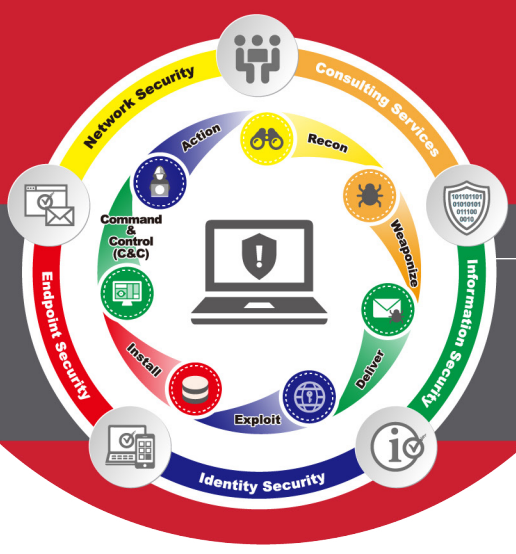

賽門鐵克端點上的網路層入侵防護系統 (IPS) 的稽核特徵，精準發現兩用工具的異常活動

2024 年 9 月 10 日發布

兩用工具

所謂兩用工具，即本身是可運行在電腦中的合法工具，但可被惡意威脅者用來發動攻擊。此類攻擊讓攻擊者不需另外撰寫惡意程式，因其工具的合法特性不易被使用者或安全工具偵測，也更難被追蹤和特定組織的關聯性。常見的兩用工具會隨作業系統一起安裝或常見的網管或遠端連線軟體。例如：Psexec、Nmap、Remote Desktop、AnyDesk。對於許多最近的威脅 (例如：RansomHub)，兩用工具被觀察到是攻擊鏈的一部分。網路掃描工具和遠端存取軟體被攻擊者用來探索受害者網路樣貌和橫向移動。在部署勒索軟體之前，通常會看到這些工具的活動。

賽門鐵克的端點上網路層入侵防護系統(IPS)之稽核特徵

賽門鐵克端點上的網路層入侵防護系統 (IPS) 引擎的主要功能之一是稽核特徵。這些稽核特徵有許多是常用於針對勒索攻擊等的雙重用途工具，已知 RansomHub 所屬的組織會利用這些工具進行橫向移動。對於不使用這些工具執行日常裝置管理任務的管理員而言，稽核特徵有助於通知網路內的不尋常活動。

政策組態

SEP 管理員可以設定政策，將稽核特徵動作設定為允許或封鎖，並將特徵記錄設定為記錄或不記錄。預設情況下，這些稽核特徵會設定為允許和不記錄流量。Broadcom 的線上技術文件說明可引導如何設定 SEP 並變更 IPS 稽核特徵偵測的動作。

RansomHub與兩用工具防護

以下是賽門鐵克發佈一些 IPS 稽核特徵，用於偵測兩用工具。根據定義，並非所有使用這些工具的行為都是惡意，但特徵名稱中提及的程式已知會在 RansomHub 感染前的階段出現。

- 30068 - Audit: PSExec Utility Activity
- 34633 - Audit: FileZilla SFTP Activity
- 33290 - Audit: Network Scanner Activity
- 33588 - Audit: WMIC Remote RPC Interface Bind Attempt
- 33211 - Audit: AnyDesk Remote Desktop Activity
- 34540 - Audit: Anydesk Tool Download
- 34697 - Audit: WinSCP Connecting to Public IP
- 33119 - Audit: RClone Tool Activity
- 33256 - Audit: RClone Tool Activity 2
- 34781 - Audit: RClone MegaSync Connect
- 34796 - Audit: RClone Tool Activity 3

稽核特徵碼33211--AnyDesk Activity

以 ID 33211--Audit：AnyDesk Remote Desktop Activity為例。賽門鐵克 IPS 每天都會在所有 SEP 端點上出現此特徵碼平均攔截約 100,000 次網路流量嘗試，因為 SEP 客戶已採取行動設定入侵防護政策，選擇加入此攔截動作。

*** SEP 的稽核特徵碼主要在提高對網路中可能不需要流量的警覺性。預設情況下，它們不會封鎖。管理員檢閱其網路上 IPS 事件日誌時，可以注意到這些稽核事件，並決定是否設定相對應的稽核特徵碼以封鎖流量。*

建議客戶在桌機／筆電和伺服器上啟用 IPS，以獲得最佳保護。請點擊此處瞭解啟用 IPS 的說明。
欲瞭解如何整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站，請點擊此處。
沒有使用 SEP 也行？可使用賽門鐵克瀏覽器防護服務保護您的瀏覽器。
欲瞭解賽門鐵克的端點上的網路層入侵防護系統 (IPS) 的稽核特徵，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**。