DeepSeek風暴⑤

揭秘DeepSeek遇襲 美國IP幕後黑手

殭屍網節節敗退 守護者愈戰愈勇

數天前，中國杭州DeepSeek發布的推理模型R1登頂蘋果美國地區應用商店免費App下載排行榜，在性能逼近OpenAI o1正式版的同時訓練費用約為GPT-4o的5%，以算法制勝，美國科企以高成本打造高算力的護城河不復再。

不為人知的是，就在各界憧憬DeepSeek為全球AI發展帶來利好之際，針對DeepSeek的網攻變本加厲，如同網絡恐怖主義。業界監測發現，黑暗的網絡攻擊，其中大部分IP來源是美國。在這場被網友們稱為數字時代「上甘嶺」的戰役中，360、奇安信、華為等多家中企與DeepSeek聯手抵禦攻擊，愈戰愈勇，黑客節節敗退。一波波的惡意攻擊，不會讓中國DeepSeek倒下。打不死的，只會讓它更強大。

大公報記者 劉凝哲

網絡恐怖襲擊：如同10萬掃地機器人傾巢而出堵塞家門

多個監測信息顯示，DeepSeek近期遭遇的網攻愈加猛烈，特別是近期出現的兩個變種殭屍網絡攻擊，就像「黑客用遙控器同時劫持10萬台掃地機器人，讓它們全部堵在家門口」一樣令人窒息，形同網絡恐怖主義襲擊。令人意想不到的是，在多家美國AI領域企業對DS在口頭上表示稱讚之同時，監測顯示，黑暗網攻大部分IP來源是美國。奇安信XLab實驗室通過持續近1個月的監測發現：攻擊模式從最初的易被清洗的放大攻擊，升級至1月28日的HTTP代理攻擊（應用層攻擊，防禦難度提升），到大年初二1月30日凌晨，亦即是登頂下載榜未幾，攻擊烈度大增，指令暴增上百倍，至少有2個殭屍網絡（botnet）參與攻擊。

據內地《新安全》報道，360安全專家分析DeepSeek此次被攻擊的情況，發現攻擊類型豐富多樣，呈現出高度組織化、規模化特徵。從1月30日凌晨開始，攻擊猛烈程度前所未見。RapperBot、HailBot等殭屍網絡團夥開始參與攻擊。監測數據顯示，殭屍網絡攻擊指令捕獲數在1月30日凌晨的3個小時內暴增，迫使DeepSeek新增一個服務IP「防禦」。

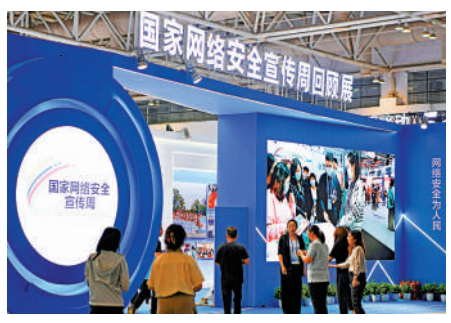
胡錫進在個人微信公眾號中指出，最難處理的是「殭屍網絡」攻擊，這也是現階段DeepSeek最常見遭到攻擊的方式。攻擊者控制被病毒感染的智能設備，如攝像頭、路由器等，要求它們像提線木偶一樣集體發動攻擊，最終目的是耗盡目標服務器的網絡帶寬和系統資源，使其最終癱瘓或服務中斷。

警惕國家級對手 加固壁壘

《新安全》指出，DDoS（阻斷服務）攻擊成大規模攻擊必殺技，警惕國家級對手。針對DeepSeek高度組織化、規模化的攻擊事件，揭示眾多AI企業可能面臨國家級對手挑戰。單純依靠增加軟硬件安全產品的投入，試圖構建一道堅不可摧的防線來抵禦外部威脅，已被證明是不現實的。

360集團創始人周鴻禕認為，美國之所以採用一系列強硬手段，不僅因為DeepSeek技術領先導致美股大跌，更主要由於其開源系統能力強大，遠超OpenAI等在美國佔據主流的閉源系統，此舉或將動搖美國的人工智能基礎設施。美國的人工智能基礎設施都用一家中國公司提供的系統，對美國來講，這才是讓它寢食難安的噩夢。近日，周鴻禕宣布將無償為DeepSeek免費提供全方位網絡安全防護。360將以安全大模型國家級安全能力協助DeepSeek構建更堅固的防護壁壘，粉碎惡意攻擊的圖謀，全力保障用戶體驗。

從戰勝殭屍網攻，到獲得英偉達公開認可，並迎來OpenAI的CEO「認錯」，在風浪中成長的DeepSeek，被問及怎麼看自己受到的惡意攻擊和詛咒，其回答很平靜，說：「創業的路的確不好走，但看看手機裏70%的國產APP，看看滿街跑的電動車，哪樣不是這麼過來的？我們只管把產品做好，剩下的就交給時間。」



▲多家中企與DeepSeek聯手抵禦攻擊，黑客節節敗退。圖為觀眾在2023年福州網絡安全博覽會上參觀。 中新社

緊隨DeepSeek 印度研建大模型

緊跟潮流

新加坡《聯合早報》網站1月31日報道，印度鐵道、通信以及電子和信息技術部長阿什維尼·瓦伊什瑙30日說，印度政府已選定18項提案，它們將獲得計算基礎設施、數據和資本支持，以在農業和氣候變化等領域構建與AI相關的應用。

瓦伊什瑙告訴記者，印度將資助這些提案40%的計算費用。就在該計劃出台的同一個月內，DeepSeek在與OpenAI等美國行業領導者的競爭中取得進展，令世界驚嘆不已。彭博新聞社引述瓦伊什瑙的話說，「印度製造的基礎模型將能夠與世界上最優秀的模型媲美」，並稱六家主要開發商將能夠在八至十個月內構建基礎人工智能模型。

長安街知事

終結AI霸權 開源就是力量

▲觀眾在雄安新區中關村科技園參觀科技園入駐企業。 中新社

專家解讀

DeepSeek在部分西方國家遭遇網絡攻擊、硬件受限、應用下架等遏制「組合拳」。復旦大學國際政治系教授、復旦大學網絡空間國際治理研究基地主任沈逸在接受大公報採訪時表示，DeepSeek的出現，有望擊破美國AI霸權，讓昂貴的美國堆算力AI金融模式不再具有競爭力，打破一些西方國家在數字時代重複「割韭菜」妄想。「基於護持美國霸權的本能反應，這樣的DeepSeek必將招致遠超於華為當年的制裁」，沈逸表示，歷史和經驗證明，此類舉措注定是徒勞的，美國對中國行業的制裁和限制，只能讓中國自身更強大。

制裁倒逼中國提升自身能力

沈逸說，美國未來也許會出現針對中國AI的系統性的政府文件或者國家戰略，並嘗試構建一整套新的針對性的霸凌規則。沈逸認為，全球AI領域的美式霸主遊戲規則正在一個關鍵的構建過程中。美國計劃是充分利用自身暫時獲得的壟斷性的技術和能力優勢，為各個國家發展AI戰略設置符合美國國家利益的條件，並對全球市場進行分割，實現最大化的壟斷利潤獲取。

「中國人是不會看着DeepSeek被『打死』的」，沈逸說，「事實證明，所有的制裁措施，除讓中國自身的能力提升之外，起不到任何別的效果」。沈逸表示，DeepSeek是一個開源模型，是很難被徹底封鎖和禁止的。這將是一個巨大的轉折點——中美科技競爭的態勢將發生重大而顯著的變化。

大公報記者劉凝哲

騰訊華為 牽手DeepSeek

▲人們在廣州舉辦的2024網絡安全博覽會上的企業展台前參觀。 新華社

強強聯合

騰訊雲、華為雲近日發文宣布，已上線基於其雲服務的DeepSeek-R1相關服務。據悉，微軟、英偉達、亞馬遜、英特爾、AMD等科技巨頭也已於近日上線DeepSeek模型服務。業內人士認為，DeepSeek的火熱雖然在一定程度上衝擊了投資者對AI算力和成本的預期，但模型成本的下降對產業鏈上的雲服務廠商可能存在利好。

共拓雲服務商機

騰訊雲表示，DeepSeek-R1大模型可一鍵部署至騰訊雲「HAI」上，開發者僅需3分鐘就能接入調用。通過「HAI」，開發者只需兩步即可調用DeepSeek-R1模型。此外，在「HAI」上，除了調用DeepSeek-R1模型，開發者還可以無縫聯動騰訊雲Cloud Studio、對象存儲等服務，快速搭建企業級AI應用。騰訊雲TI也已支持R1、V3模型部署。

華為雲表示，硅基流動與華為雲團隊聯合首發並上線基於華為雲昇騰雲服務的DeepSeek R1/V3推理服務。得益於自研推理加速引擎加持，硅基流動和華為雲昇騰雲服務支持部署的DeepSeek模型可獲得持平全球高端GPU部署模型的效果；另一方面，提供穩定的、生產級服務能力，讓模型能夠在大規模生產環境中穩定運行，並滿足業務商用部署需求，華為雲昇騰雲服務可以提供澎湃、彈性、充足的算力。

上海證券報