PHÂN LOẠI TẤN CÔNG DDOS VÀ CÁC BIỆN PHÁP PHÒNG CHỐNG

Hoàng Xuân Dậu
Học viện Công nghệ Bưu Chính Viễn Thông
Email: dauhx@ptit.edu.vn

Tóm tắt. Tấn công từ chối dịch vụ phân tán (DDoS) đã phát triển mạnh mẽ trong những năm gần đây và là một mối đe dọa thường trực đối với hệ thống mạng và máy chủ dịch vụ của các cơ quan và tổ chức. Tấn công từ chối dịch vụ gây cạn kiệt tài nguyên hệ thống hoặc ngập lụt đường truyền, làm ngắt quãng quá trình cung cấp dịch vụ cho người dùng hợp pháp, hoặc thậm chí khiến cả hệ thống ngừng hoạt động. Tấn công DDoS rất khó phát hiện và phòng chống hiệu quả do số lượng các host bị điều khiển tham gia tấn công thường rất lớn và nằm rải rác ở nhiều nơi. Để có giải pháp phòng chống tấn công DDoS hiệu quả, việc nghiên cứu về các dạng tấn công DDoS là cần thiết. Bài báo này tổng hợp các phương pháp phân loại các dạng tấn công DDoS và các biện pháp phòng chống tấn công DDoS, giúp nâng cao hiểu biết về dạng tấn công này và trên cơ sở đó lựa chọn các biện pháp phòng chống hiệu quả cho từng hệ thống cụ thể.

1. GIỚI THIỆU

Tấn công từ chối dịch vụ (Denial of Service - DoS) là dạng tấn công nhằm ngăn chặn người dùng hợp pháp truy nhập các tài nguyên mạng. Tấn công DoS đã xuất hiện từ khá sớm, vào đầu những năm 80 của thế kỷ trước [1]. Tấn công từ chối dịch vụ phân tán (Distributed Denial of Service - DDoS) là một dạng phát triển ở mức độ cao của tấn công DoS được phát hiện lần đầu tiên vào năm 1999 [2]. Khác biệt cơ bản của tấn công DoS và DDoS là phạm vi tấn công. Trong khi lưu lượng tấn công DoS thường phát sinh từ một hoặc một số ít host nguồn, lưu lượng tấn công DDoS thường phát sinh từ rất nhiều host nằm rải rác trên mạng Internet. Hiện nay, có hai phương pháp tấn công DDoS chủ yếu [1]. Trong phương pháp thứ nhất, kẻ tấn công gửi các gói tin được tạo theo dạng đặc biệt gây lỗi trong giao thức truyền hoặc lỗi trong ứng dụng chạy trên máy nạn nhân. Một dạng tấn công DDoS điển hình theo phương pháp này là tấn công khai thác lỗ hổng an ninh của các giao thức hoặc dịch vụ trên máy nạn nhân. Phương pháp tấn công DDoS thứ hai phổ biến hơn phương pháp thứ nhất, gồm hai dạng [1]: (i) dạng tấn công DDoS gây ngắt quãng kết nối của người dùng đến máy chủ dịch vụ bằng cách làm ngập lụt đường truyền mạng, cạn kiệt băng thông hoặc tài nguyên mạng, và (ii) dạng tấn công DDoS gây ngắt quãng dịch vụ cung cấp cho người dùng bằng cách làm cạn kiệt các tài nguyên của máy chủ dịch vụ, như thời gian xử lý của CPU, bộ nhớ, băng thông đĩa, cơ sở dữ liệu. Dạng tấn công này bao gồm các loại tấn công gây ngập lụt ở mức ứng dụng.

Kể từ cuộc tấn công DDoS đầu tiên được xác nhận vào năm 1999 [2], nhiều cuộc tấn công DDoS gây ngập lụt đã được thực hiện vào hệ thống mạng của các công ty và các tổ chức. Hầu hết các cuộc tấn công DDoS gây ngập lụt cho đến hiện nay đều tập trung vào làm ngắt quãng hoặc ngừng dịch vụ chạy trên hệ thống nạn nhân. Hậu quả là làm giảm doanh thu, tăng chi phí phòng chống và phục hồi dịch vụ. Ví dụ, vào tháng Hai năm 2000, hệ thống mạng của công ty Internet Yahoo phải hứng chịu đợt tấn công DDoS đầu tiên làm các dịch vụ của công ty phải ngừng hoạt động trong 2 giờ, gây thiệt hại lớn về doanh thu quảng cáo [1]. Tháng Hai năm 2004, một đợt tấn công DDoS rất lớn xuất phát từ một lượng rất lớn các máy tính bị nhiễm virus Mydoom làm trang web của tập đoàn SCO không thể truy nhập. Virus Mydoom chứa các đoạn mã độc hại chạy trên hàng ngàn máy tính bị lây nhiễm đồng loạt tấn công trang web của tập đoàn SCO [1]. Mã độc của virus Mydoom còn được tái sử dụng vào tháng Bảy năm 2009 để tấn công một loạt các trang web của Chính phủ và các tổ chức tài chính ở Hàn Quốc và Mỹ gây nhiều hậu quả nghiêm trọng [1]. Vào tháng Mười Hai năm 2010, một nhóm tin tặc có tên là "Anonymous" đã đạo diễn một loạt các cuộc tấn công DDoS gây ngừng hoạt động các trang web của các tổ chức tài chính, như Mastercard, Visa International, Paypal và PostFinance. Tháng Chín năm

2012, một đợt tấn công DDoS rất lớn do nhóm tin tặc "Izz ad-Din al-Qassam Cyber Fighters" thực hiện gây ngắt quãng hoặt ngừng hoạt động các trang web ngân hàng trực tuyến của 9 ngân hàng lớn của Mỹ [1]. Các dạng tấn công DDoS được thực hiện ngày một nhiều với quy mô ngày một lớn và tinh vi hơn nhờ sự phát triển của các kỹ thuật tấn công và sự lan tràn của các công cụ tấn công.

Động cơ của tin tặc tấn công DDoS khá đa dạng. Tuy nhiên, có thể chia các dạng tấn công DDoS dựa trên động cơ của tin tặc thành 5 loại chính [1]:

a) Nhằm giành được các lợi ích tài chính, kinh tế: Tin tặc tấn công DDoS thuộc loại này thường có kỹ thuật tinh vi và nhiều kinh nghiệm tấn công và chúng luôn là mối đe dọa thường trực đối với các công ty, tập đoàn lớn. Các tấn công DDoS nhằm giành được các lợi ích tài chính là những tấn công nguy hiểm và khó phòng chống nhất.

b) Để trả thù: Tin tặc tấn công DDoS thuộc loại này thường là những cá nhân bất mãn và họ thực hiện tấn công để trả đũa những sự việc mà họ cho là bất công.

c) Gây chiến tranh trên không gian mạng: Tin tặc tấn công DDoS thuộc loại này thường thuộc về các tổ chức quân sự hoặc khủng bố của một nước thực hiện tấn công vào các hệ thống trọng yếu của một nước khác vì mục đích chính trị. Các đích tấn công thường gặp là các hệ thống mạng của các cơ quan chính phủ, các tổ chức tài chính ngân hàng, hệ thống cung cấp điện nước và các nhà cung cấp dịch vụ viễn thông. Tin tặc loại này thường được đào tạo tốt và được sử dụng nguồn lực mạnh phục vụ tấn công trong thời gian dài. Hậu quả của dạng tấn công này thường rất lớn, gây ngưng trệ nhiều dịch vụ và có thể gây thiệt hại lớn về kinh tế cho một quốc gia.

d) Do niềm tin ý thức hệ: Tin tặc tấn công DDoS thuộc loại này chiếm tỷ trọng lớn các cuộc tấn công DDoS và thường thực hiện tấn công do niềm tin ý thức hệ, bao gồm tấn công vì các mục đích chính trị, tôn giáo.

e) Để thử thách trí tuệ: Tin tặc tấn công DDoS thuộc loại này thường là những người trẻ tuổi thích thể hiện bản thân, thực hiện tấn công để thử nghiệm và học cách thực hiện các dạng tấn công khác nhau. Loại tin tặc này đang tăng nhanh chóng do ngày nay có sẵn nhiều công cụ tấn công mạng rất dễ dùng và một người nghiệp dư cũng có thể sử dụng để thực hiện thành công một tấn công DDoS.

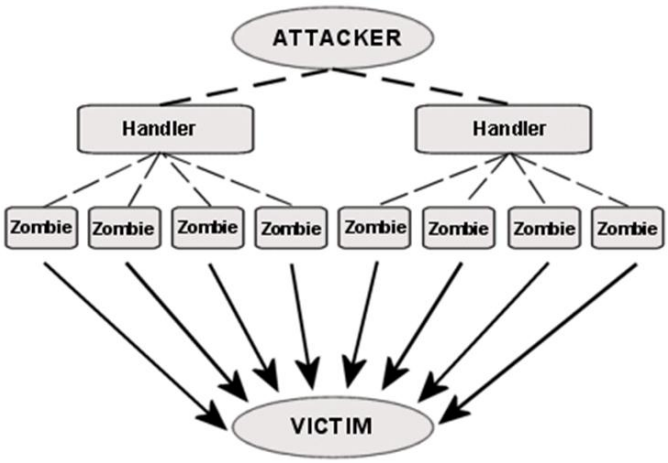
Để phòng chống tấn công DDoS một cách hiệu quả nhằm hạn chế và giảm thiểu thiệt hại do tấn công DDoS gây ra, việc nghiên cứu về các dạng tấn công và các biện pháp phòng chống là cần thiết. Nhiều công trình nghiên cứu về phân loại các dạng tấn công DDoS và các biện pháp phòng chống đã được công bố [1][3][4][5][8][9][11]. Một cách tổng quát, Douligeris và cộng sự [11] phân loại các tấn công DDoS thành 2 dạng: (i) dạng tấn công gây cạn kiệt băng thông đường truyền mạng và (ii) dạng tấn công gây cạn kiệt tài nguyên máy chủ dịch vụ. Dạng tấn công cạn kiệt băng thông lại được chia thành tấn công gây ngập lụt và tấn công khuếch đại, còn dạng tấn công gây cạn kiệt tài nguyên máy chủ được chia tiếp thành tấn công khai thác lỗi giao thức và tấn công sử dụng các gói tin đặc biệt. Zargar và các cộng sự [1] phân loại các tấn công DDoS thành 2 dạng dựa trên lớp mạng, gồm tấn công gây ngập lụt ở lớp mạng/giao vận và tấn công gây ngập lụt ở lớp ứng dụng. Theo một hướng khác, Mirkovic và cộng sự [3] và Bhuyan và cộng sự [8] phân loại các tấn công DDoS dựa trên 4 tiêu chí: (i) mức độ tự động, (ii) khai thác các lỗ hổng an ninh, (iii) cường độ tấn công và (iv) mức độ ảnh hưởng. Tuy có sự khác biệt về phương pháp và tiêu chí phân loại, các công trình nghiên cứu đều có chung đánh giá về mức độ nguy hiểm và sự tăng trưởng đáng lo ngại của tấn công DDoS cả về phạm vi, mức độ tinh vi và khả năng phá hoại. Về các phương pháp phòng chống tấn công DDoS, nhiều nghiên cứu [1][3][5] có chung cách phân loại dựa trên 2 tiêu chí chính: (i) vị trí triển khai và (ii) thời điểm hành động.

Bài báo này tổng hợp các phương pháp phân loại các dạng tấn công DDoS và các biện pháp phòng chống tấn công DDoS, giúp nâng cao hiểu biết về dạng tấn công này và trên cơ sở đó lựa chọn các biện pháp phòng chống hiệu quả cho từng hệ thống cụ thể. Phần còn lại của bài báo được bố cục như sau: Mục 2 trình bày kiến trúc và các phương pháp phân loại tấn công DDoS; Mục 3 trình bày các biện pháp phòng chống điển hình và Mục 4 là phần Kết luận.

2. PHÂN LOẠI TẤN CÔNG DDOS

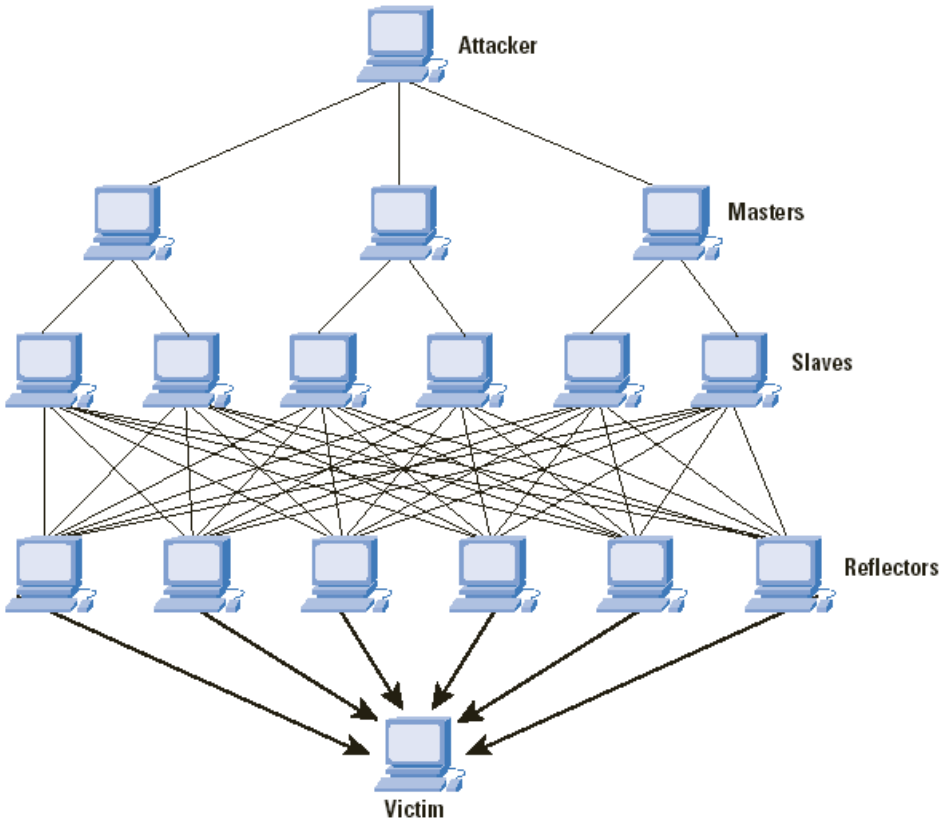
2.1. Kiến trúc tấn công DDoS

Mặc dù có nhiều dạng tấn công DDoS được ghi nhận, nhưng tựu trung có thể chia kiến trúc tấn công DDoS thành 2 loại chính: (i) kiến trúc tấn công DDoS trực tiếp và (i) kiến trúc tấn công DDoS gián tiếp hay phản chiếu. Hình 1 minh họa kiến trúc tấn công DDoS trực tiếp, theo đó tin tặc (Attacker) trước hết thực hiện chiếm quyền điều khiển hàng ngàn máy tính có kết nối Internet, biến các máy tính này thành các Zombie – những máy tính bị kiểm soát và điều khiển từ xa bởi tin tặc. Tin tặc thường điều khiển các Zombie thông qua các máy trung gian (Handler). Hệ thống các Zombie chịu sự điều khiển của tin tặc còn được gọi là mạng máy tính ma hay botnet.



Hình 1. Kiến trúc tấn công DDoS trực tiếp

Theo lệnh gửi từ tin tặc, các Zombie đồng loạt tạo và gửi các yêu cầu truy nhập giả mạo đến hệ thống nạn nhân (Victim), gây ngập lụt đường truyền mạng hoặc làm cạn kiệt tài nguyên của máy chủ, dẫn đến ngắt quãng hoặc ngừng dịch vụ cung cấp cho người dùng.



Hình 2. Kiến trúc tấn công DDoS gián tiếp hay phản chiếu

Hình 2 minh họa kiến trúc tấn công DDoS gián tiếp hay còn gọi là kiến trúc tấn công DDoS phản chiếu. Tương tự như kiến trúc tấn công DDoS trực tiếp, tin tặc (Attacker) trước hết thực hiện chiếm quyền điều khiển một lượng rất lớn máy tính có kết nối Internet, biến các máy tính này thành các Zombie, hay còn gọi la Slave. Tin tặc điều khiển các Slave thông qua các máy trung gian (Master). Theo lệnh gửi từ tin tặc, các Slave đồng loạt tạo và gửi các yêu cầu truy nhập giả mạo với địa chỉ nguồn của các gói tin là địa chỉ của máy nạn nhân (Victim) đến đến một số lớn các máy khác (Reflectors) trên mạng Internet. Các Reflectors gửi phản hồi (Reply) đến máy nạn nhân do địa chỉ của máy nạn nhân được đặt vào yêu cầu giả mạo. Khi các Reflectors có số lượng lớn, số phản hồi sẽ rất lớn và gây ngập lụt đường truyền mạng hoặc làm cạn kiệt tài nguyên của máy nạn nhân, dẫn đến ngắt quãng hoặc ngừng dịch vụ cung cấp cho người dùng. Các Reflectors bị lợi dụng để tham gia tấn công thường là các hệ thống máy chủ có công suất lớn trên mạng Internet và không chịu sự điều khiển của tin tặc.

2.2. Phân loại tấn công DDoS

Các cuộc tấn công DDoS thường được tin tặc thực hiện bằng cách huy động một số lượng rất lớn các máy tính có kết nối Internet bị chiếm quyền điều khiển – tập hợp các máy này được gọi là mạng máy tính ma hay mạng bot, hoặc botnet. Các máy của botnet có khả năng gửi hàng ngàn yêu cầu giả mạo mỗi giây đến hệ thống nạn nhân, gây ảnh hưởng nghiêm trọng đến chất lượng dịch vụ cung cấp cho người dùng. Do các yêu cầu của tấn công DDoS được gửi rải rác từ nhiều máy ở nhiều vị trí địa lý nên rất khó phân biệt với các yêu cầu của người dùng hợp pháp. Một trong các khâu cần thiết trong việc đề ra các biện pháp phòng chống tấn công DDoS hiệu quả là phân loại các dạng tấn công DDoS và từ đó có biện pháp phòng chống thích hợp. Nhiều phương pháp phân loại tấn công DDoS đã được đề xuất như trong các công trình

[1][3][4][5][8][9][11]. Một cách khái quát, tấn công DDoS có thể được phân loại dựa trên 6 tiêu chí chính: (1) Dựa trên phương pháp tấn công, (2) Dựa trên mức độ tự động, (3) Dựa trên giao thức mạng, (4) Dựa trên phương thức giao tiếp, (5) Dựa trên cường độ tấn công và (6) Dựa trên việc khai thác các lỗ hổng an ninh. Phần tiếp theo của mục này trình bày chi tiết từng loại.

2.2.1. Dựa trên phương pháp tấn công

Phân loại DDoS dựa trên phương pháp tấn công là một trong phương pháp phân loại cơ bản nhất. Theo tiêu chí này, DDoS có thể được chia thành 2 dạng [5]:

1) Tấn công gây ngập lụt (Flooding attacks): Trong tấn công gây ngập lụt, tin tặc tạo một lượng lớn các gói tin tấn công giống như các gói tin hợp lệ và gửi đến hệ thống nạn nhân làm cho hệ thống không thể phục vụ người dùng hợp pháp. Đối tượng của tấn công dạng này là băng thông mạng, không gian đĩa, thời gian của CPU,…

2) Tấn công logic (Logical attacks): Tấn công logic thường khai thác các tính năng hoặc các lỗi cài đặt của các giao thức hoặc dịch vụ chạy trên hệ thống nạn nhân, nhằm làm cạn kiệt tài nguyên hệ thống. Ví dụ tấn công TCP SYN khai thác quá trình bắt tay 3 bước trong khởi tạo kết nối TCP, trong đó mỗi yêu cầu kết nối được cấp một phần không gian trong bảng lưu yêu cầu kết nối trong khi chờ xác nhận kết nối. Tin tặc có thể gửi một lượng lớn yêu cầu kết nối giả mạo – các kết nối không thể thực hiện, chiếm đầy không gian bảng kết nối và hệ thống nạn nhân không thể tiếp nhận yêu cầu kết nối của người dùng hợp pháp.

2.2.2. Dựa trên mức độ tự động

Theo mức độ tự động, có thể chia tấn công DDoS thành 3 dạng [3]:

1) Tấn công thủ công: Tin tặc trực tiếp quét các hệ thống tìm lỗ hổng, đột nhập vào hệ thống, cài đặt mã tấn công và ra lệnh kích hoạt tấn công. Chỉ những tấn công DDoS trong giai đoạn đầu mới được thực hiện thủ công.

2) Tấn công bán tự động: Trong dạng này, mạng lưới thực hiện tấn công DDoS bao gồm các máy điều khiển (master/handler) và các máy agent (slave, deamon, zombie, bot). Các giai đoạn tuyển chọn máy agent, khai thác lỗ hổng và lây nhiễm được thực hiện tự động. Trong đoạn tấn công, tin tặc gửi các thông tin bao gồm kiểu tấn công, thời điểm bắt đầu, khoảng thời gian duy trì tấn công và đích tấn công đến các agent thông qua các handler. Các agent sẽ theo lệnh gửi các gói tin tấn công đến hệ thống nạn nhân.

3) Tấn công tự động: Tất cả các giai đoạn trong quá trình tấn công DDoS, từ tuyển chọn máy agent, khai thác lỗ hổng, lây nhiễm đến thực hiện tấn công đều được thực hiện tự động. Tất cả các tham số tấn công đều được lập trình sẵn và đưa vào mã tấn công. Tấn công dạng này giảm đến tối thiểu giao tiếp giữa tin tặc và mạng lưới tấn công, và tin tặc chỉ cần kích hoạt giai đoạn tuyển chọn các máy agent.

2.2.3. Dựa trên giao thức mạng

Dựa trên giao thức mạng, tấn công DDoS có thể chia thành 2 dạng [1]:

1) Tấn công vào tầng mạng hoặc giao vận: Ở dạng này, các gói tin TCP, UDP và ICMP được sử dụng để thực hiện tấn công.

2) Tấn công vào tầng ứng dụng: Ở dạng này, các tấn công thường hướng đến các dịch vụ thông dụng ứng với các giao thức tầng ứng dụng như HTTP, DNS và SMTP. Tấn công DDoS tầng ứng dụng cũng có thể gây ngập lụt đường truyền và tiêu hao tài nguyên máy chủ, làm ngắt quãng khả năng cung cấp dịch vụ cho người dùng hợp pháp. Dạng tấn công này rất khó phát hiện do các yêu cầu tấn công tương tự yêu cầu từ người dùng hợp pháp.

2.2.4. Dựa trên phương thức giao tiếp

Thông thường, để thực hiện tấn công DDoS, tin tặc phải tuyển chọn và chiếm quyền điều khiển một số lượng lớn các máy tính có kết nối Internet, và các máy tính này sau khi bị cài phần mềm agent trở thành các bots - công cụ giúp tin tặc thực hiện tấn công DDoS. Tin tặc thông qua các máy điều khiển (master) giao tiếp với các bots để gửi thông tin và các lệnh điều khiển tấn công. Theo phương thức giao tiếp giữa các master và bots, có thể chia tấn công DDoS thành 4 dạng [5]:

1) DDoS dựa trên agent-handler: Tấn công DDoS dựa trên dạng này bao gồm các thành phần: clients, handlers và agents (bots/zombies). Tin tặc chỉ giao tiếp trực tiếp với clients. Clients sẽ giao tiếp với agents thông qua handlers. Nhận được lệnh và các thông tin thực hiện tấn công, agents trực tiếp thực hiện việc tấn công.

2) DDoS dựa trên IRC: Internet Relay Chat (IRC) là một hệ thống truyền thông điệp trực tuyến cho phép nhiều người dùng tạo kết nối và trao đổi các thông điệp theo thời gian thực. Trong dạng tấn công DDoS này tin tặc sử dụng IRC làm kênh giao tiếp với các agents, không sử dụng handlers.

3) DDoS dựa trên web: Trong dạng tấn công này, tin tặc sử dụng các trang web làm phương tiện giao tiếp qua kênh HTTP thay cho kênh IRC. Các trang web của tin tặc được sử dụng làm trung tâm điều khiển và lây nhiễm các phần mềm độc hại, các công cụ khai thác các lỗ hổng an ninh, cài đặt các agents chiếm quyền điều khiển hệ thống máy tính và biến chúng thành các bots. Các bots có thể được xác lập cấu hình hoạt động từ đầu, hoặc chúng có thể gửi các thông điệp đến trang web điều khiển thông qua các giao thức web phổ biến như HTTP và HTTPS.

4) DDoS dựa trên P2P: Ở dạng này, tin tặc sử dụng giao thức Peer to Peer – một giao thức ở tầng ứng dụng làm kênh giao tiếp. Bản chất của các mạng P2P là phân tán nên rất khó để phát hiện các bots giao tiếp với nhau thông qua kênh này.

2.2.5. Dựa trên cường độ tấn công

Dựa trên cường độ hoặc tần suất gửi yêu cầu tấn công, có thể phân loại tấn công DDoS thành 5 dạng [3]:

1) Tấn công cường độ cao: Là dạng tấn công gây ngắt quãng dịch vụ bằng cách gửi cùng một thời điểm một lượng rất lớn các yêu cầu từ các máy agents/zombies nằm phân tán trên mạng.

2) Tấn công cường độ thấp: Các agents/zombies được phối hợp sử dụng để gửi một lượng lớn các yêu cầu giả mạo, nhưng với tần suất thấp, làm suy giảm dần dần hiệu năng mạng. Dạng tấn công này rất khó bị phát hiện do lưu lương tấn công tương tự như lưu lượng đến từ người dùng hợp pháp.

3) Tấn công cường độ hỗn hợp: Là dạng kết hợp giữa tấn công cường độ cao và tấn công cường độ thấp. Đây là dạng tấn công phức hợp, trong đó tin tặc thường sử dụng các công cụ để sinh các gói tin tấn công gửi với tần suất cao và thấp.

4) Tấn công cường độ liên tục: Là dạng tấn công được thực hiện liên tục với cường độ tối đa trong suốt khoảng thời gian từ khi bắt đầu đến khi kết thúc.

5) Tấn công cường độ thay đổi: Đây là dạng tấn công có cường độ thay đổi động nhằm tránh bị phát hiện và đáp trả.

2.2.6. Dựa trên việc khai thác các lỗ hổng an ninh

Dựa trên việc khai thác các điểm yếu và lỗ hổng an ninh, tấn công DDoS có thể được phân loại thành 2 dạng [5]:

1) Tấn công gây cạn kiệt băng thông: Các tấn công DDoS dạng này được thiết kế để gây ngập lụt hệ thống mạng của nạn nhân bằng các yêu cầu truy nhập giả mạo, làm người dùng hợp pháp không thể truy nhập dịch vụ. Tấn công dạng này thường gây tắc nghẽn đường truyền bằng lượng yêu cầu giả mạo rất lớn gửi bởi các máy tính ma (zombie) của các botnets. Dạng tấn công này cũng còn được gọi là tấn công gây ngập lụt hoặc tấn công khuếch đại.

2) Tấn công gây cạn kiệt tài nguyên: Các tấn công DDoS dạng này được thiết kế để tiêu dùng hết các tài nguyên trên hệ thống nạn nhân, làm cho nó không thể phục vụ các yêu cầu của người dùng hợp pháp. Dạng tấn công DDoS này có thể được chia nhỏ thành 2 dạng (i) tấn công khai thác tính năng hoặc lỗi cài đặt của các giao thức và (ii) tấn công sử dụng các gói tin được tạo đặc biệt. Trong dạng thứ nhất, tin tặc khai thác các lỗi hoặc các tính năng đặc biệt của các giao thức trên hệ thống nạn nhân để gây cạn kiệt tài nguyên. Trong dạng thứ hai, kẻ tấn công tạo ra các gói tin đặc biệt, như các gói sai định dạng, gói có khiếm khuyết, gửi đến hệ thống nạn nhân. Hệ thống nạn nhân có thể bị trục trặc khi cố gắng xử lý các gói tin dạng này. Ví dụ, trong tấn công Ping of Death, tin tặc gửi các gói tin ICMP có kích thước lớn hơn 64KB gây lỗi các máy chạy hệ điều hành Windows XP.

3. CÁC BIỆN PHÁP PHÒNG CHỐNG

Do tính chất nghiêm trọng của tấn công DDoS, nhiều giải pháp phòng chống đã được nghiên cứu và đề xuất trong những năm qua. Tuy nhiên, cho đến hiện nay gần như chưa có giải pháp nào có khả năng phòng chống DDoS một cách toàn diện và hiệu quả do tính chất phức tạp, quy mô lớn và tính phân tán rất cao của tấn công DDoS. Thông thường, khi phát hiện tấn công DDoS, việc có thể thực hiện được tốt nhất là ngắt hệ thống nạn nhân khỏi tất cả các tài nguyên do mọi hành động phản ứng lại tấn công đều cần đến các tài nguyên trong khi các tài nguyên này đã bị tấn công DDoS làm cho cạn kiệt. Sau khi hệ thống nạn nhân được ngắt khỏi các tài nguyên, việc truy tìm nguồn gốc và nhận dạng tấn công có thể được tiến hành. Nhiều biện pháp phòng chống tấn công DDoS đã được nghiên cứu trong những năm gần đây [1][3][4][5][11]. Tựu chung có thể chia các biện pháp phòng chống tấn công DDoS thành 3 dạng theo 3 tiêu chí chính: (i) Dựa trên vị trí triển khai, (ii) Dựa trên giao thức mạng và

(iii) Dựa trên thời điểm hành động. Phần tiết theo mô tả các biện pháp phòng chống tấn công DDoS thuộc 3 dạng trên.

3.1. Dựa trên vị trí triển khai

Các biện pháp phòng chống tấn công DDoS được phân loại vào dạng này dựa trên vị trí cài đặt và tiếp tục được chia nhỏ thành 3 dạng con [5]:

1) Triển khai ở nguồn tấn công: Các biện pháp phòng chống tấn công DDoS được triển khai ở gần nguồn của tấn công. Phương pháp này nhằm hạn chế các mạng người dùng tham gia tấn công DDoS. Một số biện pháp cụ thể bao gồm:

- Thực hiện lọc các gói tin sử dụng địa chỉ giả mạo tại các bộ định tuyến ở cổng mạng;
- Sử dụng các tường lửa có khả năng nhận dạng và giảm tần suất chuyển các gói tin hoặc yêu cầu không được xác nhận.

2) Triển khai ở đích tấn công: Các biện pháp phòng chống tấn công DDoS được triển khai ở gần đích của tấn công, tức là tại bộ định tuyến ở cổng mạng hoặc bộ định tuyến của hệ thống đích. Các biện pháp cụ thể có thể gồm:

- Truy tìm địa chỉ IP: Gồm các kỹ thuật nhận dạng địa chỉ và người dùng giả mạo.
- Lọc và đánh dấu các gói tin: Các gói tin hợp lệ được đánh dấu sao cho hệ thống nạn nhân có thể phân biệt các gói tin hợp lệ và gói tin tấn công. Một số kỹ thuật lọc và đánh

dấu gói tin được đề xuất gồm: Lọc IP dựa trên lịch sử, Lọc dựa trên đếm hop, Nhận dạng đường dẫn,…

3) Triển khai ở mạng đích tấn công: Các biện pháp phòng chống tấn công DDoS được triển khai ở các bộ định tuyến của mạng đích dựa trên lọc gói tin, phát hiện và lọc các gói tin độc hại.

3.2. Dựa trên giao thức mạng

Các biện pháp phòng chống tấn công DDoS được chia nhỏ theo tầng mạng: IP, TCP và ứng dụng [5]:

1) Phòng chống tấn công DDoS ở tầng IP bao gồm một số biện pháp:

- Pushback: Là cơ chế phòng chống tấn công DDoS ở tầng IP cho phép một bộ định tuyến yêu cầu các bộ định tuyến liền kề phía trước giảm tần suất truyền các gói tin.
- SIP defender: Một kiến trúc an ninh mở cho phép giám sát luồng các gói tin giữa các máy chủ SIP và người dùng và proxy bên ngoài với mục đích phát hiện và ngăn chặn tấn công vào các máy chủ SIP.
- Các phương pháp dựa trên ô đố chữ: Gồm các phương pháp dựa trên ô đố chữ mật mã để chống lại tấn công DDoS ở mức IP.

2) Phòng chống tấn công DDoS ở tầng TCP bao gồm một số biện pháp:

- Sử dụng các kỹ thuật lọc gói tin dựa trên địa chỉ IP.
- Tăng kích thước Backlogs giúp tăng khả năng chấp nhận kết nối mới của hệ thống đích.
- Giảm thời gian chờ xác nhận yêu cầu kết nối TCP-SYN giúp máy chủ hủy bỏ các yêu cầu kết nối không được xác nhận trong khoảng thời gian ngắn hơn, giải phóng tài nguyên các kết nối chờ chiếm giữ.
- Sử dụng SYN cache giúp duy trì Backlogs chung cho toàn máy chủ thay vì Backlogs riêng cho mỗi ứng dụng. Nhờ vậy có thể tăng số lượng kết nối đang chờ xác nhận.
- Sử dụng SYN Cookies cho phép chỉ cấp phát tài nguyên cho kết nối khi nó đã được xác nhận. Các yêu cầu SYN sẽ bị hủy nếu không được xác nhận trước khi được chuyển cho máy chủ đích. Phương pháp này có thể giúp phòng chống tấn công SYN Flood hiệu quả.
- Sử dụng tường lửa hoặc proxy để lọc các gói tin hoặc thực thi các chính sách an ninh đã xác lập trước.

3) Phòng chống tấn công DDoS ở tầng ứng dụng có thể bao gồm:

- Tối thiểu hóa hành vi truy nhập trang để phòng chống tấn công gây ngập lụt HTTP.
- Sử dụng các phương pháp thống kê để phát hiện tấn công DDoS ở mức HTTP.
- Giám sát hành vi của người dùng trong các phiên làm việc để phát hiện tấn công.

3.3. Dựa trên thời điểm hành động

Dựa trên thời điểm hành động, có thể phân loại các biện pháp phòng chống tấn công DDoS thành 3 dạng theo 3 thời điểm [5]:

1) Trước khi xảy ra tấn công: Các biện pháp phòng chống tấn công DDoS thuộc dạng này được triển khai nhằm ngăn chặn tấn công xảy ra. Một phần lớn các biện pháp thuộc dạng này bao gồm việc cập nhật hệ thống, đảm bảo cấu hình an ninh phù hợp, sửa lỗi, vá các lỗ hổng để giảm thiểu khả năng bị tin tặc khai thác phục vụ tấn công.

2) Trong khi xảy ra tấn công: Các biện pháp phòng chống tấn công DDoS thuộc dạng này tập trung phát hiện và ngăn chặn tấn công. Tường lửa và các hệ thống IDS/IPS thuộc nhóm này.

3) Sau khi xảy ra tấn công: Gồm các biện pháp được triển khai để lần vết và truy tìm nguồn gốc của tấn công DDoS.

4. KẾT LUẬN

Tấn công từ chối dịch vụ phân tán (DDoS) đã phát triển đáng lo ngại trong những năm gần đây và là mối đe dọa thường trực với hệ thống mạng của các cơ quan chính phủ và các doanh nghiệp. Nhiều cuộc tấn công DDoS với quy mô rất lớn đã được thực hiện gây tê liệt hệ thống mạng của Chính phủ Hàn Quốc và gây ngắt quãng hoạt động của các mạng dịch vụ trực truyến nổi tiếng như Yahoo. Tấn công DDoS rất khó phòng chống hiệu quả do quy mô rất lớn và bản chất phân tán của nó.

Nhiều kỹ thuật và công cụ tấn công DDoS phức tạp đã được phát triển, trong đó hỗ trợ đắc lực nhất cho tấn công DDoS là sự phát triển nhanh chóng của các kỹ thuật lây nhiễm các phần mềm độc hại, xây dựng hệ thống mạng máy tính ma (zombie, botnets). Tin tặc có thể chiếm quyền điều khiển các máy tính có kết nối Internet, điều khiển mạng botnet với hàng trăm ngàn máy tính để thực hiện tấn công DDoS. Để có giải pháp toàn diện phòng chống tấn công DDoS hiệu quả, việc nghiên cứu về các dạng tấn công DDoS là khâu cần thực hiện đầu tiên. Bài báo này tổng hợp các phương pháp phân loại các dạng tấn công DDoS và các biện pháp phòng chống tấn công DDoS. Trên cơ sở đó có thể có đánh giá đúng về khả năng bị tấn công và lựa chọn tập các biện pháp phòng ngừa, phát hiện và ngăn chặn tấn công một cách hiệu quả.

TÀI LIỆU THAM KHẢO

[1] Saman Taghavi Zargar, James Joshi, Member and David Tippe, A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks, IEEE Communications Surveys & Tutorials, 2013.

[2] P. J. Criscuolo, Distributed Denial of Service, Tribe Flood Network 2000 and Stacheldraht CIAC-2319, Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev. 1., Lawrence Livermore National Laboratory, February 2000.

[3] Jelena Mirkovic, Janice Martin and Peter Reiher, A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms, ACM SIGCOMM Computer Communication Review, 2004.

[4] Jameel Hashmi, Manish Saxena, and Rajesh Saini, Classification of DDoS Attacks and their Defense Techniques using Intrusion Prevention System, International Journal of Computer Science & Communication Networks, 2012.

[5] Rajkumar, Manisha Jitendra Nene, A Survey on Latest DoS Attacks:Classification and Defense Mechanisms, International Journal of Innovative Research in Computer and Communication Engineering, 2013.

[6] Thwe Thwe Oo, Thandar Phyu, A Statistical Approach to Classify and Identify DDoS Attacks using UCLA Dataset, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2013.

[7] Tony Scheid, DDoS Detection and Mitigation Best Practices, Arbor Networks, 2011.

[8] Monowar H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyya and J. K. Kalita, Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions, The Computer Journal, 2013.

[9] Mohammed Alenezi, Methodologies for detecting DoS/DDoS attacks against network servers, The Seventh International Conference on Systems and Networks Communications - ICSNC 2012.

[10] Kanwal Garg, Rshma Chawla, Detection Of DDoS Attacks Using Data Mining, International Journal of Computing and Business Research (IJCBR), 2011.

[11] Christos Douligeris and Aikaterini Mitrokotsa, DDoS Attacks And Defense Mechanisms: A Classification, Signal Processing and Information Technology, 2003. ISSPIT 2003.