


# 賽門鐵克重要主機防護系統：DCS～Data Center Security--針對好工具總被來當凶器的就地取材攻擊(LOTL)提供強大防護～以PowerShell攻擊為例

2025 年 4 月 29 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

## 就地取材攻擊 (LOTL-Living Off the Land) 如何運作？

與傳統的惡意軟體攻擊不同，LOTL 會利用系統內建或合法工具軟體來執行攻擊計畫，它是無檔案攻擊的一種--攻擊者不需要在目標系統安裝任何程式碼或腳本。相反地，攻擊者會使用環境中已有的工具，例如：PowerShell、Windows Management Instrumentation (WMI) 或密碼儲存工具 Mimikatz 來執行攻擊。

PowerShell 是常用於執行例行性排程自動化和組態管理的工具。網路威脅份子經常利用就地取材攻擊戰略濫用此公用程式。PowerShell 是用於排程自動化和組態管理的強大工具，建構在 .NET 架構上。它由指令 shell 和腳本語言組成，支援多種平台，包括 Windows 和 Linux。一旦入侵受害者環境，多數的勒索軟體和惡意軟體會使用 PowerShell 執行各種任務。PowerShell 腳本也常用於部署勒索軟體、停止 Windows Defender 等服務、刪除陰影複本、修改本機帳號、廣播 MAC 位址，以及包含修改 README 檔案的關聯以允許雙擊開啟等諸多惡意行為。

LOTL 威脅不是將惡意程式碼引入系統，而是使用系統上的現有工具來規避資安軟體偵測，這使得這些網路攻擊更難被偵測和緩解。這些技術可能發生在多種類型的 IT 環境中，包括本地端、雲端或混合環境。國家級駭客組織經常使用這些技術來逃避偵測。

## 對組織的資安衝擊

由於成功利用漏洞會導致遠端程式碼執行、竊取敏感資訊及組織網路的進一步橫向移動，因此其影響程度被視為嚴重等級。這些漏洞在網路上會被大肆濫用。更廣泛的安全社群已聯合起來保護 PowerShell，並發表多份相關的詳細刊物，包括賽門鐵克的多份刊物。他們協助全球受影響的使用者，深入分析威脅份子所使用的技術、可用的防護範圍，並提供進一步的指導，讓使用者留意入侵指標與緩解策略。

## 賽門鐵克重要主機防護系統：DCS～Data Center Security--防禦 LOTL 攻擊的有效零時差解決方案

賽門鐵克重要主機防護系統：DCS～Data Center Security 的入侵防護預設政策能為 Windows 和 Linux 伺服器提供零時差防護。傳統的防毒軟體使用定義檔偵測來識別惡意軟體。然而，過去幾年來，無檔案惡意軟體和 LotL 攻擊的增加，迫使業界重新思考如何偵測惡意軟體，進而需要啟發式演算法。

PowerShell 與其他指令碼語言一樣，可以直接在記憶體中啟用，並執行遠端下載有效酬載的指令，繞過安全防護機制，而且幾乎不會在磁碟上留下任何蛛絲馬跡供防禦人員識別和分析。使用 PowerShell 的惡意軟體可以進行權限提升、混淆和遠端程式碼執行等活動。近年來，有幾種惡意軟體家族將 PowerShell 做為凶器，包括 Netwalker、RogueRobin、PowerWare 和 POWELIK。此外，許多合法的後期攻擊框架 (例如：Metasploit、PowerSploit 和 Mimikatz) 也使用 PowerShell，這些框架也可以兼作 CTA 用來攻擊系統和竊取憑證的武器。說到底，濫用 PowerShell 的攻擊不會在短時間內消失，這也就是為什麼在日常工作中使用 PowerShell 的同時，必須加強防禦以免好工具總被來當凶器的主要原因。

## DCS 入侵防護系統

DCS 入侵防護系統提供零時差保護，包括：作業系統鎖定、應用程式控制以及實體和虛擬伺服器工作負載的應用程式隔離。針對作業系統和應用程式 (包括 PowerShell) 的底層沙箱技術和政策強制的行為控制，可針對未知威脅提供主動式防護，而無需一直依賴持續的定義檔更新。DCS 為全球客戶的關鍵基礎架構提供保護，二十多年來，大型企業對 DCS 技術堆棧深信不疑。

## 預設 DCS 的Windows 強化政策

預設的 DCS Windows 強化政策與其預先定義的沙箱可防止威脅者在攻擊期間和攻擊後使用的多種攻擊技術。縱深防護策略可在攻擊鏈的各個階段提供如下 (不限於) 保護：

- DCS 可防止透過子程序使用就地取材技術的執行。
- 啟用沙箱執行控制，以防止任何程序啟動可疑的子程序。
- 將 *\cmd.exe、*\powershell.exe、*\powershell_ISE.exe、*\rundll32.exe、*\net.exe 加入不應由其他應用程式啟動的程式清單。
- 兩用工具可從預先定義的全域原則服務清單中讓它不應被啟動。如果需要執行特定工具，則可根據部署中的使用情況，新增 cmdline 參數和/或使用者名稱的例外。
- 將*.zip、*.rar、*.7z、*.php、*.asp、*.aspx、*.asmx、*.asax、*.jsp、*.js 新增至「Read only Resource」清單，以防止從 powershell.exe 及其子程序寫入更多任意檔案。在政策沙箱中阻止修改這些檔案。與眾不同的是 DCS 可非常精細地控制允許例外。

賽門鐵克重要主機防護系統：DCS～Data Center Security 能提供最完整的伺服器防護，可在私有雲／公有雲資料中心實現微分段、限縮管理員權限、緩解進行修補的急迫性，以及防護零時差威脅。

關於賽門鐵克的重要主機防護系統：DCS～Data Center Security 的完整資訊可點擊網頁說明或最新簡報檔。網頁或簡報如有說明不夠清楚的地方，歡迎與保安資訊的業務或技術顧問提供建議。

## 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**。