living-off-the land 技術勒索軟體防護的最新功能(SES和SEP)

最新更新日期：2025 年 1 月 27 日

Symantec Endpoint Protection (SEP) 和 Symantec Endpoint Security (SES) 包含一些增強功能，可保護用戶端電腦免受 living-off-the-land (LotL) 工具及惡意軟體市場的檔案、網路工具和其他一般攻擊工具的危害。

Living-off-the-land 策略—攻擊者利用目標系統上已存在的原生工具和服務，這些方法已被目標攻擊訓組和常見的網路犯罪集團所使用。

以下技術將防止目標性勒索軟體威脅。

14.3 RU9

- 已更新對以下勒索軟體威脅的保護：Akira、Albabat、Babuk、BiBi wiper、Black Basta、Blackcat、BlackHunt、BlackSuit、DoNex、Freeworld、Hunter International、Inc、Knight、Kuiper、Lockbit、Medusa、Mimic、Qilin、Phobos、Phoenix、Stop、Trigona、Tuga 勒索軟體系列以及勒索軟體攻擊中使用的各種工具。
- 改進了各種預勒索軟體和外滲工具 (包括 impacket、MegaSync、FileZilla 和 WinSCP) 的端點網路防護。

14.3 RU8

- 已更新針對以下勒索軟體威脅的保護：Akira、Bianlin、Blackbyte、Blackcat、BlackBasta、Crosslock、Hardbit、Hsharada、IceFire、Lockbit、Magniber、Moneybird、Moneymessage、Noberus、Nokoyawa、Rancoz、Royal 以及勒索軟體攻擊中使用的各種工具。
- 已更新針對以下惡意軟體的保護：Qakbot、AgentTesla、Gopuram、Icedid、Malicious Chrome WebExtensions、VipersoftX、Xworm。
- 已改善攻擊群組矯正 (AGR) 功能以支援更多程序終止。AGR 會識別偵測到的攻擊中所有元件，並確保移除攻擊中的每個程序和執行緒。
- 已增強針對 MSI 惡意軟體的掃描流程。
- 已增強對 IcedID 所使用 VBA 下載器的模擬支援。
- 已發佈針對 PDF 惡意軟體的新偵測框架。
- 已改善 OneNote 剖析器以擷取其他檔案類型。

14.3 RU7

- Hardbit、IceFire、Lockbit、Magniber、Moneymessage、Noberus、Nokoyawa、Royal 和各種前勒索軟體工具。

14.3 RU6

網路保護技術

- 對勒索軟體系列 (如 Conti、Avoslocker 和 Hive) 的改良網路保護。
- 改良的網路檢測和保護，避免在勒索軟體攻擊中使用的前勒索軟體工具。
- 改良的網路檢測和保護，避免在勒索軟體攻擊中使用的初始存取和水平擴散技術。

檔案檢測技術

- 對 LNK 威脅的改良模擬和分析。
- 對 HTML 威脅 (如 Qakbot 和 Gamaredon) 的改良模擬和分析。
- 改良的模擬和分析，避免在前勒索軟體活動中使用的 BAT 指令碼。
- 對前勒索軟體活動的改良 PowerShell 模擬。
- 對 VBA 擷取和 VBE/JSE 解碼的改良引擎功能。
- 已啟用非 PE 雲端查詢，進而提升非 PE 威脅的效力。

行為防護

- 對重新命名 LotLBins 的改良分析。
- 改良的 BASH 記憶體掃描效能和效力 (勒索軟體、Cobalt Strike)。
- 對 Bumblebee 等威脅的改良執行緒插入防護。
- 對巨大檔案威脅的改良 BPE 涵蓋範圍。
- AEP 和 JESE 掃描流程增強功能，以處理利用 svg 屬性來放置酬載的 Qakbot。
- 改良的一般勒索軟體 BPE 偵測，以減少大迴圈、多執行緒和免責問題。

14.3 RU5

網路保護技術

- 對勒索軟體系列 (如 Conti、Avoslocker 和 Hive) 的改良網路保護。
- 改良的網路檢測和保護，避免在勒索軟體攻擊中使用的前勒索軟體工具。
- 改良的網路檢測和保護，避免在勒索軟體攻擊中使用的初始存取和水平擴散技術。

行為防護

- 改良的一般勒索軟體 BPE 偵測，以減少大迴圈、多執行緒和免責問題。

14.3 RU4

網路保護技術

- 對勒索軟體系列 (如 Conti、Avoslocker 和 Hive) 的改良網路保護。
- 改良的網路檢測和保護，避免在勒索軟體攻擊中使用的前勒索軟體工具。
- 改良的網路檢測和保護，避免在勒索軟體攻擊中使用的初始存取和水平擴散技術。

檔案檢測技術

- 使用分析的強大保護，克服惡意軟體參與者濫用紅隊工具。
- 多建立了兩個指令行 subscanners (wbadmin.

exe 和 wevtutil.exe) 以改進前勒索軟體活動偵測。
- 針對 Macro 檔案電腦病毒改良的修復功能。
- 針對 PowerPoint 威脅改良的 Macro 擷取支援。

行為防護

- 針對基於 Python 勒索軟體改良的靜態和行為偵測。
- 為勒索軟體系列 (如 Conti) 啟用 DLL 格式的 BASH 記憶體掃描。Conti 勒索軟體將加密的 DLL 載入記憶體並執行。
- 建立四個新的指令行 subscanners 和多個新偵測，改進駭客工具和 LOLBins 的前勒索軟體活動檢測。LOLBins 是一種複雜的威脅，需要進階工具才能偵測到。
- 針對 Emotet 垃圾郵件活動改良的分數分析和 AMSI 偵測。
- 增強的記憶體掃描使用 SONAR 行為政策強制執行 (BPE) 來處理 Cobalt Strike 使用的程序注入技術。

14.3 RU3

網路保護技術

- 檢測在目標勒索軟體攻擊中使用的可疑程序鏈。
- 遙測增強功能，可在勒索軟體或前勒索軟體工具影響新的用戶端電腦時發出警告。
- 防止 Cobalt Strike 侵入後動作和水平擴散。
- 防止高普及率惡意軟體，如 IcedID。

檔案檢測技術

- 透過防惡意軟體掃描介面 (AMSI) 對 Office Open XML (OOXML)、Windows Management Instrumentation (WMI)、dotnet 和 XLM 進行加密的保護。
- Microsoft PowerShell 模擬啟發式改進，使用 AMSI 停用技術來檢測惡意軟體。
- 強化指令行啟發式技術，可防禦勒索軟體和 Cobalt Strike 駭客攻擊工具。
- 新增 PE 模擬器後繼掃描支援，利用垃圾迴圈和反模擬來改進惡意軟體的檢測。
- Visual Basic (VB) 和 dotnet 模擬器增強功能，可防止惡意軟體，如 Mass Logger、FormBook 和 Agent Tesla。
- 實施 Microsoft Office Scanner，檢測 VBA stomping 和非 PE 放置器，如 Hancitor。
- 包括常見解析器，用於支援 Microsoft Publisher 和 Microsoft Access 檔的 VBA 提取和模擬。
- 增強 AMSI 和指令碼模擬字串掃描，識別和矯正 LotL 惡意軟體，如 IsErIk。

行為防護

- 最小化對 lsass.exe 的讀取存取權限，增強憑證盜竊保護。
- 在可信任程序上觸發勒索軟體檢測時，鎖定檔案寫入存取，藉此增強勒索軟體保護。
- 增強對父程序詐騙技術的程序跟蹤。
- 將主執行緒的進入點位址與從磁片檔解析的進入點位址進行比較，對程序空白技術進行檢測。
- 檢測已停用的程序建立。
- 複雜勒索軟體的行為檢測，如 Ryuk、REvil/Sodinokibi、Conti、Darkside、Burglar 和 Lorenz。
- 一般勒索軟體預加密行為檢測，和使用檔

案重新命名事件新屬性的後加密檢測。

- 對 Cobalt Strike 侵入後動作和水平擴散的行為檢測，以及針對 Cobalt Strike 信號的記憶體檢測。
- 在程序控制代碼開啟時使用 SetThreadContext 函數和權限標誌，對 DLL 重新整理和程序注入技術進行的行為檢測。
- 對 Microsoft Office Excel 和 Microsoft Office PowerPoint 威脅的行為檢測。
- Symantec Endpoint Detection and Response (SEDR) 可視性，可將一些 BPE 檢測結果為進階攻擊技術 (AAT)。
- LoLBins 上的新 ACM 事件。

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**。

原廠網址：https://techdocs.broadcom.com/tw/zh-tw/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/Enhancements-that-protect-against-living-off-the-land-tools.html

本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。2025/1