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

賽門鐵克重要主機防護系統--Data Center Security(DCS)的安全強化機制，保障系統管理員的合法好工具不會淪為勒索軟體攻擊中之壞凶器

2024 年 12 月 24 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

資料中心遭勒索軟體攻擊越來越普遍

勒索軟體是當今網路安全的最大威脅之一，每年都以驚人的速度增長。從個人、小型政府機構到全球化的大型組織，無一能倖免。由於其對地緣政治目標、企業業務系統和關鍵公共基礎設施造成前所未有的損害，勒索軟體現在被歸類為網路恐怖主義。勒索軟體攻擊者以多種不同的方式策劃他們的攻擊，並利用基礎架構中已有的多種工具或在攻擊期間下載的各式工具。這些工具在其自身的使用場景中通常是合法的，並被管理員廣泛使用。但當這些工具在攻擊情境中被威脅行為者濫用時，它們就會變得具有破壞性，並可能造成極大的損害。只需突破一個端點，攻擊者就可以利用合適的工具存取多個互有關聯的系統和應用程式，其潛在的風險說多大就有多大。

為了防禦勒索軟體，企業組織需要採取完整而全面、全員參與、縱深防禦的方式，充分利用整個組織的資源。

Data Center Security--重要主機最有效的防護解決方案

賽門鐵克的重要主機防護系統：Data Center Security(DCS) 提供完整而全面縱深防禦的方式，以保護和保障 IT 基礎結構和連線端點的安全。我們的解決方案在提供針對日益增加的某些流行合法工具在勒索軟體攻擊和其他類型網路犯罪中使用的零日保護方面非常有效。

勒索軟體攻擊中常見的使用的工具

在本節中，我們將探討一些在勒索軟體攻擊中常被濫用的合法工具及 DCS 如何防禦它們。

- **Cobalt Strike**：一種現成的工具，可用於執行指令、注入其他程序、提升目前程序或冒充其他程序，以及上傳和下載檔案。表面上，它有合法的用途，可作為滲透測試工具，但終究遭惡意行為者濫用。目前被 Clop、Conti、DoppelPaymer、Egregor、Hello(WickrMe)、Nefilim、NetWalker、ProLock、RansomExx、Ryuk 等勒索軟體家族大肆濫用。

DCS 已內建重要主機常見使用情境的防禦政策集 (default prevention policies)，套用該防禦政策會鎖定端點網路，以減少其攻擊面。預防政策中「Suspicious Process Execution」等規則可防止 Cobalt Strike 注入程式／beacon 在系統上注入或執行。也可以阻止資料外洩。程序存取控制 (Process Access Control) 可保護所有系統程序，防止非法注入、冒充或提升權限。

- **Mimikatz**：用於憑證轉存的漏洞利用工具。目前被 DoppelPaymer、Nefilim、NetWalker、Maze、ProLock、RansomExx、Sodinokibi 等勒索軟體家族大肆濫用。

DCS 已內建重要主機常見使用情境的防禦政策集 (default prevention policies)，套用該防禦政策會阻止此工具執行。該政策將限制 Mimikatz 取得 LSASS 或 LSA 等程序的轉存，以竊取憑證。

- **PsExec**：用於在遠端系統中執行程序。在勒索軟體攻擊中，它通常用於執行任意指令 shell 和橫向移動。幾乎所有現存的勒索軟體家族都會使用它。

DCS 已內建重要主機常見使用情境的防禦政策集 (default prevention policies)，套用該防禦政策預設會阻止 PsExec 執行。

- **AnyDesk**：合法的遠端桌面應用程式。透過安裝它，攻擊者可以遠端存取網路中的電腦。

DCS 已內建重要主機常見使用情境的防禦政策集 (default prevention policies)，套用該防禦政策會阻止系統使用任何遠端桌面功能。任何人都無法從系統存取 RDP。

- **ADFind**：可用於從活動目錄 (AD) 收集資訊的免費工具。AdFind 可以查詢 AD 中的電腦、識別網域使用者和網域群組、從 AD 中提取子網路資訊。

DCS 已內建重要主機常見使用情境的防禦政策集 (default prevention policies)，套用該防禦政策會阻止該工具的執行。它也會阻止查詢 AD 的任何資訊。

- **RDP**：遠端桌面通訊協定 (Remote Desktop Protocol)。微軟開發的通訊協定，允許電腦使用用戶端／伺服器軟體，連線並控制另一台電腦。攻擊者可嘗試使用各種技術啟用 RDP，包括利用多種就地取材 (LOTL) 工具。一旦啟用 RDP，就會讓攻擊者利用 RDP 通訊協定的任何兩用工具。

DCS 已內建重要主機常見使用情境的防禦政策集 (default prevention policies)，套用該防禦政策會阻止系統使用任何遠端桌面功能。任何人都無法從系統存取 RDP。

- **WinRAR／WinSCP**：可用於封存或「壓縮」檔案的壓縮檔管理程式。攻擊者使用 WinRAR 和類似的工具 (例如：7-Zip) 來準備檔案以進行外洩。

DCS 已內建重要主機常見使用情境的防禦政策集 (default prevention policies)，套用該防禦政策會鎖定網路，因此會封鎖任何入埠或離埠的 ftp 連線。

- **PowerShell**：一種微軟指令碼工具，可用於執行指令、下載有效酬載、遍歷受攻擊網路以及進行偵查。在數次的勒索軟體攻擊中，攻擊者執行特定指令進行資料外洩，包括使用 Compress-Archive cmdlet。

DCS 已內建重要主機常見使用情境的防禦政策集 (default prevention policies)，套用該防禦政策會防止針對「受攻擊」(例如：IIS Worker) 程序在攻擊鏈的任何階段，以程序譜系啟動任意 cmd 和 PowerShell。

- **多種工具**：有些攻擊行動會同時使用多種工具，而非只使用單一工具，因為一種工具可用來啟用另一種工具。例如：可被濫用來竊取憑證的 Mimikatz 可以允許存取需要管理員權限的 PsExec 功能。勒索軟體 Nefilim 涉入的攻擊行動同時會使用多種工具，它使用 AdFind、Cobalt Strike、Mimikatz、Process Hacker、PsExec 和 MegaSync 等工具。

DCS 已內建常見使用情境的防禦政策集 (default prevention policies) 套用該防禦政策會將系統程序置於獨立的沙箱中，以防止它們受到外部工具的攻擊。此外，管理員帳戶會被鎖定，以防止任何工具嘗試將自己提權為管理員權限。

DCS 安全強化機制，保障兩用工具沒有被濫用的空間

DCS 安全強化提供作業系統和應用程式程序運行所需剛好的沙箱控制、網路、檔案系統、登錄檔、程序間記憶體的存取、系統呼叫，以及應用程式和子程序啟動的細部存取控制。這些強化能力可有效限制上述攻擊情境中使用的工具，使其只能用於合法用途，進而讓攻擊無效。

欲了解有關賽門鐵克的重要主機防護系統：Data Center Security(DCS) 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**。