陳志華｜從Mythos模型測試敲響的金融網絡安全警鐘

編輯：子涵 責編：韓進珞

AI播報

2026-07-07 10:47

AI技術在網絡安全領域已達到前所未有的能力水平。

文：陳志華

近日，一則有關人工智能模型參與美國國家安全測試的消息，引起了全球網絡安全界的廣泛關注。據外媒報道，人工智能公司Anthropic旗下的Mythos模型，在與美國情報機構合作的測試演練中，僅耗費數小時便成功識別出美國政府高度敏感的機密電腦系統中存在多處安全漏洞。弗吉尼亞州聯邦參議員馬克·羅伯特·華納（Mark Robert Warner）更在國會聽證會上引述美國國家安全局局長的表述指出，Mythos「不是花上數周，而是數小時內就突破了我們幾乎所有機密系統」。雖然有關官員強調，模型在數小時內識別漏洞，並不代表能夠在同一時間內利用這些漏洞發動攻擊，但這一事件所揭示的趨勢，對香港作為國際金融中心的網絡安全防禦體系而言，無疑是一次重要的警示。

從「人的速度」到「機器速度」的範式轉移

Anthropic於今年4月啟動了名為「Project Glasswing」的網絡安全計劃，目標是在攻擊者利用漏洞之前，先找出並修補關鍵軟件系統中的安全缺陷。該項目聯合了超過50個合作夥伴，利用Mythos模型掃描超過1,000個開源項目，迄今已發現約一萬個高危或嚴重級別的安全漏洞。在其中一輪掃描中，Mythos Preview發現了6,202個高危或嚴重漏洞，經獨立安全研究機構驗證，超過九成被確認為真實有效的漏洞。

有網絡安全專家指出，**Mythos的出現帶來了四個根本性的變化：漏洞發現速度提升百倍，從「人的速度」進入「機器的速度」；漏洞數量大幅增加，AI可全天候持續分析代碼進行地毯式搜索；挖掘漏洞的成本大幅下降；攻擊能力平民化，即使不懂編程的人也能借助AI生成攻擊代碼。這一範式轉移意味着，過去建立在「漏洞難找」基礎上的網絡攻防平衡正在被徹底改寫。對於金融機構而言，從漏洞被發現到被利用之間的時間窗口正在急劇收窄，傳統的修補程序已難以應對AI驅動的攻擊速度。**

香港金融業面臨的現實風險

香港作為國際金融中心，匯聚了大量銀行、證券經紀行、資產管理公司及虛擬資產交易平台，其網絡安全防禦體系的穩健性直接關係到投資者信心和市場穩定。根據香港網絡安全事故協調中心的數據，本港網絡安全事故數目已由2024年的12,536宗增至2025年的15,877宗，增幅達27%。在AI技術日益普及的背景下，這一數字恐怕只會繼續攀升。

值得留意的是，證監會已於今年6月2日向業界發出通函，明確警告由前沿AI模型驅動的新興網絡威脅正急劇升溫。證監會指出，AI模型現已具備自主策劃跨系統多步驟複雜攻擊的能力，能夠快速識別「零日漏洞」，或將多個低風險漏洞串聯利用。與此同時，AI驅動的網絡釣魚、深度偽造假冒身份及社交工程攻擊，其逼真度與定制化程度顯著提升，進一步降低了發動攻擊的技術門檻。

證監會的通函中指出，隨着前沿AI模型日趨強大且普及，由AI驅動的網絡威脅勢必迅速加劇，偵測及遏制此類威脅的工作亦將更為複雜。通函明確要求持牌機構的高級管理層肩負起最終責任，針對修補及漏洞管理、接達及權限監控、偵測及監察、第三方供應鏈風險管理，以及事故應對及復原等五大範疇，全面檢討及加強網絡安全框架。

多方協作提升整體防禦能力

精選文章


韓成科｜建設「黃金港」 爭奪定價權


梁文廣｜堅定制度自信 推動民族復興

李希榕｜恒大清盤案入稟帶來的啟示


寰宇前瞻｜大學排名制度面面觀：誰才是真正的第一？


來論｜鑄就「數智化」高效團隊 推動公務員體制變革

面對AI驅動的網絡安全新格局，單靠個別機構的努力遠遠不足以應對挑戰。政府相關部門需要從全局高度審視和提升香港的網絡安全防禦體系。

在監管層面，證監會已率先行動，要求持牌機構建立「科技資產清單」並維持每日更新，針對業務關鍵組件的已知漏洞制訂緊急修正政策。監管機構同時擴大監管沙盒機制，允許金融機構在受控環境中測試生成式AI應用。這些舉措方向正確，但面對AI攻擊手段的快速演進，監管要求本身也需要持續更新，以跟上技術發展的步伐。

在技術層面，政府電腦保安事故協調中心及香港網絡安全事故協調中心應進一步加強對AI相關威脅的監測、預警和分析能力。數字政策辦公室已計劃在下半年推出多項AI相關的重點網絡安全項目，包括統籌推出「安全AI@職場賦能計劃」，協助企業建構安全合規的AI應用生態，以及聯同業界首辦人工智能網絡安全挑戰賽。這些措施有助於提升整體社會的網絡安全意識和防禦能力，值得持續推進和深化。

在執法層面，警務處網絡安全組需要密切關注AI技術被用於網絡攻擊的最新動向，加強與國際執法機構的情報交流與協作。創新科技及工業局則應在政策層面統籌協調各相關部門的工作，確保香港的網絡安全策略能夠與時俱進。

Anthropic Mythos在數小時內發現美國機密系統漏洞的事件，揭示了AI技術在網絡安全領域已達到前所未有的能力水平。正如有專家所言，當漏洞從稀缺資源變成規模化資源，網絡安全行業運行數十年的遊戲規則將被徹底改寫。香港作為國際金融中心，其金融體系的穩定與安全不容有失。政府相關部門、監管機構、金融企業及網絡安全從業者必須攜手合作，以前瞻性的視野和果斷的行動，全面提升香港的網絡安全防禦能力，守護這座城市的國際金融中心地位。

作者為香港證券及期貨專業總會會長

本文為作者觀點，不代表本媒體立場

圖：IC photo

#人工智能模型 #網絡安全 #Mythos #安全漏洞 # 香港國際金融中心地位
#網絡威脅 #證監會 #網絡保安事故 #香港證券及期貨專業總會

觀察｜香港定能在融入和服務國家發展大局中實現更好發展

議事堂 | 3天前

龔靜儀｜完善性罪行條例須與時並進

議事堂 | 4天前

周文港｜「十五五」新征程 香港積極有為展擔當

議事堂 | 4天前