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

賽門鐵克端點偵測與回應(EDR)具有最完整的「防禦規避」偵測能力

2024 年 4 月 9 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

「防禦規避」

網路安全被比喻為一場無休止的「打地鼠：whack-a-mole」遊戲。每擊倒一個惡意軟體，似乎就會有另外兩個惡意軟體冒出來。威脅方不斷演變、根據特殊需要加以調整，並開發出更加複雜的攻擊策略。「防禦規避」是任何攻擊鏈中的關鍵因素之一。為了避免被發現並在已入侵的系統中保持常駐能力，攻擊者（通常稱為「對手」）在攻擊鏈／過程中會使用各種技術，例如：停用安全產品、濫用和利用被信任的執行緒、偽裝以及許多其他策略。

根據 MITRE ATT&CK 指南，「防禦規避」是指 「攻擊方試圖避免被偵測到」。簡潔有力的定義。然而，「防禦規避」並不簡單，它由數十種技術組成，每種技術都描述攻擊者在試圖入侵目標系統或網路時，為避免被偵測而可能使用的特定方法或伎倆 (作為參考：MITRE ATT&CK 技術是 MITRE ATT&CK 框架的一部分，該框架對攻擊者在網路攻擊的不同階段所使用的方法和戰術進行分類。有數百種不同的攻擊方式，被歸類稱為「戰術」的幾個少數類別中，「防禦規避」就是其中之一)。

賽門鐵克的端點偵測與回應 (EDR：Endpoint Detection & Response)

為了應對這些持續的攻擊，賽門鐵克不斷為其 EDR 產品組合增加新功能，投資於進階防護技術。這些新工具是我們的旗艦產品 Symantec Endpoint Security Complete(SESC) 的特色功能，主要在針對安全問題與 MITRE 攻擊鏈週期的早期攻擊做處理，以快速偵測漏洞並停止正在進行的攻擊。然後，EDR 能夠透過在回應攻擊過程中生成的 EDR 事件來自動繪製並顯示攻擊鏈。

最常用的 MITRE 防禦規避技術包括以下幾種：

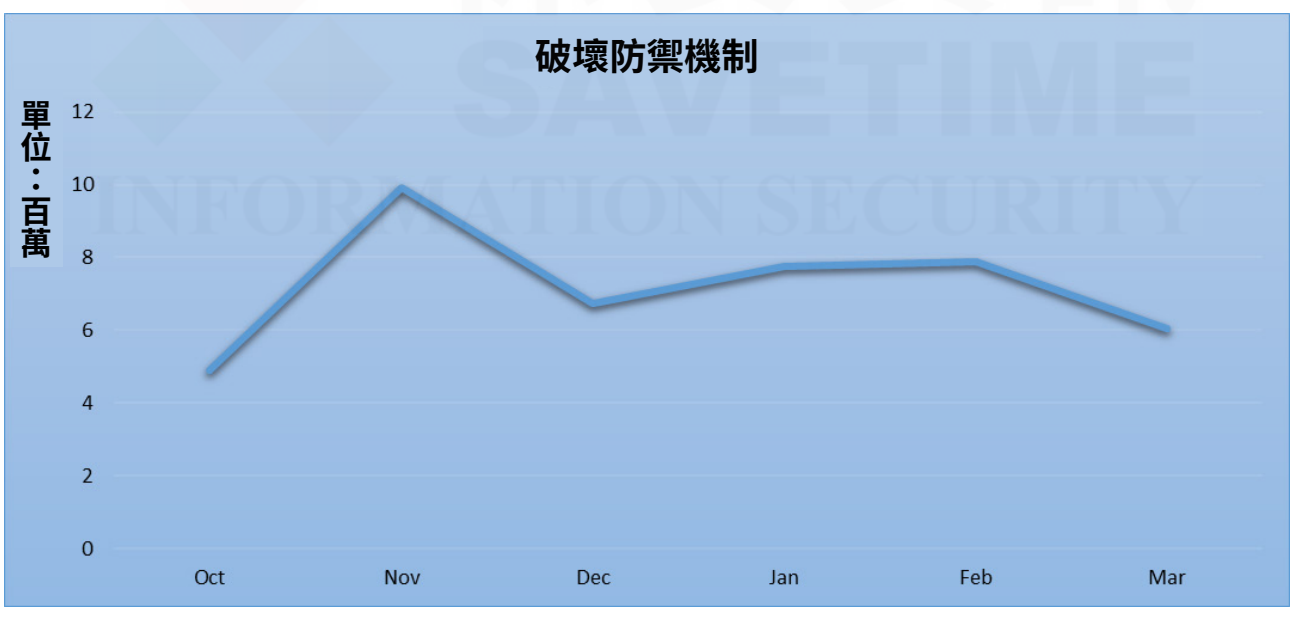
破壞防禦機制 [MITRE : T1562]

這是攻擊方用來停用安全產品的常用手段之一，方法是強制終止處理程序或透過修改登錄機碼來卸載／停用安全產品。

常用方法

- 使用 taskkill 指令來強制終止處理程序
- 使用 netsh 停用防火牆
  - netsh firewall set opmode disable
  - netsh advfirewall set currentprofile state off
- 透過修改相關登錄機碼停用安全軟體

賽門鐵克 EDR 針對攻擊方損害防禦嘗試的可見性



攻擊指標清除 [MITRE : T1070]

入侵者利用這種手法，透過刪除或修改系統內生成的數位軌跡（例如：刪除任意登錄機碼／值、清除瀏覽器歷史記錄、修改日誌等）來妨礙防禦機制。

常用方法的前幾名

- 使用 wevtutil.exe 清除 Windows 事件日誌
  - wevtutil cl security
  - wevtutil cl system
  - wevtutil cl application
- 使用 vssadmin.exe 刪除陰影副本
  - vssadmin delete shadows /All /Quiet

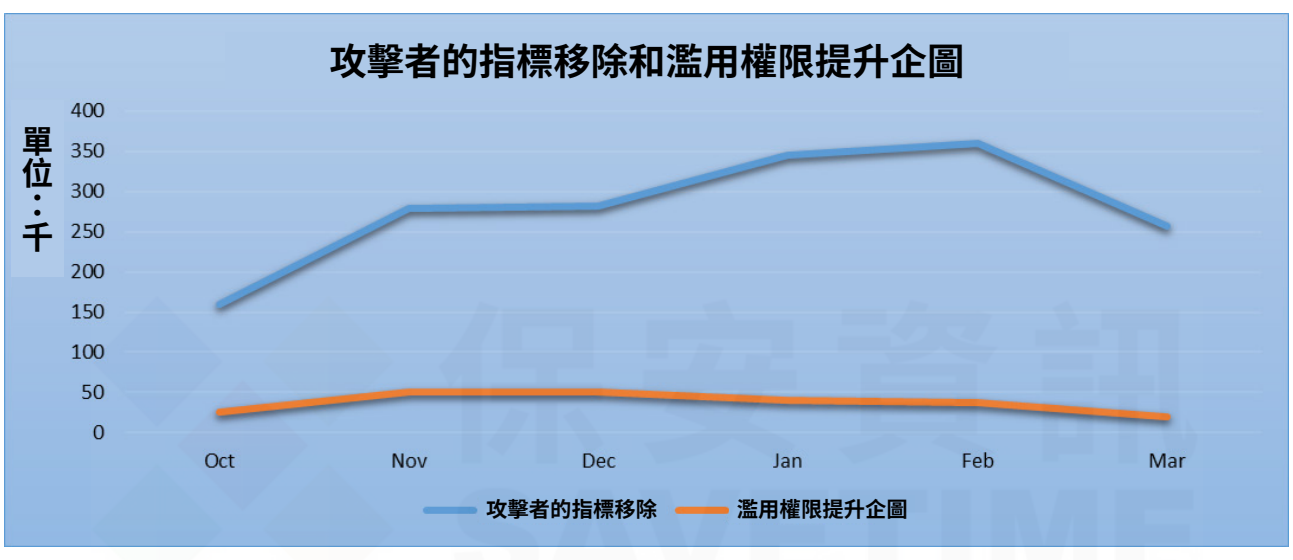
濫用提升控制權限的機制 [MITRE : T1548]

攻擊者透過濫用許可權配置、繞過 UAC、sudo 緩存等技術，來獲得更高的權限。

常用方法的前幾名

- 使用 mmc.exe、fodhelper.exe 繞過 UAC

賽門鐵克 EDR 針對攻擊者的指標移除和濫用權限提升企圖的可見性



從現實世界的角度來看，**勒索軟體**可以說是有史以來最具破壞性和危害性的網路威脅之一，它有多種變種，與我們上面討論那些變種使用類似的防禦規避技術，其中包括：

- Lockbit
- Enmity
- Snatch
- Noberus
- Blackbyte
- Hive

透過直觀簡易的管理與佈署單一平臺／單一代理程式所提供最完整多層次端點防護功能，Symantec Endpoint Security Complete 可解決這些 MITRE ATT&CK 技術和更多問題。從預防到偵測，再到在這場無休止的『打地鼠』遊戲中增強您自己的安全資源，賽門鐵克無時無刻都在創新，日以繼夜捍衛您的資訊安全。

欲深入瞭解有關 Symantec 端點檢測和響應的訊息，請點擊此處。

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。

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**。