Chuẩn bị và đối phó với các cuộc tấn công từ-chối-dịch-vụ (Denial-of-Service Attacks)

Xuất bản lần đầu tiên : tháng 9 năm 2011
Cập nhật lần sau cùng: Tháng 3 năm 2025

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

Giới thiệu

Ấn bản này được soạn thảo bởi Tổng cục Tín hiệu Úc (Australian Signals Directorate - ASD) phối hợp với Trung tâm An ninh Mạng Quốc gia Tân Tây Lan (New Zealand's National Cyber Security Centre - NCSC-NZ), công ty Akamai Technologies Ltd và Cloudflare Pty Ltd, nhằm đối phó với xu hướng gia tăng các cuộc tấn công từ-chối-dịch-vụ (denial-of-service - DoS) trong khu vực của chúng ta. Tài liệu này cung cấp hướng dẫn cho các tổ chức về các thực hành tốt nhất về biện pháp giảm thiểu dựa trên các kỹ thuật đe dọa hiện đại, để chuẩn bị và đối phó với các cuộc tấn công DoS.

Chúng tôi đề nghị quý vị đọc lời khuyên này cùng với các ấn bản của ASD có chủ đề *Internet of Things devices (Thiết bị Internet của Vạn vật)* và *Bảo mật Wi-Fi và bộ định tuyến*. Các ấn bản này giúp người sử dụng tránh việc vô tình góp phần vào các cuộc tấn công DoS có thể làm ảnh hưởng đến người khác.

Các cuộc tấn công DoS là những cuộc tấn công mạng được thiết kế nhằm làm gián đoạn hoặc suy giảm các dịch vụ trực tuyến như trang mạng, email và dịch vụ Hệ thống Tên miền (Domain Name System - DNS), khiến người sử dụng hợp pháp không thể truy cập. Điều này thường đạt được bằng cách làm 'ngập' dịch vụ trực tuyến bằng dữ liệu, kết nối hoặc các yêu cầu nhằm làm quá tải dịch vụ và làm giảm hiệu quả hoạt động của nó.

Các cuộc tấn công DoS thường đòi hỏi một lưu lượng mạng lớn để có thể thành công. Chúng ngày càng trở nên phổ biến, một phần là do số lượng thiết bị Internet của Vạn vật (Internet of Things - IoT) dễ bị xâm phạm ngày càng gia tăng. Vì các nhà sản xuất thiết bị IoT thường ưu tiên trải nghiệm của người dùng hơn là an ninh mạng, vì vậy các thiết bị dễ bị tấn công có thể bao gồm các đồ vật gia dụng thông thường có kết nối internet như TV thông minh, ấm đun nước bằng điện, máy hút bụi và hệ thống an ninh. Những thiết bị này thường có thể bị các tác nhân độc hại xâm nhập từ xa để tạo thành một "botnet" (là một mạng lưới các máy vi tính hoặc thiết bị có kết nối internet đã bị nhiễm phần mềm độc hại và bị điều khiển từ xa) gồm nhiều thiết bị, từ đó phát sinh ra lưu lượng mạng lớn này. Điều này có thể khiến các hộ gia đình và tổ chức vô tình trở thành một phần của hạ tầng cơ sở góp phần cho các cuộc tấn công DoS.

Hoạt động gần đây cho thấy rằng sau khi những tác nhân độc hại xâm nhập được vào một số lượng lớn thiết bị IoT, chúng có thể cho thuê hoặc bán hạ tầng cơ sở này cho tội phạm mạng và những kẻ truy cập trái phép, những kẻ này càng ngày càng chú tâm đến việc thực hiện các cuộc tấn công DoS vào các mục tiêu mà chúng lựa chọn. Trong hầu hết các trường hợp, các cuộc tấn công DoS được thực hiện nhằm gây thiệt hại về năng suất và tài chính cho một tổ chức, hoặc để thu hút sự chú ý của công chúng cho một mục đích nào đó. Một ví dụ về hoạt động này được mô tả trong khuyến cáo của ASD có chủ đề *Các tác nhân có liên quan đến Cộng hòa Nhân dân Trung Hoa xâm phạm bộ định tuyến và thiết bị IoT để thực hiện hoạt động botnet*.

Khi nền kinh tế của chúng ta ngày càng được kỹ thuật số hoá và số lượng thiết bị IoT có bảo mật kém kết nối với internet ngày càng nhiều, các cuộc tấn công DoS có thể sẽ tiếp tục gia tăng.

Để làm gián đoạn hoặc suy giảm các dịch vụ trực tuyến của một tổ chức, các tác nhân độc hại sử dụng nhiều phương pháp khác nhau, bao gồm:

- đưa một lưu lượng mạng lớn không mong muốn tới các dịch vụ trực tuyến nhằm cố gắng tiêu thụ hết toàn bộ băng thông mạng hiện có
- đưa lưu lượng mạng đã được điều chỉnh phù hợp đến các dịch vụ trực tuyến nhằm mục đích tiêu thụ hết nguồn lực xử lý máy vi tính của các dịch vụ trực tuyến này
- sử dụng nhiều máy vi tính, thiết bị IoT hoặc các thiết bị có kết nối internet khác để điều hướng lưu lượng mạng tới các dịch vụ trực tuyến từ nhiều hướng và trên quy mô lớn hơn nhiều, một loại tấn công DoS phổ biến được gọi là tấn công từ chối dịch vụ phân tán (distributed DoS - DDoS)
- chiếm quyền kiểm soát đăng ký tên miền hoặc máy chủ DNS của một tổ chức nhằm cố gắng chuyển hướng người dùng hợp pháp ra khỏi các dịch vụ trực tuyến của tổ chức đó.

Các tổ chức không thể tránh khỏi việc trở thành mục tiêu của các cuộc tấn công DoS, nhưng có một số biện pháp mà các tổ chức có thể thực hiện để chuẩn bị và có thể giảm thiểu tác động của chúng. Chuẩn bị cho các cuộc tấn công DoS trước khi chúng xảy ra là cách tốt nhất. Vì nếu không có sự chuẩn bị, sẽ rất khó khăn và kém hiệu quả để đối phó khi quý vị bị tấn công DoS.

Mặc dù các tổ chức chủ yếu tập trung vào việc bảo vệ mình khỏi các cuộc tấn công DoS, nhưng họ cũng nên thực hiện các bước để ngăn chặn các dịch vụ trực tuyến và thiết bị có kết nối internet của mình bị kẻ xấu lợi dụng để nhắm vào người khác.

Chuẩn bị cho các cuộc tấn công DoS

Trong bối cảnh những tấn công DoS ngày càng gia tăng trên khắp khu vực của chúng ta, trước khi đưa ra bất kỳ biện pháp nào để chuẩn bị đối phó với các cuộc tấn công DoS, tổ chức của quý vị trước tiên nên đánh giá các yêu cầu kinh doanh để xác định xem từng dịch vụ trực tuyến của quý vị có cần phải được tiếp tục hoạt động trong thời gian xảy ra các cuộc tấn công DoS hay không? hoặc việc gián đoạn dịch vụ tạm thời là điều có thể chấp nhận được.

Nếu tổ chức của quý vị muốn tăng cường sức chống chọi để đương đầu với các cuộc tấn công DoS, quý vị nên chủ động áp dụng ra các biện pháp sau đây vào thời điểm thích hợp và khả thi, trước khi các cuộc tấn công DoS xảy ra.

- Nếu tổ chức của quý vị đang sử dụng mạng phân phối nội dung (content delivery network - CDN), quý vị nên áp dụng các biện pháp bổ sung sau đây, khi thích hợp và khả thi.
  - Hãy cân nhắc sử dụng CDN có chức năng bảo vệ máy chủ trang mạng gốc của quý vị khỏi nhiều cuộc tấn công ở tầng ứng dụng và tầng mạng – một số CDN có thể bao gồm các tính năng này như một phần của tường lửa (firewall) ứng dụng trang mạng ở rìa mạng.
  - Tránh tiết lộ công khai không cần thiết địa chỉ Giao thức Internet (Internet Protocol - IP) của máy chủ trang mạng gốc, và phải bảo đảm rằng mọi thông tin công khai đều được bảo vệ khỏi các cuộc tấn công DoS.
  - Tránh sử dụng địa chỉ IP cho máy chủ trang mạng gốc mà tác nhân có thể dự đoán được, ví dụ, địa chỉ IP trong cùng mạng con với các địa chỉ IP được tiết lộ công khai của các dịch vụ trực tuyến của quý vị.
  - Sử dụng các biện pháp kiểm soát truy cập mạng (như tường lửa) để bảo đảm rằng chỉ có CDN và các mạng quản lý được ủy quyền của tổ chức quý vị mới có thể truy cập vào máy chủ trang mạng gốc của quý vị mà thôi.
  - Hãy xem xét đến việc sử dụng kết nối mạng đa dạng, có thể bao gồm kết nối mạng riêng giữa máy chủ trang mạng gốc và nhà cung cấp CDN của quý vị nếu quý vị cần mức độ bảo vệ cao hơn cho máy chủ trang mạng gốc của mình.

  - Cấu hình CDN, máy chủ trang mạng gốc và chủ đề HTTP của máy khách để tối ưu hóa lượng bộ nhớ đệm được thực hiện.
  - Hãy xem xét đến việc phân vùng máy chủ trang mạng gốc để các yêu cầu từ địa chỉ IP có rủi ro thấp được giải quyết riêng biệt so với các yêu cầu từ địa chỉ IP có rủi ro cao hơn nếu quý vị cần mức độ khả dụng cao hơn.
- Xác định chức năng và phẩm chất dịch vụ nào được chấp nhận đối với người sử dụng hợp pháp của dịch vụ trực tuyến của quý vị, cách thức để duy trì chức năng đó và chức năng nào không cần thiết trong các cuộc tấn công DoS.
- Mua và sử dụng dịch vụ giảm thiểu tấn công DoS dựa trên đám mây.
- Hãy cân nhắc việc giảm bề mặt tấn công của tổ chức quý vị bằng cách:
  - thuê các dịch vụ trực tuyến cơ bản (như DNS) cho các nhà cung cấp dịch vụ có uy tín có khả năng chống lại các cuộc tấn công DoS
  - phân chia các dịch vụ trực tuyến quan trọng (như email) khỏi các dịch vụ trực tuyến khác vì những dịch vụ này có thể trở thành mục tiêu (ví dụ như trang mạng)
  - phải bảo đảm rằng dịch vụ giảm thiểu tấn công DoS chỉ cho phép lưu lượng mạng liên quan đến các cổng mạng của dịch vụ trực tuyến mà thôi.
- Thảo luận với các nhà cung cấp dịch vụ của quý vị về các chi tiết về chiến lược phòng ngừa và giảm thiểu tấn công DoS của họ, cụ thể là:
  - các phương pháp đã được chứng minh để đương đầu với các cuộc tấn công DoS từ khắp nơi trên thế giới
  - chứng minh cụ thể đối các phương pháp chống chọi với các cuộc tấn công Dos trước đây, và thử nghiệm tấn công DoS toàn diện được ủy quyền
  - khả năng tự động giảm thiểu hầu hết các loại tấn công DoS mà không cần sự tham gia của con người, chẳng hạn như phân tích thủ công lưu lượng mạng
  - cách thức để định giá dịch vụ của họ, chẳng hạn như lệ phí là cố định hay thay đổi dựa trên lượng lưu lượng mạng và nguồn lực xử lý máy vi tính được sử dụng, và liệu quý vị có thể đặt giới hạn cho lệ phí thanh toán hay không?
  - mức giới hạn để thông báo cho quý vị hoặc tắt dịch vụ trực tuyến của họ trong các cuộc tấn công DoS
  - các hành động được chấp thuận trước có thể được thực hiện trong các cuộc tấn công DoS
  - các thỏa thuận phòng ngừa tấn công DoS với các nhà cung cấp thượng nguồn.
- Thực hiện các biện pháp phát hiện các cuộc tấn công DoS, chẳng hạn như theo dõi và cảnh báo theo thời gian thực về tính khả dụng của hệ thống, lưu lượng mạng, nguồn lực xử lý máy vi tính và các chi phí liên quan.
- Chuẩn bị một phiên bản tĩnh của trang mạng của quý vị với mức xử băng thông xử lý tối thiểu nhằm bảo đảm tính liên tục của dịch vụ trong thời gian bị tấn công DoS.
- Mua và sử dụng các dịch vụ trực tuyến có khả năng phục hồi cao với băng thông lớn, nguồn lực xử lý máy vi tính đầy đủ, vị trí lưu trữ phân tán về mặt địa lý và lọc lưu lượng truy cập dựa trên đám mây để loại bỏ lưu lượng mạng không mong muốn – điều này thường bao gồm việc sử dụng CDN có uy tín để lưu trữ nội dung trang mạng tĩnh và bảo vệ máy chủ trang mạng gốc của quý vị khỏi lưu lượng mạng không mong muốn.
- Bảo vệ tên miền của tổ chức quý vị bằng cách sử dụng khóa đăng ký, xác nhận thông tin liên lạc đăng ký tên miền và các thông tin chi tiết khác là chính xác và làm theo hướng dẫn bổ sung được nêu trong ấn bản của ASD có chủ đề *Bảo mật Hệ thống Tên Miền cho chủ sở hữu tên miền*.
- Duy trì thông tin liên lạc luôn được cập nhật của các nhà cung cấp dịch vụ và chia sẻ thông tin liên lạc của tổ chức của quý vị với họ, hãy bảo đảm rằng tất cả các kênh liên lạc đều sẵn sàng theo yêu cầu của tổ chức của quý vị, ví dụ như 24 giờ mỗi ngày, 7 ngày mỗi tuần.
- Cung cấp thông tin liên lạc ngoài băng thông (out-of-band) của tổ chức của quý vị cho các nhà cung cấp dịch vụ, nhằm bảo đảm có một kênh liên lạc đáng tin cậy trong trường hợp các kênh liên lạc thông thường bị gián đoạn.

- Soạn thảo, thực hiện và duy trì kế hoạch đối phó với các vấn đề an ninh mạng, bao gồm nhiều loại tấn công DoS vào từng dịch vụ trực tuyến của quý vị, và thực hiện kế hoạch ít nhất một lần mỗi năm.
- Thiết kế kiến trúc ứng dụng để bảo vệ các chức năng thường bị lạm dụng có thể tiêu tốn nhiều nguồn lực xử lý của máy vi tính, hoặc phát sinh thêm chi phí tài chính (chẳng hạn như gởi tin nhắn SMS).
  - Các biện pháp bảo vệ bao gồm giới hạn tốc độ (rate limiting) và xác minh rằng các yêu cầu là đến từ con người.
  - Thực hiện kiểm tra tấn công từ chối dịch vụ (DoS), bao gồm cả việc nhắm mục tiêu vào các luồng logic không hợp lý trong chức năng của ứng dụng.
  - Thực hiện kiểm tra tải ở phạm vi rộng hơn để xác định và khắc phục các vector (phương pháp) tấn công DoS.

Đối phó với các cuộc tấn công từ chối dịch vụ (DoS)

Nếu tổ chức của quý vị chưa chuẩn bị để đối phó với các cuộc tấn công từ chối dịch vụ (DoS), quý vị có thể thử áp dụng một số biện pháp được nêu bên trên trong thời gian xảy ra các cuộc tấn công DoS. Tuy nhiên, các biện pháp này có thể kém hiệu quả hơn và mất thời gian để thực hiện, làm giảm khả năng đối phó của tổ chức của quý vị.

Tổ chức của quý vị nên áp dụng các biện pháp sau đây trong thời gian xảy ra các cuộc tấn công DoS nếu thấy phù hợp và khả thi.

- Thực hiện kế hoạch đối phó các vấn đề an ninh mạng của quý vị.
- Hỏi các nhà cung cấp dịch vụ của quý vị xem họ có thể áp dụng các phản hồi ngay lập tức hay không – nếu quý vị chưa từng thảo luận trước đó về khả năng đối phó của họ, quý vị có thể phát hiện rằng họ không thể hoặc không sẵn sàng phản hồi, hoặc sẽ tính thêm lệ phí.
- Vô hiệu hóa các chức năng không quan trọng hoặc loại bỏ các nội dung không thiết yếu khỏi dịch vụ trực tuyến của quý vị mà đang bị sử dụng để làm cho cuộc tấn công DoS hiện tại trở nên hiệu quả. Ví dụ như, đưa ra một phiên bản trang mạng của quý vị mà không có chức năng tìm kiếm, nội dung sống động hoặc các tập hồ sơ lớn.
- Duy trì liên lạc với khách hàng và các nhà cung cấp dịch vụ của quý vị, bao gồm cả nhà cung cấp dịch vụ giảm thiểu tấn công DoS, đồng thời tiếp tục theo dõi tính khả dụng của các dịch vụ trực tuyến của quý vị.
- Xem xét việc thay đổi địa chỉ IP của máy chủ trang mạng gốc nếu nó đang bị tấn công trực tiếp, và tránh công khai địa chỉ IP mới nếu chưa có các biện pháp bảo vệ thích hợp.
- Trình báo các cuộc tấn công DoS với các bên liên quan, bao gồm ASD và NCSC-NZ theo mục “Chi tiết liên lạc” trong tài liệu này.

Tránh góp phần vào các cuộc tấn công DoS

Tổ chức của quý vị nên thực hiện các biện pháp sau đây để tránh vô tình góp phần gây ra các cuộc tấn công DoS có thể ảnh hưởng đến những người khác.

- Tránh để lộ các dịch vụ, thiết bị IoT và các thiết bị có kết nối internet khác không cần thiết, cấu hình không an toàn hoặc bảo trì không đầy đủ ra internet.

- Cấu hình, duy trì, và theo dõi một cách an toàn các dịch vụ, thiết bị IoT và các thiết bị có kết nối internet khác được phép tiếp xúc với internet.
  - Hướng dẫn bổ sung dành cho các doanh nghiệp nhỏ có sẵn trong ấn bản của ASD có chủ đề *Thiết bị Internet của Vạn vật* và *Bảo mật Wi-Fi và bộ định tuyến*.

Nếu tổ chức của quý vị đang chạy dịch vụ trực tuyến, quý vị nên thực hiện các biện pháp bổ sung sau đây.

- Ưu tiên xem xét các giao thức được nêu trong hướng dẫn về *Tấn công Khuếch đại Dựa trên UDP* của Cơ quan An ninh Mạng và Hạ tầng Cơ sở Hoa Kỳ (CISA).
- Theo dõi các vector (phương pháp) khuếch đại mới khi chúng được phát hiện và bảo vệ các dịch vụ trực tuyến của quý vị từ những phương pháp đó.
- Cấu hình kiểm soát truy cập mạng đến và đi để hạn chế quyền truy cập vào các dịch vụ và tổ chức trực tuyến được ủy quyền.
- Chặn quyền truy cập công khai ẩn danh đối với các dịch vụ trực tuyến dễ bị khuếch đại nếu không cần thiết.
- Xem xét việc áp dụng công cụ giới hạn tốc độ (rate-limiting) để giảm thiểu hậu quả của việc lạm dụng, khi không thể hoặc không phù hợp để ngăn chặn hoặc áp dụng các biện pháp kiểm soát truy cập.

Tham khảo thêm

Cẩm nang bảo mật thông tin của ASD là một khuôn khổ bảo mật mạng mà các tổ chức có thể áp dụng để bảo vệ hệ thống và dữ liệu của họ khỏi các mối đe dọa mạng. Các khuyến nghị trong *Chiến lược giảm nhẹ vấn đề an ninh mạng*, cùng với Bộ Tám Yếu tố Thiết yếu (Essential Eight), bổ sung cho khuôn khổ này.

Cẩm nang An ninh Thông tin Tân Tây Lan là tài liệu hướng dẫn của Chính phủ Tân Tây Lan về bảo đảm thông tin và an ninh hệ thống thông tin. Đây là cẩm nang dành cho người hành nghề được thiết kế để đáp ứng nhu cầu của các giám đốc điều hành an ninh thông tin của cơ quan cũng như các nhà cung cấp, nhà thầu và nhà cố vấn cung cấp dịch vụ cho các cơ quan.

Thông tin chi tiết về các loại tấn công DoS có thể được tìm thấy trong tài liệu của CISA: *Hướng dẫn Nhanh về DDoS* và *Hiểu và Đối phó với các Cuộc tấn công Từ chối Dịch vụ Phân tán*.

Thông tin liên lạc

Tại Úc, nếu quý vị có bất kỳ câu hỏi nào về hướng dẫn này, hãy *gởi thư cho ASD* hoặc gọi số 1300 CYBER1 (1300 292 371).

Tại Tân Tây Lan, để trình báo các vấn đề ninh mạng, hãy gởi email tới incidents@ncsc.govt.nz hoặc truy cập trang mạng của NCSC-NZ Trình báo các vấn đề.

Tuyên bố miễn trừ trách nhiệm

Tài liệu trong hướng dẫn này mang tính chất tổng quát và không nên được coi là cố vấn pháp lý, hoặc được dựa vào để được hỗ trợ trong bất kỳ trường hợp cụ thể hoặc tình huống khẩn cấp nào. Đối với bất kỳ vấn đề quan trọng nào, quý vị nên tìm kiếm lời khuyên chuyên môn thích hợp, độc lập và liên quan đến hoàn cảnh của mình.

Chính phủ Liên bang không chịu trách nhiệm hoặc trách nhiệm pháp lý nào đối với bất kỳ thiệt hại, mất mát hoặc chi phí nào phát sinh do việc trông cậy vào thông tin có trong hướng dẫn này.

Bản quyền

Sử dụng Quốc huy

Các điều khoản về việc sử dụng Quốc huy như được trình bày chi tiết trên trang mạng của Bộ Thủ tướng và Nội các Thông tin và Hướng dẫn về Quốc huy của Liên bang | pmc.gov.au.

Muốn biết thêm thông tin, hoặc muốn phúc trình vấn đề an ninh mạng, hãy liên lạc với chúng tôi:

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

Số điện thoại này chỉ được sử dụng ở trong nước Úc mà thôi.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre