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

LockBit-- 多產、持久、可預防

2023 年 6 月 26 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

LockBit 是一種勒索軟體即服務 (RaaS)，早在 2019 年 9 月就由賽門鐵克追踪為 Syrphid 的駭客集團所營運。它攻擊不同規模的組織，包括但不限於金融服務、專業服務、食品和農業、法律、教育、能源、緊急服務、醫療保健、製造和運輸，據信迄今為止共發動多達 1,700 起的網路攻擊，其中 1 起在 2022 年期間發生 6 組駭客一起針對美國政府的勒索軟體攻擊。LockBit 採用勒索軟體即服務 (RaaS) 營運模式，招募新的聯盟夥伴使用 LockBit 勒索軟體工具和基礎設施進行攻擊。這種多樣化的聯盟夥伴導致 LockBit 勒索軟體攻擊在其觀察到的戰術、技巧，以及程序 (TTPs) 等面向差異很大，使得組織更難以防禦。

LockBit 多年來不斷發展。最初在 2019 年首次發佈時稱自己為「ABCD 勒索軟體」，該聯盟夥伴計劃於 2020 年 1 月推出，然後 2020 年 9 月推出一個洩漏網站（其中列出拒絕支付贖金的受感染組織），LockBit 也採用雙重勒索戰術。2021 年，LockBit 2.0 開採利用一個名為 CVE-2018-13379 的陳年漏洞，針對澳洲亞組織。到 2021 年底，發布一個針對 VMware ESXi 虛擬機的 Linux 變種。2022 年 6 月出現 3.0 變種由於程式碼與 BlackMatter 和 Darkside 勒索軟體變種相似，因此被稱為「LockBit Black」。LockBit 3.0 可以刪除許多預定義的服務並終止某些程序。

同年 7 月，攻擊者被發現使用名為 Terminator 的工具來嘗試停用安全軟體。這些類型的攻擊就是利用含有弱點的驅動程式檔案，進行自帶驅動程式攻擊（BYOVD：Bring Your Own Vulnerable Driver），涉及使用有效數位簽章的合法驅動程式，這些驅動程式能夠執行特權指令，並被植入到受害者設備上以停用安全解決方案並接管系統。

賽門鐵克用戶應注意，只有當攻擊者擁有管理憑證並且 SEP 管理員已停用防篡改保護時，任何嘗試停止 SEP 的命令或工具才會起作用。

就在今年 4 月，還發現一種針對 macOS 平台的新 LockBit 變種，這些樣本似乎基於 LockBit 的 Linux 加密器，並且僅針對 macOS 進行編譯。來自安全研究人員的最新情報是，LockBit 操作似乎已經開始試驗其有效籌載的新版本，能夠攻擊多種架構，包括 Apple M1、ARM v6、ARM v7、FreeBSD 等。

像 LockBit 這樣危險且不斷演變的威脅需要同樣積極的回應。

賽門鐵克針對 LockBit 的眾多變種及其各個組件提供了**全面的保護**：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- OSX.Ransom.Lockbit
- Packed.Generic.686
- Ransom.Lockbit
- Ransom.Lockbit!g1
- Ransom.Lockbit!g2
- Ransom.Lockbit!g6
- Ransom.Lockbit!g7
- Ransom.Lockbit!gen3
- Ransom.Lockbit!gen4
- Ransom.Lockbit!gen5
- Ransom.Lockbit!gm1
- Scr.Malscript!gen1
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan Horse
- WS.Malware.1

基於行為偵測技術(SONAR)的防護：

- Ransom.Blackmater!gm1
- SONAR.Cryptlocker!g42
- SONAR.ProcHijack!gen5
- SONAR.ProcHijack!g45
- SONAR.Ransomware!g2
- SONAR.Ransomware!g7
- SONAR.RansomLckbit!g1
- SONAR.RansomLckbit!g2
- SONAR.RansomLckbit!g3
- SONAR.RansomLckbit!g4
- SONAR.RansomLckbit!g5
- SONAR.RansomNokibi!g1
- SONAR.SuspBeh!gen82
- SONAR.SuspBeh!gen742
- SONAR.SuspLaunch!gen4
- SONAR.SuspLaunch!gen18
- SONAR.SuspLaunch!g189
- SONAR.SuspLaunch!g190
- SONAR.SuspLaunch!g193
- SONAR.SuspLaunch!g195
- SONAR.SuspLaunch!g253
- SONAR.SuspReg!gen28
- SONAR.UACBypass!gen30

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C
- Heur.AdvML.B!100
- Heur.AdvML.B!200

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：

- Attack: Ransom.Lockbit Activity
- Attack: Ransom.Lockbit Activity 2
- Attack: Ransom.Lockbit Activity 3
- Web Attack: Webpulse Bad Reputation Domain Request
- Web Attack: Fortinet FortiOS Directory Traversal CVE-2018-13379
- Attack: Lockbit Ransomware Binary Copy GPO Config
- Attack: Lockbit Ransomware Enable Share GPO Config
- Attack: Lockbit Ransomware Security Services Taskkill GPO
- Attack: Lockbit Ransomware Services Disable GPO Config

基於安全強化政策(適用於使用DCS)：

- DCS 內建的強化政策可針對 LockBit 勒索軟體的零時差保護。
- 可疑程序執行：預防策略防止惡意軟體在系統上被植入或執行。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

郵件安全防護機制：

不管是地端自建 (SMG／SMSEX) 的郵件過濾／安全閘道及主機防護、雲端郵件安全服務 (E-mail Security.Cloud) 以及郵件威脅隔離 (ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護 (威脅不落地)。

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

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。
欲瞭解有關於賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，請點擊此處。
欲瞭解有關賽門鐵克基於雲的網路安全服務 (WebPulse) 的更多訊息，請單擊此處。

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**。