NGHIÊN CỨU VỀ SỰ PHÁT TRIỂN CỦA TẤN CÔNG DDOS TRONG 10 NĂM TRỞ LẠI ĐÂY

Ngô Hồ Anh Khôi[15], Phạm Đình Quốc[16], Nguyễn Hoàng Đạt[17]

Tóm tắt: *Ngày nay với sự phát triển của mạng internet mọi người được kết nối với nhau dễ dàng hơn. Công việc cũng như nhiều hoạt động mua bán, trao đổi thông tin, giao dịch đa số đều thực hiện trên mạng internet. Vì vậy nên các cuộc tấn công mạng ngày càng phổ biến và các kiểu tấn công cũng đa dạng nguy hiểm gây thiệt hại lớn qua mạng. Một trong những cuộc tấn cống trực tuyến có mức độ gây thiệt hại lớn là cuộc tấn công từ chối dịch vụ phân tán (DDoS - viết tắt của Distributed Denial of Service). DDoS là một cuộc tấn công phổ biến và có mức độ gây hậu quả nặng nề nhất cho các tổ chức cá nhân. Ngoài ra, cuộc tấn công còn xảy ra liên tiếp và nhanh chóng làm cho hệ thống máy tính không thể xử lý kịp các tác vụ, phản hồi và dẫn đến quá tải và treo hệ thống. Bài báo sẽ tìm hiểu các kiểu tấn công của loại tấn công từ chối dịch vụ phân tán và cách thức phòng chống giảm thiểu thiệt hại do tấn công DDoS gây nên. Qua đó, tìm hiểu thêm được các cuộc tấn công từ chối dịch vụ phân tán từ cuộc tấn công đầu tiên cho đến nay, để thấy rõ sự phát triển nhanh chóng của tấn công DDoS và thiệt của nó qua từng cuộc tấn công vòng 10 năm qua.*

Từ khóa: *Tấn công từ chối dịch vụ phân tán, DDoS, distributed denial of service.*

Abstract: *Nowadays the growth of the internet helps our connection easier. Many activities of buying, selling, exchanging information and transactions are done on the internet. As a result, cyber attacks are more and more common and dangerous with diverse types causing great damages over the network. One of the most damaging online attacks is the distributed denial of service (DDoS - Distributed Denial of Service) . DDoS is the most common attack and has the most severe consequences for organizations and individuals. In addition, attacks happening continuously and quickly makes the computer system unable to handle tasks,so it leads to system overload and crashes. The article will explore the types of attack of a distributed denial of service, damage prevention and mitigation . Thereby, we can learn more about distributed denial of service attacks from the first attack to date, clearly see the rapid development of DDoS attack and its damage throughout ten years*

Từ khóa: *Attacks is the distributed denial of service, DDoS, distributed denial of service.*

1. Giới thiệu

Sự phát triển nhanh chóng của Internet trong các thập kỷ qua đi cùng sự phát triển đó là các sự số của các cuộc tấn công trực tuyến cũng tăng lên đáng kể và ngày càng phức tạp, tinh

[15] Giảng viên Khoa Kỹ thuật - Công nghệ, Trường Đại học Nam Cần Thơ

[16] Giảng viên Anh văn, Trường Đại học Nam Cần Thơ

[17] Sinh viên Khoa Kỹ thuật - Công nghệ, Trường Đại học Nam Cần Thơ

vi hơn nhiều so với các cuộc tấn công trong quá khứ. Một trong những các cuộc tấn công có mức độ gây thiệt hại lớn là cuộc tấn công từ chối dịch vụ (DoS - viết tắt của Denial of Service). Sau đây là cấu trúc bài viết có bốn phần, phần một giới thiệu tổng quan các khái niệm và mục đích cũng như động cơ tấn công của các thủ phạm. Phần hai nói về có mấy phân loại các loại tấn công DDoS, các khái niệm của các kiểu tấn công phổ biến và cách phòng chống cũng như là giảm thiểu các thiệt hại do các cuộc tấn công gây ra. Phần ba là lịch sử của các cuộc tấn công của DDoS từ lúc cuộc tấn công đầu tiên được phát hiện tới năm 2020. Phần bốn sự phát triển của tấn công DDoS đến năm 2020. Dưới đây là một số khái niệm cơ bản trong bài viết.

DoS là một cuộc tấn công xảy ra liên tiếp nhanh chóng với mục đích là làm cho hệ thống máy tính không thể xử lý kịp các tác vụ, phản hồi và dẫn đến quá tải. Nó thực hiện điều này thông qua nhiều kết nối, yêu cầu và đầu vào dữ liệu khác có ý định làm quá tải hệ thống của nạn nhân.(Kiên Nguyễn, 2016)

Một cách tiếp cận khác là tấn công từ chối dịch vụ phân tán (DDoS - viết tắt của Distributed Denial of Service) đưa lên một cấp độ khác so với DoS nó mạnh hơn rất nhiều lần DoS. Điểm mạnh của cách thức tấn công này là được phân tán từ nhiều dải IP khác nhau vì thế mà các hệ thống máy tính hay cá nhân người bị tấn công sẽ rất khó phát hiện để ngăn chặn. Một cuộc tấn công DDoS được thực hiện từ nhiều thiết bị xâm nhập, thường được phân phối trên toàn cầu dưới dạng mạng botnet.(Nguyên Thoại, 2018)

Mạng botnet là một tập hợp các thiết bị kết nối bị xâm nhập được sử dụng cho các cuộc tấn công mạng được điều khiển từ xa Command & Control Center (C&C - Command & Control Center). Chúng thường bao gồm máy tính cá nhân, điện thoại di động, thiết bị IoT không an toàn và thậm chí cả tài nguyên từ các dịch vụ đám mây công cộng. Những kẻ tấn công sử dụng phần mềm độc hại (các bản Crack của các phần mềm) và các kỹ thuật khác để xâm nhập một thiết bị, biến nó thành "thây ma" trong mạng botnet của kẻ tấn công. Botnet cho phép những kẻ tấn công thực hiện các cuộc tấn công DDoS bằng cách khai thác sức mạnh của nhiều máy và che khuất nguồn lưu lượng truy cập. Vì lưu lượng truy cập được phân tán, các công cụ và nhóm bảo mật khó có thể phát hiện ra rằng một cuộc tấn công DDoS đang xảy ra cho đến khi hệ thống đã bị quá tải không thể truy cập được nữa.(Phương Phùng, 2019)

Cách thức của các cuộc tấn công DDoS được thực hiện với mạng của các máy kết nối Internet. Các mạng này bao gồm máy tính và các thiết bị khác (chẳng hạn như thiết bị IoT) đã bị nhiễm phần mềm độc hại, cho phép kẻ tấn công điều khiển chúng từ xa. Những thiết bị riêng lẻ này được gọi là bot (hoặc thây ma) và một nhóm bot được gọi là botnet. Sau khi mạng botnet đã được thiết lập, kẻ tấn công có thể chỉ đạo một cuộc tấn công bằng cách gửi các hướng dẫn từ xa đến từng bot. Khi máy chủ hoặc mạng của nạn nhân bị botnet nhắm mục tiêu, mỗi bot sẽ gửi yêu cầu đến địa chỉ IP của mục tiêu, có khả năng khiến máy chủ hoặc mạng bị quá tải, dẫn đến từ chối dịch vụ đối với lưu lượng truy cập bình thường. Vì mỗi bot là một thiết bị Internet hợp pháp, việc tách lưu lượng tấn công khỏi lưu lượng thông thường có thể khó khăn.

Sự khác nhau giữa các cuộc tấn công từ chối dịch vụ và tấn công từ chối dịch vụ phân tán là rất khác biệt. Trong một cuộc tấn công DoS, người tấn công chỉ sử dụng một kết nối

Internet duy nhất để khai thác lỗ hổng phần mềm hoặc làm quá tải mục tiêu bằng các yêu cầu giả mạo. Mặt khác, các cuộc tấn công từ chối dịch vụ phân tán (DDoS) liên quan đến nhiều thiết bị được kết nối gọi là Botnet thông qua một mạng lưới các máy tính được kiểm soát. (Quách Tỉnh, 2020)

Mục đích của việc DDoS của những kẻ tấn công được thúc đẩy

Hacktivis - Các hacker sử dụng các cuộc tấn công DoS như một phương tiện để bày tỏ sự chỉ trích đối với mọi thứ từ các chính phủ và chính trị gia bao gồm cả "doanh nghiệp lớn". Nếu những kẻ hacktivists không đồng ý với cá nhân hay tổ chức nào sẽ bị tấn công. Ít hiểu biết về kỹ thuật hơn các loại kẻ tấn công khác, những kẻ tấn công có xu hướng sử dụng các công cụ làm sẵn để thực hiện các cuộc tấn công nhằm vào mục tiêu của chúng. Anonymous có lẽ là một trong những nhóm hacktivist nổi tiếng nhất. Anonymous chịu trách nhiệm cho cuộc tấn công mạng vào tháng 2 năm 2015 chống lại IS, sau cuộc tấn công khủng bố sau đó nhằm vào văn phòng Charlie Hebdo ở Paris, cũng như cuộc tấn công chống lại chính phủ Brazil và các nhà tài trợ World Cup vào tháng 6 năm 2014. (Zev Brodsky, 2020)

Phá hoại trên mạng - Những kẻ phá hoại trên mạng thường được gọi là "script kiddies" vì chúng phụ thuộc vào các tập lệnh và công cụ tạo sẵn để gây ra các vụ tấn công cho người tham gia Internet của chúng. Những kẻ phá hoại này thường là những thanh thiếu niên buồn chán tìm kiếm một cơn sốt adrenaline tìm cách trút giận hoặc tấn công vào một tổ chức hoặc người mà kẻ đó cảm thấy đã đối xử tệ với họ. Tất nhiên, một số chỉ tìm kiếm sự chú ý và sự tôn trọng của đồng nghiệp. Bên cạnh các công cụ và tập lệnh được tạo sẵn, những kẻ phá hoại mạng cũng sẽ dẫn đến việc sử dụng các dịch vụ DDoS cho thuê. (Zev Brodsky, 2020)

Chiến tranh mạng - Các cuộc tấn công DDoS này do nhà nước bảo trợ được sử dụng để bịt miệng những người chỉ trích chính phủ và phản đối nội bộ, cũng như một phương tiện để phá vỡ các dịch vụ tài chính, y tế và cơ sở hạ tầng quan trọng ở các nước kẻ thù. Các cuộc tấn công này được hỗ trợ bởi các quốc gia có nghĩa là chúng là các chiến dịch được tổ chức và tài trợ tốt được thực hiện bởi các chuyên gia hiểu biết về công nghệ. (Zev Brodsky, 2020)

Tống tiền - Động lực ngày càng phổ biến cho các cuộc tấn công DDoS là tống tiền, nghĩa là tội phạm mạng đòi tiền để đổi lấy việc dừng (hoặc không thực hiện) một cuộc tấn công DDoS làm tê liệt hệ thống. Một số công ty phần mềm trực tuyến nổi tiếng như MeetUp, Bitly, Vimeo và Basecamp đã nhận được các ghi chú DDoS này một số sẽ bị tấn công sau khi không chịu khuất phục trước các mối đe dọa của những kẻ tống tiền. (Zev Brodsky, 2020)

Cạnh tranh kinh doanh - Các cuộc tấn công DDoS ngày càng được sử dụng như một công cụ kinh doanh cạnh tranh. Một số cuộc tấn công này được thiết kế để ngăn đối thủ cạnh tranh tham gia vào một sự kiện quan trọng trong khi những cuộc tấn công khác được đưa ra với mục tiêu làm sập hệ thống hoàn toàn của các doanh nghiệp trong nhiều ngày, tháng. (Zev Brodsky, 2020)

Ganh đua cá nhân - Các cuộc tấn công DoS có thể được sử dụng để dàn xếp tỷ số cá nhân hoặc làm gián đoạn các cuộc thi trực tuyến. Những cuộc tấn công như vậy thường xảy ra trong

bối cảnh trò chơi trực tuyến nhiều người chơi, nơi người chơi khởi chạy các cuộc tấn công DDoS chống lại nhau và thậm chí chống lại máy chủ trò chơi để giành lợi thế hoặc tránh thất bại sắp xảy ra bằng cách "lật bàn". (Zev Brodsky, 2020)

2. Phân loại các kiểu tấn công và cách phòng chống tấn công DDoS

2.1. Phân loại các cuộc tấn công DDoS

Các cuộc tấn công DDoS có thể chia thành ba loại. Các cuộc tấn công dựa trên khối lượng loại tấn công này cố gắng tạo ra tắc nghẽn bằng cách chiếm sử dụng tất cả băng thông có sẵn giữa người truy cập thực tế và băng thông mạng. Một lượng lớn dữ liệu được gửi đến mục tiêu bằng cách sử dụng một hình thức khuếch đại hoặc một phương tiện khác để tạo ra lưu lượng truy cập lớn, chẳng hạn như các yêu cầu từ mạng botnet. Các kiểu tấn công dựa trên khối lượng bao gồm flood UDP, flood ICMP, khuếch đại DNS và lũ gói tin giả mạo khác (Ericka Chickowski, 2020). Quy mô của một cuộc tấn công dựa trên khối lượng được đo bằng bit trên giây (BPS). (Dima Beckrman, 2017)

Loại thứ hai là tấn công giao thức gây ra gián đoạn dịch vụ bằng cách sử dụng tất cả dung lượng truy cập có sẵn của máy chủ ứng dụng web hoặc tài nguyên trung gian như tường lửa và bộ cân bằng tải. Các cuộc tấn công giao thức sử dụng các điểm yếu trong lớp 3 và lớp 4 của ngăn xếp giao thức để khiến mục tiêu không thể truy cập được. Các kiểu tấn công giao thức bao gồm Flood SYN, khuếch đại NTP, khuếch đại DNS, khuếch đại SSDP, Ping of Death, Smurf Attack, tấn công gói phân mảnh và hơn thế nữa. Kích thước của các cuộc tấn công giao thức hoặc lớp mạng được đo bằng gói mỗi giây (PPS). (Ericka Chickowski, 2020)

Loại cuối cùng là tấn công lớp ứng dụng mục tiêu của các cuộc tấn công là áp đảo một ứng dụng mục tiêu với các yêu cầu. Điều này gây ra việc sử dụng CPU và bộ nhớ cao cuối cùng làm treo cả hệ thống của mục tiêu. Các kiểu tấn công DDoS ở lớp ứng dụng bao gồm Flood HTTP, tấn công chậm (Slowloris, RUDY) tấn công zero-day nhắm vào mục tiêu là các lỗ hổng trong hệ điều hành, ứng dụng web và giao thức truyền thông. Loại tấn công này là loại nguy hiểm, tinh vi và nghiêm trọng nhất trong ba loại tấn công của DDoS. (Ericka Chickowski, 2020) Kích thước của các cuộc tấn công lớp ứng dụng được đo bằng yêu cầu mỗi giây (RPS). (Le Linh, 2018)

2.2. Các kiểu tấn công phổ biến của tấn công DDoS

UDP Flood là bất kỳ cuộc tấn công DDoS nào làm ngập mục tiêu bằng các gói giao thức dữ liệu người dùng (UDP). Mục tiêu của cuộc tấn công là làm ngập các cổng ngẫu nhiên trên một máy chủ từ xa. Điều này khiến máy chủ liên tục kiểm tra ứng dụng đang tiếp nhân yêu cầu tại cổng đó và khi không tìm thấy ứng dụng nào trả lời bằng gói ICMP 'Destination Unreachable'. Quá trình này làm cạn kiệt tài nguyên của máy chủ, cuối cùng có thể dẫn đến không thể truy cập. (Chien Tran, 2018)

ICMP Flood về nguyên tắc tương tự như cuộc tấn công Flood UDP, một cuộc tấn công Flood ICMP làm cạn kiệt tài nguyên mục tiêu với các gói ICMP Echo Request (ping) thường gửi các gói nhanh nhất có thể mà không cần chờ trả lời. Loại tấn công này có thể tiêu thụ cả

băng thông đi và đến vì máy chủ của nạn nhân thường cố gắng phản hồi bằng các gói ICMP Echo Reply dẫn đến hệ thống chậm lại đáng kể thậm chí là treo. (Thien Nguyen , 2020)

Tấn công Flood SYN khai thác một điểm yếu đã biết trong quá trình tự kết nối TCP (bắt tay ba bước) trong đó yêu cầu SYN để bắt đầu kết nối TCP với máy chủ phải được trả lời bằng phản hồi SYN-ACK từ máy chủ đó và sau đó được xác nhận bởi phản hồi ACK từ người yêu cầu. Trong trường hợp Flood SYN người yêu cầu gửi nhiều yêu cầu SYN nhưng không phản hồi phản hồi SYN-ACK của máy chủ hoặc gửi các yêu cầu SYN từ một địa chỉ IP giả mạo. Dù bằng cách nào, hệ thống máy chủ vẫn tiếp tục chờ xác nhận cho từng yêu cầu, chiếm dụng tài nguyên cho đến khi không thể thực hiện kết nối mới và cuối cùng dẫn đến từ chối dịch vụ. (Nguyễn Thanh Tùng, 2020)

Trong cuộc tấn công DDoS Flood HTTP kẻ tấn công khai thác các yêu cầu HTTP GET hoặc POST dường như hợp pháp để tấn công máy chủ web hoặc ứng dụng. Flood HTTP không sử dụng các gói tin sai định dạng, kỹ thuật giả mạo hoặc phản ánh và yêu cầu ít băng thông hơn các cuộc tấn công khác để đánh sập trang web hoặc máy chủ được nhắm mục tiêu. Cuộc tấn công hiệu quả nhất khi nó buộc máy chủ hoặc ứng dụng phân bổ tài nguyên tối đa có thể để đáp ứng mọi yêu cầu đơn lẻ.(Nguyễn Trang, 2019)

Ping of Death ("POD") là kẻ tấn công gửi nhiều ping không đúng định dạng hoặc độc hại đến một máy tính. Chiều dài gói tối đa của một gói IP (bao gồm cả tiêu đề) là 65,535 byte. Tuy nhiên, Lớp liên kết dữ liệu thường đặt ra giới hạn đối với kích thước khung hình tối đa ví dụ 1500 byte qua mạng Ethernet. Trong trường hợp này, một gói IP lớn được chia thành nhiều gói IP (được gọi là các đoạn) và máy chủ nhận sẽ tập hợp lại các đoạn IP thành gói hoàn chỉnh. Trong kịch bản Ping of Death, sau khi thao túng nội dung phân mảnh một cách độc hại, người nhận kết thúc với một gói IP lớn hơn 65,535 byte khi được tập hợp lại. Điều này có thể làm tràn bộ nhớ đệm được cấp phát cho gói gây từ chối dịch vụ cho các gói hợp pháp. (TOP9XY, 2015)

Tấn công Smurf khai thác Giao thức Internet (IP) và Giao thức Internet Control Message Protocol (ICMP) bằng cách sử dụng một chương trình phần mềm độc hại có tên smurf. Nó giả mạo địa chỉ IP và sử dụng ICMP gửi các địa chỉ IP trên một mạng nhất định.(TOP9XY, 2015)

Một cuộc tấn công Fraggle sử dụng một lượng lớn lưu lượng UDP vào mạng quảng bá của bộ định tuyến. Nó tương tự như một cuộc tấn công smurf, sử dụng UDP chứ không phải ICMP.

Slowloris là một cuộc tấn công có mục tiêu cao, cho phép một máy chủ web hạ gục một máy chủ khác mà không ảnh hưởng đến các dịch vụ hoặc cổng khác trên mạng mục tiêu. Slowloris thực hiện điều này bằng cách giữ càng nhiều kết nối đến máy chủ web mục tiêu mở càng lâu càng tốt. Nó thực hiện điều này bằng cách tạo kết nối đến máy chủ đích, nhưng chỉ gửi một phần yêu cầu. Slowloris liên tục gửi nhiều tiêu đề HTTP hơn, nhưng không bao giờ hoàn thành một yêu cầu. Máy chủ được nhắm mục tiêu giữ cho mỗi kết nối sai này luôn mở. Điều này cuối cùng làm tràn nhóm kết nối đồng thời tối đa và dẫn đến việc từ chối các kết nối bổ sung từ các máy khách hợp pháp. (Hoàng Tùng, 2020)

Tấn công khuếch đại NTP là thủ phạm khai thác các máy chủ Giao thức Thời gian Mạng (NTP) có thể truy cập công khai để áp đảo một máy chủ được nhắm mục tiêu với lưu lượng UDP. Cuộc tấn công được định nghĩa là một cuộc tấn công khuếch đại bởi vì tỷ lệ truy vấn trên phản hồi trong các tình huống như vậy nằm trong khoảng từ 1:20 đến 1: 200 hoặc hơn. Điều này có nghĩa là bất kỳ kẻ tấn công nào có được danh sách các máy chủ NTP đang mở (ví dụ: bằng một công cụ sử dụng như Metasploit hoặc dữ liệu từ Open NTP Project) đều có thể dễ dàng tạo ra một cuộc tấn công DDoS khối lượng lớn, băng thông cao. (Nguyen Minh Duc, 2014)

Advanced Persistent DoS (APDoS) là một kiểu tấn công được sử dụng bởi các tin tặc muốn gây ra thiệt hại nghiêm trọng. Nó sử dụng nhiều kiểu tấn công đã đề cập trước đó (tràn ngập HTTP, tràn ngập SYN, v.v.) và thường xuyên nhắm mục tiêu vào nhiều vectơ tấn công gửi hàng triệu yêu cầu mỗi giây. Các cuộc tấn công APDoS có thể kéo dài hàng tuần, phần lớn là do tin tặc có thể chuyển đổi chiến thuật bất cứ lúc nào và tạo ra sự chuyển hướng để né tránh các biện pháp phòng thủ an ninh. (Tùng Xuân, 2018)

SSDP còn được gọi là Simple Service Discovery Protocol là một giao thức dựa trên mạng được sử dụng để quảng cáo và khám phá các dịch vụ mạng. SSDP cho phép các thiết bị chạy phổ biến gửi và nhận thông tin bằng UDP trên cổng 1900. SSDP hấp dẫn những kẻ tấn công DDoS vì trạng thái mở cho phép giả mạo và khuếch đại. Cuộc tấn công DDoS SSDP thuộc cùng loại với các cuộc tấn công DDoS khuếch đại DNS và NTP trong đó những kẻ tấn công sử dụng một mạng botnet nhỏ hơn để giả mạo địa chỉ IP của nạn nhân. Tiếp theo, những kẻ tấn công sử dụng mạng botnet đó để truy vấn bộ định tuyến gia đình, tường lửa, máy in, điểm truy cập và những thứ tương tự có dịch vụ uPnP mở trên internet. Các cuộc tấn công khuếch đại DDoS DNS hiện có nhiều khả năng sử dụng SSDP hơn NTP.

Tấn công khếch đại DNS là cuộc tấn công kẻ tấn công sử dụng chức năng của các trình phân giải DNS mở để áp đảo một máy chủ hoặc mạng mục tiêu với lượng lưu lượng truy cập được khuếch đại, làm cho máy chủ và các thiết bị người dụng bên ngoài không thể truy cập được. (Thu Hương, 2009)

Tấn công Memcached hoạt động tương tự như tất cả các cuộc tấn công khuếch đại DDoS như khuếch đại NTP và khuếch đại DNS. Cuộc tấn công hoạt động bằng cách gửi các yêu cầu giả mạo đến một máy chủ dễ bị tấn công, sau đó máy chủ này sẽ phản hồi với lượng dữ liệu lớn hơn so với yêu cầu ban đầu, làm tăng lưu lượng truy cập. (giangpth, 2018)

Định nghĩa "Zero-day" bao gồm tất cả các cuộc tấn công chưa biết hoặc mới, khai thác các lỗ hổng mà chưa có bản vá nào được phát hành. Thuật ngữ này rất nổi tiếng trong số các thành viên của cộng đồng hacker, nơi hoạt động giao dịch lỗ hổng zero-day đã trở thành một hoạt động phổ biến.

2.3. Phòng chống các cuộc tấn công DDoS

Theo dõi lưu lượng truy cập để tìm kiếm các bất thường bao gồm lưu lượng đột biến tăng không giải thích được và các lượt truy cập từ địa chỉ IP và vị trí địa lý đáng ngờ. Tất cả những điều này có thể là dấu hiệu của việc những kẻ tấn công đang thực hiện thăm dò để kiểm tra khả năng phòng thủ trước khi thực hiện một cuộc tấn công chính thức. Nhận biết những điều này để biết chúng là gì có thể giúp cho việc chuẩn bị một cuộc tấn công dữ dội gần diễn ra.

Theo dõi các phương tiện truyền thông xã hội (đặc biệt là Twitter) và các thùng rác công cộng (ví dụ: Pastebin.com) để biết các mối đe dọa về một cuộc tấn công sắp xảy ra. Cân nhắc sử dụng kiểm tra DDoS của bên thứ ba để mô phỏng một cuộc tấn công nhằm vào cơ sở hạ tầng CNTT của hệ thống để họ có thể chuẩn bị khi thời điểm bị tấn công đến. Khi chọn cách thực hiện điều này, hãy thử nghiệm chống lại nhiều loại tấn công, không chỉ những cuộc tấn công đã quen thuộc.

Tạo một kế hoạch ứng phó và một nhóm phản ứng nhanh cho các cuộc tấn công nghĩa là một nhóm người được chỉ định có nhiệm vụ giảm thiểu tác động của một cuộc tấn công. Khi lập kế hoạch hãy đưa ra các thủ tục cho nhóm hỗ trợ khách hàng và giao tiếp chứ không chỉ cho các chuyên gia CNTT trong hệ thống.

Để thực sự bảo vệ khỏi các cuộc tấn công DDoS hiện đại nên sử dụng giải pháp giảm thiểu DDoS. Các giải pháp có thể được triển khai tại chỗ nhưng thường được các nhà cung cấp bên thứ ba cung cấp dưới dạng dịch vụ.

3. Các cuộc tấn công DDoS nguy hiểm nhất trong lịch sử DDoS

3.1. Giai đoạn khi mới xuất hiện đến năm 2010

Sự kiện đầu tiên được ghi nhận đó là vào năm 1988 khi Robert Morris viết một chương trình máy tính tự sao chép, chương trình này sau này đã có ảnh hưởng đáng kể đến Web. (Phương Hiển, 2018)

Vào tháng 9 năm 1996 (mặc dù các tài liệu khác nhau) chống lại Panix, nhà cung cấp dịch vụ Internet lâu đời nhất của Thành phố New York . Cuộc tấn công nhắm vào các máy tính khác nhau trong mạng của nhà cung cấp, bao gồm các máy chủ mail, tin tức, tên và Web cùng với các máy "đăng nhập" của người dùng.

Những năm 90 việc sử dụng DDoS bởi Electronic Disturbance Theater (EDT) một công ty điện tử. EDT lần đầu tiên thực thi FloodNet phần mềm sẽ giúp tấn công các mục tiêu đã nhắm tới từ trước của họ cả các trang web của chính phủ Mexico và Mỹ đại diện cho Tổng thống Mexico Ernesto Zedillo và Tổng thống Mỹ Bill Clinton.

Năm 2001,Code Red đã tấn công các máy tính chạy máy chủ web IIS của Microsoft. Nó để lại thông báo 'Bị tấn công bởi người Trung Quốc' và thậm chí còn đưa trang web của Nhà Trắng xuống.

Năm 2005, tên miền "panix.com" đã bị tấn công một lần nữa trong kỳ nghỉ lễ dài cuối tuần ở Hoa Kỳ. Cuộc tấn công đã ngăn chăn truy cập khách hàng và các nhân viên của Panix đã làm việc suốt ngày đêm để phục hồi các dịch vụ sau khi được rút ra khỏi hoạt động kinh doanh của hãng.

Vào tháng 4 năm 2007, quốc gia Estonia đã phải hứng chịu một cuộc tấn công DDoS lớn nhắm vào các dịch vụ chính phủ, các tổ chức tài chính và các hãng truyền thông. Điều này đã có một tác động lớn vì chính phủ Estonia là nước sớm áp dụng chính phủ trực tuyến và thực tế là không cần giấy tờ vào thời điểm đó thậm chí các cuộc bầu cử quốc gia đã được thực hiện

trực tuyến. Cuộc tấn công được nhiều người coi là hành động đầu tiên của chiến tranh mạng nhằm phản ứng với một cuộc xung đột chính trị với Nga về việc di dời 'Đồng chiến sĩ Tallinn' một tượng đài trong Thế chiến II. Chính phủ Nga đã bị nghi ngờ có liên quan và một công dân Estonia đến từ Nga đã bị bắt giữ nhưng chính phủ Nga đã không để cơ quan thực thi pháp luật Estonia tiến hành bất kỳ cuộc điều tra nào ở Nga. Sự việc này dẫn đến việc tạo ra các luật quốc tế cho chiến tranh mạng. (Hòa Thu, 2014)

Năm 2008, Anonymous phát động một cuộc bao vây DDoS chống lại Nhà thờ Khoa học. Đó là phản ứng trước nỗ lực của nhà thờ nhằm xóa cuộc phỏng vấn được công khai rộng rãi về Tom Cruise một thành viên nổi tiếng của nhà thờ khỏi Internet vào tháng 1 năm 2008.

Vào tháng 7 năm 2009, một loạt các cuộc tấn công mạng phối hợp đã xảy ra nhằm vào các trang web chính phủ, tài chính và các hãng thông tấn lớn của cả Hoa Kỳ và Hàn Quốc có liên quan đến việc sử dụng mạng botnet. Số lượng máy tính bị tấn công thay đổi tùy theo nguồn và bao gồm 50.000 từ Nhóm ứng phó công nghệ bảo mật của Symantec, 20.000 từ Cục Tình báo Quốc gia Hàn Quốc và hơn 166.000 từ các nhà nghiên cứu bảo mật máy tính Việt Nam khi họ phân tích hai máy chủ mà kẻ xâm lược sử dụng. Trong một loạt ba đợt tấn công, các mạng botnet đã ảnh hưởng đến các trang web của Lầu Năm Góc, Nhà Trắng, Bộ Ngoại giao Hoa Kỳ, Cục Tình báo Quốc gia Hàn Quốc và nhiều trang web khác. (Minh Việt, 2012)

3.2. Giai đoạn từ năm 2010 đến năm 2020

Vào tháng 12 năm 2010, trang web lưu trữ tài liệu WikiLeaks được sử dụng bởi những người tố cáo đã bị áp lực mạnh mẽ để ngừng công bố các tài liệu ngoại giao bí mật của Hoa Kỳ. Đáp lại, Anonymous tuyên bố ủng hộ WikiLeaks và tiến hành các cuộc tấn công DDoS nhằm vào Amazon, PayPal, MasterCard, Visa và ngân hàng Thụy Sĩ PostFinance như một hành động trả đũa đối với hành vi chống WikiLeaks. Mặt trận thứ hai trong cuộc tấn công tháng 12 được thực hiện với mật danh Chiến dịch Avenge Assange. Do các cuộc tấn công cả trang web của MasterCard và Visa đều bị sập vào ngày 8 tháng 12. Một nhà nghiên cứu về mối đe dọa tại PandaLabs cho biết Anonymous cũng đã phát động một cuộc tấn công nhằm đánh sập trang web của công tố viên Thụy Điển khi người sáng lập WikiLeaks Julian Assange bị bắt ở London và từ chối bảo lãnh liên quan đến dẫn độ đến Thụy Điển.

Năm 2011, các trang web của chính phủ Tunisia là mục tiêu của Anonymous do kiểm duyệt các tài liệu của WikiLeaks và cuộc Cách mạng Tunisia. Nhóm này đã đánh sập ít nhất 8 trang web của chính phủ bị tấn công DDoS bắt đầu từ ngày 2 tháng 1. Chính phủ Tunisia đã phản ứng bằng cách khiến các trang web của họ không thể truy cập được từ bên ngoài Tunisia.

Tiếp theo vào năm 2011, trong cuộc cách mạng Ai Cập để phản ánh tâm trạng trên đường phố Cairo các tin tặc đã quyết định tấn công phương tiện truyền thông hoặc kích động bạo lực. Các trang web của chính phủ Ai Cập cùng với trang web của Đảng Dân chủ Quốc gia cầm quyền đã bị Anonymous xâm nhập và đưa vào ngoại tuyến. Các trang web vẫn ngoại tuyến cho đến khi Tổng thống Hosni Mubarak từ chức. Những kẻ hacktivists cũng tiết lộ tên và mật khẩu của địa chỉ email của các quan chức chính phủ Trung Đông để ủng hộ mùa xuân Ả Rập. Các quan chức từ Bahrain, Jordan, Libya và Morocco cũng bị nhắm tới.

Vào ngày 12 tháng 3 năm 2012, sáu ngân hàng Hoa Kỳ đã bị nhắm là mục tiêu bởi làn sóng tấn công DDoS - Bank of America, JPMorgan Chase, US Bank, Citigroup, Wells Fargo và PNC Bank. Các cuộc tấn công được thực hiện bởi hàng trăm máy chủ bị tấn công từ một mạng botnet có tên là Brobot với mỗi cuộc tấn công tạo ra hơn 60 gigabit lưu lượng tấn công DDoS mỗi giây. (Nguyễn Tuấn Nam, 2016)

Vào năm 2013, một cuộc tấn công DDoS khổng lồ đã được phát động nhằm vào Spamhaus một nhà cung cấp thông tin tình báo về mối đe dọa phi lợi nhuận. Mặc dù Spamhaus với tư cách là một tổ chức chống thư rác, vẫn thường xuyên bị đe dọa và tấn công và đã có các dịch vụ bảo vệ chống DDoS cuộc tấn công này ước tính khoảng 300 gigabit lưu lượng truy cập mỗi giây đủ lớn để đánh sập trang web của Spamhaus và một phần của các dịch vụ email của Spamhaus ngoại tuyến. (Nguyễn Hải, 2016)

Vào năm 2014, CloudFlare một nhà cung cấp an ninh mạng đã bị tấn công DDoS với ước tính khoảng 400 gigabit/giây lưu lượng truy cập. Cuộc tấn công nhắm vào một khách hàng CloudFlare duy nhất và nhắm mục tiêu vào các máy chủ ở Châu Âu được thực hiện bằng cách sử dụng lỗ hổng trong giao thức Network Time Protocol (NTP) được sử dụng để đảm bảo đồng hồ máy tính là chính xác. Mặc dù cuộc tấn công chỉ nhắm vào một trong những khách hàng của CloudFlare,nhưng nó mạnh đến mức làm suy giảm đáng kể mạng của cả hệ thống CloudFlare. (Phong Vân, 2014)

Vào năm 2015, trang web Greatfire.org của nhà hoạt động Trung Quốc che giấu lưu lượng truy cập bị kiểm duyệt vào nước này đã bị tấn công từ chối dịch vụ phân tán (DDoS) kéo dài khiến chi phí máy chủ lên tới 30.000 USD mỗi ngày. Những kẻ tấn công đang cố gắng DDoS khiến trang web bị phá sản. Quản trị viên trang web Charlie Smith báo cáo rằng cuộc tấn công đã gửi 2,6 tỷ yêu cầu mỗi giờ gấp khoảng 2.500 lần so với mức bình thường. (Xuân Trường, 2020)

Cuộc tấn công DDoS lớn nhất từ trước đến 2015, lần này đã xảy ra nhằm vào GitHub. Cuộc tấn công có động cơ chính trị này kéo dài vài ngày và tự điều chỉnh xung quanh các chiến lược giảm thiểu DDoS đã thực hiện. Lưu lượng truy cập DDoS bắt nguồn từ Trung Quốc và nhắm mục tiêu cụ thể đến các URL của hai dự án GitHub nhằm phá vỡ sự kiểm duyệt của nhà nước Trung Quốc. Người ta suy đoán rằng mục đích của cuộc tấn công là cố gắng và gây áp lực buộc GitHub loại bỏ các dự án đó. (Ginny Hà, 2015)

Vào tháng 1 năm 2016, một nhóm gọi là nhóm New World Hacking đã lên tiếng nhận trách nhiệm về việc hạ gục cả trang web toàn cầu của BBC và trang web của Donald Trump. Nhóm đã nhắm mục tiêu tất cả các trang của BBC, bao gồm cả dịch vụ theo yêu cầu iPlayer của họ và đã gỡ chúng xuống trong ít nhất ba giờ vào đêm giao thừa. Cuộc tấn công ban đầu được mô tả là cuộc tấn công lớn nhất trong lịch sử và nó được cho là đo được hơn 600 Gbps mà chưa bao giờ được chứng minh.

Vào ngày 20 tháng 9 năm 2016, blog của chuyên gia an ninh mạng Brian Krebs đã bị tấn công bởi một công DDoS tấn công trong quá 620 Gbps mà vào thời điểm đó là vụ tấn công lớn nhất từng được ghi nhận. (Phan Tiến Đạt, 2020)

Vào ngày 28 tháng 2 năm 2018, GitHub một nền tảng dành cho các nhà phát triển phần mềm đã bị tấn công DDoS với tốc độ 1,35 terabit mỗi giây và kéo dài khoảng 20 phút. Theo GitHub, lưu lượng truy cập được bắt nguồn từ " hơn một nghìn hệ thống tự trị (ASN) khác nhau trên hàng chục nghìn điểm cuối duy nhất. (Techtalk, 2018)

Amazon Web Services đã bị tấn công DDoS khổng lồ vào tháng 2 năm 2020. Đây là cuộc tấn công DDoS gần đây nhất từ trước đến nay và nó nhắm mục tiêu vào một khách hàng AWS không xác định bằng cách sử dụng kỹ thuật có tên là Connection-less Lightweight Directory Access Protocol (CLDAP). Kỹ thuật này dựa trên các máy chủ CLDAP của bên thứ ba dễ bị tấn công và khuếch đại lượng dữ liệu được gửi đến địa chỉ IP của nạn nhân từ 56 đến 70 lần. Cuộc tấn công kéo dài trong ba ngày và đạt đỉnh điểm đáng kinh ngạc 2,3 terabyte mỗi giây.

4. Công nghệ Internet phát triển cùng với các kiểu tấn công DDoS

4.1. Từ ngày đầu DDoS phát triển đến năm 2010

Vào cuối những năm 1990, các nhóm hoạt động bắt đầu sử dụng Internet như một cách để tạo ra các trang web ảo chặn truy cập vào các trang web như một hình thức phản đối. Có lẽ nhóm đầu tiên thực hiện quyền lực này là Mạng lưới Strano một tập hợp những người cùng chí hướng hoạt động để phản đối chính sách hạt nhân của chính phủ Pháp. Thay vì sử dụng một chương trình để kết nối liên tục với một trang Web, Strano Network yêu cầu những người tham gia truy cập và tải lại nhiều lần các trang được nhắm mục tiêu.

Vài năm sau Mạng lưới Strano (1998), một nhóm quản trị một diễn dàn và những người thành viên khác đã phát triển một công cụ có tên FloodNet mà những người là thành viên có thể tải xuống và chạy trên máy tính của riêng họ. Sau đó, công cụ tấn công sẽ sử dụng danh sách các mục tiêu do EDT cung cấp để tấn công các trang Web cụ thể. Việc sử dụng chính thức đầu tiên của công cụ này là hỗ trợ Quân đội Zapatista ở Mexico chống lại chính phủ vào năm 1998 và sau đó tấn công Tổ chức Thương mại Thế giới vào năm 1999.

Các cuộc tấn công khuếch đại và phản chiếu lớn đầu tiên cũng xuất hiện vào năm 1998 khi những kẻ xấu trực tuyến sử dụng khả năng của chúng để khiến các máy chủ khác "ping" một mục tiêu bằng Giao thức Thông báo Kiểm soát Internet (ICMP). Được biết đến như một cuộc tấn công của Smurf, những trận lũ gói này rất đơn giản nhưng hiệu quả. Bằng cách gửi một địa chỉ nguồn giả mạo trong gói tin, kẻ tấn công có thể phản ánh lưu lượng truy cập đến mục tiêu và che giấu nguồn thực sự của cuộc tấn công. Bằng cách sử dụng địa chỉ quảng bá mạng kẻ tấn công có thể khuếch đại số lượng gói được gửi theo hệ số 255. Cuộc tấn công đã được sử dụng để chống lại Đại học Minnesota vào tháng 3 năm 1998 gây ra một phản ứng dây chuyền dẫn đến sự cố đáng kể và mất 30% gói tin.

Không lâu sau đó, vào tháng 8 năm 1999 trường đại học Minnesota bị tấn công bằng chương trình bot Trinoo, chương trình này đã được cài đặt trên ít nhất 227 máy chủ Solaris bị xâm phạm. Trinoo đã bắt đầu xu hướng xâm nhập máy chủ để tấn công từ chối dịch vụ. Một chương trình phổ biến có tên Stacheldraht (tiếng Đức có nghĩa là "dây thép gai") được tạo ra

bởi một hacker sử dụng tên Mixter và sau đó được những người khác sử dụng để tấn công nhiều trang web. Một chương trình khác được gọi là Tribe Flood Network, tương tự như Trinoo. (Khuyet Danh, 2018)

Chắc chắn không phải là cuộc tấn công DDoS đầu tiên, nhưng loạt cuộc tấn công thành công và công khai đó đã biến các cuộc tấn công từ chối dịch vụ từ mới lạ và phiền toái nhỏ thành những kẻ phá rối kinh doanh mạnh mẽ trong tâm trí của CISO và CIO mãi mãi.

Kể từ đó, các cuộc tấn công DDoS đã trở thành một mối đe dọa quá thường xuyên vì chúng thường được sử dụng để trả thù, tiến hành tống tiền như một phương tiện hoạt động trực tuyến và thậm chí để tiến hành chiến tranh mạng. DDoS cũng đã trở nên phát triển hơn trong những năm qua. Vào giữa những năm 1990 một cuộc tấn công có thể bao gồm 150 yêu cầu mỗi giây và nó đã đủ để đánh sập nhiều hệ thống. Ngày nay, chúng có thể vượt quá 1.000 Gbps. Điều này phần lớn được thúc đẩy bởi kích thước lớn của các mạng botnet hiện đại.

Các gói dịch vụ tên miền (DNS) thường được những kẻ tấn công sử dụng như một trọng tải trong các cuộc tấn công từ chối dịch vụ. Nhưng bắt đầu từ năm 2000, Trung tâm Điều phối Nhóm Ứng cứu Khẩn cấp Máy tính (CERT) cảnh báo rằng ngày càng nhiều các cuộc tấn công bắt đầu sử dụng DNS như một phương tiện khuếch đại băng thông. Các công ty phần lớn không chú ý đến cảnh báo. Trong một lời khuyên khác sáu năm sau, United States CERT lưu ý rằng 75 đến 80% máy chủ vẫn cho phép đệ quy, khả năng của máy chủ DNS cho phép các cuộc tấn công khuếch đại.

Năm 2001, Code Red đây là một cái khác xuất hiện trước kỷ nguyên tội phạm mạng như được biết ngày nay nó chỉ đơn giản là ác ý vì lợi ích ngớ ngẩn của nó. Code Red đã tấn công các máy tính chạy máy chủ web IIS của Microsoft. Nó để lại thông báo 'Bị tấn công bởi người Trung Quốc' và thậm chí còn đưa trang web của Nhà Trắng xuống. Con sâu đó đã làm ba việc: Nó đã thay thế nội dung hữu ích của một trang bằng cụm từ bí tích, nó tự phân phối trên các máy chủ web mới, nó đã thực hiện các cuộc tấn công DDoS vào một tập hợp các địa chỉ web được xác định trước bao gồm cả địa chỉ của Nhà Trắng được đưa xuống vào một thời điểm được xác định trước tương tự theo mục nhập tương ứng trong mã. Người ta tính rằng nó đã ảnh hưởng đến hơn một triệu máy chủ web trên khắp thế giới một tỷ lệ đáng kể của toàn bộ Internet. Nó chỉ tồn tại trong bộ nhớ của máy tính nạn nhân và không tạo ra tệp nào. Ai đã viết Code Red và tại sao nó được phát hành vẫn là một bí ẩn và nó đã được Microsoft vá một tháng sau khi bùng phát.

Vào tháng 1 năm 2003, thế giới gặp phải loại sâu flash đầu tiên của sâu MS SQL Slammer 376 byte lây lan nhanh đến mức khiến số lượng hệ thống bị nhiễm tăng gấp đôi sau mỗi 8,5 giây và làm bão hòa băng thông mạng cục bộ trong 3 vòng phút. Năm phút sau khi nó bắt đầu lây lan, sâu Slammer đạt 80 triệu gói tin mỗi giây một mức độ sẽ không xuất hiện lại trong một thập kỷ nữa. Nó đã lây nhiễm hàng trăm nghìn máy chủ trên khắp thế giới trong 15 phút tăng 25% lưu lượng truy cập toàn cầu và khiến Hàn Quốc không có Internet và viễn thông di động. Trong vài giờ, khiến đất nước này bị DDoS đến màn hình nhỏ và mất tháng sau để vá lỗ hổng của nó khai thác. (thaipro, 2015)

Theo ước tính có gần 40 phương thức tấn công DDoS cho thấy những kẻ tấn công mạng ngầm đã cố gắng bằng mọi cách để khai thác các lỗ hổng trong kiến trúc mạng, giao thức mạng và cơ sở dịch vụ. Từ quan điểm của mô hình OSI, các cuộc tấn công DDoS được chia thành các cuộc tấn công lớp ứng dụng, cuộc tấn công lớp truyền tải và cuộc tấn công lớp mạng. Các cuộc tấn công ở tầng ứng dụng chủ yếu nhằm mục đích làm cạn kiệt tài nguyên dịch vụ. Flood HTTP là một ví dụ điển hình của các cuộc tấn công như vậy. Các cuộc tấn công ở lớp vận chuyển bao gồm các cuộc tấn công Flood SYN, Flood ACK và Flood UDP. Các cuộc tấn công lớp mạng chủ yếu là Flood ICMP. Từ quan điểm của vectơ tấn công, các cuộc tấn công DDoS được chia thành các cuộc tấn công trực tiếp (các cuộc tấn công lũ lụt khác nhau như Flood SYN đã đề cập ở trên) và cuộc tấn công phản ánh. Trong một cuộc tấn công phản ánh, thủ phạm bắt đầu với các yêu cầu sử dụng địa chỉ IP giả mạo của nạn nhân dự định làm địa chỉ IP nguồn, do đó chuyển hướng các gói phản hồi của các dịch vụ yêu cầu đến nạn nhân. Số lượng gói phản hồi thường gấp nhiều lần số gói yêu cầu. Do đó, kiểu tấn công này còn được gọi là tấn công khuếch đại phản xạ. Ví dụ về các cuộc tấn công phản chiếu là các cuộc tấn công phản chiếu DNS và phản ánh SSDP.

Kể từ khi xuất hiện giao thức TCP/IP đã đóng góp rất nhiều vào tính khả dụng và mạnh mẽ của các mạng để truyền thông và trực tiếp thúc đẩy việc áp dụng Internet. Tuy nhiên, vào thời điểm thiết kế giao thức và kiến trúc không có cơ chế quản trị và xác thực hiệu quả nào được triển khai do đó làm lộ các lỗ hổng của chúng cho những kẻ tấn công. Các hoạt động và đặc điểm như bắt tay ba chiều TCP và giao tiếp UDP không kết nối dễ bị tấn công bởi các cuộc tấn công cạn kiệt tài nguyên khác nhau bao gồm Flood SYN, Flood ACK, Flood UDP và Flood ICMP luôn đứng đầu danh sách vũ khí được các nhóm hack sử dụng. Kể từ khi web 2.0 được đề xuất vào năm 2004 các ứng dụng web nhấn mạnh vào nội dung do người dùng tạo như mạng xã hội và blog đã trải qua một sự phát triển theo cấp số nhân.

Vào mùa hè nóng nực năm 2007 ở vùng Krasnodar ở miền nam nước Nga, các thành phố Adygea và Astrakhan chỉ có phạm vi phủ sóng Internet không liên tục - nó tắt đi, hoạt động trở lại nhiều lần. Hóa ra lý do là một DDoS đã hạ gục nhà cung cấp mạng lớn nhất trong khu vực. Các cuộc tấn công xảy ra từng đợt trong cả tháng, đạt mức đáng kinh ngạc (năm 2007) 10 gigabyte mỗi giây. Các cuộc tấn công cũng rất bất thường họ sử dụng mạng botnet nhưng sử dụng nhiều hơn các trang web ngang hàng trao đổi tệp điều chưa từng có trước đây vào các dự án nghiên cứu bên ngoài. DDoS này là một thời điểm quan trọng đối với Nga. Internet của cả một vùng được bật tắt như ngọn đuốc và không ai có thể làm gì được. Trước sự cố này, không ai có bất kỳ thông báo nào về các mối đe dọa DDoS. DDoS được coi là những mối đe dọa hiện tại cấp tính cần được xem xét một cách nghiêm túc. Các công nghệ xuất hiện và các công ty viễn thông bắt đầu tích cực lắp đặt bộ công cụ chuyên dụng mới.

Kể từ năm 2008, khái niệm dữ liệu lớn đã trở nên phổ biến trên khắp thế giới. Trước nhu cầu xử lý dữ liệu lớn và trong bối cảnh các kỹ thuật như ảo hóa, điện toán phân tán và lưu trữ quy mô lớn đang dần phát triển, điện toán đám mây đã trở thành mô hình điện toán được ưa chuộng.

Trong năm 2009, khoảng 50.000 máy tính bị nhiễm sâu MyDoom đã được những kẻ tấn công sử dụng để nhắm mục tiêu vào các trang web chính phủ, tài chính và doanh nghiệp ở Hoa Kỳ và các trang web của chính phủ ở Hàn Quốc. Cuộc tấn công đạt tốc độ băng thông cao nhất là 13 Gbps, gây ra một khoảng thời gian ngừng hoạt động nhưng khiến các chính trị gia đổ lỗi cho Triều Tiên vì đã phát động cuộc tấn công. Cuộc tấn công xảy ra 5 năm sau khi các biến thể của sâu MyDoom được sử dụng để thực hiện một cuộc tấn công DDoS vào trang web của công ty phần mềm Unix SCO Group, mục tiêu là do công ty này tuyên bố trong một vụ kiện rằng họ sở hữu hệ điều hành Linux. Microsoft cũng bị tấn công trong cuộc tấn công tương tự cho thấy hiệu quả của việc sử dụng một số lượng lớn máy tính tiêu dùng chống lại các trang web và mạng.

Memcached có nghĩa là chỉ được sử dụng trên các máy chủ được bảo vệ chạy trên mạng nội bộ và thường có ít cách bảo mật để ngăn những kẻ tấn công độc hại giả mạo địa chỉ IP và gửi một lượng lớn dữ liệu đến những nạn nhân không nghi ngờ. Thật không may, hàng nghìn máy chủ Memcached đang hoạt động trên Internet mở và đã có một sự bùng nổ lớn trong việc sử dụng chúng trong các cuộc tấn công DDoS. Nói rằng các máy chủ bị "chiếm quyền điều khiển" là không công bằng, vì họ sẽ vui vẻ gửi các gói tin đến bất cứ nơi nào họ được yêu cầu mà không cần đặt câu hỏi. Kể từ năm 2010, nhiều dịch vụ Memcached được định cấu hình không đúng hiển thị trên Internet qua cổng UDP đã bị các nhóm hack tận dụng. Hệ số khuếch đại của Memcached rất lớn. Yêu cầu 203 byte có thể khiến máy chủ trả lại phản hồi lớn tới 100 MB. Ngược lại, hệ số khuếch đại tối đa của dịch vụ DNS và NTP chỉ dao động từ 1000 đến 2000.

4.2. Sự phát triển của DDoS từ năm 2010 đến năm 2020

Kể từ năm 2011, những đột phá lớn đã được thực hiện trong kỹ thuật học sâu, với khái niệm AI thu hút sự chú ý. Tất nhiên, các nhóm hack không bao giờ bỏ lỡ cơ hội tốt như vậy và họ bắt đầu sử dụng các kỹ thuật mới này để tăng hiệu quả của các cuộc tấn công DDoS hiện tại. Khái niệm DDoS dựa trên AI được đề xuất để thực hiện các cuộc tấn công tự động không có con người và cho phép thủ phạm thay đổi loại lỗ hổng được khai thác và tấn công vectơ dựa trên phản ứng của người bảo vệ. Các kỹ thuật mới chẳng hạn như học sâu, tiếp tục hạ thấp ngưỡng kỹ thuật và chi phí của các cuộc tấn công. Các phương pháp tự động hóa tấn công và tự động hóa phần mềm độc hại dựa trên AI phổ biến trong giới tin tặc. Các cuộc tấn công DDoS lớn hơn được hỗ trợ bởi trí thông minh máy móc đang xuất hiện rất nhiều trong bối cảnh an ninh mạng.

Từ năm 2014 đến năm 2017, quy mô thị trường IoT toàn cầu tăng gần gấp đôi đạt hàng nghìn tỷ đô la. Không tương xứng với tốc độ ngày càng nhiều thiết bị IoT kết nối Internet, các kỹ thuật và tiêu chuẩn bảo mật liên quan vẫn chưa hoàn thiện tạo cơ hội cho tin tặc kiếm tiền dễ dàng bằng cách khai thác các lỗ hổng trong SSDP thuộc UPnP. Kiến trúc UPnP bao gồm một loạt các giao thức có liên quan thực hiện việc khám phá thiết bị lập bản đồ mạng và điều khiển bên cạnh việc hỗ trợ kết nối mạng của các thiết bị. Open Connectivity Foundation (OCF) một tổ chức đã phát triển UPnP, quy định rõ ràng rằng các dịch vụ UPnP phải được giới hạn cho các mạng nội bộ. Tuy nhiên, trong quá trình triển khai UPnP, nhà cung cấp thiết bị có thể sử dụng các bộ phát triển phần mềm (SDK) cũ hơn người dùng có thể định cấu hình thiết bị

không đúng cách hoặc một số nhà cung cấp thậm chí cố tình để lại các tệp độc hại trong thiết bị của họ để khi cần điều khiển các thiết bị bot. Tất cả những điều này gây ra những mối đe dọa lớn đối với bối cảnh an ninh mạng. Dựa trên UDP các dịch vụ SSD một khi được tiếp xúc có thể dễ dàng được sử dụng làm phản xạ DDoS. Điều này giải thích tại sao các cuộc tấn công phản ánh liên tục tăng về quy mô và số lượng qua từng năm.

Bên cạnh các cuộc tấn công khuếch đại phản xạ, các nhóm hack cũng sử dụng sâu và vi rút để lây nhiễm số lượng lớn các thiết bị IoT là những đối tượng chính tham gia vào các cuộc tấn công DDoS. Vào tháng 10 năm 2016, nhà cung cấp dịch vụ cơ sở hạ tầng internet Dyn DNS (Bây giờ là Oracle DYN) đã bị treo bởi một làn sóng truy vấn DNS từ hàng chục triệu địa chỉ IP. Cuộc tấn công đó, được thực hiện thông qua mạng botnet Mirai, đã lây nhiễm cho hơn 100.000 thiết bị IoT bao gồm cả camera IP và máy in. Vào thời kỳ đỉnh cao Mirai đạt tới 400.000 bot. Các dịch vụ bao gồm Amazon, Netflix, Reddit, Spotify, Tumblr và Twitter đã bị tấn công làm cho gián đoạn.

Năm 2017, IPv6 chính thức được đưa vào làm tiêu chuẩn Internet mới. Chỉ một năm sau, cuộc tấn công DDoS dựa trên IPv6 đầu tiên đã được phát hiện. Sẽ có nhiều dịch vụ và thiết bị đầu cuối hỗ trợ IPv6. IPv6 sẽ trở thành một công cụ quan trọng cho các cuộc tấn công DDoS trong tương lai và các cuộc tấn công nhắm vào cơ sở hạ tầng IPv6 sẽ nổi lên như một nguyên nhân chính của các mối đe dọa mới.

Vào đầu năm 2018, một kỹ thuật DDoS mới bắt đầu xuất hiện. Vào ngày 28 tháng 2, dịch vụ lưu trữ kiểm soát phiên bản GitHub đã bị tấn công từ chối dịch vụ lớn với 1,35 TB mỗi giây lưu lượng truy cập vào trang web phổ biến. Mặc dù GitHub chỉ bị đánh ngoại tuyến không liên tục và cố gắng ngăn chặn cuộc tấn công và trở lại hoạt động hoàn toàn sau chưa đầy 20 phút nhưng quy mô lớn nhất của cuộc tấn công rất đáng lo ngại vì nó vượt xa cuộc tấn công Dyn vốn đã đạt đỉnh 1,2 TB một giây. Chỉ vài ngày sau cuộc tấn công GitHub một cuộc tấn công DDoS dựa trên Memecached khác đã tấn công một nhà cung cấp dịch vụ của Mỹ với 1,7 TB dữ liệu mỗi giây.

Một phân tích về công nghệ thúc đẩy cuộc tấn công cho thấy nó đơn giản hơn so với các cuộc tấn công khác. Trong khi cuộc tấn công Dyn là sản phẩm của mạng botnet Mirai, yêu cầu phần mềm độc hại lây nhiễm hàng nghìn thiết bị IoT, cuộc tấn công GitHub đã khai thác các máy chủ chạy hệ thống bộ nhớ đệm Memcached có thể trả về khối lượng dữ liệu rất lớn để đáp ứng các yêu cầu đơn giản.

Botnet Mirai có ý nghĩa quan trọng ở chỗ, không giống như hầu hết các cuộc tấn công DDoS, nó tận dụng các thiết bị IoT dễ bị tấn công thay vì PC và máy chủ. Đặc biệt đáng sợ khi người ta cho rằng vào năm 2020 sẽ có 34 tỷ thiết bị được kết nối internet và phần lớn (24 tỷ) sẽ là các thiết bị IoT.(Hoàng Tùng, 2020)

Thật không may, Mirai sẽ không phải là botnet cuối cùng được hỗ trợ bởi IoT. Một cuộc điều tra giữa các nhóm bảo mật trong Akamai, Cloudflare, Flashpoint, Google, RiskIQ và Team Cymru đã phát hiện ra một mạng botnet có kích thước tương tự, được đặt tên là WireX, bao gồm 100.000 thiết bị Android bị xâm phạm tại 100 quốc gia. Một loạt các cuộc tấn công DDoS lớn nhắm vào các nhà cung cấp nội dung và mạng phân phối nội dung đã thúc đẩy cuộc điều tra.

Amazon Web Services đã bị tấn công DDoS khổng lồ vào tháng 2 năm 2020. Đây là cuộc tấn công DDoS nhắm mục tiêu vào một khách hàng AWS không xác định bằng cách sử dụng kỹ thuật có tên là Giao thức truy cập thư mục hạng nhẹ không kết nối (CLDAP) Phản ánh. Kỹ thuật này dựa trên các máy chủ CLDAP của bên thứ ba dễ bị tấn công và khuếch đại lượng dữ liệu được gửi đến địa chỉ IP của nạn nhân từ 56 đến 70 lần. Cuộc tấn công kéo dài trong ba ngày và đạt đỉnh điểm đáng kinh ngạc 2,3 terabyte mỗi giây.

Vào ngày 21 tháng 6 năm 2020, Akamai báo cáo rằng họ đã giảm thiểu một cuộc tấn công DDoS vào một ngân hàng lớn ở Châu Âu, với đỉnh điểm là 809 triệu gói mỗi giây (Mpps), khối lượng gói lớn nhất từ trước đến nay. Cuộc tấn công này được thiết kế để áp đảo thiết bị mạng và các ứng dụng trong trung tâm dữ liệu của mục tiêu bằng cách gửi hàng tỷ gói tin nhỏ (29 byte bao gồm tiêu đề IPv4).

5. Kết luận

Báo viết được xây dựng với mục đích để nghiên cứu, tìm hiểu những phương pháp phòng chống tấn công DDOS và các sự kiện liên quan đến sự hình thành, phát triển của tấn công DDoS. Bài báo viết này đi sâu vào các giải pháp tấn công từ chối dịch vụ phân tán. Từ đó đúc kết được những kinh nghiệm cho cá nhân, từ những giải pháp trên khi triển khai nó sẽ ngăn chặn được các cuộc tấn công đồng loạt đến từ các hacker. Khi đó hệ thống sẽ nhận biết và ngăn cản các cuộc tấn công ấy. Sự tìm hiểu các kiểu tấn công của loại tấn công từ chối dịch vụ phân tán và sự phát triển của DdoS trong 10 năm trở lại đây. Các công nghệ mới như IoT và AI các công nghệ mới này góp phần không nhỏ cho các vụ tấn công lớn vì nó còn khá mới nên các lỗ hổng về bảo mật còn nhiều và chưa được khắc phục đã được các tin tặc tận dụng để làm công cụ tấn công với mục đích làm lợi ích cá nhân cho bản thân gây thiệt hại cho các tổ chức.

Cuộc tấn công từ chối dịch vụ là sự vi phạm chính sách sử dụng internet của IAB (Internet Architecture Board) và những người tấn công hiển nhiên vi phạm luật. Các cuộc tấn công DDoS đang trở nên phổ biến và số lượng ngày càng tăng, vì vậy các chuyên gia bảo mật CNTT cần giải quyết mối đe dọa DDoS và quyết định giải pháp phù hợp nhất cho tổ chức. Các giải pháp thay đổi tùy theo tổng chi phí sở hữu, hiệu quả bảo mật và hiệu suất. Từ đó, tạo nên những phần mềm chống cuộc tấn công DDoS cao cấp hơn. Vì các cuộc DDoS không có cách nào ngăn chặn DDoS chỉ có cách phòng chống, giảm thiểu các thiệt hại của DDoS gây ra cho cá nhân hay một tổ chức nào đó.

TÀI LIỆU THAM KHẢO

[1] Ginny Hà (2015), Hệ thống quản lý source code nổi tiếng GitHub đã hoạt động trở lại sau khi bị tấn công DDoS vào ngày thứ 3 (25/8), truy cập 14/01/2021, <https://whitehat.vn/threads/github-hoat-dong-tro-lai-sau-khi-bi-tan-cong-ddos.5651/>

[2] Phạm Tiến Đạt (2020), Nguy cơ đe dọa an ninh mạng từ IoT, truy cập 14/01/2021, <https://vjst.vn/vn/tin-tuc/3383/nguy-co-de-doa-an-ninh-mang-tu-iot.aspx>

[3] Techtalk (2018), GitHub bị sập do một cuộc tấn công DDoS qui mô lớn, truy cập 14/01/2021 <https://www.codehub.com.vn/GitHub-bi-sap-do-mot-cuoc-tan-cong-DDoS-qui-mo-lon-2018-09-08>

[4] ugreenvietnam.com (2020), AMAZON BỊ TẤN CÔNG DDOS LÊN ĐẾN 2,3 TBPS, CAO NHẤT TỪ TRƯỚC ĐẾN NAY, truy cập 14/01/2021, <https://ugreenvietnam.com/amazon-bi-tan-cong-ddos-len-den-2-3-tbps-cao-nhat-tu-truoc-den-nay.html>

[5] Evan Porter (2019), Tấn công DDoS là gì và làm thế nào bảo vệ trước DDoS trong năm 2020, truy cập 15/01/2021, <https://vi.safetydetectives.com/blog/tan-cong-ddos-la-gi/>

[6] Phương Phùng (2019), Botnet là gì, truy cập 15/01/2021, <https://quantrimang.com/botnet-la-gi-no-dung-de-tan-cong-ai-va-ban-co-the-ngua-botnet-ra-sao-126843>

[7] Phương Hiển (2018), Nhìn lại vụ tấn công mạng đầu tiên trong lịch sử, truy cập 15/01/2021, <https://khoahocphattrien.vn/kham-pha/joseph-woodlandnguoi-sang-che-ma-vach/202009031118579p1c879.htm>

[8] GenK (2016), Tấn công mạng bằng DDoS - hình thức chiến tranh thế giới mới không cần đến binh lính và vũ khí, truy cập 15/01/2021 < https://baodansinh.vn/tan-cong-mang-bang-ddos---hinh-thuc-chien-tranh-the-gioi-moi-49278.htm>

[9] Ericka Chickowski (2020), Types of DDoS attacks explained , truy cập 16/01/2021, <https://cybersecurity.att.com/blogs/security-essentials/types-of-ddos-attacks-explained>

[10] Thu Hương (2009), DNS Amplification: tin tặc mở rộng tấn công DNS, truy cập 16/01/2021, <https://quantrimang.com/dns-amplification-tin-tac-mo-rong-tan-cong-dns-54123>

[11] Ben Dickson (2019), 20 years of DDoS attacks: What has changed? , truy cập 16/01/2021, <https://portswigger.net/daily-swig/20-years-of-ddos-attacks-what-has-changed>

[12] Joon Ian Wong (2016), DDoS attacks have gone from a minor nuisance to a possible new form of global warfare, truy cập 17/01/2021, <https://qz.com/860630/ddos-attacks-have-gone-from-a-minor-nuisance-to-a-possible-new-form-of-global-warfare/>

[13] Quách Tỉnh (2020), Tấn công từ chối dịch vụ DoS và DDoS là gì? Tác hại của chúng ra sao?, truy cập 17/01/2021, <https://quantrimang.com/tim-hieu-ve-tan-cong-tu-choi-dich-vu-dos-34926>

[14] Zev Brodsky (2020), The Psychology Behind DDoS: Motivations and Methos, truy cập 17/01/2021, <https://www.perimeter81.com/blog/network/the-psychology-behind-ddos-attacks/>

[15] Securitydaily (2018), Tấn công từ chối dịch vụ DDoS/DoS, truy cập 18/01/2021, <https://techinsight.com.vn/tan-cong-tu-choi-dich-vu-ddos-dos/>

[16] Mona (2019), DDOS là gì? Tất tần tật về tấn công từ chối dịch vụ trên internet, truy cập 18/01/2021, <https://mona.media/ddos-la-gi-tan-cong-tu-choi-dich-vu-tren-internet/#ftoc-heading-23>

[17] Dima Bekerman (2017), gbps pps rps DDoS attacks, truy cập 19/01/2021, <https:// www.imperva.com/ blog/gbps-pps-rps-ddos-attacks/>

[18] Le Linh (2018), Tấn công DDos: các loại tấn công và cách phòng ngừa, truy cập 19/01/2021, <https://viblo.asia/p/tan-cong-ddos-cac-loai-tan-cong-va-cach-phong-ngua-naQZRAPjKvx>

[19] VNIST (2020), Khác biệt giữa tấn công DoS và DdoS, truy cập 19/01/2021, <https://vnist.vn/khac-biet-giua-tan-cong-dos-va-ddos/>

[20] Securitybox (2019), 12 LOẠI TẤN CÔNG DDOS | TẤN CÔNG TỪ CHỐI DỊCH VỤ DDOS, truy cập 19/01/2021, <https://securitybox.vn/1353/12-loai-tan-cong-ddos-tan-cong-tu-choi-dich-vu-ddos/>

[21] Thien Nguyen (2020), Ping (ICMP) flood attack ! Tấn công ddos bằng Ping Flood là gì?, truy cập 19/01/2021, <https://vnso.vn/ping-icmp-flood-attack-tan-cong-ddos-bang-ping-flood-la-gi/>

[22] longvan.net (2019), TẤN CÔNG TỪ CHỐI DỊCH VỤ BẰNG UDP FLOOD VÀ CÁCH PHÒNG CHỐNG, truy cập 19/01/2021, < https://longvan.net/tan-cong-tu-choi-dich-vu-bang-udp-flood-va-cach-phong-chong.html>

[23] Chien Tran (2018), Các hiểu biết về một cuộc tấn công từ chối dịch vụ DDOS/DOS, truy cập 19/01/2021, <https://securitydaily.net/cac-hieu-biet-ve-mot-cuoc-tan-cong-tu-choi-dich-vu-ddosdos/>

[24] Nguyễn Thanh Tùng (2020), Tấn công TCP Syn Flood, truy cập 19/01/2021, <https://medium.com/@ngtung/t%E1%BA%A5n-c%C3%B4ng-tcp-syn-flood-4dea6b426917>

[25] kaitoukid (2015), DDoS attack sử dụng TCP SYN Flood, truy cập 19/01/2021, <https://whitehat.vn/threads/tan-cong-tcp-syn-flood.5652/>

[26] Vietsunshine (2019), Tấn công từ chối dịch vụ (DDoS) là gì? Giải pháp giảm thiểu DDoS Attack , truy cập 19/01/2021, <https://www.vietsunshine.com.vn/2019/01/29/tan-cong-tu-choi-dich-vu-ddos-la-gi-giai-phap-giam-thieu-ddos-attack/>

[27] Kiên Nguyễn (2016), DoS - DDoS là gì? Hacker tấn công DDoS bằng cách nào?, truy cập 19/01/2021, <https://blogchiasekienthuc.com/dan-cong-nghe/dos-ddos-la-gi-hacker-tan-cong-ddos-bang-cach-nao.html>

[28] Nguyên Thoại (2018), DDoS là gì? Hệ thống chống DDoS (Anti DDoS), truy cập 19/01/2021, <https://longvan.net/ddos-la-gi-he-thong-chong-ddos.html>

[29] Nguyễn Trang (2019), Tấn công HTTP flood là gì?, truy cập 19/01/2021, <https://quantrimang.com/http-flood-la-gi-167188>

[30] Hoàng Tùng (2019), HTTP Flood là gì? Làm thế nào để phòng chống tấn công HTTP Flood?, truy cập 19/01/2021, <https://ssl.vn/http-flood-la-gi-lam-the-nao-de-phong-chong-tan-cong-http-flood.html>

[31] TOP9XY (2015), TẤN CÔNG PING OF DEATH, truy cập 21/01/2021, <https://it.die.vn/t/tan-cong-ping-death/>

[32] vnso.vn (2019), Smurf attack là gì? Tấn công ddos bằng phương thức Internet Control Message Protocol, truy cập 21/01/2021, <https://vnso.vn/smurf-attack-la-gi-tan-cong-ddos-bang-phuong-thuc-internet-control-message-protocol/>

[33] TOP9XY (2015), SMURT ATTACK (TẤN CÔNG SMURT), truy cập 21/01/2021, <https://it.die.vn/s/smurt-attack-tan-cong-smurt/>

[34] Hoàng Tùng (2020), Tấn công Slowloris attack là gì?, truy cập 21/01/2021, <https://ssl.vn/tan-cong-slowloris-attack-la-gi.html>

[35] vnso.vn (2019), NTP Amplification Attack ! DDoS khuếch đại thực sự nguy hiểm đến Máy Chủ?, truy cập 21/01/2021, <https://vnso.vn/ntp-amplification-attack-ddos-khuech-dai-thuc-su-nguy-hiem-den-may-chu/>

[36] Nguyen Minh Duc (2014), Phân tích kỹ thuật tấn công DDOS qua NTP, truy cập 21/01/2021, <https://securitydaily.net/phan-tich-ky-thuat-tan-cong-ddos-qua-ntp/>

[37] Tùng Xuân (2018), DDoS và những vấn đề liên quan, truy cập 21/01/2021, <https://sites.google.com/site/fullcrackcoder/ddos-va-nhung-van-de-lien-quan>

[38] vinahost.vn (2018), Ddos Là Gì? Cách hạn chế và phòng chống tấn công Ddos, truy cập 21/01/2021, <https://vinahost.vn/ddos-la-gi.html>

[39] vnso.vn (2019), DNS Amplification Attack! DDoS khuếch đại từ máy chủ DNS, truy cập 21/01/2021, <https://vnso.vn/dns-amplification-attack-ddos-khuech-dai-tu-may-chu-dns/>

[40] giangpth (2018), Máy chủ Memcached bị tấn công bởi DDoS khuyếch đại khổng lồ, truy cập 22/01/2021, <https://bizflycloud.vn/tin-tuc/may-chu-memcached-bi-tan-cong-boi-ddos-khuyech-dai-khong-lo-20180309122211668.htm>

[41] vietnambiz.vn (2020), Cuộc tấn công khai thác lỗ hổng Zero-day (Zero Day Attack) là gì? Đặc điểm, truy cập 22/01/2021, <https://vietnambiz.vn/cuoc-tan-cong-khai-thac-lo-hong-zero-day-zero-day-attack-la-gi-dac-diem-20200414210442937.htm>

[42] Hòa Thu (2014), Tấn công mạng vào Estonia - Bài học cho các nhà quản lý mạng (Phần 1), truy cập 22/01/2021, <https://petrotimes.vn/tan-cong-mang-vao-estonia-bai-hoc-cho-cac-nha-quan-ly-mang-phan-1-236391.html>

[43] Minh Việt (2012), 15 vụ tấn công DDoS nổi tiếng nhất lịch sử, truy cập 22/01/2021, <https://www.nguoiduatin.vn/15-vu-tan-cong-ddos-noi-tieng-nhat-lich-su-a2415.html>

[44] Nguyễn Tuấn Nam (2013), Tình hình an ninh mạng năm 2012, truy cập 22/01/2021, <https://www.uit.edu.vn/tinh-hinh-ninh-mang-nam-2012>

[45] Nguyễn Hải (2016), Hacker từng làm sụp đổ toàn bộ mạng Internet châu Âu đã ra khỏi trại giam <https://genk.vn/hacker-tung-lam-sup-do-internet-chau-au-da-thoat-khoi-trai-giam-20161116152406811.chn>

[46] Phong Vân (2014, Mốc lịch sử mới của tấn công mạng DDoS <https://congnghe.tuoitre.vn/moc-lich-su-moi-cua-tan-cong-mang-ddos-593830.htm>

[47] Xuân Trường (2020), Khi Đảng Cộng sản Trung Quốc bắt Mạng xã hội phải câm lặng <https://www.ntdvn.com/chuyen-de/dcstq-bat-mang-xa-hoi-phai-cam-lang-68587.html>

[48] Khuyet Danh (2018), Distributed denial of service (DDOS), truy cập 22/01/2021, <https://voer.edu.vn/m/distributed-denial-of-service-ddos/9dd616a0>

[49] thaipro (2015), Giới thiệu về sâu máy tính (phần 5) - Một số loại sâu điển hình, truy cập 22/01/2021, <https://thaipro.wordpress.com/2015/12/23/gioi-thieu-ve-sau-may-tinh-phan-5-mot-so-loai-sau-dien-hinh/>

[50] Hoàng Tùng (2020), Mirai botnet là gì?, truy cập 22/01/2021, <https://ssl.vn/mirai-botnet-la-gi.html>

Thùy Dương (2020), DDoS - Mục đích phía sau một cuộc tấn công , truy cập 22/01/2021, https://tinnhanhchungkhoan.vn/ddos-muc-dich-phia-sau-mot-cuoc-tan-cong-post246853.html