- Warp AVKiller：此工具利用易受攻擊的 Avira 的 anti-rootkit 驅動程式來停用安全產品。

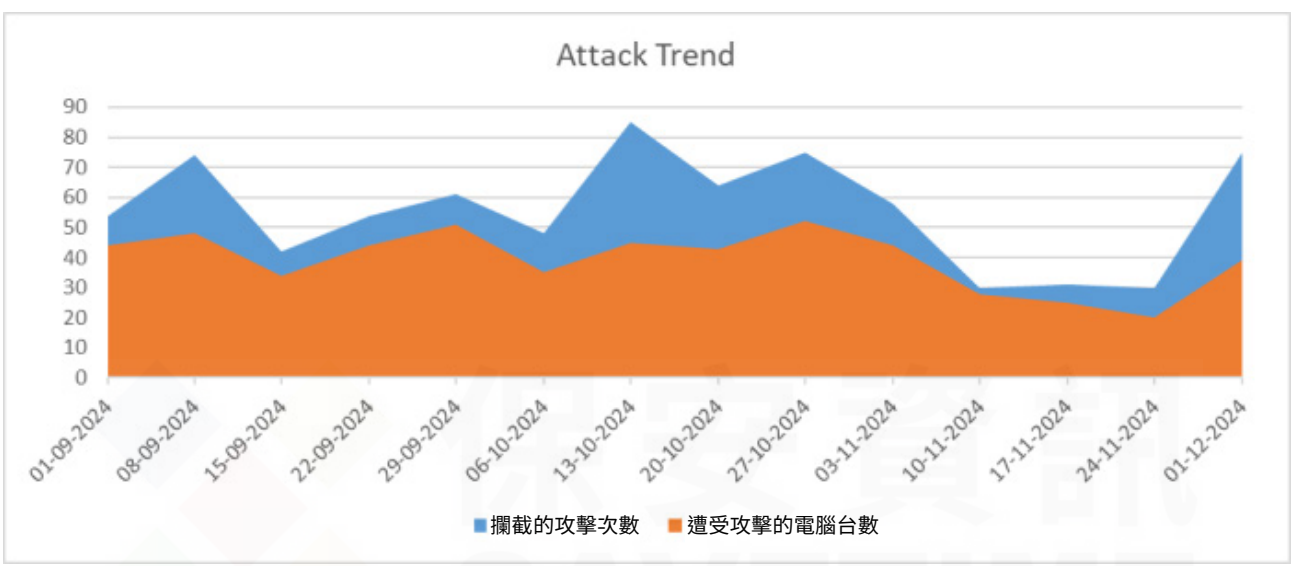
已有許多安全軟體殺手工具(AV/EDR Killers)涉入勒索軟體攻擊鏈



力抗安全軟體殺手工具(AV/EDR Killers)只是賽門鐵克端點偵測與回應(EDR)的效益之一

賽門鐵克端點偵測與回應 (EDR) 能力抗安全軟體殺手工具 (AV／EDR Killers)，保護客戶免受威脅，並在建立事件的同時產生警示。賽門鐵克 EDR 使用機器學習和行為分析來偵測和揭露可疑的網路活動。EDR 會針對潛在的有害活動發出警示，排定事件的優先順序以快速進行分類處理，並允許事件回應人員瀏覽裝置活動記錄，以便對潛在攻擊進行鑑識分析。

使用安全軟體殺手工具(AV/EDR Killers)癱瘓防禦能力的案日益增多



威脅獵捕查詢

請點擊此處，以檢視 GitHub 上 Symantec EDR 相關的威脅獵捕查詢。

欲瞭解有關 Symantec 端點偵測與回應 (EDR) 最新簡報檔，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**。