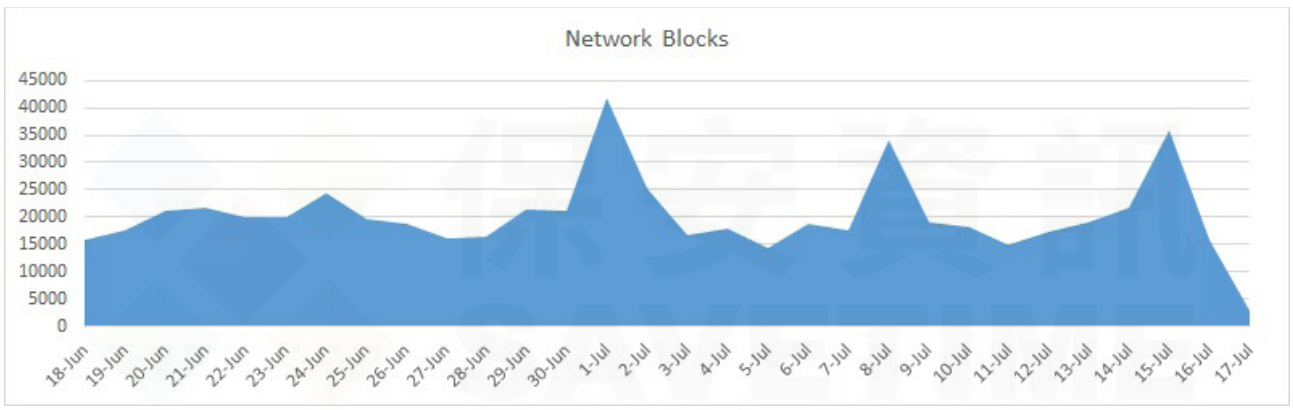
BlackByte 勒索軟體

2023 年 7 月 18 日發布

惡名昭章的勒索軟體攻擊者多年來一直在利用各種與威脅相關的策略、技術和程序 (Tactics、Techniques、Procedures，TTPs) 來執行攻擊並實現其目標。在這些攻擊者中，BlackByte 脫穎而出。最近報告顯示，他們可以在五天內就利用一系列的漏洞、後門和工具進行滲透、常駐、偵察、橫向移動、竊取資料和加密資訊，而完成致命性的攻擊。

ProxyShell 和 ProxyLogon 漏洞是各種威脅（包括勒索軟體）的目標，作為滲透系統的初始手段。下圖顯示了最近這些被封鎖的網路嘗試。



在 BlackByte 攻擊鏈中所採用的 TTPs 依 MITRE 所分類的包括以下內容：

* 濫用執行已簽章的代理程式：Rundll32 [T1218.011]
* 命令和腳本解釋器：Windows Command Shell [T1059.003]
* 啟動或登錄自動啟動執行：註冊表裡的Run Keys／啟動資料夾 [T1547.001]
* 軟體搜尋：安全軟體搜尋 [T1518.001]
* 遠端存取軟體 [T1219]
* 遠端系統搜尋 [T1018]
* 系統網路配置搜尋：Internet 連接搜尋 [T1016.001]
* 削弱防禦：禁用安全軟體或修改工具 [T1562.001]
* 禁止系統恢復 [T1490]
* 修改註冊表 [T1112]
* 網域信任搜尋 [T1482]
* 系統網路配置搜尋 [T1016]
* 帳戶搜尋 [T1087]
* 權限群組搜尋 [T1069]

BlackByte 勒索軟體最早在 2021 年首次發現，多年來，它針對醫療保健、製造和政府機構等不同行業所造成的災難而多次成為頭條新聞。目前，該攻擊者仍然活躍，據報導在過去兩個月裡已讓多個機構受害。

賽門鐵克針對BlackByte勒索軟體，提供完整的**零時差**保護，具體說明如下：

基於行為偵測技術(SONAR)的防護：

- SACM.Adfnd-Lnch!g1

端點偵測與回應(EDR)：

- 賽門鐵克 EDR 能夠監控和標記該威脅攻擊者的策略、技術和程序 (Tactics、Techniques、Procedures，TTPs)。
- 賽門鐵克新增特定惡意軟體的威脅搜尋查詢，客戶可以在 iCDM 控制台上觸發這些查詢。有關這些查詢的更多訊息，請參閱此 GitHub 儲存庫。

賽門鐵克端點檢測和回應 (EDR) 使用機器學習和行為分析來檢測和揭露可疑網路活動。EDR 會發出有關潛在有害活動的警報，對事件進行優先級排序以便快速分類，並允許事件回應人員瀏覽設備活動記錄以對潛在攻擊進行鑑識分析。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Blackbyte

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Audit: AnyDesk Remote Desktop Activity
- Audit: ADFind Tool Activity
- Attack: Microsoft Exchange Server CVE-2021-26855
- Web Attack: Microsoft Exchange Server RCE CVE-2021-34473
- Web Attack: Microsoft Exchange Server CVE-2021-34473
- Web Attack: Microsoft Exchange Server Elevation of Privilege CVE-2021-34523

SEP 的稽核用特徵資料庫 (Audit Signaturesare) 旨在提高對網路中潛在有害流量的認識。預設情況下，它們不會攔截。查看網路中 IPS 事件日誌的管理員可以記下這些稽核事件，並決定是否配置相應的簽章稽核來攔截流量。

基於機器學習的防禦技術：

- Heur.AdvML.B

基於安全強化政策(適用於使用DCS)：

- Symantec Data Center Security (DCS) 的Windows 版本，出廠即內建預設的強化策略提供針對未知威脅的零時差防護，包括以前未見過的勒索軟體變種和相關行為。
- Symantec DCS 針對 Microsoft Exchange 伺服器的預設強化策略就可防止 ProxyShell 漏洞。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

欲深入瞭解更多有關於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。
欲瞭解更多有關於賽門鐵克端點安全入侵防護系統 (IPS) 的更多訊息，請點擊此處。
欲瞭解賽門鐵克行為安全性技術如何防禦就地取材攻擊的威脅，請點擊此處。
欲深入瞭解賽門鐵克端點防護 (SEP) 的進階機器學習防護技術，請點擊此處。
欲瞭解有關賽門鐵克 (DCS：Data Center Security～資料中心安全的更多訊息，請點擊此處。
欲瞭解有關 Symantec 端點檢測和響應的訊息，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**。