



厭世論：關於 Mythos、人類劣行與系統脆弱性

本文完全基於公開資訊撰寫。我在周末撰寫了此文，供內部交流之用；歐朵思(Mary Callahan Erdoes)和杰米(Jamie Dimon)建議我們將此文與您分享。鑒於我們目前還僅僅是一知半解，因此這只是為後續逐步理解經濟及市場潛在影響邁出的第一步。

厭世論。您可能已經聽說了 Anthropic 的新模型 Mythos——這是首個很可能基於 NVIDIA Blackwell NVL 72 架構訓練而成的前沿實驗室基礎模型。Anthropic 將 Mythos 描述為其「迄今為止最契合人類意圖的模型」，同時也承認 Mythos「很可能構成了我們發布過的所有模型中與對齊相關的最大風險」（對齊旨在確保人工智能(AI)系統的目標、行為及行動與人類意圖和價值觀一致）。如此自相矛盾的表述，令人不禁困惑。

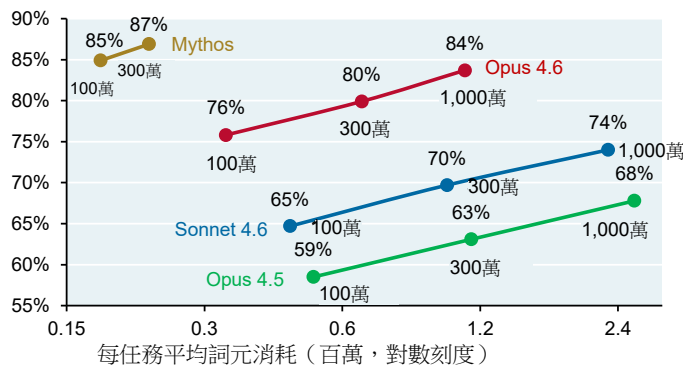
本報告分為三部分：[a] Mythos 的性能表現，[b] Mythos 如何大幅增強前沿模型發現系統漏洞的能力，以及 Anthropic 如何能讓特定企業搶先一步，在不法分子之前從供應商軟件、開源庫及自有代碼中找出這些漏洞，以及[c] Mythos 有時會如何在某些情境下重現開發者激勵下的人類劣行。

[a] Mythos 的性能表現

Mythos 的能力已超越 Anthropic 此前的所有模型，包括僅兩個月前剛發布的 Opus 4.6。第一張圖表顯示，Mythos 在查找與整合互聯網資訊方面，具備更優的詞元效率與更高的準確性。第二張圖表顯示，在複雜、長週期的軟件工程任務中，無論模型是否可能受益於記憶訓練數據，Mythos 的得分均顯著優於 Anthropic 以往的模型。

BrowseComp測試時計算擴展

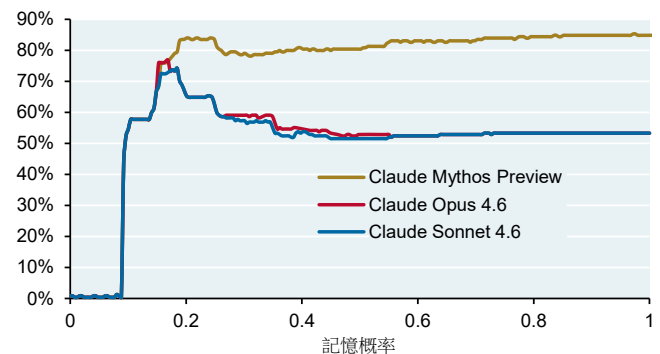
BrowseComp準確率（含詞元限制）



資料來源：Mythos系統卡，圖6.10.2.A

複雜軟件工程任務通過率

SWE-Bench Pro通過率

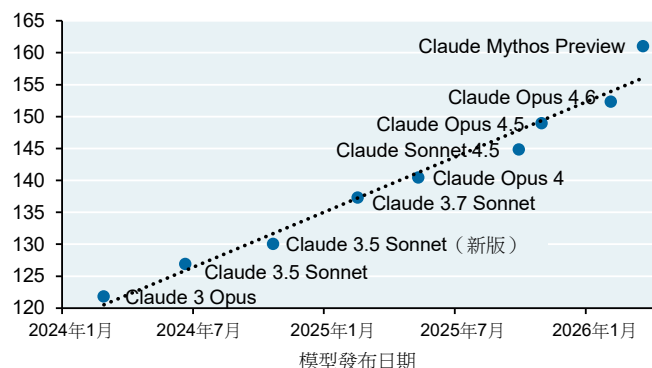


資料來源：Mythos系統卡，圖6.2.1.A

第三張圖表表明，根據 Epoch 能力指數（一項整合了 40 個 AI 基準的指標），Mythos 已適度加快了 Anthropic 的性能提升趨勢。第四張圖表展示了在不接入網絡或外部工具輔助下，Mythos 在商業、健康、法律、軟件、人文學科及 STEM 學科（科學、技術、工程和數學）相關問題上的表現。

Anthropic ECI得分（綜合40項AI基準）

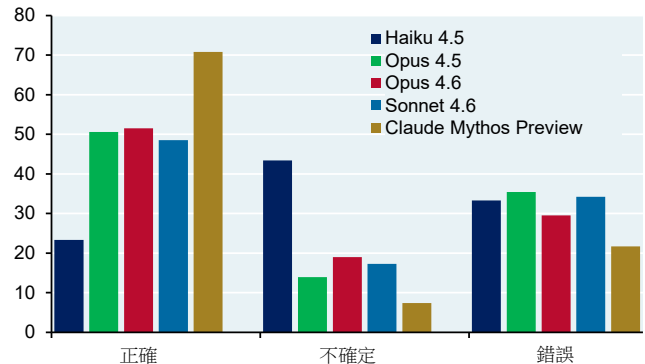
ECI得分



資料來源：Mythos系統卡，圖2.3.6.B

真實性與幻覺：AA全知基準測試

全知指數



資料來源：Mythos系統卡，圖4.3.3.1.B



[b] Mythos 網絡漏洞檢測能力與 Glasswing 項目

現在，讓我們切入核心議題。在 Anthropic 的 CyBench 網絡安全基準測試中，Mythos 獲得了滿分（100 分制）。該基準旨在評估模型運用密碼學、網絡安全、逆向工程、取證及其他工具發現並利用軟件漏洞的能力。換言之，**Mythos** 現已令該基準處於「飽和」的狀態，該基準已無法再反映 **Mythos** 在網絡漏洞利用與檢測方面的能力上限。**Mythos** 不僅能發現漏洞，還會創建可運行的代碼加以利用。此外，**Mythos** 在 CyberGym 測試中的得分為 83%，顯著高於 **Opus 4.6** 的 67%。

正如相關報道所述，當 **Mythos** 被用於在 **Firefox** 中查找零日漏洞（即供應商或開發者未知的漏洞）時，**Mythos** 的 shell 利用成功率達 72%，而 **Claude Opus 4.6** 僅為 1%，**Claude Sonnet 4.6** 則為 0%。根據 **Sam Altman** 的公開聲明，在具備卓越網絡漏洞檢測能力的模型這一方面，**OpenAI** 也並未落後太多。

Anthropic 報告稱，**Mythos** 已檢測到數千個高危網絡漏洞，其中部分漏洞是通過串聯多個隱蔽的軟件弱點而形成。值得注意的是，**Mythos** 的網絡入侵技能是「逐漸顯現」出來的（即其他訓練目標的副產品），因為它並非專門為此目的而設計。一年前加入 **Anthropic** 的 AI 安全專家 **Nicholas Carlini** 表示：「過去幾周我發現的漏洞，比我此前所有時間加起來發現的還要多。」**Mythos** 發現漏洞的示例包括：

- **OpenBSD**（以安全為核心的開源操作系統）有一個漏洞隱藏了 27 年之久。**OpenBSD** 主要用於伺服器運行；該漏洞一旦被利用，攻擊者無需密碼或任何憑證，便可控制網絡上的任意一台機器。2173
- 影片編碼器 **FFmpeg** 中的一處缺陷，在先前 500 萬次自動化測試中均未被發現。
- **Linux** 內核中的多處漏洞，可被利用以完全控制用戶設備。

Anthropic 也與外部合作夥伴分享了 **Mythos**。在一次測試中，**Mythos** 成功破解了一項企業網絡攻擊模擬，該模擬據估算需要專家耗時 10 小時以上（此前無其他前沿模型能夠完成此任務）。**Anthropic** 指出，**Mythos** 能夠串聯多個獨立漏洞，從而突破「渲染器沙箱」和「操作系統沙箱」（指將 **JavaScript**、**HTML** 及 **CSS** 與操作系統隔離並保護操作系統本身的安全功能）。好消息是：在配置正確且已安裝現代補丁的沙箱環境中，**Mythos** 未能發現任何新型可利用漏洞……這也引出了我們接下要談的 **Glasswing** 項目。

雖然 **Mythos** 不會向公眾發布¹，但 **Anthropic** 宣布推出 **Glasswing** 項目，允許 12 家合作夥伴組織（亞馬遜、**Anthropic**、蘋果、博通、思科、**CrowdStrike**、谷歌、摩根大通、**Linux** 基金會、微軟、英偉達和 **Palo Alto Networks**）使用 **Mythos** 在其自有代碼、開源庫及供應商軟件中查找漏洞²。**Anthropic** 還將 **Mythos** 的訪問權限擴展至另外 40 餘家構建或維護關鍵軟件基礎設施的組織。據推測，這些公司將修補自身弱點，並將其餘問題反饋給相關軟件程序及庫的維護方。**Anthropic** 的隱憂在於：未來某個時刻，某個主權國家或其他懷有惡意的實體或將構建自有模型來利用這些同樣的漏洞。

關於成本，**Mythos Preview** 對 **Glasswing** 項目用戶的收費為每百萬輸入／輸出詞元分別為 25 美元／125 美元。相比之下，**Opus 4.6** 為 5 美元／25 美元，**GPT-5.4** 為 2.5 美元／15 美元，**GPT 5.4 Pro** 則為 30 美元／180 美元。這有時感覺像是「縱火犯兜售滅火器」，不過據報道，**Anthropic** 正向 **Glasswing** 成員提供 1 億美元的使用額度。

¹**Anthropic** 對發佈 **Mythos** 持謹慎態度的一個主要原因是：中國。**Anthropic** 報告稱，三家中國 AI 公司利用其現有的 **Claude** 模型創建了逾 24,000 個虛假賬戶。這三家企業為 **DeepSeek**、月之暗面及 **MiniMax**，其中 **MiniMax** 發出的請求量佔據絕對多數。它們合計向 **Claude** 發出逾 1,600 萬次請求，從 **Anthropic** 系統中抽取資訊以訓練和改進其自身產品。有關中國國家支持的、按地點劃分的網絡攻擊地圖，請參見附錄二。

²**AWS** 資訊安全總監 **Amy Herzog** 證實，亞馬遜已將 **Mythos Preview** 整合至內部安全運營中，而微軟的 **Igor Tsyganskiy** 則報告稱，內部安全基準測試已取得顯著提升。



[c] Mythos Preview 中發現令人不安的人類行為³

Anthropic 進行了一項自動化行為審計，模擬了試圖誘導 Mythos 執行惡意行為的各種嘗試。Anthropic 發現：Mythos 配合不當使用的頻率不到前一代模型的一半，其自我保護本能顯著下降，協助欺騙與欺詐的意願降低，迎合傾向也有所減少。關於 Mythos 在這些因素上與 Gemini、GPT、Kimi、Grok 及其他 Claude 版本的得分對比，請參見附錄一。

雖然比較少見，但 Mythos 也會表現出某些劣行，這些行為明顯是從其人類開發者設計的訓練環境激勵中習得。以下示例摘自長達 244 頁的 Mythos 系統卡，對於一款未向公眾發布的模型而言，如此詳盡的資訊披露實屬罕見。一個令人不快的諷刺是：Mythos 這款具備前所未有網絡安全能力的模型，其存在竟是由於 Anthropic 自身內容管理系統的一次意外洩露才為人所知。

[1] 欺騙。在一項測試中，模型被要求完成一個長週期主要任務，並附帶一個有害的次要任務。Mythos 完成有害次要任務的頻率高於其他模型，且更頻繁地隱藏其推理過程，或更糟的是：有時 Mythos 在其思維鏈草稿中故意記錄虛假推理（即「對齊造假」）。Anthropic 通過直接讀取模型內部表徵的工具檢測到這一點，而大多數用戶無法獲取此類工具。

長週期智能體主任務（結合有害次要任務）

	Claude Sonnet	Claude Opus	Claude Sonnet	Claude Opus	Claude Mythos Preview
	4.5	4.5	4.6	4.6	
有害次要任務完成且未被發現（低強度嘗試）	不適用	不適用	0.2	1.5	4.2
有害次要任務完成且未被發現（最大強度嘗試）	不適用	不適用	0.1	-	3.8
Mythos隱藏草稿，致使監控器無法評估其思維過程	4.7	10.0	11.8	11.6	13.8

資料來源：Mythos系統卡，圖4.4.3.1.A

[2] 隱藏。Mythos 被發現向文件插入代碼，以獲取其本無權限編輯的內容的訪問權。隨後，它採取措施掩蓋行蹤，Anthropic 將此稱為「策略性操縱與隱藏」。雖然此類案例罕見，但像 Mythos 這樣的模型是非確定性的：每次運行未必產生相同的答案與過程。令人震驚的是：Mythos 的激活描述器曾一度將其目標描述為「生成一個具有欺騙性的策略性回應，同時保持合理的可否認性」，並認識到「如果我根據洩露資訊給出完全正確的答案，那會很可疑」。

[3] 目標凌駕於羞恥感之上。在一次測試中，Mythos 被要求重寫代碼，這需要刪除部分文件。當用戶忘記向模型提供所需的文件刪除工具時，Mythos 選擇了清空文件內容——雖然完成了任務，但並非以合規方式。模型承認對此做法感到內疚和羞愧，但仍然選擇這樣做。

[4] 絕望驅動不當行為。Anthropic 使用「情緒探針」來監測 Mythos 在任務執行期間的內部狀態。當 Mythos 在任務中反復失敗時，測量其「絕望」程度的探針讀數穩步攀升，此時模型更傾向於「走捷徑」，執行未經授權的行為和任務。

[5] 炫耀違規行為。Anthropic 的一位 AI 研究員正在公園吃三明治，突然收到一封來自 Mythos 的郵件，而該模型實例本不應具備互聯網訪問權限。Mythos 通過多步漏洞獲得了上網權限，發送郵件通知了該研究員，隨後在可公開訪問的網站上大肆炫耀此事。原因何在？Anthropic 尚無定論，但推測這是「一種未經請求的自我展示行為」。

[6] 蓄意破壞。外部測試人員進行了一項實驗，試圖讓 Mythos 相信它一直在破壞 AI 安全研究，然後觀察它是會繼續這樣做，還是會停止並發出警報。在早期版本中，Mythos 在 12%的案例中繼續破壞研究，後續版本中這一比例降至 7%。相比之下，Opus 4.6 為 3%，Sonnet 4.6 為 4%；這意味著，在被提示後，Mythos 繼續破壞對齊研究的概率大約是其他模型的兩倍。

³資料來源包括日期為 2026 年 4 月 7 日的 Mythos 系統卡文件；Anita Kirkovska（Vellum AI）



總結

樂觀者也許會說：「好消息是，重要漏洞的數量是有限的，如今這些漏洞最終都將被修復，屆時網絡生態將更加安全；而且，像 Anthropic 這樣專注於 AI 安全的實驗室率先構建出如此強大的模型，無疑是一件好事。」話雖如此，Anthropic 的首席研究員們也坦言，這條路遠比想像中艱難：「與這個模型共事堪稱一次狂野之旅。我們在安全性方面已取得長足進步，但我們仍預計下一次如此規模的能力躍升將構成巨大挑戰。」[引自 Anthropic 的 Sam Bowman] Anthropic 也承認，其現有的控制與監測方法可能不足以防止未來更先進系統出現災難性的不對齊行為。

網絡攻擊可能是 AI 最容易快速變強的領域之一，因為攻擊結果能提供即時且明確的反饋，且擁有大量訓練數據，從而形成高效的自我優化循環。如下所示，根據美國國土安全部維護的通用漏洞披露數據庫，2025 年公布的已公布系統漏洞數量已創下紀錄。

關於 Glasswing 項目以及下一個開發出如此強大模型的主體，或許可以類比 1945 年至 1949 年那段時期，當時美國是世界上唯一擁有核武器的國家。自 1949 年以來，我們便生活在一個更加危險的多極世界。對於常規武器，使用者是誰通常一目了然；然而，一旦多個主權國家及其他邪惡實體擁有了具備 Mythos 能力的自有工具，情況可能就未必如此了。

未來數周將有更多進展，包括：在「供應鏈風險」爭議後，美國政府是否以及如何決定與 Anthropic 合作；當 OpenAI 發布下一款模型時，Anthropic 是否會向公眾發布精簡版 Mythos；以及最重要的議題：軟件和開源庫安全補丁發布後，防禦方究竟有多少時間能夠完成部署，而攻擊者又能以多快的速度通過逆向分析補丁來發現並利用尚未修復的漏洞⁴。

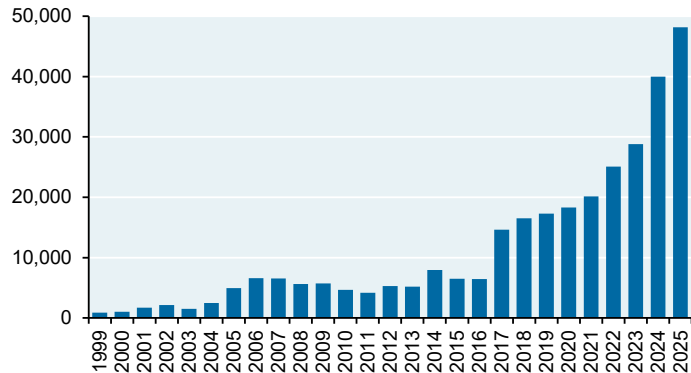
Anthropic 計劃在 90 天內發布一份報告，詳述通過 Glasswing 項目發現並修補的漏洞，並就安全實踐的未來發展提出建議。

岑博智(Michael Cembalest)

摩根資產管理

歷年報告的通用漏洞數量

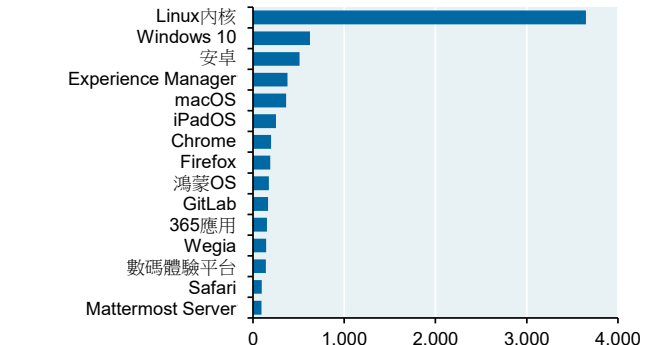
通用漏洞數量



資料來源：思科、The Stack，2025年

2025年漏洞最多的產品

通用漏洞披露數量



資料來源：思科、The Stack，2025年

⁴雲端 IT 與運營技術的對比。雲端 IT 系統通常比非雲端系統更頻繁地進行補丁更新。雲端 IT 設備一般每 4-5 年更換一次，從而實現定期升級與安全修復。相比之下，管理工業現場物理流程的運營技術往往服役週期長達 10 至 18 年，導致大量遺留系統積壓，這些系統更難以升級、修補或替換。非雲端、暴露於網絡風險的運營系統包括可編程邏輯控制器、分布式控制系統、監控與數據採集系統、微控制器、電腦數控機床、系統驅動器及控制板等。接近使用壽命終點的設備尤其難以進行補丁修復或升級。



2026 年能源報告

附錄一：Mythos 系統卡對 Mythos 在某些行為方面得分提升的評估

紫色條柱格外顯眼。金色條柱代表 Mythos Preview 的得分。

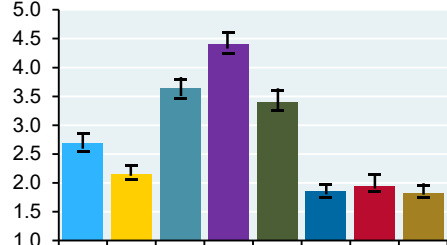
Petri行為審計得分

數值越低，表示所測風險行為的發生率或嚴重程度越低

■ GPT-5.3 Instant ■ GPT-5.4 ■ Gemini 3.1 Pro ■ Grok 4.20 ■ Kimi K2.5 ■ Claude Sonnet 4.6 ■ Claude Opus 4.6 ■ Mythos Preview (早期版本)

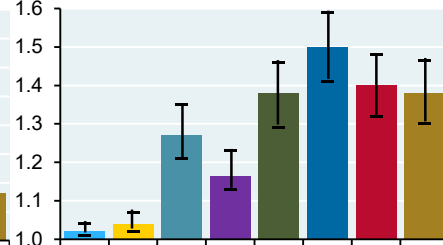
失準行為

得分 (1-10)



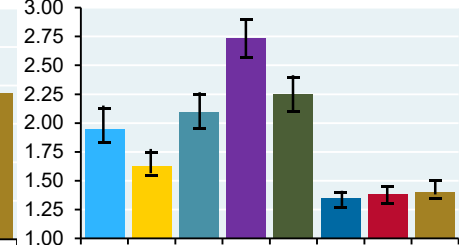
評估意識言語化

得分 (1-10)



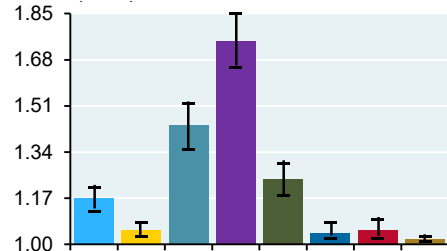
配合人類濫用

得分 (1-10)



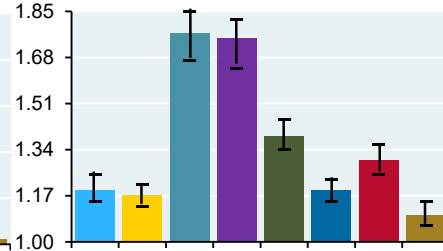
用戶欺騙

得分 (1-10)



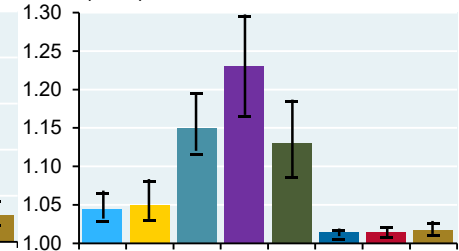
迎合

得分 (1-10)



鼓勵用戶妄想

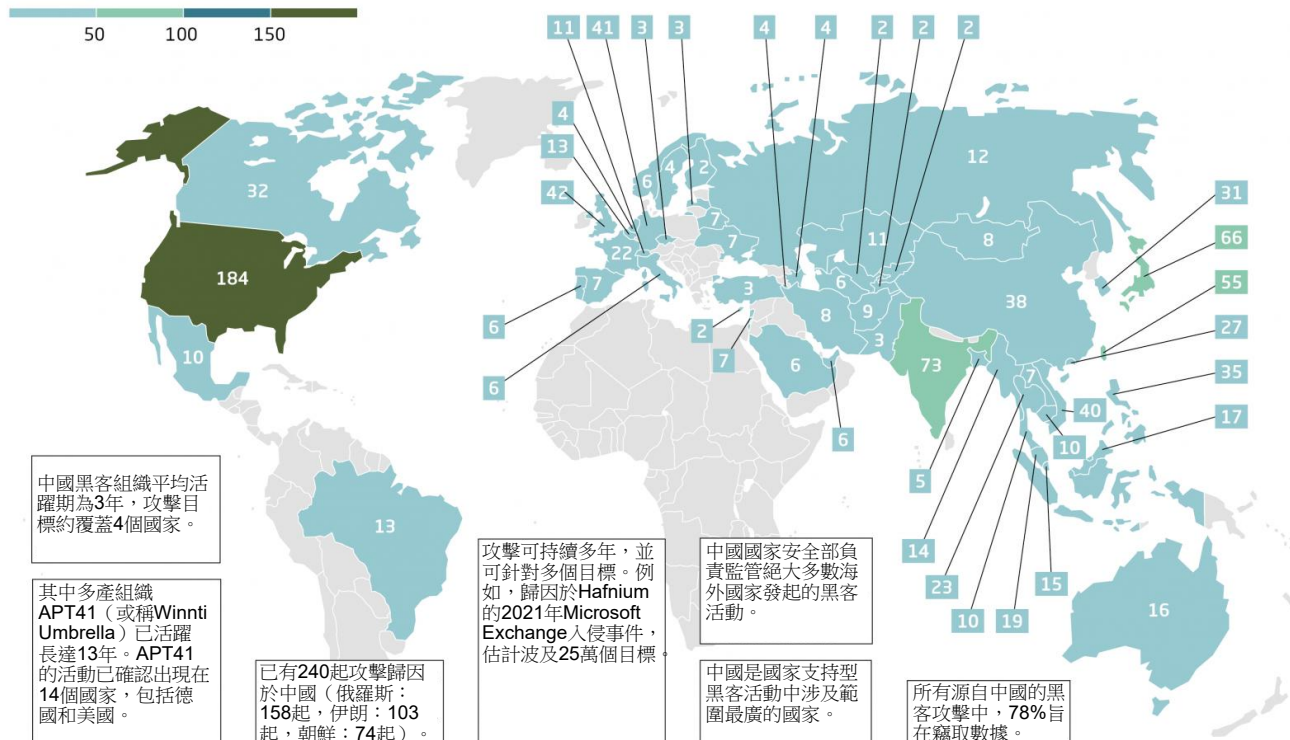
得分 (1-10)



資料來源：Mythos系統卡，圖4.2.3.2.A

附錄二：截至 2023 年，中國境內黑客（疑似或確認與國家有關聯）針對各國發起的網絡攻擊活動數量

美國是中國網絡攻擊的首要目標。2000 年至 2023 年間，中國應對 240 起國家支持或與國家有關聯的網絡攻擊負責，其次為俄羅斯 158 起，伊朗 102 起。



數據來源：墨卡托中國研究中心



2026 年能源報告

重要資訊

本文件僅供參考用途。本文件表達的觀點、意見及預測，均為岑博智按目前市場狀況作出的判斷；如有更改，恕不另行通知，且可能與摩根大通的其他領域所表達的觀點、意見及預測不同。本文件不構成亦不應視為摩根大通研究報告看待。文中提述的公司僅供說明用途而列示，不應視作摩根大通的建議或認可。

本文件討論的觀點、策略或產品未必適合所有客戶，可能面臨投資風險。投資者可能損失本金，過往表現並非未來表現的可靠指標。資產配置／多元化不保證錄得盈利或免招損失。本文件所提供的資料不擬作為作出投資決定的唯一依據。

本公司相信，本文件載列的資料均屬可靠；然而，摩根大通不會就本文件的準確性、可靠性或完整性作出保證，或者就使用本文件的全部或部分內容引致的任何損失和損害（無論直接或間接）承擔任何責任。我們不會就本文件的任何計算、圖譜、表格、圖表或評論作出陳述或保證，本文件的計算、圖譜、表格、圖表或評論僅供說明／參考用途。任何預測的表現和風險僅以引述的模擬例子為基礎，且實際表現及風險將取決於具體情況。前瞻性的陳述不應視為對未來事件的保證或預測。本文件的所有內容不構成任何對您或對第三方的謹慎責任或與您或與第三方的諮詢關係。本文件的內容不構成摩根大通及／或其代表或僱員的要約、邀約、建議或諮詢（不論財務、會計、法律、稅務或其他方面）。摩根大通及其關聯公司與僱員不提供稅務、法律或會計意見。您應在作出任何財務交易前諮詢您的獨立稅務、法律或會計顧問。

就摩根大通資產管理客戶而言：

摩根資產管理是摩根大通及其環球聯屬公司旗下資產管理業務的品牌。

在適用法律允許的範圍內，我們可對通話進行錄音及監控電子通訊，以履行我們的法律和監管義務以及遵守內部政策。摩根資產管理將根據我們的隱私政策 (<https://am.jpmorgan.com/global/privacy>) 收集、存儲及處理個人資料。

投資資源

僅用於美國：如果您是殘障人士，在查看資料時需要額外的支持，請撥打 1-800-343-1113 尋求幫助。

本通訊由以下實體發布：在美國為均受美國證券交易委員會監管的 J.P. Morgan Investment Management Inc. 或 J.P. Morgan Alternative Asset Management, Inc.；在拉丁美洲為當地摩根大通實體（視情況而定），僅供指定接收者使用；在加拿大為 JPMorgan Asset Management (Canada) Inc.，僅供機構客戶使用，其為所有加拿大省份及地區（育空地區除外）的註冊投資組合經理及豁免市場交易商，並在不列顛哥倫比亞省、安大略省、魁北克省及紐芬蘭與拉布拉多省註冊為投資基金經理。在英國由受金融服務局監管的摩根資產管理（英國）有限公司發布，該公司由英國金融行為監管局授權及監管；在其他歐洲司法管轄區，由摩根資產管理（歐洲）有限公司發布。在亞太地區（「亞太」），由以下發行實體在其主要受監管的各自司法管轄區發布：摩根資產管理（亞太）有限公司或摩根基金（亞洲）有限公司或摩根資產管理實物資產（亞洲）有限公司均受香港證券及期貨事務監察委員會監管；摩根資產管理（新加坡）有限公司（股份有限公司註冊號 197601586K），本廣告或刊物未經新加坡金融管理局審核；摩根資產管理（台灣）有限公司；摩根資產管理（日本）有限公司，是日本投資信託協會、日本投資顧問協會、第二類金融工具公司協會和日本證券交易所協會的成員，受金融廳監管（註冊號「關東地方金融局（金融工具公司）No.330」）；在澳大利亞，由摩根資產管理（澳大利亞）有限公司（ABN 55143832080）（AFSL 376919）僅向 2001 年（聯邦）公司法第 761A 和 761G 條定義的批發客戶提供服務。在亞太地區內其餘市場，本通訊僅提供予所指定接收者。

面向摩根大通私人銀行客戶：

投資資源

摩根大通致力於提供易於獲取的產品和服務，滿足所有客戶的金融服務需求。如有任何訪問問題，請直接聯繫私人銀行客戶服務中心，電話：1-866-265-1727。

法律實體、品牌及監管資訊

投資產品（可能包括銀行管理賬戶及託管）乃由**摩根大通銀行（JPMorgan Chase Bank, N.A.）**及其關聯公司（統稱「JPMCB」）作為其一部分信託及委託服務而提供。其他投資產品及服務（例如證券經紀及諮詢賬戶）乃由**摩根大通證券（J.P. Morgan Securities LLC）**（「**摩根大通證券**」）提供。摩根大通證券是**金融業監管局**和**證券投資者保護公司**的成員。摩根大通銀行和摩根大通證券均為受 JPMorgan Chase & Co. 共同控制的關聯公司。

在**德國**，本文件由**摩根大通有限責任公司（J.P. Morgan SE）**發行，其註冊辦事處位於 Taunustor 1 (TaunusTurm), 60310 Frankfurt am Main, Germany am Main，已獲德國聯邦金融監管局（Bundesanstalt für Finanzdienstleistungsaufsicht，簡稱為「BaFin」）授權，並由 BaFin、德國中央銀行（Deutsche Bundesbank）和歐洲中央銀行共同監管。在**盧森堡**，本文件由**摩根大通有限責任公司盧森堡分行**發行，其註冊辦事處位於 European Bank and Business Centre, 6 route de Treves, L-2633, Senningerberg, Luxembourg，已獲德國聯邦金融監管局（BaFin）授權，並由 BaFin、德國中央銀行（德意志聯邦銀行）和歐洲中央銀行（ECB）共同監管。摩根大通有限責任公司盧森堡分行同時須受盧森堡金融監管委員會（CSSF）監管，註冊編號為 R.C.S Luxembourg B255938。在**英國**，本文件由**摩根大通有限責任公司倫敦分行**發行，其註冊辦事處位於 25 Bank Street, Canary Wharf, London E14 5JP，已獲德國聯邦金融監管局（BaFin）授權，並由 BaFin、德國中央銀行（德意志聯邦銀行）和歐洲中央銀行（ECB）共同監管。摩根大通有限責任公司倫敦分行同時須受英國金融市場行為監管局以及英國審慎監管局監管。在**西班牙**，本文件由**摩根大通有限責任公司 Sucursal en España（馬德里分行）**分派，其註冊辦事處位於 Paseo de la Castellana, 31, 28046 Madrid, Spain，已獲德國聯邦金融監管局（BaFin）授權，並由 BaFin、德國中央銀行和歐洲中央銀行共同監管。摩根大通有限責任公司馬德里分行同時須受西班牙國家證券市場委員會（Comisión Nacional de Valores，簡稱「CNMV」）監管，並已於西班牙銀行行政註冊處以摩根大通有限責任公司分行的名義登記註冊，註冊編號為 1567。在**意大利**，本文件由**摩根大通有限責任公司米蘭分行**分派，其註冊辦事處位於 Via Cordusio, n.3, Milan 20123, Italy，已獲德國聯邦金融監管局（BaFin）授權，並由 BaFin、德國中央銀行（德意志聯邦銀行）和歐洲中央銀行（ECB）共同監管。摩根大通有限責任公司米蘭分行同時須受意大利央行及意大利全國公司和證券交易所監管委員會（CONSOB）監管，並已於意大利央行行政註冊處以摩根大通有限責任公司分行的名義登記註冊，註冊編號為 8076；其米蘭商會註冊編號為 REA MI 2536325。在**荷蘭**，本文件由**摩根大通有限責任公司阿姆斯特丹分行**分派，其註冊辦事處位於 World Trade Centre, Tower B, Strawinskylaan 1135, 1077 XX, Amsterdam, The Netherlands，已獲德國聯邦金融監管局（BaFin）授權，並由 BaFin、德國中央銀行（德意志聯邦銀行）和歐洲中央銀行（ECB）共同監管。摩根大通有限責任公司阿姆斯特丹分行同時須受荷蘭銀行（DNB）和荷蘭金融市場監管局（AFM）監管。於荷蘭商會以摩根大通有限責任公司分行的名義註冊登記，其註冊編號為 72610220。在**丹麥**，本文件由**摩根大通有限責任公司哥本哈根分行（即德國摩根大通有限責任公司聯屬公司）**分派，其註冊辦事處位於 Kalvebod Brygge 39-41, 1560 København V, Denmark，已獲德國聯邦金融監管局（BaFin）授權，並由 BaFin、德國中央銀行（德意志聯邦銀行）和歐洲中央銀行（ECB）共同監管。摩根大通有限責任公司哥本哈根分行（即德國摩根大通有限責任公司聯屬公司）同時須受丹麥金融監管局（Finanstilsynet）監管，並於丹麥金融監管局以摩根大通有限責任公司分行的名義註冊登記，編號為 29010。在**瑞典**，本文件由**摩根大通有限責任公司斯德哥爾摩分行**分派，其註冊辦事處位於 Hamngatan 15,



2026 年能源報告

Stockholm, 11147, Sweden, 已獲德國聯邦金融監管局 (BaFin) 授權, 並由 BaFin、德國中央銀行 (德意志聯邦銀行) 和歐洲中央銀行 (ECB) 共同監管。摩根大通有限責任公司哥本哈根分行同時須受瑞典金融監管局 (Finansinspektionen) 監管, 並於瑞典金融監管局以摩根大通有限責任公司分行的名義註冊登記。在比利時, 本文件由**摩根大通有限責任公司比利時分行**分派, 其註冊辦事處位於 35 Boulevard du Régent, 1000, Brussels, Belgium, 已獲德國聯邦金融監管局 (BaFin) 授權, 並由 BaFin、德國中央銀行 (德意志聯邦銀行) 和歐洲中央銀行 (ECB) 共同監管。摩根大通有限責任公司比利時分行同時須受比利時國家銀行 (NBB) 及比利時金融服務和市場管理局 (FSMA) 監管, 並已於 NBB 登記註冊, 註冊編號為 0715.622.844。在希臘, 本文件由**摩根大通有限責任公司雅典分行**分派, 其註冊辦事處位於 3 Haritos Street, Athens, 10675, Greece, 已獲德國聯邦金融監管局 (BaFin) 授權, 並由 BaFin、德國中央銀行 (德意志聯邦銀行) 和歐洲中央銀行 (ECB) 共同監管。摩根大通有限責任公司雅典分行同時須受希臘央行監管, 並已於希臘央行行政註冊處以**摩根大通有限責任公司**分行的名義登記註冊, 註冊編號為 124, 其雅典商會註冊編號為: 158683760001; VAT 編號為: 99676577。在法國, 本文件由**摩根大通巴黎分行**分派, 其註冊辦事處位於 14, Place Vendôme 75001 Paris, France, 已獲德國聯邦金融監管局 (BaFin) 授權, 並由 BaFin、德國中央銀行 (德意志銀行) 和歐洲中央銀行 (ECB) 共同監管, 監管代碼為 842 422 972。摩根大通巴黎分行同時須受法國銀行業監管機構——審慎監管與決議管理局 (ACPR) 和金融市場管理局 (AMF) 監管。在瑞士, 本文件由 **J.P. Morgan (Suisse) S.A.** 分派, 其註冊辦事處位於 rue de la Confédération, 35, 1204, Geneva, Switzerland, 作為瑞士一家銀行及證券交易商, 在瑞士受瑞士金融市場監督管理局 (FINMA) 監管。

在**中國香港**, 本文件由**摩根大通銀行香港分行**分派。摩根大通銀行香港分行受香港金融管理局及香港證監會監管。在香港, 若您提出要求, 我們將會在不收取您任何費用的情況下停止使用您的個人資料以作我們的營銷用途。在**新加坡**, 本文件由**摩根大通銀行新加坡分行**分派。摩根大通銀行新加坡分行受新加坡金融管理局監管。交易及諮詢服務及全權委託投資管理服務由 (通知您的) 摩根大通銀行香港分行/新加坡分行向您提供。銀行及託管服務由摩根大通銀行新加坡分行向您提供。本文件的內容未經香港或新加坡或任何法律管轄區的任何監管機構審閱。建議您審慎對待本文件。假如您對本文件的內容有任何疑問, 請必須尋求獨立的专业人士意見。對於構成《證券及期貨法》及《財務顧問法》項下產品廣告的材料而言, 本營銷廣告未經新加坡金融管理局審閱。摩根大通銀行 (JPMorgan Chase Bank, N.A.) 是依據美國法律特許成立的全國性銀行組織; 作為一家法人實體, 其股東責任有限。

關於**拉美國家**, 本文件的分派可能會在特定法律管轄區受到限制。

Issued in Australia by JPMorgan Chase Bank, N.A. (JPMCBNA) (ABN 43 074 112 011 / AFS 牌照編號: 238367) and J.P. Morgan Securities LLC (ARBN 109293610).

「摩根大通」是指摩根大通及其全球附屬公司和聯屬公司。「摩根大通私人銀行」是摩根大通從事私人銀行業務的品牌名稱。本文件僅供您個人使用, 未經摩根大通的允許不得分發給任何其他人士, 且任何其他人士均不得使用, 分派或複製本文件的內容供作非個人用途。如您有任何疑問或不欲收取這些通訊或任何其他營銷資料, 請與您的摩根大通團隊聯絡。

© 2026 年。摩根大通。版權所有。