準備和應對阻斷服務攻擊（DoS）

初版：2011年9月
最後更新：2025年3月

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Te Tira Tiaki
Government Communications Security Bureau

National Cyber Security Centre
PART OF THE GCSB

引言

本指南由澳洲訊號局（ASD）、紐西蘭國家網路安全中心（NCSC-NZ）、Akamai Technologies Ltd及Cloudflare Pty Ltd所準備，旨在應對在我們區域內阻斷服務攻擊（DoS）日益增加的趨勢，為機構提供根據現今威脅技術的而提出的最佳實踐緩解指引，以準備和應對 DoS 攻擊。

我們建議您同時參閱 ASD的指南 *物聯網裝置 (Internet of Things devices)* 和 *保護您的Wi-Fi 和路由器 (Secure your Wi-Fi and router)*。這些指南能幫助個人，避免在無意間助長會影響他人的 DoS 攻擊。

DoS 攻擊是一種網路攻擊，目的是中斷或降低網站、電郵和網域名稱系統 (DNS) 等線上服務，以阻止合法使用者存取。通常的方法是透過向網上服務傳輸大量數據、連接或請求，使服務不堪負荷及降低其功能。

DoS攻擊通常需要大量網路流量才能成功，而這種攻擊變得越來越普遍，部分原因是由於較易被入侵的物聯網(IoT)裝置數量的日益增加。由於物聯網裝置的製造商通常優先考慮使用者體驗，而不是網路安全，因此而受到攻擊的設備包括能連接上網的日常家居設備，例如智能電視、水壺、吸塵機和保安系統。這些設備往往會被惡意行為者從遠端攻擊，用作透過創建一個由物聯網絡裝置的「殭屍網路」(botnet)，進而產生網路流量，令家庭和機構無意間為DoS攻擊提供基礎裝置。

最近的活動顯示，當惡意行為者成功入侵大量的物聯網設備後，他們或會把這些設備出租或出售給網路犯罪分子和駭客，這些不法分子近來越有興趣使用DoS攻擊他們的目標。通常發動DoS攻擊是為了令機構的生產力和財政有所損失，或引起大眾的關注。這類活動的其中一個例子，於ASD的*「與中華人民共和國有關的人士入侵路由器和物聯網裝置以操作殭屍網路」*公告有所描述。

隨著我們的經濟進一步數碼化，以及能連接上網但安全性較差的物聯網裝置數量日益俱增，DoS攻擊的可能會持續增加。

為了中斷或降低機構的線上服務,惡意行為者會利用多種方法,包括:

- 引導大量多餘的網路流量至網上服務,試圖消耗所有可用的網路頻寬
- 引導針對性的網路流量至網上服務,試圖消耗電腦的處理資源
- 使用多部電腦、物聯網裝置或其他網絡連線裝置,從多方向、更大規模地將網路流量引導至網上服務,這常見的 DoS 攻擊被稱為分散式 DoS (DDoS) 攻擊
- 騎劫機構的網域名稱註冊或 DNS 伺服器,試圖將合法用戶從機構的網上服務中導向離開。

雖然機構無法避免成為 DoS 攻擊的目標,但仍可採取多項措施,做足準備,盡可能減少其影響。最佳策略是在 DoS 攻擊發生前做好準備,因為若沒有準備,受到 DoS 攻擊時會較難反應,且反應的效果會較低。

縱使機構的主要目標是保護免受 DoS 攻擊,但也應該採取措施,防止其網上服務和網路連線裝置,被惡意行為者利用作攻擊他人的工具。

準備應對 DoS 攻擊

鑑於我們地區的 DoS 攻擊數量不斷增加,在實施任何 DoS 攻擊防範措施之前,貴機構應首作業務需求評估,以確定機構的各項網上服務是否必須在受到 DoS 攻擊期間仍保持正常運作,或是可以接受服務暫時中斷。

如果貴機構希望增強抵禦 DoS 攻擊的能力,則應在被 DoS 攻擊前,於適當且可行的情況下,主動採取下列措施:

- 如果貴機構有利用內容傳遞網路(CDN),則應在適當且可行的情況下實施下列的附加措施。
  - 選用CDN時考慮所具備功能,保護來源網絡伺服器免受各種應用程式和網路層攻擊 — 某些 CDN 或會將這些功能部署在網絡邊緣的應用程式防火牆。
  - 避免在不必要的情況下公開披露來源網絡伺服器的IP位址,並僅在受保護的情況下才公開披露,以免受 DoS 攻擊。
  - 避免讓惡意行為者輕易預測到來源網絡伺服器的IP位址,例如不要與網上服務的公開 IP 位址共存於同一子網路。
  - 使用網路存取控制(例如防火牆),確保只有 CDN 和機構的授權網絡管理人員能存取來源網絡伺服器。
  - 如果您的來源網絡伺服器需要更高級別的保護,可考慮在來源伺服器和 CDN 供應商之間使用具韌性的多樣化網路連接,包括專用的網路連接。
  - 設定 CDN、來源網絡伺服器和用戶端的HTTP標頭,來提高快取運作效率。
  - 如果您需要更高級別的可及性,可考慮對來源網絡伺服器進行區域分割,分別處理來自低風險和高風險IP 位址的請求。
- 釐定網上服務的正當用戶對功能和服務品質的接受水平、如何維護其功能性,以及在受到 DoS 攻擊期間非必要的功能。
- 採購並使用以雲端為基礎的 DoS 攻擊緩解服務。
- 考慮透過下列方式以減少機構的攻擊面:
  - 將基礎網上服務(如 DNS)外判給能抵禦 DoS 攻擊的知名服務供應商
  - 將關鍵網上服務(例如電郵)和其他更可能成為攻擊目標的網上服務(例如網站)分割出來
  - 確保 DoS 攻擊緩解服務只允許與網上服務所使用之網路埠相關的流量。

- 與您的服務供應商討論 DoS 攻擊預防和緩解策略的細節,特別是:
  - 抵禦來自世界各地的 DoS 攻擊的實證
  - 有處理 DoS 攻擊和全面授權 DoS 攻擊測試的往績
  - 無需人手干預(如人手分析網路流量)即可自動緩解大多數類型 DoS 攻擊的能力
  - 瞭解服務的收費方式,例如是固定費用還是根據網路流量或電腦處理資源而調整,以及可否設定費用上限
  - 在 DoS 攻擊期間通知您或關閉網上服務的門檻
  - 預先批准在 DoS 攻擊期間可採取的行動
  - 與上游供應商制定預防 DoS 攻擊的安排。
- 制定能偵測 DoS 攻擊的標準,例如對系統可用性進行實時監控及警示、網路流量、電腦處理資源和相關成本。
- 準備網站的靜態版本,以減少處理和頻寬需求,從而在受到DoS 攻擊期間仍能繼續提供服務。
- 採購並使用高韌性的網上服務,例如具有大量頻寬、充足的電腦處理資源、地理上分散的托管伺服位置,和雲端流量清理以丟棄不需要的網路流量 — 這通常包括選用信譽良好的 CDN,以快取靜態網站內容,並保護您的來源網絡伺服器免收不必要的網路流量。
- 保護機構的域名,包括利用註冊鎖定、確認域名註冊中的聯絡資訊和其他詳細資料皆正確無誤,並遵循 ASD 的 *域名持有人的DNS安全指南 (Domain Name System security for domain owners)*中概述的其他指引。
- 確保持有服務供應商的最新聯絡方式,並與他們分享機構的聯絡方式,確保機構在有需要時能聯絡他們,如每日24 小時、每周7 天。
- 向您的服務供應商提供緊急聯絡方式,確保有可信賴的聯絡渠道,可在正常渠道受阻時使用。
- 制定、實施和維護網路安全事故應變計劃,涵蓋各項必須能抵禦 DoS 攻擊的網上服務,以抵禦各類型的 DoS 攻擊,並至少每年演練一次該計劃。
- 設計應用程式時,保護常被濫用的功能,因為這些功能會消耗更多的電腦處理資源,或衍生額外的成本(如發送短訊)。
  - 加入保護措施,包括限制速率和驗證請求是否來自人類。
  - 執行 DoS 攻擊測試,包括針對應用程式功能中的不正確邏輯流程。
  - 執行更廣泛的負載測試,以識別和修復 DoS 向量。

應對 DoS 攻擊

如果貴機構尚未做好應對DoS攻擊的準備,您可以嘗試在遭受DoS攻擊時實施上述的一些措施,惟效果或會較差且實施費時,令機構的應對能力有所降低。

機構在遭受DoS攻擊時,應在適當和可行的情況下實施下列措施。

- 制定網路安全事故應變計畫。
- 向您的服務供應商查詢能否採取措施即時回應 — 如果您們未曾討論過他們的回應能力,您或會發現他們無法或不願意回應,或要求收取額外費用。
- 停用非必要的功能,或從網上服務中移除非必要內容,令目前的DoS攻擊不再有效,如部署沒有搜尋功能、動態內容或大檔案的網站版本。

- 與您的客戶和服務供應商(包括您的DoS攻擊緩解服務供應商)保持溝通,並繼續監察您網上服務的可用性。
- 如果您的來源網絡伺服器被直接攻擊,請考慮變更其IP位址,並避免在沒有採取保護措施的情況下公開披露新的IP位址。
- 依照本指南的「聯絡」部分,向相關方面(包括 ASD 和 NCSC-NZ)報告DoS攻擊。

避免成為 DoS 攻擊的幫凶

貴機構應實施下列措施,避免無意間成為DoS攻擊的幫凶,影響他人。

- 避免在網上曝露不需要的、設定不安全的或維護不足的服務、物聯網裝置及其他網絡連線裝置。
- 安全地設定、維護和監察曝露在網上的服務、物聯網設備和其他網絡連線裝置。
  - 在 ASD的 *物聯網設備 (Internet of Things devices)* 和 *保護您的 Wi-Fi 和路由器安全 (Secure your Wi-Fi and router)* 中有更多適合小型企業的指引。

如果貴機構已在運行網上服務,您應實施下列額外措施。

- 優先審視美國網路安全和基礎設施安全局(CISA) *基於 UDP 的放大型攻擊 (UDP-Based Amplification Attacks)* 建議中概述的協定。
- 監察新發現的放大攻擊向量,以保護您的網上服務免受其侵害。
- 實施進入和離開的網路存取控制,使授權網上服務和機構的存取能力有所限制。
- 對於易受放大型攻擊所影響的網上服務,應阻檔匿名的公開存取(如非必要)。
- 如果未能或未適合實施阻擋或限制應用存取,請考慮實施速率限制,以減少濫用的影響。

更多資訊

ASD 的 *資訊安全手冊 (Information security manual)* 是一個網路安全框架,供各機構參考應用於系統和資料的保護,免受網路威脅。在 *緩解網路安全事件的策略 (Strategies to mitigate cyber security incidents)*,以及 *八項基本措施 (Essential Eight)* 中的建議均有補充此框架的資訊。

紐西蘭資訊安全手冊 (New Zealand Information Security Manual) 是紐西蘭政府關於資訊保安與資訊系統安全的手冊。該本從業員手冊旨在滿足機構資訊安全主管、為機構提供服務的供應商、承包商和顧問的需求。

有關各種 DoS 攻擊類型的更多資訊,請參閱 CISA 的 *DDoS 快速指南 (DDos Quick Guide)* 和 *了解與應對分散式拒絕服務攻擊 (Understanding and Responding to Distriubted Denial-Of-Service Attacks)* 指南。

聯絡方式

如您在澳洲對本指南有任何疑問,*請聯絡 ASD* 或致電 1300 CYBER1 (1300 292 371)。

如您在紐西蘭要通報網路安全事故,請發送電郵至 incidents@ncsc.govt.nz 或瀏覽 NCSC-NZ 的報告事件 網頁。

免責聲明

本指南的內容只屬一般性資料，不應被視為法律建議，或是在任何特定或緊急情況下依賴作為幫助。在任何重要事項上，您都應該根據個人情況，尋求適當的獨立專業建議。

若因依賴本指南的資訊而引致任何損害、損失或費用，聯邦政府是不會承擔任何責任或義務的。

如需了解詳情或通報網絡安全事件，請聯繫我們：

cyber.gov.au | 1300 CYBER1 (1300 292 371)

此號碼僅適用於澳洲境內。

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre