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

勒索軟體即服務(Ransomware-as-a-Service)的演進、影響以及緩解措施

2024 年 7 月 30 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

浪頭上的 Eldorado：長江後浪催前浪，一代新人換舊人--勒索軟體即服務 (RaaS) 興起的這 12 年的寫照

威脅環境中惡意軟體之演進是網路安全專家無法安枕無憂的唯一原因，勒索軟體即服務 (RaaS) 的崛起與演化更是不遑多讓。從 2012 年首次出現的 Reveton，到最近 Eldorado 勒索軟體的出現，早期事件據稱每月賺取 40 萬美元，到現今資料外洩的成本超過 100 萬美元，有時甚至遠遠超過這個數字。本公報將簡單探討此趨勢，以及賽門鐵克的調適型防護 (Adaptive Security Protection) 如何幫助企業降低與 RaaS 攻擊鏈相關的風險。

認識勒索軟體即服務 (RaaS) 的攻擊鏈

勒索軟體集團非常依賴「就地取材」(LOTL：living-off-the-land) 戰術來運行其攻擊鏈的自動化，意即他們使用已遭感染系統上已有的現成工具。舉例來說，網路釣魚行動可能會傳送一封電子郵件，其中包含一個含有巨集或腳本的 Office(word／excel…) 或 PDF 附件。巨集會執行 PowerShell 指令碼，而 PowerShell 指令碼則會下載工具並將其注入記憶體以避免被偵測。然後，它會執行偵查指令，以瞭解被攻擊的系統，包括使用者權限和網路存取。一旦取得存取權限，攻擊者就可以為所欲為，從竊取資料到部署勒索軟體。

Eldorado 與過往勒索軟體即服務 (RaaS) 的交集

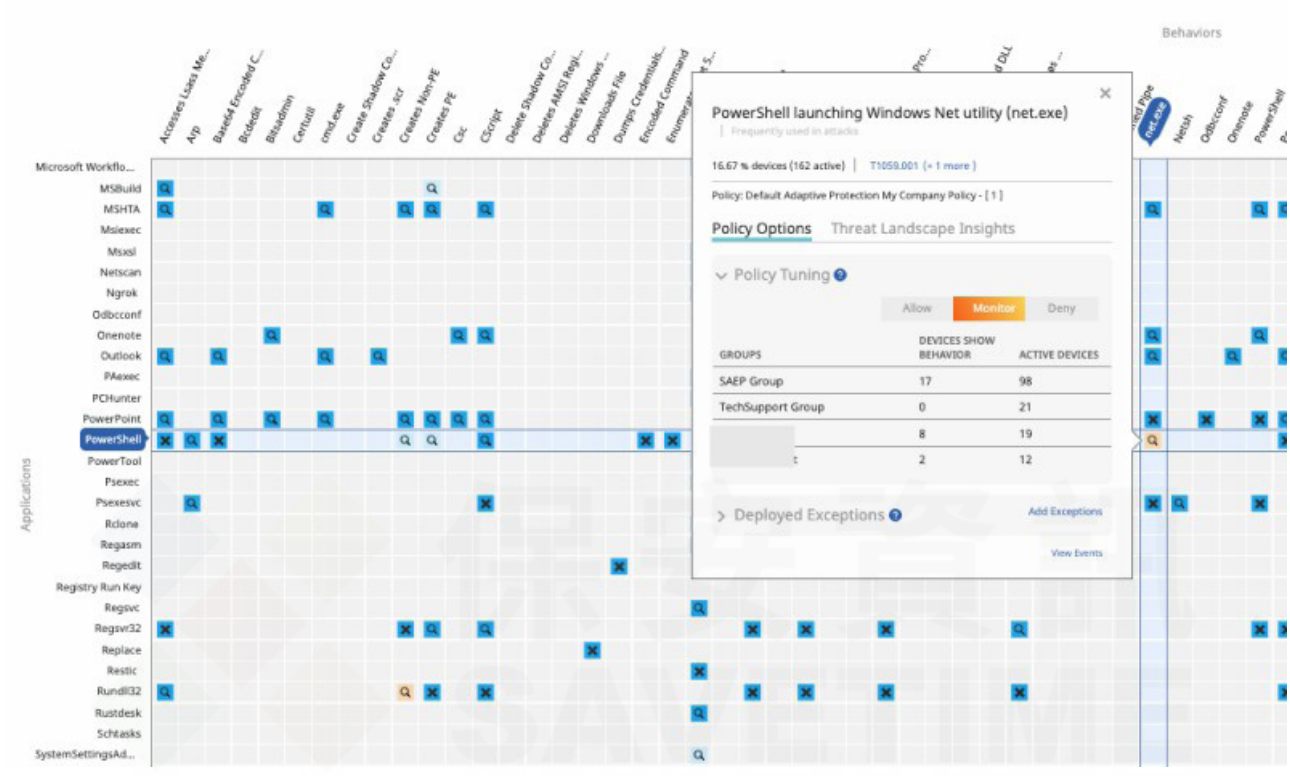
下表說明 Eldorado 與過去 RaaS 攻擊之間的交集，顯示使用共同的合法工具，例如：PowerShell、Scripts、WMI 和 Vssadmin。儘管威脅隨著時間演變，但工具和戰術仍保持一致。透過停用公司內不必要的應用程式行為，賽門鐵克的調適型防護 (Adaptive Security Protection) 可協助關閉攻擊者利用這些工具的大門，進而降低 LOTL 攻擊的風險。

下表列出了這些攻擊中發生的一些典型步驟：

行　為	Eldorado	Hive	LockBit
Word 下載／建立可執行或不可執行檔案	Y	Y	Y
Excel 下載／建立可執行或不可執行檔案	Y	N	N
PDF 下載／建立可執行或不可執行檔案	N	N	Y
Powershell 下載／建立可執行或不可執行檔案	Y	Y	Y
Powershell 執行網路指令	Y	Y	Y
Powershell 存取 http/https	N	Y	Y
Psexec／WMI 關閉安全軟體	Y	Y	Y
啟動 netscan 以掃描／診斷／調查／瞭解網路	N	Y	Y
Vssadmin 刪除磁碟區陰影複本	Y	Y	Y
使用 rclone.exe 竊取受害者資料	Y	N	Y

洞察力是改善防護的關鍵

以下 Adaptive Security 熱圖可深入瞭解組織內的行為使用情況，讓 IT 管理員可設定允許、監控或拒絕的行為。此外，它還可以建立例外情況，例如：一般將行為設定為拒絕，但在特定情況下則允許。



透過瞭解 RaaS 的演進並採用賽門鐵克的調適型防護 (Adaptive Security Protection)，企業可以更有效地防禦複雜的勒索軟體攻擊。停用不必要的工具和監控行為是降低 LOTL 戰術所造成風險的關鍵步驟。

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 Symantec Endpoint Security 中啟用調適型防護的資訊，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好用資源。

保安資訊連絡電話：**0800-381-500**。