本月威脅：SMB 與蠕蟲重現

這是什麼？

SMB（伺服器訊息區）是一種網路通訊協定，能加速電腦對電腦的互通，例如檔案共用、網路列印，或與各種裝置連線。由於 Microsoft 自 1990 年代初期起採用、建置和投資，SMB 曾是最熱門的一種網路檔案共用通訊協定。在 Windows 中設定及使用 SMB 非常簡單，只需簡單幾個步驟就可完成，同時就能應用於多種不同用途。SMB 能提供無縫式體驗：您可以從電腦自由存取遠端電腦的檔案。由於電腦間可以直接連線，因此您不需要另外準備伺服器來建立通訊。

為何您應該關心？

儘管非常方便，SMB 也有著缺點。作為電腦間通訊用的通訊協定，想入侵網路的駭客自然會將 SMB 視為攻擊目標。另外，駭客也理所當然選擇將蠕蟲散布到網路上，並在電腦間互相感染，植入惡意攻擊軟體。

哪些威脅會以 SMB 為目標？

其中一種 SMB 的主要漏洞是 2017 年發現的永恆之藍 (EternalBlue)。駭客會利用這個漏洞在受害者的電腦中安裝惡意軟體。在發現漏洞後不久，利用永恆之藍來傳播 WannaCry 病毒就出現了。再過一個月後，又出現了名為 Nyetya 的威脅。另外，包括 SamSam、Bad Rabbit 和 Olympic Destroyer 在內，還有許多威脅雖然不會利用永恆之藍漏洞，但仍會運用 SMB 來入侵電腦。

為何我們重視這一點？

SMB 讓人輕鬆設定當地電腦間的網路。然而，簡單易用的特性也帶來了許多風險。SMB 在連線共用時幾乎完全不需要驗證，而且連線時也不會加密。雖然後續版本改善安全性，但由於回溯相容性的關係，儘管已遭指出不安全很長一段時間，仍有人持續在使用舊版。在連線至電腦的方式如此不安全的情況下，這種通訊協定自然會成為駭客和蠕蟲的攻擊目標。

深入閱讀

https://blog.talosintelligence.com/2017/05/wannacry.html

https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html

https://blog.talosintelligence.com/2018/01/samsam-evolution-continues-netting-over.html

https://blog.talosintelligence.com/2017/10/bad-rabbit.html

https://blog.talosintelligence.com/2018/02/olympic-destroyer.html

CXX-XXXXXX-00 01/19

瞭解我該怎麼做？

時至今日，已經沒有多少繼續使用 SMB 的理由了，因此最簡單的解決方案就是停止使用 SMB。若要共用檔案，比起透過 SMB 連結電腦，使用專屬的檔案伺服器或雲端型服務是更好的選擇。請將網路印表機設定為改用其他通訊協議。若您無法關閉環境中的 SMB，至少停用 SMB1。封鎖網路邊界的 TCP 連接埠 445 和 139，確保 SMB 通訊限制在內部網路中。此外，您也不應讓端點能透過 SMB 與其他端點通訊。

思科如何保護您？

新世代防火牆/新世代入侵防禦系統	偵測並封鎖與 SMB 攻擊有關的惡意流量。
進階惡意軟體防護 (AMP) 終端版	透過持續監控和回溯安全功能，阻止SMB 帶來的威脅。
思科 Stealthwatch®	偵測 SMB 共用的連線，建立與此活動的關聯來警告管理員。
Threat Grid	協助識別惡意檔案行為，並自動通知所有思科資安產品。