賽門鐵克調適型防護(Adaptive Security Protection)有效對抗 Ymir 勒索軟體

2024 年 12 月 3 日發布

Ymir 的出現

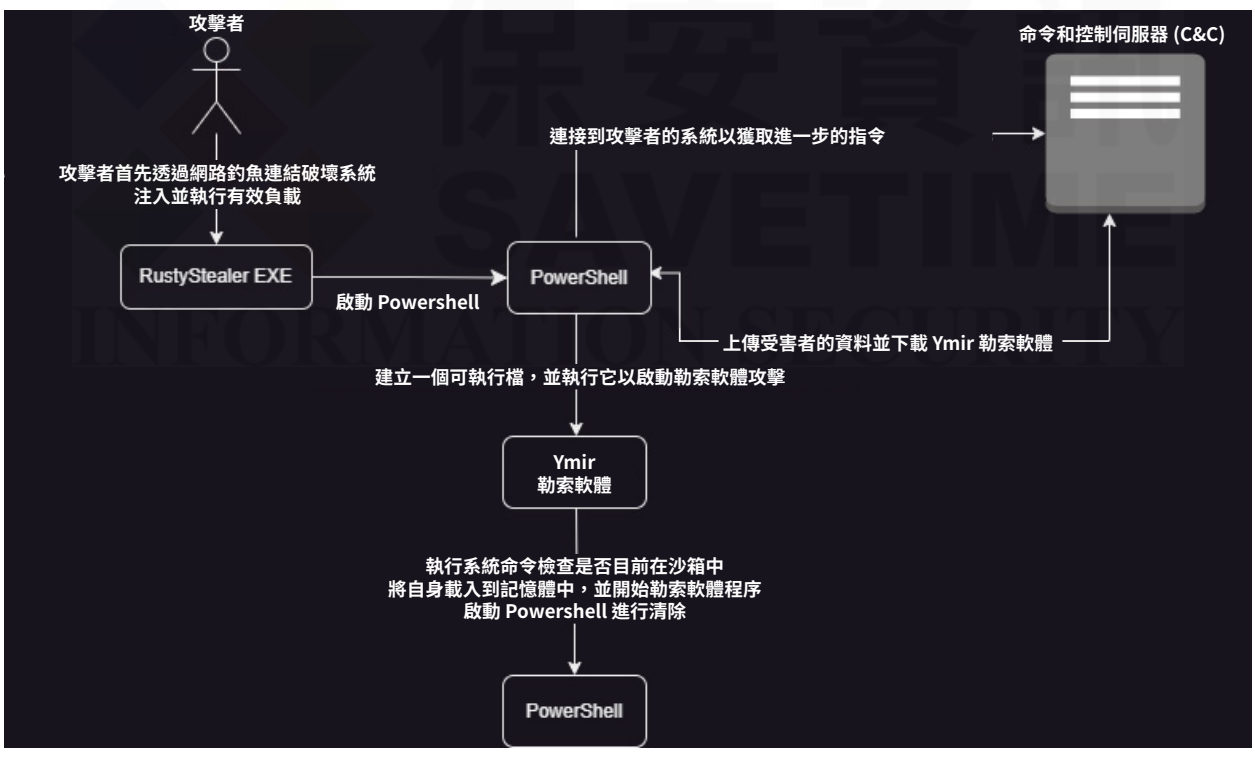
近期出現全新勒索軟體：Ymir，目標是哥倫比亞的一個組織。它利用先進的記憶體管理功能來執行惡意程式碼，並將惡意竊密程式 RustyStealer 整合到其攻擊鏈中。透過採用創新策略，Ymir 繞過許多針對現有勒索軟體家族所設計的安全防護措施。然而，賽門鐵克的調適型防護 (Adaptive Security Protection) 已經證明有能力降低此類新興威脅的風險。調適型防護 (Adaptive Security Protection) 可中斷攻擊鏈，即使是針對前所未見的威脅。

調適型防護(Adaptive Security Protection)：奠定端點防護日後長期發展的策略優勢

勒索軟體攻擊者通常會濫用，就像一般使用者或 IT 管理員操作的軟體或管理工具，這在資安範疇稱為就地取材 (LOTL：Living Off the Land) 攻擊。由於這些軟體或管理工具在組織內有其正當的用途，因此完全停用並不可行。雖然不同的攻擊者會個別修改特定步驟以逃避偵測，但他們對 LOTL 的依賴程度，相當一致。調適型防護 (Adaptive Security Protection) 以有益的方式解決這些挑戰，更可讓組織在不中斷其正當操作的情況下阻止 LOTL 攻擊。

Ymir 攻擊鏈：關鍵事件與防禦

下圖拆解成一個個步驟來說明 Ymir 勒索軟體攻擊鏈，凸顯其與 RustyStealer 惡意軟體和 PowerShell 的整合，以執行與其命令與控制 (C&C) 伺服器的通訊。



調適型防護 (Adaptive Security Protection) 在攻擊鏈的不同階段皆能有效力抗 Ymir 攻擊：

行　　為	調適型防護	曾出現在過往的勒索軟體攻擊？
執行 RustyStealer (不受信任的程序)	是	否
不受信任的程序執行 Powershell 指令碼，並與控制伺服器建立連線	是	是
Powershell 腳本上傳檔案	是	是
Powershell 執行 Base64 指令	是	是
InfoStealer 會建立 PE 檔案 (勒索軟體範例)	是	是
InfoStealer 會啟動 PE 檔案 (勒索軟體範例)	是	是
執行勒索軟體樣本	是	是
勒索軟體樣本啟動 Powershell	是	是

數字會說話：調適型防護 (Adaptive Security Protection) 有效力抗 Ymir 勒索軟體攻擊鏈

- 追蹤的行為： 橫跨 70 種應用程式的 493 種行為
- 受保護的端點： 超過 290 萬個
- 拒絕模式使用量： 客戶每次部署平均封鎖 342 個行為

調適型防護 (Adaptive Security Protection) 可確保對 Ymir 及類似演進中勒索軟體威脅進行強大的防禦，同時維持組織的作業效率。想要立即啟用 Adaptive Protection？查看以下連結了解詳情。

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。

欲瞭解賽門鐵克端點安全完整版(SESC)的調適型防護(Adaptive Security Protection)，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**。