這裡是DLP機密文件測試

針對後[疫情](https://udn.com/search/tagging/2/%E7%96%AB%E6%83%85)時代的工作模式，Cisco強調將以旗下技術強化混合辦公體驗，同時也針對企業需求打造更安全的5G專網託管服務，並且以旗下自製處理器Silicon One打造高功率Catalyst 9000X系列交換器，藉此確保企業網路存取安全、穩定性與高速效能表現。

依照Cisco在《科技的未來》研究報告公布數據，顯示90%比例台灣地區受訪者表示透過網路完成主要工作事項，同時也有多達93%台灣地區受訪者認為能無障礙地透過網路取用所需應用服務相當重要，另外更凸顯高效網路將能提高員工工作效率，而網路傳輸效能更高更可激發員工產能。

而在越來越多企業因為疫情影響，加速進行數位化轉型，開始大幅擁抱上雲，並且接受混合式工作型態，讓員工能以遠距方式彈性上線完成工作事項，背後重要支撐便是穩定且具安全可靠的網路連接技術。

65%台灣受訪者表示，一旦能夠使用選擇傳輸頻寬更高的Wi-Fi 6E無線網路，將會願意在居家或辦公環境升級使用，同時在規劃5G專網 (Private 5G)的台灣受訪者中，更有66%表示是為了更快的連網速度、55%則是為了更高的可靠性，同時也有47%比例表示是為了獲得更高畫質的影像串流表現。

極機密

極機密

程式碼程式碼

程式碼



[YouTube周二（7/29）宣布](https://blog.youtube/news-and-events/extending-our-built-in-protections-to-more-teens-on-youtube/)，將開始於美國市場採用機器學習技術來估算用戶年紀，以保護青少年族群，初期僅會針對一小部分的使用者，之後才會擴大部署並延伸至其它市場。

該平臺解釋，該技術將利用人工智慧來解釋各種訊號，包括使用者正在搜尋的影片類型、所觀看過的影片類型或是帳戶的壽命等，以區分年輕觀眾或是成年人，並推斷其年齡，再藉由相關訊號來提供適合其年齡層的產品體驗與保護，不管相關帳戶中所填寫的生日日期為何。

當系統辨識出用戶為青少年時，就會自動啟用該年齡層的保護機制，包括禁止個人化廣告，啟用數位健康工具，在建議上添增保護措施，以限制對某些類型內容的重覆瀏覽，也會自動封鎖那些有年齡限制的內容。

如果系統錯了，那麼青少年也可以利用信用卡或是政府簽發的身分證件來驗證自己的年齡。

YouTube說，先前已於其它市場部署該機制，且效果良好。不過YouTube並未公布已部署名單。

**【資安週報】0714~0718，中國駭客網釣信鎖定臺灣半導體人資單位！全球還有Vishing、AI偽冒攻擊擴大**

在2025年7月第三星期資安新聞中，社交工程攻擊威脅是主要焦點，不僅有臺灣半導體人資遭中國駭客網釣信鎖定，全球還有濫用瀏覽器上傳的FileFix、ClickFix事件不斷，以及Vishing、Deepfake偽冒語音攻擊實例大增

文/[羅正漢](https://www.ithome.com.tw/users/%E7%BE%85%E6%AD%A3%E6%BC%A2)|2025-07-21發表



[](https://itadapi.ithome.com.tw/ads/click?q=B3%7Eithome_index%7E2507B3010)

回顧2025年7月第三星期資安新聞，社交工程攻擊成為主要焦點，有多起新聞與之有關，涵蓋傳統網路釣魚，駭客濫用瀏覽器上傳的ClickFix、FileFix新手法，還有語音網釣與AI語音偽冒，我們整理如下：

（一）臺灣半導體產業與相關機構的人資部門注意！資安業者Proofpoint揭露中國駭客狂發假冒研究生求職的釣魚信，時間發生在今年3到6月，並且是盜用臺灣大專院校電子郵件信箱發送，引誘收信人開啟附件的履歷並點選惡意URL，目前研判這起行動與TA415有交集，還有國內投資分析師也遭鎖定。  
（二）勒索軟體駭客組織Interlock新一波攻擊曝光，自5月開始濫用瀏覽器的檔案上傳機制，利用FileFix網釣手法（ClickFix衍生版本），以散布木馬程式Interlock RAT，這是FileFix首度被發現用於實際攻擊活動。  
（三）近來語音網釣、AI偽冒的新聞事件不斷，我們近期發布的封面故事介紹最新攻擊實例，尤其日本山形地區遭遇的Vishing攻擊相當特殊，攻擊者不只寄送網釣郵件，更從自動語音開場、真人偽冒客服來誘導，目標是讓員工被騙交出企業網路銀行帳戶的存取權限；而在AI偽冒通話方面，新加坡與馬來西亞的企業財務主管，也接連傳出遭遇Deepfake視訊會議的詐騙攻擊，還有義大利與美國官員聲音遭偽冒並遭假冒聯繫他人。

本星期還有一起網路防護烏龍事件，引發國人熱議，微軟Azurewebsites.net根網域在臺灣網路遭到封鎖，影響時間將近2小時，起因是刑事局提供涉毒網站給TWNIC進行DNS RPZ屏蔽封鎖，但由於轉檔作業發生疏失，造成原網址清單的子網域被誤刪。雖然政府打詐打毒看重處理的時效，但這類誤封事故並非第一次發生，如何改善事前審核，以及事中發生誤封該如何盡快修正，都需要相關單位盡快協商出相關辦法。

在資安事件方面，知名精品業者LV系統遭駭事件備受矚目，因為不只臺灣分公司證實這項消息，LV的韓國、英國、土耳其分公司也陸續有通知客戶的消息，傳出已有10多國的分公司受波及，目前已知該廠商通知客戶有未經授權第三方人士短暫存取該公司系統，部分個資遭竊。

在威脅態勢方面，有兩起鎖定WordPress網站與外掛的攻擊，突顯攻擊新手法與軟體供應鏈攻擊依然嚴峻

●駭客針對WordPress網站攻擊有新手法，將惡意程式碼埋入ZIP壓縮檔，再透過zip://通訊協定呼叫、解除混淆、載入並執行，將使用者重新導向至特定網域。  
●WordPress表單外掛Gravity Forms遭供應鏈攻擊，駭客於特定版本外掛程式植入後門，目的是收集網站系統資訊並部署其他作案工具。  
●有駭客針對Cursor AI打造模仿正牌工具Solidity的惡意延伸套件，兩個月被下載5.4萬次，有區塊鏈開發人員發現加密貨幣遭竊尋求資安業者幫助才讓此事曝光。

在漏洞消息方面，首先Chrome修補已遭利用的零時差漏洞CVE-2025-6558，其次是有兩個上星期才修補的漏洞，已經出現鎖定利用情形必需重視，一是Fortinet WAF產品的漏洞CVE-2025-25257，一是Wing FTP Server的漏洞CVE-2025-47812。還有6月下旬Citrix修補的漏洞CVE-2025-5777（CitrixBleed 2），同樣被證實已出現鎖定利用狀況。

另外，研究人員揭露美國麥當勞的徵才對話機器人McHire（以Paradox.ai的Olivia機器人打造）有兩個弱點，一是其系統的管理後臺竟採用帳號與密碼皆為123456的預設帳號，另一是Paradox.ai存在IDOR漏洞。此新聞在本星期亦受到許多關注。

至於資安防禦動態方面，國際AI資安合規出現重要突破：歐盟執委會（EC）發布通用AI實踐準則，以協助製造商及供應商符合AI Act的規定，外界預料將對AI產業治理模式帶來深刻影響。

[**【7月14日】臺美關稅遲遲未定，美國大型律師事務所驚傳遭中國駭客入侵**](https://www.ithome.com.tw/news/170051)

這個週末有許多事故傳出，其中，最值得留意的是中國駭客傳出入侵美國大型律師事務所Wiley Rein的事故，由於該事務所協助美國政府與企業應對中國貿易嚴，再加上美國始終沒有公告臺灣的關稅比例，這起事故帶來的後續效應，相當值得留意。

除此之外，另一起引起外界關注的消息，是關於麥當勞的招募對話機器人McHire的漏洞揭露，其中最引起外界關注的是，這套系統竟留存了測試階段使用的管理員帳號，其帳號密碼皆為123456。

[**【7月15日】IDE開發工具Cursor AI出現惡意延伸套件，有用戶因此損失50萬美元**](https://www.ithome.com.tw/news/170074)

針對開發人員的惡意套件攻擊，從NPM、PyPI套件，到IDE開發工具Visual Studio Code（VSCode）的延伸套件市集，如今也有針對Cursor AI用戶的攻擊行動，駭客鎖定的目標，是名為Open VSX的套件庫，且有開發人員因不慎安裝惡意套件損失50萬美元（約新臺幣1,465萬元）。

在惡意套件攻擊事故之外，最近出現的新型態攻擊手法相當值得留意，例如：FileFix網釣手法、搭配ZIP檔的網站攻擊活動、濫用Inno Setup內建指令碼功能載入惡意軟體的手段，都更難以察覺及防範。

[**【7月16日】VMware修補虛擬化平臺重大漏洞**](https://www.ithome.com.tw/news/170085)

本週VMware修補一系列與虛擬化平臺有關的資安漏洞，皆來自漏洞挖掘競賽Pwn2Own參賽者的研究，且影響範圍相當廣泛，包含ESXi、Workstation、Fusion，以及Windows版虛擬機器公用程式VMware Tools，用戶都應儘速套用相關更新因應。

另一個相當值得留意的情況，是WordPress網站有關的資安威脅加劇，在我們昨天報導有人[利用ZIP檔案發動攻擊](https://www.ithome.com.tw/news/170072)，將網站用戶重新導向的事故，今天整理兩篇與表單外掛程式有關的消息，其中一個是Gravity Forms遭遇供應鏈攻擊的情況，另一個是SureForms存在任意檔案刪除漏洞，恐影響20萬個網站。

[**【7月17日】精品品牌LV在多國的分公司接連傳出網路攻擊事故**](https://www.ithome.com.tw/news/170105)

繼英國零售業者接進傳出受害，精品業者迪奧（Dior）、[卡地亞（Cartier）](https://www.ithome.com.tw/news/169348)，[運動品牌愛迪達（Adidas）](https://www.ithome.com.tw/news/169222)、以及[女性內衣業者維多莉亞的秘密（Victoria's Secret）](https://www.ithome.com.tw/news/169292)接連傳出資安事故，最新一起事故是發生在Louis Vuitton（LV），由於陸續傳出多個國家的分公司資料外洩的情況，使得這起事故格外受到關注。

除此之外，近期公布的資安弱點也相當值得留意，其中又以Google修補Chrome今年第5個零時差漏洞影響相當廣泛，再者，資安業者Binarly找到的技嘉主機版漏洞，用戶也要儘速套用相關韌體更新因應。

[**【7月18日】中國駭客鎖定臺灣半導體生態系從事大規模網釣，假冒研究生求職與投資分析合作**](https://www.ithome.com.tw/news/170130)

隨著國際局勢日益緊張，臺海危機升溫，中國駭客對臺灣發動攻擊的情況也越來越頻繁，其中資安業者Proofpoint發布的調查報告引起全臺高度關注，因為這些駭客廣泛對臺灣重要經濟命脈半導體生態系從事網釣，從半導體公司人資部門到投資分析師，都是他們下手的目標。

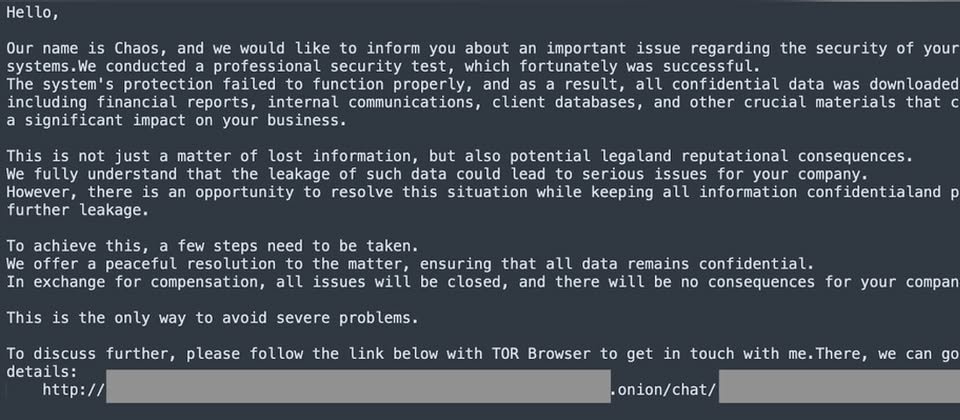
在上述的攻擊行動之外，本週證交所祭出的裁罰也與半導體產業有關，他們處罰的對象，是今年1月、5月兩度遭到勒索軟體攻擊的矽光子及光電封測大廠聯鈞光電。

程式碼

**勒索軟體BlackSuit成員傳出另起爐灶，打造Chaos並提供租用服務**

思科旗下的威脅情報團隊Talos指出，近期活動升溫的勒索軟體駭客Chaos，疑似是BlackSuit的前成員建立，他們在俄羅斯網路犯罪論壇尋找加盟主進行合作，宣稱對受害組織進行滲透測試來犯案程式碼

文/[周峻佑](https://www.ithome.com.tw/users/%E5%91%A8%E5%B3%BB%E4%BD%91)|2025-07-30發表



[](https://itadapi.ithome.com.tw/ads/click?q=B3%7Eithome_index%7E2507B3010)

駭客組織遭受執法單位的壓力，在即將遭到程式碼

圍剿的前夕另起爐灶，這樣的情況不時傳出，例如，[7月宣布關閉業務](https://www.ithome.com.tw/news/169934)的勒索軟體駭客組織Hunter International，今年初傳出已使用World Leaks的名號成立新的團隊，如今有另一個興起的[勒索軟體Chaos](https://blog.talosintelligence.com/new-chaos-ransomware/)，很可能就是近期執法單位出手的勒索軟體BlackSuit（Royal）前成員組成。

思科旗下的威脅情報團隊Talos近期揭露Chaos的攻擊手法，這些駭客通常運用洪水式垃圾郵件攻擊手法接觸受害者，藉著語音網釣得到受害組織的初期存取管道，並濫用遠端管理工具（RMM）持續連線，以及透過檔案共享軟體外傳竊得資料，這些駭客聲稱，他們大部分的受害組織位於美國，但英國、紐西蘭、印度也有企業組織受害。

針對攻擊者的身分，Talos指出，這個駭客組織與[先前使用相同名稱的殭屍網路](https://blog.lumen.com/chaos-is-a-go-based-swiss-army-knife-of-malware/)沒有直接關聯，他們根據勒索軟體加密機制、勒索訊息的結構、駭客使用的工具集，推測Chaos可能是BlackSuit前成員組成的新團體。巧合的是，這篇調查報告發布的時間，同一天[傳出](https://www.bleepingcomputer.com/news/security/law-enforcement-seizes-blacksuit-ransomware-leak-sites/)跨國執法行動Operation Checkmate當中，執法機關成功接管了BlackSuit暗網網站，[參與行動的資安業者Bitdefender指出](https://www.bitdefender.com/en-us/blog/businessinsights/blacksuit-ransomware-seized-takedown)，自2023年夏天出現的BlackSuit，迄今已有至少185個企業組織受害，部分企業組織付出超過200萬美元的贖金。其中一起大型攻擊事故，是去年6月[日本角川集團遭到攻擊](https://www.ithome.com.tw/news/163704)，導致多項業務中斷。

此駭客組織約自今年2月出現，他們透過俄羅斯網路犯罪論壇Ransom Anon Market Place（RAMP）尋找加盟主，並以租用模式提供勒索軟體（Ransomware-as-a-Service，RaaS），號稱他們的作案工具能用於攻擊Windows、macOS、Linux作業系統，也可對網路儲存設備發動攻擊，具有獨特的檔案加密金鑰，極為快速的檔案加密能力，並能掃描網路環境的所有設備。

Chaos提供加盟主自動化的管理主控臺，並明確禁止攻擊金磚國家（BRIICS）與獨立國家國協（CIS）成員國，以及政府機關、醫療機構。

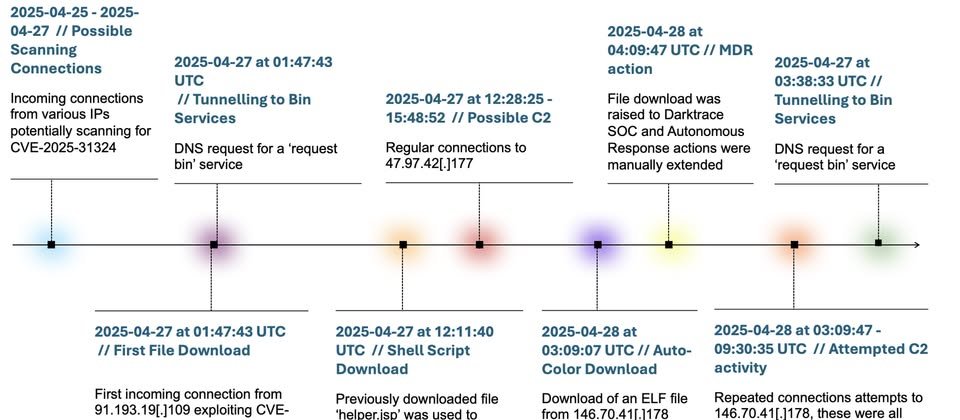
若是受害組織的檔案遭到加密，這些駭客留下的勒索訊息裡，會聲稱他們是進行專業的資安測試，並成功達到目的，導致系統防護失效，該組織聲稱已下載了所有內部機密資料，假如受害組織不予理會或是不付贖金，他們將會外流資料。

一般來說，這些駭客會向受害組織索討30萬美元贖金，假若付錢，受害組織不僅會得到解密工具，駭客還會提供滲透測試報告，並保證他們不會重複發動攻擊，也會將竊得資料刪除。若是受害組織不願向駭客低頭，對方就會揚言將資料外洩的消息散布給受害組織的競爭對手與客戶，並對受害組織網路上的服務發動DDoS攻擊。

**SAP Netweaver滿分漏洞遭到利用，駭客企圖散布惡意程式Auto-Color**

針對4月下旬SAP緊急修補的NetWeaver滿分漏洞CVE-2025-31324，資安業者Darktrace指出，有人試圖用於散布Linux後門程式Auto-Color

文/[周峻佑](https://www.ithome.com.tw/users/%E5%91%A8%E5%B3%BB%E4%BD%91)|2025-07-30發表



[](https://itadapi.ithome.com.tw/ads/click?q=B3%7Eithome_index%7E2504B3033)

今年[4月下旬](https://www.ithome.com.tw/news/168625)SAP緊急修補應用程式伺服器NetWeaver重大層級資安漏洞[CVE-2025-31324](https://www.ithome.com.tw/tags/cve-2025-31324)，由於這項漏洞被發現時，已被用於攻擊NetWeaver，再加上危險程度達到滿分10分，後續傳出[中國駭客Chaya\_004](https://www.ithome.com.tw/news/168892)、[CL-STA-0048、UNC5221、UNC5174](https://www.ithome.com.tw/news/168966)、[Earth Lamia](https://www.ithome.com.tw/news/169419)，勒索軟體駭客[「變臉（BianLian）」與RansomEXX](https://www.ithome.com.tw/news/168966)也出手，將此漏洞用於實際攻擊，如今又有資安業者[公布相關調查結果](https://www.darktrace.com/blog/auto-color-backdoor-how-darktrace-thwarted-a-stealthy-linux-intrusion)，指出他們看到駭客利用這項漏洞部署Linux後門程式。

美國一家化學公司於今年4月，遭受名為Auto-Color的Linux後門程式攻擊，駭客於3天的時間裡，成功入侵該公司的網路環境，下載有問題的檔案，並試圖與Auto-Color的惡意基礎設施進行通訊。揭露此事的資安業者Darktrace指出，他們封鎖相關惡意行為、進行深度調查，發現駭客利用CVE-2025-31324，趁機滲透這家化學公司的NetWeaver主機。

Darktrace之所以察覺這起事故，主要是因為他們的資安維運中心4月28日收到警報，有人從網際網路存取的主機下載可疑的ELF檔案，而此伺服器的用途，似乎是NetWeaver主機。經入侵指標（IoC）的比對，這個ELF執行檔就是Auto-Color。

該公司循線調查，找到的第一個不尋常的行為，出現於4月25日，駭客正在尋找存在CVE-2025-31324的NetWeaver平臺，但兩天後才開始積極利用：他們在27日偵測到來自惡意IP位址91.193.19[.]109[.] 6的連線，駭客觸發漏洞，藉由特定的URI下載ZIP檔案，此時NetWeaver主機隨即向特定的界外應用程式安全測試（Out-of-Band Application Security Testing，OAST）平臺發出DNS請求。

駭客持續透過URI下載作案工具，並在10個小時後透過NetWeaver發出另一個DNS請求，下載Shell指令碼config.sh。此指令碼透過名為helper.jsp的檔案執行。接著，DarkTrace看到NetWeaver對相同的端點建立DNS與SSL連線，並對後門程式Supershell有某種關聯的IP位址，經由3232埠建立數個連線，最終在間隔近12個小時之後，駭客從<http://146.70.41.178:4444/logs>下載ELF檔案，從開始利用漏洞到成功部署後門程式，駭客花費不到一天的時間。

攻擊上述化學公司的惡意程式Auto-Color，[約從去年11月、12月開始活動](https://www.ithome.com.tw/news/167594)，駭客的主要目標是北美及亞洲的大學及政府機關辦公室，當時揭露這起攻擊行動的資安業者Palo Alto Networks指出，這款後門程式能讓攻擊者完全存取受害電腦，防守方若要清除，必須搭配特定工具，否則會很難徹底杜絕。而在4月下旬的資安事故裡，Darktrace發現的Auto-Color變得更加刁鑽，此惡意程式在啟動時會先檢查具備的權限，若是以root權限運作，就會試圖透過一系列工作來建立持續存取的管道，並與C2伺服器連線。

**中華電信：已完成商業及政府機關網站憑證換發**

為降低Google Chrome憑證撤信事件對中華電信客戶的影響，中華電信推動客戶更新或換發憑證，以延長憑證效期，7月25日完成政府機關及商業客戶的網站憑證更新及換發。

文/[蘇文彬](https://www.ithome.com.tw/users/%E8%98%87%E6%96%87%E5%BD%AC)|2025-07-29發表



[](https://itadapi.ithome.com.tw/ads/click?q=B3%7Eithome_index%7E2507B3010)

針對[Google Chrome移除中華電信8月1日起核發新TLS憑證的預設信任](https://www.ithome.com.tw/news/169318)，導致使用中華電信憑證的商業及政府機關網站受到影響，中華電信今天（7/29）宣布已完成商業及政府機關網站憑證的更新，憑證效期可達一年，並強化內部憑證管理，爭取明年3月重新取得Chrome瀏覽器的預設信任。

Google在今年5月底至6月初之間宣布，基於中華電信憑證管理不符規定，未按期改善，Chreom瀏覽器將移除對中華電信從8月1日起核發的新TLS憑證的預設信任，中華電信也宣布8月起不再簽發新的憑證，同時為了降低事件帶來的衝擊，推動商業、政府機關網站更新憑證。

中華電信今天表示，已在7月25日提前完成政府機關及商業客戶的網站憑證更新及換發，所有同意更新憑證的客戶網站都已完成憑證換發，憑證效期一年，確保民眾能正常瀏覽商業或政府機關的網站。換言之，利用更新換發憑證，來延長憑證的效期，等待爭取明年3月重新恢復Chrome瀏覽器的預設信任。

由於先前在憑證營運管理的疏忽，中華電信也加強內部憑證營運管理制度，例如拉高內部「憑證政策管理委員會」的層級，導入第三方稽核，來確保符合透明、合規的要求，並且改善自動化憑證換發流程，提高憑證管理的效率，以爭取在明年3月回復Chrome預設信任名單之中，未來也會加強對國際憑證政策動態的關注，避免憑證營運管理無法跟上國際最新憑證政策。

由於中華電信簽發的TLS憑證以政府機關居多，數發部在今年3月掌握情資後已推動政府機關導入雙憑證機制，即在中華電信憑證之外，再導入TWCA憑證作為備援憑證，當單一憑證因效期或管理不合規而被瀏覽信移除信任後，可以切換至另一個憑證，提高政府機關網站的服務韌性。