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

DCS提供固若金湯、堅如磐石的伺服主機保護，號稱攻無不克的全新Royal 勒索軟體家族，也無功而返

2023 年 2 月 6 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

我們最近陸續發布幾則與『Royal』加密勒索軟體相關的公告，它是近期才出現比較新的勒索軟體家族。Royal 會透過各種方式傳播，例如：「回撥網釣」(Callback Phishing)、Batloader 和 Qbot 等惡意軟體酬載載入程序、應用程式漏洞 (CVE-2022-27510 是最近的一個漏洞) 以及各種廣泛可用的開放原始碼工具。據報導，它並鎖定虛擬平台環境為目標。惡意軟體酬載載入程序是在攻擊者和目標系統之間建立通訊的程序，通常代表攻擊的初始階段。這些前段載入程序使用常見的方法傳播，例如：惡意廣告、包含惡意鏈接或嵌入惡意檔案的垃圾郵件、虛假網站、論壇等。

被 Royal 加密後的檔案會被新增 .royal 的副檔名並留下一個 readme.txt 文字檔，將受害者引導至 Tor 的支付贖金網站，並刪除備份和磁碟區陰影複製，以脅迫並增加對贖金支付的壓力。它還會加密網路分享磁碟，並採用可加速的多執行緒加密機制。Royal 背後的駭客集團織針對多個商業領域，包括醫療保健、保險、工業公司，甚至攻擊一個廣受歡迎的英國賽車場。

正如我們之前關於 Royal 的貼文所表明的那樣，賽門鐵克在我們的好幾種保護技術都能同時偵測到這種新型的勒索軟體，包括靜態檔案分析、行為偵測、啟發式機器學習和網路層的特徵碼，然而，根據我們對瞄準 Windows 伺服器的 Royal 勒索軟體在網路的觀察方面，我們還想重點介紹我們的重要伺服器等級的安全解決方案 Symantec Data Center Security (DCS)。

只要有安裝 Symantec Data Center Security 就能套用預設的安全強化政策來提供針對未知威脅的**零時差**攻擊，當然預設強化安全政策就能偵測到以前從未見過的 Royal 勒索軟體變種和行為，如下所示：

基於安全強化政策(適用於使用DCS)：

- DCS 可限制任何軟體的安裝， 當然能防止惡意軟體工的安裝與執行，不管是本地端安裝還是透過遠端執行工具 PsExec 來進行遠端安裝和執行 Royal 勒索軟體。
- 最底層的程序 (Process) 層級的禁用技術，可最有效防止任意系統命令執行和濫用兩用工具進行惡意活動。
- DCS 專屬最小權限與最低資源 "夠用就好" 的工作環境沙箱機制，可防止篡改關鍵系統檔案和註冊表資源。
- 為了確保滴水不漏的最高等級的保護，使用者可以設置綿密與嚴謹的 DCS 網路保護規則，為需要高權限的服務和應用程序設置最嚴謹的網路邊界管控與限制。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

對固若金湯、堅如磐石的賽門鐵克重要伺服主機保護方案--DCS(Data Center Security) 想深入了解，歡迎瀏覽我們的網站，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**。