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

賽門鐵克網路層入侵預防 (IPS) 技術有效封鎖端點上的 SMB 攻擊

2023 年 4 月 17 日發布

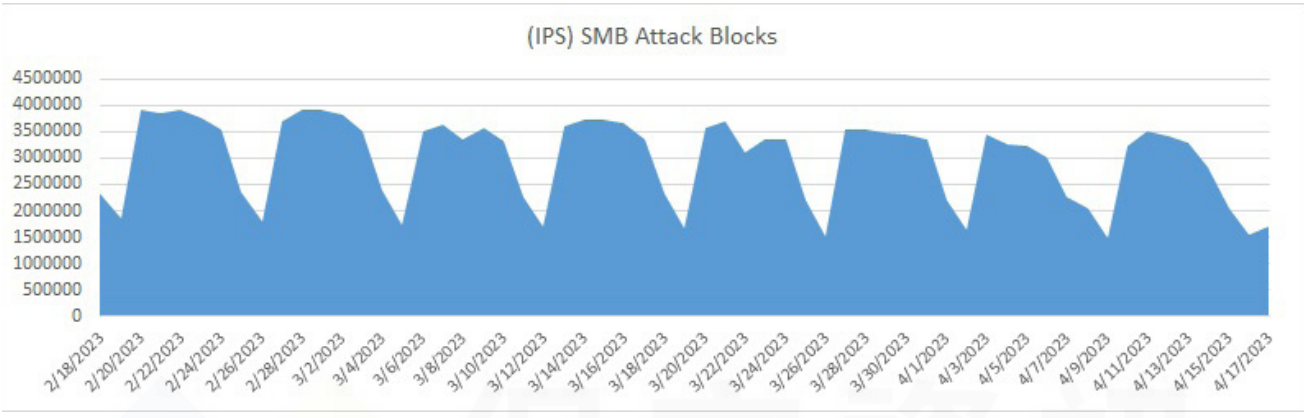
點擊此處可獲取--最完整的賽門鐵克解決方案資訊

伺服器訊息區塊 (SMB:Server Message Block) 一種用戶端 (Client)--伺服器 (Server) 應用層網路傳輸協定，主要由 Windows 作業系統使用，但也在 Linux 和 macOS 電腦上使用，主要功能是讓網路上的機器能夠共享檔案、印表機、串列埠及通訊等資源。由 IBM 早在 1980 年代早期就開發出來，隨即備受網路工程師矚目並廣受應用，其通訊是透過使用 TCP 139 和 445 埠號。直到今天，SMB 仍然是工作場所共享檔案的最常見方法之一。但是，儘管多年來該協議已多次更新以滿足不斷變化的網路要求，但許多設備仍在運行較舊、安全性較低的版本，這不可避免地使其成為網路犯罪分子的主要目標。

SMB 攻擊是一種網路攻擊，其目標是 SMB 傳輸協定中的漏洞，以便獲得對網路未經授權的存取權限，再進展到內網的橫向移動（橫向移動是攻擊者用來推進攻擊鏈從初始入口點進入網路的伎倆）獲得對其他網路資源的存取權限。兩個舉世皆知的 SMB 攻擊--包括 2017 年的“永恆之藍”漏洞利用 (CVE-2017-0144)，同樣惡名昭彰“WannaCry”勒索軟體利用它產生巨大影響，以及最近 SolarWinds 發動供應鏈攻擊，也利用 SMB 協議中的漏洞。

常見的 SMB 攻擊包括：

* SMB 暴力攻擊：暴力攻擊是一種反覆試驗不同帳號與密碼以獲取存取目標電腦的方法。可以手動完成 ，也可以透過自動化工具完成。
* SMB 中繼攻擊：一種中間人 (MITM) 攻擊，攻擊者攔截兩台機器之間的 SMB 流量，再將流量中繼到攻擊者操控的第三方電腦。這允許攻擊者無需有效憑證即可存取目標系統。
* SMB 蠕蟲化攻擊：這些攻擊使用通過利用 SMB 協議中的漏洞，在網路中傳播惡意軟體。一旦惡意軟體感染了一個系統，它就可以傳播到網路上的其他系統。
* SMB 阻斷服務攻擊：此類攻擊涉及用大量 SMB 請求讓目標系統無法負荷，導致系統崩潰或影響其可用性。



賽門鐵克已經於第一時間提供多種有效保護 (**SEP**/**SESC**/**SMG**/**SMSMEX**/**Email.Security.cloud**/**DCS**/**EDR**)。以下說明為 Symantec **零時差**防護技術偵測到的惡意程式名稱及有效對應的防護機制：

網路層攔截防護技術的特徵檔名稱：

- Attack: Bluwimps SMB Activity
- Attack: Fake SMB Server Response
- Attack: SMB Arbitrary Service Create Request 2
- Attack: SMB Double Pulsar Ping
- Attack: SMB Double Pulsar Response
- Attack: SMB PE File Drop Startup Directory
- OS Attack: Microsoft SMB MS17-010 Disclosure Attempt
- OS Attack: Microsoft SMB MS17-010 Shellcode Attempt
- OS Attack: Microsoft Windows SMB RCE CVE-2017-0144
- OS Attack: Microsoft Windows SMB Remote Code Execution CVE-2017-0143*
- OS Attack: Microsoft Windows SMB Remote Code Execution CVE-2017-0144*
- OS Attack: MS SMB2 Validate Provider Callback CVE-2009-3103
- OS Attack: SMB EFS NTLM Relay Attempt
- OS Attack: SMB Validate Provider Callback CVE-2009-3103
- OS Attack: Windows SMBv3 CVE-2020-1206
- System Infected: Bad Reputation File SMB Request

網路層稽核管理技術的特徵檔名稱：**

- Audit: Bad Reputation File SMB Request
- Audit: Microsoft Compressed SMB Packet
- Audit: SMB Admin Share Connect Request
- Audit: SMB Bruteforce Attempt
- Audit: SMB Exchange Server WebShell Access Attempt
- Audit: SMB Request From External Host
- Audit: SMB Suspicious DLL Create Attempt
- Audit: SMB Suspicious Folder File Creation
- Audit: SMB Unimplemented Trans2 Subcommand
- Audit: SMB Windows Print Spooler RpcAddPrinterDriverEx Attempt
- Audit: SMBv1 NTLM Authentication Attempt
- Audit: SMBv1 Traffic Request
- Audit: SMBv2 NTLM Authentication Attempt
- Audit: Suspicious SMB Client Activity
- Audit: Suspicious SMB Client Request*
- Audit: Suspicious SMB Server Response

* *這表示存在多個類似名稱的檢測，例如：Audit: Suspicious SMB Client Request2、Audit: Suspicious SMB Client Request3……等。*

** *SEP 的稽核特徵檔旨在提高對網路中可能不需要的流量認識。預設情況下，它們不會攔截。管理員可以查看網路中 IPS 事件日誌所記錄這些稽核事件，並決定是否配置相應的稽核特徵檔來攔截流量。*

要了解更多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。

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**。