思科安全端點取證快照資訊

目錄

簡介

本文檔介紹取證快照可以從端點收集的特權資訊。

作者：思科軟體工程師Pedro Medina。

必要條件

- 思科「安全終端」控制檯
- 思科「軌道」

需求

- 通過管理員或非管理員使用者訪問「安全終端」
- 訪問思科「軌道」

  附註：如果您的使用者是非管理員，則必須通過TAC支援團隊請求啟用「非管理員的取證快照」功能。

一般資訊

請求取證快照後，資訊將以表格式顯示，基於所需的資訊，使用者可基於此說明表找到任何所需的資訊：

名稱	它意味著什麼	隱私問題
Autoexec專案	電腦啟動時運行的項	無
Bitlocker加密監視	每個已裝載驅動器的加密狀態	對檔案的未加密版本有一些可見性
DNS快取表監控	最近搜尋的域	最近的瀏覽器歷史記錄。
主機檔案資料	hosts檔案中的專案	無
主機上已安裝的程式	已安裝的應用程式	無

偵聽埠	列出開啟網路偵聽器的程式	無
已載入的模組雜湊	運行動態連結庫(DLL)檔案的雜湊值	無
已載入的模組進程	正在運行的進程的名稱、路徑和PID	無
已載入的模組與進程	從已載入模組到「進程」表中PID的模組ID對映	無
登入會話	登入使用者，包括系統使用者	無
對映驅動器	本地和遠端掛載點、檔案系統型別、引導分割槽資訊、加密資訊。	無
網路連線 — 進程	將內和出站網路連線對映到特定PID，並顯示啟動該過程的啟動命令列。	可能暴露某些應用程式的網路連線（可私有的）。
網路介面	裝置上所有物理和虛擬網路介面的清單	無
網路設定檔登錄檔	電腦所連線的網路的清單。	WIFI SSID可能洩漏。
作業系統版本	作業系統的版本	無
Powershell歷史記錄	裝置上運行並儲存在系統中的所有Powershell命令的清單。	可能暴露密碼、秘密API金鑰和編碼到指中的其他敏感資料。
預回遷目錄	記憶體管理功能 — 作業系統將嘗試預載入頻繁的執行檔，以節省啟動時間。	使用者習慣的暴露。
最近的檔案資料	最近使用/訪問的檔案	暴露使用者習慣和私有檔名。
運行檔案雜湊	名稱、路徑、命令列、PID、所有正在運行的執行檔的所有者。	無
運行服務監控	所有運行服務的名稱、服務型別、PID和啟動型別	無
計畫任務	設定為在系統上定期運行的所有自動任務清單	無
共用資源	開啟系統中的共用	無
啟動專案	在電腦啟動時運行的項 — 與autoexec不同，這些項儲存在登錄檔項中	無
系統網路狀態監控	網路統計資訊	無
臨時目錄檔案資料	進程建立的臨時檔案	使用者瀏覽歷史的可能曝光次數。
受信任的根證書	受信任的根證書儲存資料轉儲	無

UBSTOR登錄檔項	插入USB裝置的歷史記錄	顯示裝置序列號。
使用者組	電腦上的本地組	無
UserAssist監控	顯示最近執行的檔案	可能暴露隱藏行為，例如運行加密或擦具。
使用者	裝置上的本地使用者	無
使用者 — 已登入	當前登入到裝置的本地使用者	無
WMI事件過濾器監視	監視特定專案的事件日誌	無
Windows AV產品監控	系統上安裝了防病毒軟體（如果有）	無
Windows BAM條目監視	提供檔案執行證據	可能暴露行為
Windows環境變數	顯示路徑資訊、系統變數等。	無
Windows修補程式	所有已安裝的修補程式清單	無
Windows NT域搜尋	電腦可以對其進行身份驗證的域清單	無
Windows ShellBags監視	提供有關使用者對資料夾的訪問許可權、檢視該資料夾的首選項等的資訊。	使用者習慣的暴露。
Windows ShimCache監視	跟蹤與執行檔的相容性	使用者行為的暴露。
Chrome擴充模組	列出Chrome擴展	使用者行為的暴露。
Windows Office MRU	列出每個Office應用程式最近使用的檔案	敏感檔名的暴露、使用者行為