賽門鐵克端點防護(SEP: Symantec Endpoint Protection) 針對加密勒索軟體最棘手的就地取材 (living-off-the land)攻擊的強化防護技術說明

最新更新日期：2023/04/15

賽門鐵克端點防護 (SEP：Symantec Endpoint Protection) 包括增強功能，可保護您的用戶端電腦免受惡意軟體市場中可用的就地取材 (LotL：living-off-the-land) 工具以及檔案、網路工具和其他一般攻擊工具的侵害。

有針對性的攻擊組織和常見的網路犯罪集團都在使用就地取材 (LotL：living-off-the-land) 戰術--攻擊者利用目標系統上已經存在的本地軟體工具和服務。

賽門鐵克端點防護 (SEP：Symantec Endpoint Protection) 最新版本新增以下技術來特別防禦目標式勒索軟體攻擊。

最新 14.3 RU7 (釋出時間 2023/03/27)

◎14.3 RU6

網路層防護技術

- 對勒索軟體系列 (例如：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 (例如：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。

基於行為的防護技術

- 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

網路層防護技術

- 對勒索軟體系列 (例如：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。

基於行為的防護技術

- 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

網路層防護技術

- 強化對 Conti、Avoslocker 和 Hive 等勒索軟體系列的網路層保護。
- 強化對勒索軟體攻擊中使用勒索軟體套裝工具組的網路檢測和保護。
- 強化對勒索軟體攻擊中使用的初始存取和橫向移動技術的網路檢測和保護。

檔案檢測技術

- 增強分析能力來減少惡意軟體參與者濫用紅隊工具的強大保護。
- 新建立另外兩個命令列子掃描執行序（wbadmin.exe 和 wevtutil.exe）以強化勒索軟體活動檢測。
- 強化巨集檔案受感染時的修復能力。
- 強化對 PowerPoint 威脅的巨集參數解析支援。

基於行為的防護技術

- 強化對於 Python 所撰寫的勒索軟體的靜態和行為檢測。
- 為 Conti 等勒索軟體系列啟用 DLL 格式的 BASH (Behavioural Analysis and System Heuristics 行為分析和系統啟發式) 記憶體掃描。Conti 勒索軟體會將加密的 DLL 載入到記憶體中，然後執行它。
- 透過建立四個新的命令列子掃描程式和多個新檢測方法，強化了針對駭客工具和就地取材 (LOLBins) 的套裝勒索軟體活動檢測。就地取材 (LOLBins) 是一種複雜的威脅，檢測它們需要更進階的工具。
- 強化 Emotet 垃圾郵件活動的啟發式評分和防惡意軟體掃描介面 AMSI (Antimalware Scan Interface) 檢測。
- 使用 SONAR 行為政策執行 (BPE：Behavioral Policy Enforcement) 的記憶體增強掃描，以處理 Cobalt Strike 使用的執行緒載入技術。

◎14.3 RU3

網路層防護技術

- 偵測被使用於目標性式勒索軟體攻擊的可疑程序鏈。
- 增強遙測大數據分析功能，可在勒索軟體或勒索軟體工具影響新用戶的電腦前發送警報。
- 防止 Cobalt Strike 漏洞利用後的攻擊行動和橫向移動。
- 防禦最常見的惡意軟體，例如：IcedID。

檔案檢測技術

- 使用防惡意軟體掃描介面 AMSI(Antimalware Scan Interface)來加密 Office Open XML (OOXML)、Windows Management Instrumentation (WMI)、dotnet 和 XLM 以提高防護。
- 使用 AMSI 停用技術偵測惡意軟體的 Microsoft PowerShell 模擬啓發式強化功能。
- 增強命令列啟發式以防止勒索軟體和 Cobalt Strike 駭客工具。
- 新增 PE 模擬器執行後掃描支援，以增進具

有垃圾迴圈和反仿真技術的惡意軟體偵測。

- Visual Basic (VB) 和 dotnet 模擬器增強功能，可防禦 Mass Logger、FormBook 和 Agent Tesla 等惡意軟體。
- 實施 Microsoft Office Scanner 以偵測 VBA stomping 和非 PE 型植入程式 (dropper) (如：Hancitor)。
- 包含支援從 Microsoft Publisher 和 Microsoft Access 檔案中提取和模擬 VBA 的通用分析器。
- 增強了 AMSI 和腳本模擬字符掃描，以識別和修復就地取材 (LotL) 惡意軟體，例如：IsErIk。

基於行為的防護技術

- 透過去除對 lsass.exe 的讀取權限，增強了憑證盜竊保護。
- 當在受信任的程序上觸發勒索軟體偵測時，透過鎖定檔案寫入權限來增強勒索軟體保護。
- 增強父程序欺騙技術的程序追踪。
- 透過將主線程的入口點位址與從磁碟檔案解析的入口點位址進行比較，來偵測程序挖空技術。
- 偵測暫停的程序建立。
- 惡名昭彰的勒索軟體之行為偵測，例如：Ryuk、REvil／Sodinokibi、Conti、Darkside、Burglar 和 Lorenz。
- 利用檔案重命名事件新屬性的通用勒索軟體加密前行為偵測和加密後偵測。
- Cobalt Strike 漏洞利用後動作和橫向移動，以及 Cobalt Strike信標 (beacon) 記憶體偵測的行為偵測。
- 透過在程序處理初啟時使用 SetThreadContext 函數和權限標誌來偵測 DLL 重新整理和程序注入技術的行為。
- 與 Microsoft Office Excel 和 Microsoft Office PowerPoint 相關威脅的行為偵測。
- 賽門鐵克端點偵測和回應 (SEDR) 的可視性可將一些 SONAR 行為政策強制 (BPE：Behavioral Policy Enforcement) 偵測轉換為進階攻擊技術 (AAT：Advanced Attack Techniques)。
- 針對就地取材攻擊方法 (LoLBins) 提供新的 ACM 事件紀錄。

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

更多資訊 請造訪我們的網站 **http://www.SaveTime.com.tw**
(好記：幫您節省時間.的公司.在台灣)

關於保安資訊：

從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

- 保安資訊被業界公認為最專業的賽門鐵克解決方案的專家。
- 保安資訊的團隊自 1995 年起就專注於賽門鐵克資訊安全解決方案的銷售、規劃與整合、技術支援、教育訓練、顧問服務，特別是提供企業 IT 專業人員的技能傳承 (Knowledge Transfer) 的效益上，以及比原廠更快速的技術支援回應，深獲許多中大型企業與組織的青睞(特別是有 IT Team 的組織)，長期合作的意願與滿意度極高。
- 與許多系統整合或服務公司不同的是，我們不吝惜分享我們的專業技能與經驗給顧客的 IT Team，經由常態性的教育訓練、精簡的快速手冊、標準 SOP 文件的提供，以及基於比原廠更孰悉顧客的使用環境與現況的快速回應的品質，在業界建立扎實的口碑。
- 保安資訊一直專注於賽門鐵克領先業界的資訊系統基礎架構上的安全性與可用性的解決方案。進而累積了許多與基礎架構整合的成功經驗，讓導入 Symantec 解決方方案的成效非常卓越。我們的顧客都能免除 Try & Error 的時間浪費及不確定的投入或自行摸索的運作風險。
- 保關於我們：

保安資訊有限公司
http://www.savetime.com.tw
0800-381500、0936-285588