TÌM HIỂU VỀ SỰ PHÁT TRIỂN CỦA BOTNET TRONG 20 NĂM TRỞ LẠI ĐÂY

Trần Văn Thiện[1], Huỳnh Trọng Tuấn Anh[2]

Tóm tắt: *Khi nhắc đến Botnet thì ta hiểu nó là một mạng lưới bao gồm các máy tính bị xâm nhập chi phối và điều khiển từ xa bởi một máy tính để tấn công DDoS, spam, gian lận, đánh cắp thông tin hoặc lừa đảo. Điều này đã dẫn đến tổn thất rất nặng nề. Vì thế bài báo này sẽ tìm hiểu rõ cách thức hoạt động của Botnet và một số cách tiếp cận để hạn chế những thiệt hại mà nó gây ra cũng như cách để phòng ngừa và xử lý khi máy tính bị tấn công. Ý nghĩa của bài báo là đem đến cho người đọc cái nhìn tổng thể về Botnet và cách thức hoạt động cũng như những mặt có lợi có hại của nó để có những hiểu biết hơn về loại mạng này.*

Từ khóa: *Botnet, tấn công DDoS, đánh cắp thông tin, các mối đe dọa.*

Abstract: *When mentioning Botnet, we understand it as a network of intrusive computers governed and remotely controlled by another computer to attack DDoS, spam, cheat and harm information. This has led to huge losses, so the article will explore how Botnet works and some approaches to mitigate damages as well as convey how to prevent it and suggest solutions when the computer is attacked. The aim of the article is to give the reader an overview of how Botnet works and its pros and cons to have a better understanding of this type of network.*

Keywords: *Botnet, attack DDoS, harm information, threats.*

1. Giới thiệu

Botnet có tên đầy đủ là Bots network nó bao gồm các máy tính đã bị điều khiển bởi các hacker. Botnet được thiết kế rất đơn giản với mục đích là một hệ thống sinh ra để chạy các nhiệm vụ lặp đi lặp lặp lại, những thứ mà sử dụng được Internet để Botnet có thể tồn tại trên nó. Không chỉ hoàn thành mục tiêu ban đầu được tạo ra mà Botnet hoàn thành nó một cách tốt hơn cả mong đợi và các công nghệ này đến tay các hacker thì nó trở thành thứ vũ khí lợi lại của họ. (Citron DK. 2006)

Các botnet do hacker tạo ra thường tấn công các website nào đó bằng cách lây nhiễm các phần mềm mang theo mã độc hại cho các máy tính và thậm chí là điện thoại bị lây nhiễm để sau đó chúng thực hiện các mong muốn thông qua máy tính bị lây nhiễm. Cách hoạt động của botnet cũng rất đơn giản, các botnet độc hại được tạo thành từ một hoặc nhiều máy tính bị lây nhiễm và được phát triển thông qua các lần mà người dùng tải xuống hoặc thông qua trojan (Mansfield-Devine S. 2014).

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

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

Trên thực tế rất khó xác định được thời gian mà các botnet này xuất hiện nhưng cho đến nay chúng đã trải qua nhiều giai đoạn tiến hóa và ngày càng trở nên tinh vi hơn nguy hiểm hơn, khó có thể biết được máy tính đang sử dụng có bị nhiễm hay chưa. Theo số lượng được thống kê về các máy tính bị nhiễm, thì có đến hàng ngàn máy tính bị kiểm soát và vẫn hoạt động, dù đã có rất nhiều vụ được ngăn chặn nhưng không lấy gì đảm bảo là không còn các vụ tấn công khác không xảy ra. Hoạt động thường nhật của Internet được sự tiếp sức bởi các máy tính liên lạc với nhau gọi là botnet, thực tế chúng không xấu như thế giới vẫn thường nghĩ, chúng không phải là các hệ thống độc hại mà chúng thực hiện nhiều công việc nền và nhiệm vụ lặp lại cần thiết để cung cấp các dịch vụ trực tuyến. Điều này thực sự trở nên rắc rối khi có một số người tìm ra cách huy động lại mạng này nhằm mục đích chống lại người khác. (Bu Z, Bueno P, Kashyap R. 2010).

Mục đích chính mà các botnet này được tạo ra là có thể tự lan truyền và tự lây lan các mã độc bằng các thao tác của người dùng khác dựa trên các trojan ẩn và như thế nó được kích hoạt. Sau khi bị nhiễm, các hệ thống này sẽ hoạt động song song các thiết bị khác trên mạng Bot, đóng góp tài nguyên để cùng thực hiện một hoạt động. Thông thường thì các người điều khiển botnet sẽ sử dụng sức mạnh của botnet để khởi động các cuộc tấn công từ chối dịch vụ để nhằm mục đích chống lại các mạng khác, các cuộc tấn công này còn gọi là Denial of Service- DoS.

Thông thường những hoạt động của botnet này sẽ được triển khai một cách tự động để tự động hóa, nghĩa là một hành động nào đó được lập trình sẵn ví dụ như tạo ra hàng loạt các email rác để gửi đến hàng ngàn hàng triệu người khác hoặc nó được dùng để tăng số lượng khách truy cập ảo trang web (Weyers B; 25/10/2016). Bài báo được chia thành năm phần bao gồm phần giới thiệu, lịch sử hình thành, tìm hiểu về Botnet, các cuộc tấn công Botnet và cuối cùng là kết luận.

2. Lịch sử phát triển

2.1. Từ trước những năm 2000

Thực sự rất khó để xác định thời gian mà botnet ra đời theo những con số đã được đưa ra, từ những năm 1988 Robert Morris,Jr một sinh viên trường Cornell là người đầu tiên phát hành sâu của Internet và cũng được thiết kế để thực hiện các cuộc gọi về nhà được máy chủ chỉ huy và điều khiển, đây là những phần mềm khởi động cho sự phát triển của botnet. Các phần mềm này được phát hiện trước khi thế giới bắt đầu chuyển mình qua một thiên niên kỷ mới với nhiều sự cải tiến mới. Không những thế, chính những khái niệm này đã giới thiệu khái quát phần nào về một loại hình mà máy tính bị lây nhiễm khi chúng cùng ở chung một phòng và cùng thực hiện thảo luận liên lạc với nhau thông qua kênh IRC(Internet Relay Chat) và lúc đó các lệnh độc hại sẽ được thực hiện (Cyber Insecure. 2008).

Đến năm 1999 sự xuất hiện của một trong những trở thủ đắc lực của tin tặc là trojan và sâu máy tính chúng được biết đến với sự xuất hiện của các phần mềm độc hại kết nối máy tính của nạn nhân đến một kênh IRC để thực hiện các lệnh xấu mà tin tặc yêu cầu.(Susan CH. 2002)

2.2. Từ năm 2000 đến nay

Năm 2000 sự xuất hiện của Global Threat Bot ra đời đánh dấu sự thay đổi lớn đối với thế giới. Botnet này là một Botnet rất mới nó có năng lực rất cao là đáp ứng tất cả yêu cầu trên IRC và được cấp quyền để kết nối truy cập vào TCP gốc và các cổng logic của UDP, vì vậy nó hoàn hảo đối với các cuộc tấn công DDoS đơn giản. Điều này bắt buộc tin tặc phải cải hóa mới cách xây dựng Botnet theo thời gian khi mà cũng trong năm 2000 đã có sự thay đổi rất lớn về mặt truyền thông tin là giao thức IRC được đổi sang mạng ngang hàng (peer-to-peer - P2P) mạng này còn được gọi là mạng đồng đẳng, tức là một mạng mà máy tính hoạt động chủ yếu dựa vào khả năng tính toán và băng thông của các máy tham gia chứ không còn tập trung vào máy chủ như trước (Hao S., Feamster, N. 2008).

Tuy nhiên, qua thời gian IRC đã cho con người thấy được những mặt tốt, khả năng và sự hiệu quả của mình, các nhà nghiên cứu về vấn đề bảo mật sớm nhìn thấy và phát hiện ra rằng họ chỉ cần đưa IRC dựa trên các máy chủ lệnh và kiểm soát (Command-and-Control - C&C) vào danh sách đen để diệt các botnet. Tin tặc là nhóm người có kiến thức và am hiểu về thế giới ảo, chúng tìm đến các mạng P2P thay vì các cơ sở hạ tầng không tập trung C&C. Các máy tồn tại như những con zombie, tức là các chủ nhân của máy tính bị nhiễm mạng này không biết được rằng máy mình đang sử dụng đang thực hiện một loạt các hành động bất hợp pháp, vì chúng bị điều khiển bởi các máy tính ma, điều này nhằm cung cấp một mạng P2P có thể ẩn đi máy chủ một cách hiệu quả. Dẫn đến làm cho việc phá vỡ hoàn toàn hoạt động của botnet này gần như là không thể (Anomali. 2019).

Năm 2002 sự xuất hiện của Agobot nó là một họ khác của sâu máy tính, nó là một chương trình được viết theo dạng đa luồng, hướng đối tượng và được viết bằng ngôn ngữ lập trình C++, chính vì thế việc sử dụng nó rất dễ vì nó không cần nhiều kiến thức để có thể hiểu và sử dụng nó theo ý của mình. Chính vì thế đã có thêm một khái niệm về cuộc tấn công nữa bằng cách chia nhỏ các cuộc tấn công theo từng giai đoạn và các dữ liệu vận chuyển của một gói tin sẽ được phân phối lần lượt chia điều cho mỗi gói tin. Các cuộc tấn công sẽ phân định rõ nhiệm vụ của mình ví dụ như: cuộc tấn công đầu tiên sẽ tạo ra một cửa sau, cuộc tấn công thứ hai sẽ cố gắng hạ gục phần mềm diệt virus và cuộc tấn công thứ ba sẽ chặn sự truy cập của các nhà cung cấp bảo mật và đến lúc này việc tấn công đã hoàn tất. (G. Kirubavathi và R. Anitha. 2016)

Năm 2003 Spybot được ra đời, sự ra đời của phần mềm chống gián điệp này là do được tạo nên từ cơ sở của SDBot (là loại trojan cổng sau nó cho phép các kẻ tấn công có thể dễ dàng điều khiển máy tính bị nhiễm thông qua các kênh kênh này gọi là IRC) với các khả năng khác nhau để thực hiện các hoạt động gián điệp. Nó có khả năng là ghi các mã khóa, phần mềm gián điệp khai thác dữ liệu và nó có thể dùng để gửi các tin nhắn hoặc spam. Nó là botnet đầu tiên phát động các cuộc tấn công dạng DDoS, thậm chí hơn là nó có thể sử dụng proxy SOCKS và nó cũng là botnet đầu tiên áp dụng thuật toán nén và mật mã để tránh bị phát hiện. (Boshmaf, Y., I. Muslukhov, K. Beznosov, và M. Ripeanu. 2013).

Năm 2004, với sự xuất hiện của các phần mềm hậu duệ của Agobot là Phatbot là một trong số những phần mềm độc hại botnet đầu tiên được sử dụng P2P thay vì IRC và cũng trong năm này Polybot lần đầu tiên áp dụng các thuật toán mới, các thuật toán này gọi là các thuật toán đa hình để làm cho các mã của nó trở nên động. Trên thực tế là vi-rút đa hình có thể biến đổi bộ giải mã của chúng thành một số lượng lớn các trường hợp khác nhau có thể có hàng triệu dạng khác nhau. Bên cạnh đó việc bảo vệ phòng chống phần mềm độc hại gặp rất nhiều khó khăn vì Polybot đã có nhiều biến thể khác nhau. Cũng trong năm này Botnet cuối cùng cũng đã chuyển sang giao thức HTTP và ICMP từ IRC. (Chen, W. 2017).

Năm 2006 phần mềm độc hại Zeus (Zbot) lần đầu tiên xuất hiện với khả năng là phần mềm gián điệp và qua nhiều năm, một số bản cập nhật của các biên bản được áp dụng và các tính năng mới cũng được đưa vào. Theo như các con số đã được ghi nhận và thống kê thì Bredolab nó là một trong những Botnet lớn nhất từng được ghi nhận. Thậm chí Zeus là phần mềm đầu tiên có thể dễ dàng cho thuê trong Darknet, dù có nhiều hoạt động của tội phạm đã và đang hoạt động trên mạng này nhưng Darknet không phải là mạng xấu. (Karim, Ahmad. 2014)

Hoạt động trong năm 2007, do tính chất của máy chủ C&C những phần mềm bảo vệ đã hiệu quả hơn dựa vào định danh trên IP qua đó đòi hỏi kỹ thuật ngụy trang cao hơn nữa và đã có một dấu ấn quan trọng trong sự phát triển của ngành công nghiệp Botnet. Sự xuất hiện đó là Cutwail Botnet bao gồm cho phép các botnet tạo ra tên máy chủ, tức là có thể tự tạo ra tên máy chủ có thể giống hoặc khác so với tên máy chủ của chúng để nó có thể thay thế cho các máy chủ C&C của chúng hàng ngày và kể cả các khái niệm về kết nối sao lưu trên máy tính. Năm 2008, với sự xuất hiện của Conficker. Botnet đã tạo nên một bước ngoặt lớn bằng việc sử dụng một kỹ thuật tương tự và có khả năng tạo ra 50.000 tên thay thế mỗi ngày.(Feily, M., A. Shahrestani và S. Ramadass; 2009).

Những phát triển liên tục như thế này đã và đang tạo nên những thuận lợi giúp tội phạm mạng che giấu hoạt động botnet tốt hơn và ngày có nhiều công cụ hơn cho chúng thực hiện hành vi của mình khiến cho việc thi hành luật pháp để ngăn chặn chúng gặp phải rất nhiều khó khăn. Trên thực tế đây cũng không hoàn toàn là một việc dễ dàng đối với ngay cả tội phạm mạng, nếu không nắm vững những phát triển này chúng sẽ lạc hậu và việc thực hiện hành vi của chúng sẽ dễ bị phát hiện hơn, tuy nhiên cũng đã có một vài sự kiện lớn xảy ra trong thời gian gần đây. Trong năm 2008 sự kiện được cho là nổi bật nhất đó chính là việc gỡ bỏ McColo vào năm. (Hyslip, T. và J. Pittman. 2015).

Một công ty lưu trữ đã bị loại bỏ ngay sau khi một phóng viên của tờ Washington Post liên lạc với hai nhà cung cấp dịch vụ Internet của công ty để gửi đến họ cảnh báo về hoạt động độc hại thông qua các máy chủ McColo. Và cũng từ đó người ta đã nhận ra rằng các nhà cung cấp đã lưu trữ và bảo vệ các máy chủ C&C cho một hoặc thậm chí là rất nhiều botnet lớn mà trong đó bao gồm những cái tên rất nổi tiếng như Cutwail và Rustock. Sau đó, khi mà máy chủ độc hại đó đã bị loại khỏi Internet vào tháng 11, trên thế giới có một sự chuyển biến hết sức

quan trọng đó là mức độ spam toàn cầu giảm đi rất nhiều gần 80%. Tuy nhiên, không lấy gì là chắc chắn rằng không còn những thứ khác không xuất hiện và người ta dự báo rằng thư rác sẽ sớm thống trị trở lại (Dell Secure Works. 19/12/2016).

Trong năm 2009, sự xuất hiện với ước tính có đến 30 triệu Botnet với một mạng lưới có kích thước lớn như thế này nó có khả năng phát tán hơn 3,6 tỷ email rác độc hại mỗi ngày cho các máy tính và người dùng trên thế giới. Năm 2010 Mã Zeus được tích hợp vào SpyEye phần mềm độc hại và tiếp thị đến các khách hàng và tội phạm mạng Botnet và thư rác Waledac bị gỡ xuống đó là thư của Microsoft. Năm 2011 'Gameover Zeus' xuất hiện bằng cách sử dụng giao thức P2P để liên hệ với các trang web C&C. Năm 2012 Grum botnet bị gỡ xuống có sự phối hợp hoạt động của các nước như Nga, Ukraine, Panama, và Hà Lan (Saxe, J., Berlin, K. 2015).

Năm 2013 các chuyên gia bảo mật đã đưa ra các báo cáo đầu tiên về Botnet android như MisoSMS. Sau đó việc thực thi pháp luật chung và khu vực tư nhân đã gỡ xuống nhiều Botnet của Citadel, chịu trách nhiệm về vụ trộm 500 triệu đô-la từ tài khoản ngân hàng của người tiêu dùng và doanh nghiệp. Năm 2014 Tovar: Bộ Tư pháp (DOJ) cùng với thực thi pháp luật ở nhiều quốc gia và bắt đầu kiểm soát mạng Botnet Gameover Zeus (Kudo, T. 2018).

Sau đó hai năm tức là năm 2016 cả thế giới đã chứng kiến sự nổi lên của một thế lực đó là Mirai một Botnet được coi là khét tiếng và là kẻ đứng sau các cuộc tấn công vào mạng Dyn vào tháng 10 năm 2016 cuộc tấn công đã khiến cho Spotify, Netflix, Amazon và những mục tiêu khác ngoại tuyến bị thiệt hại nặng nề. Và cũng kể từ đó trên các website của các hacker đã và đang phân phối một dạng mã nguồn mở đó là mã nguồn của Botnet chúng xuất hiện rất nhiều và ngày càng mở rộng thêm. Năm 2017 đến nay Các Botnet IoT đã mở rộng và trở thành Botnet được lựa chọn nhất trong năm. Các nhà phát triển tuyên bố Botnet sẽ tiếp tục sáng tạo và bí mật hơn, xây dựng các mạng Botnet ngày càng khó phá vỡ.(M. Sanchez. 2017).

3. Tìm hiểu về Botnet

3.1. Cấu trúc của botnet

Botnet có nhiều loại nhưng trong bài báo này sẽ giới thiệu cho người đọc những dạng botnet phổ biến nhất như:

3.1.1. IRC Botnet

IRC nó là một giao thức thường được dùng trong việc chat qua lại với nhau có thể là các ứng dụng chat như zalo, facebook hay các trang web dùng để chat, tạo nhóm nói chuyện chat qua lại với nhau. Cũng giống như việc con người hay chat trên facebook thì IRC Botnet cũng vậy. Bot master ra lệnh cho các bot của mình thông qua 1 channel chat để từ đó tin nhắn có thể chuyển qua lại giữa hai hoặc nhiều người (Nguyễn Trọng Hưng, Hoàng Xuân Dậu, Vũ Xuân Hạnh. 12/2018).

3.1.2. P2P Botnet

Trên thực tế P2P có nhiều điểm khác biệt so với Botnet trên, mô hình mà P2P xây dựng là mô hình phân tán bởi vì các kết nối của các Botnet với máy chủ C&C thường là các kết nối P2P - kết nối này còn gọi là ngang hàng. Với mô hình ngang hàng này, rất khó để shut-down hoặc phá hủy nó bằng các cách thông thường vì ở mô hình phân tán sẽ không còn client-server mà mỗi Botnet nó vừa là một Client cũng vừa là một Server riêng biệt nên không dễ bị tấn công, phá hủy. Thông thường các Botnet này sẽ nhận lệnh bằng việc các botnet sẽ bắt đầu tạo ra các tín hiệu riêng để chúng có thể liên lạc với nhau và nhận lệnh với các search key tương ứng và gửi đến mỗi Botnet có mặt trong mạng P2P.(Wang, P., et al. 2007)

3.1.3. HTTP Botnet

Mô hình của HTTP Botnet cũng là mô hình tập trung client-server như IRC Botnet nhưng thay vì nhận lệnh thông qua kênh chat thì HTTP Botnet sẽ sử dụng giao thức HTTP để gửi request và nhận lệnh từ các bot đến Bot master. Như vậy, HTTP Botnet không thể nhận lệnh realtime như P2P Botnet được mà sẽ gửi request liên tục hoặc qua x thời gian nào đó để cập nhật tình hình.

3.1.4. Mobile Botnet

Trong những năm gần đây sự phát triển không ngừng nhanh chóng của công nghệ - kĩ thuật và sự bùng nổ các thiết bị thông minh nhất là Smartphone ngày càng khẳng định được vị thế của mình. Tiếp nối những thành công đó Botnet đã có một cuộc chuyển biến mới và cách tiếp cận nạn nhân mới hơn, việc điện thoại Smartphone xuất hiện kéo theo nhiều tiện ích mới của điện thoại ra đời và cũng nhờ đó Botnet lợi dụng dịch vụ SMS trên các Smartphone và các thiết bị di động khác để gửi, nhận lệnh. Đây là loại Botnet sử dụng giao thức mới, đó là giao thức Bluetooth để xâm nhập hoặc thực hiện những ý đồ xấu mà người đó muốn khi nạn nhân nằm trong vùng phủ sóng của Bluetooth. Nhưng loại botnet này chỉ hoạt động được khi nạn nhân nằm trong vùng phủ sóng Bluetooth còn ở ngoài vùng phủ sóng thì coi như giao thức này bị vô hiệu. (Yuan, Z., Lu, Y., Wang, Z., Xue, Y, 'DroidSec. 2014).

3.1.5. Botnet Cloud

Botmaster sử dụng cách dịch vụ cloud. Với các Botnet loại này chúng sử dụng các tính năng bảo mật cao và an toàn của google chính vì thế việc phát hiện nhận diện là rất khó khăn. Cùng với sự phát triển của các dịch vụ cloud thì việc deploy một kiến trúc để thực thi botnet nhanh hơn rất nhiều so với botnet truyền thống chưa kể việc nó luôn luôn online, sẵn sàng thực thi các hành động (Shipp, A. 2010)

3.2. Các loại tấn công botnet

3.2.1. Distributed Denial of Operations Service (DDoS)

Một Botnet có thể được sử dụng để tấn công từ chối dịch vụ phân tán(DDoS) nó được dùng để phá hủy kết nối và dịch vụ mạng dẫn đến các thiết bị sẽ không còn hoặc không thể

truy cập mạng Internet được nữa. Để làm được điều này nó đòi hỏi phải làm sao tiêu tốn băng thông hoặc làm quá tải tài nguyên của đối phương. Theo số liệu đã được thống kê và ghi nhận thì những cuộc tấn công phổ biến nhất là TCP và UDP. Các mục tiêu của DDoS không đơn giản như ta nghĩ, nó nhắm đến bất kỳ dịch vụ nào được kết nối Internet và bên cạnh đó nó còn giới hạn máy chủ. (D. Zhao, I. Traore, B. Sayed. 2013)

HTTP flood nó được sử dụng để tăng mức độ nghiêm trọng của các cuộc tấn công, với cách này trang web của nạn nhân bị tấn công mức độ thiệt hại sẽ là rất lớn. Hình thức này gọi là thêu thùa (spidering) nó được tiến hành với mục đích chính là để tăng sự hiệu quả của các cuộc tấn công. Cho đến nay có thể nói rằng một trong những cuộc tấn công Botnet bằng DDoS lớn nhất từng được diễn ra và liên quan đến IoT là sử dụng virus botnet Mirai, nó là một dạng mã độc sâu, lây nhiễm vào các thiết bị IoT. Những nạn nhân mà virus nhắm đến đó là các thiết bị được bảo vệ rất lỏng lẻo và dễ xâm nhập không chỉ một, hai mà là hàng ngàn thiết bị và sau đó các nạn nhân sẽ bị biến thành các Botnet để bắt đầu các cuộc tấn công DDoS. Ngày qua ngày những con virus Mirai này tiếp tục mở rộng và phát triển không ngừng điều đó làm cho các cuộc tấn công trở nên rất phức tạp. (Us.norton.com. 2017).

3.2.2. Spamming (phát tán thư rác) và giám sát lưu lượng

Một Botnet mà con người sử dụng chúng để có thể phát hiện các dữ liệu nhạy cảm và kể cả tìm ra các máy tính đã bị nhiễm độc, không những thế nó còn có thế tìm ra các Botnet đối thủ ở trong máy nạn nhân. Một số Botnet có thể mở proxy SOCKS (giao thức proxy chung cho mạng dựa trên TCP/IP) nó thường được người ta cài vào để trao đổi các gói mạng giữa máy chủ và máy khách thông qua proxy. Khi mà proxy SOCKS được kích hoạt trên máy tính bị xâm nhập, lúc này nó có thể được sử dụng cho nhiều mục đích khác nhau ví dụ như spamming (phát tán thư rác). (G. Zhao, K. Xu, L. Xu và B. Wu. 2015).

Botnet sử dụng packet sniffer (dạng theo dõi một mục tiêu) để theo dõi thông tin hoặc dữ liệu được truyền bởi máy bị xâm nhập, khi đó sẽ biết máy tính truyền những gì và với mục đích gì. Sniffer thường nếu không để ý thì có thể truy xuất thông tin nhạy cảm như tên người dùng và mật khẩu của chúng ta và làm những chuyện với mục đích xấu. Grum là loại thư rác được cho là rất khó bị phát hiện bởi mục đích của nó là lây nhiễm những tập tin. Không những thế mạng Botnet này đã thu hút đến sự quan tâm của các nhà nghiên cứu nhưng với số lượng không lớn chỉ khoảng 600,000 thành viên tham gia nghiên cứu nhưng Botnet này đã chiếm đến 40 tỷ email spam mỗi ngày một con số rất lớn. (B. Cusack và S. Almutairi. 12/2014).

3.2.3. Keylogging

Với sự trợ giúp của keylogger, việc botmaster dễ dàng trong việc đánh cắp các thông tin cá nhân và dữ liệu ngày càng trở nên dễ dàng và không bị phát hiện. Khi các kẻ tấn công sử dụng với mục đích xấu có thể thu thập các thông tin mà chúng tìm kiếm qua Paypal và cả Yahoo.

3.2.4. Đánh cắp danh tính khách hàng

Thông thường các loại Botnet khác nhau vẫn có thể được kết hợp với nhau để thực hiện hành vi trộm cắp danh tính với quy mô lớn, đây được xem là một hành vi phạm tội nhưng hành vi này lại phát triển rất nhanh, thậm chí là nhanh nhất. Các email spam này được gửi bởi Botnet để hướng sự chú ý truy cập đến các trang web nhưng là các trang web giả mạo nạn nhân để thu thập các dữ liệu các nhân. Botnet rất tinh vi nó có thể dùng như một công ty hợp pháp mà ở đó nó có thể yêu cầu mọi thứ từ thông tin tài khoản ngân hàng, thông tin cá nhân, số thẻ tín dụng. Hành vi đánh cắp danh tính khách hàng hàng loạt vẫn đang diễn ra bằng cách sử dụng email lừa đảo để lừa nạn nhân nhập thông tin đăng nhập trên trang web, khi nạn nhân đăng nhập trên web các thông tin về tài khoản và mật khẩu có thể bị những kẻ xấu thu thập được, trên các nền tảng như eBay, Amazon, hoặc thậm chí là ngân hàng. (C Y. Huang. 2013)

3.2.5. Lạm dụng việc trả tiền cho mỗi lần nhấp

Chương trình quảng cáo của Google cho phép các trang web hiển thị quảng cáo Google và từ đó kiếm tiền từ chúng. Google trả tiền cho chủ sở hữu trang web trên cơ sở số lần nhấp mà quảng cáo của họ thu thập được. Máy bị nhiễm được sử dụng để tự động nhấp vào một trang web, làm tăng số lần nhấp được gửi đến công ty bằng quảng cáo. (Cantón, D. 2015)

3.2.6. Lây lan botnet

Botnet còn được sử dùng với nhiều cách khác nhau ví dụ như các Botnet ra sức thuyết phục dụ dỗ người dùng tải các chương trình thông qua các email hay giao thức HTTP. Thật vậy, các Botnet như vậy nếu tiếp tục tồn tại sẽ tạo ra nhiều vấn đề nhức nhối cho nhiều người, sự mất mát lớn về tài sản cũng sẽ tiếp tục tăng và có thể phát động nhiều cuộc tấn công mạng nhắm vào những mục tiêu lớn hơn. (Zhichun Li, Anup Goyal và YanChen. 2007).

3.2.7. Phần mềm quảng cáo

Các phần mềm quảng cáo được sử dụng để thu hút người dùng bằng cách quảng cáo trên các trang web hoặc ứng dụng đem đến nhiều bất tiện cho người dùng. Chúng xuất hiện mà không có sự cho phép của người dùng, với việc xuất hiện đó có thể gây nhiều khó chịu, với quảng cáo gốc bị thay thế bởi phần mềm quảng cáo lừa đảo, lây nhiễm vào hệ thống của bất kỳ người dùng nào nhấp vào nó. Phần mềm quảng cáo trông giống như quảng cáo vô hại không ảnh hưởng gì đến người dùng nhưng sử dụng phần mềm gián điệp để thu thập dữ liệu từ trình duyệt. (K. Alieyan, A. Almomani, A. Manasrah và, M.M. Kadhum. 2017)

Để thoát khỏi phần mềm quảng cáo, cần phải có phần mềm chặn quảng cáo. Mặc dù có sẵn nhiều phiên bản phần mềm chặn quảng cáo miễn phí và trả phí, nhưng tốt nhất bạn nên sử dụng một tùy chọn có giấy phép. Nhiều gói quét virus cũng đi kèm với chương trình chống phần mềm độc hại. (Ferguson, R. Trend Micro. 2000).

3.3. Cách thức hoạt động của botnet

Dưới sự điều khiển của các hacker Botnet hoạt động rất tinh vi, cách để điều khiển Botnet là cho từng máy Botnet cùng kết nối tới một máy chủ tập trung. Máy chủ này sẽ là trung tâm điều khiển botnet. Các Botnet trên máy của người dùng sẽ kết nối tới 1 kênh IRC và đợi lệnh. (Wang, P., et al. 2007)

Một số Botnet sẽ cho phép chúng kết nối với nhau theo cách phân tán. Mỗi Botnet sẽ liên lạc với các Botnet khác ở gần nó và không có một máy chủ ra lệnh. Cách hoạt động này khá giống với các mạng ngang hàng như DHT(Distributed Hash Table) và các loại giao thức mạng P2P khác. Để chống lại Botnet này có rất nhiều cách chẳng hạn bạn có thể tạo ra nhiều lệnh giả hoặc không cho các Botnet ở gần nhau. (R. Abdullah, M. Faizal, và Z. Noh. 2014)

Một số Botnet liên lạc với nhau bằng cách sử dụng mạng Tor, mạng này mã hóa người dùng đến mức cao nhất khó có thể mà phát hiện ra các mã độc. Về mặt lý thuyết, việc tìm xem các dịch vụ này đang nằm ở đâu là gần như không thể, chỉ có các cơ quan tình báo như NSA mới có thể giải quyết được vấn đề này. Cách giải quyết của họ cũng là bất khả thi với người dùng thông thường. Do đó, việc phòng tránh bị nhiễm mã độc sẽ quan trọng hơn là bị lây nhiễm rồi tìm cách chữa trị. Các hiệu quả nhất để chống bị nhiễm mã độc và trở thành một phần của Botnet, cài đặt các phần mềm diệt và chống virus, hạn chế sử dụng các phần mềm không có bản quyền, không nguồn gốc để bảo vệ máy tính mình. (Caballero, J., Grier, C., Paxson, V., Song, D. 2010).

3.4. Cách phòng ngừa Botnet

Như được biết, phòng bao giờ cũng tốt hơn chữa, người dùng có thể ngăn hệ thống của mình bị lây nhiễm bằng cách làm theo một số bước sau. Các biện pháp phòng ngừa có thể được thực hiện ở cấp độ người dùng cá nhân và ở cấp độ mạng.

3.4.1. Cấp độ cá nhân

Cấp độ cá nhân bao gồm:

- Cài đặt phần mềm diệt virus cho máy tính hoặc chống thư rác và giữ cho chúng được cập nhật thường xuyên.
- Bật cài đặt tường lửa và hạn chế những truy cập không mong muốn với máy tính của bạn.
- Hãy chắc chắn rằng hệ điều hành được cập nhật theo thời gian.
- Không tải xuống nội dung bất hợp pháp như nhạc, game, file lậu từ Internet.
- Không nhấp vào file đính kèm hoặc liên kết từ các email không xác định để máy tính không bị xâm nhập.

3.4.2. Cấp độ mạng

Cấp độ mạng bao gồm:

- Có tường lửa, hệ thống IDS/IPS và tính năng lọc nội dung.
- Giám sát lưu lượng truy cập tăng bất thường.
- Có tính năng bảo vệ DDoS tại chỗ.
- Nếu máy tính đang dùng có phần mềm mà bạn nghi ngờ không rõ nguồn gốc thì tốt nhất là xóa ngay lập tức để tránh những thiệt hại đáng tiếc.
- Đảm bảo rằng tất cả các cá nhân trong công ty đã có phần mềm được cập nhật trên hệ thống của họ.
- Nếu bất kỳ việc lây nhiễm nào được xác định, hãy thông báo cho các nhà cung cấp phần mềm diệt virus ngay lập tức.

4. So sánh các cuộc tấn công Botnet

Botnet là một mạng lưới lớn chứa các ứng dụng độc hại dựa trên web, mạng Botnet hoạt động ngoài trung tâm dữ liệu, trong khi những mạng khác được tạo thành từ thiết bị của người dùng Internet bị nhiễm phần mềm độc hại. Một số gửi hàng triệu email spam; một số gỡ bỏ các trang web và giữ chúng để đòi tiền chuộc; một số thực hiện chiếm dụng tài khoản và tạo tài khoản giả mạo; một số ăn cắp từ các nhà quảng cáo có lập trình thông qua gian lận quảng cáo. Dưới đây là một trong nhiều cuộc tấn công tiêu biểu nhất:

Năm 2000, mạng botnet đầu tiên gây được tiếng vang cho công chúng là một kẻ gửi thư rác do Khan K. Smith xây dựng vào năm 2000. Mạng botnet này đã gửi 1,25 triệu email - những trò lừa đảo được che giấu dưới dạng liên lạc từ các trang web hợp pháp - trong vòng hơn một năm. Smith hy vọng thu thập thông tin nhạy cảm như số thẻ tín dụng hoặc vi rút đã tải xuống máy tính của nạn nhân để cung cấp thông tin cho anh ta từ xa. Cuối cùng, Smith đã bị EarthLink kiện với số tiền 25 triệu đô la vì đã sử dụng mạng của họ cho âm mưu về thư rác, điều này đã kiếm được cho Khan K. Smith ít nhất 3 triệu đô la. (B., Sharma, V.,Ni viện, C., Kang, B., Dagon, D. 2007).

Năm 2007, mạng Botnet thư rác Cutwail đã gửi 51 triệu email mỗi phút, đóng góp tới 46,5% tổng lượng thư rác trên toàn thế giới. Vì Cutwail đã có khoảng 1,5 triệu máy bị nhiễm, các nỗ lực để tắt nó đã không hiệu quả một cách đáng thất vọng. Ngay cả sau một nỗ lực gỡ xuống của FBI, Europol và các cơ quan thực thi pháp luật khác vào năm 2014, mạng botnet vẫn hoạt động và có sẵn cho thuê cho đến nay. (Rege, A. 2014).

Grum là một botnet thư rác chuyên về thư rác dược phẩm, nhưng có quy mô lớn. Năm 2009, nó có khả năng gửi 39,9 tỷ tin nhắn mỗi ngày, chiếm 18% tổng lượng thư rác trên thế giới. Cơ quan thực thi pháp luật đã phát hiện ra các trung tâm chỉ huy và kiểm soát của Grum

ở các địa điểm trên thế giới, từ Hà Lan đến Panama, đã đóng cửa hoạt động thành công vào năm 2012. (Krebs, B. Krebs. 2010).

Thật khó để biết chính xác mạng botnet Kraken lớn như thế nào, nhưng không thể phủ nhận phạm vi tiếp cận khổng lồ của nó. Những nhà nghiên cứu ước tính rằng Kraken đã lây nhiễm cho 10% tổng số công ty trong danh sách và mỗi bot trong số 495.000 bot của nó có thể gửi tới 600.000 email mỗi ngày. Botnet là một trong những mạng đầu tiên được quan sát thấy sử dụng các kỹ thuật trốn tránh cho phép nó tránh bị phần mềm chống phần mềm độc hại phát hiện, ngay cả khi được cập nhật tự động. Mặc dù Kraken ngày nay không hoạt động, nhưng tàn tích của nó đã được các hệ thống an ninh phát hiện trong quá khứ và có thể sẽ hoạt động trở lại. (Linari, A., Buckley, O., Duce, D., Mitchell, F., Morris, S. 2010).

Mariposa là một mạng botnet có nguồn gốc từ Tây Ban Nha, có khả năng đánh cắp hàng triệu đô la từ những người dùng không nghi ngờ bằng cách lấy số thẻ tín dụng và mật khẩu của họ để vào tài khoản của họ trên các trang dịch vụ tài chính. Nó đã sử dụng quảng cáo độc hại - việc sử dụng quảng cáo kỹ thuật số để phát tán phần mềm độc hại - để tiếp quản một con số khổng lồ mười triệu máy, khiến nó trở thành mạng Botnet lớn thứ hai được phát hiện cho đến nay. Tuy nhiên, cơ quan thực thi pháp luật Tây Ban Nha đã có thể dẹp bỏ hoạt động này trong một lần khi họ phát hiện ra hồ sơ của tất cả những người đã trả tiền để thuê mạng (Krebs, B. Krebs. 2010)

Methbot đã mua lại một cách gian lận hàng trăm nghìn địa chỉ IP từ hai cơ quan đăng ký Internet toàn cầu và liên kết chúng với các ISP có trụ sở tại xứ sở cờ hoa. Các nhà điều hành của Methbot đã tạo hơn 6.000 miền và có đến 250.267 URL tách biệt với nhau dường như đến từ các nhà xuất bản cao cấp, yêu cầu các nhà quảng cáo đặt giá thầu trên chúng, sau đó gửi bot của họ để "xem" 300 triệu quảng cáo video mỗi ngày. Methbot đã được White Ops phát hiện và "nhổ" vào năm 2015, nhưng chúng tôi luôn tìm kiếm các dấu hiệu cho thấy nó sẽ xuất hiện trở lại. (Fossi, M., Egan, G., Haley, K., và cộng sự. 2011)

Mạng botnet Mirai đứng sau một cuộc tấn công từ chối dịch vụ (DDoS) phân tán lớn khiến phần lớn Internet không thể truy cập được ở bờ biển phía đông Hoa Kỳ. Nhưng, điều khiến Mirai đáng chú ý nhất là nó là mạng botnet lớn đầu tiên lây nhiễm các thiết bị IoT không an toàn. Vào lúc cao điểm, con sâu này đã lây nhiễm hơn 600.000 thiết bị. Đáng ngạc nhiên nhất Botnet được tạo ra bởi một nhóm sinh viên đại học đang tìm cách đạt được lợi thế trong Minecraft. (Dittrich, D., Dietrich, S. Stevens CS. 2008).

Storm là một trong những mạng botnet ngang hàng đầu tiên được biết đến - tức là nó nằm trong số những mạng đầu tiên được điều khiển bởi một số máy chủ khác nhau. Hệ thống mạng rất lớn, có từ 250.000 đến 1 triệu máy tính bị nhiễm và có thể được cho bất kỳ tên tội phạm nào sẵn sàng trả tiền cho nó trên web đen để thuê. Vì điều này, Storm đã tham gia vào một loạt các hoạt động tội phạm, từ tấn công DDoS để xác định hành vi trộm cắp. Một số máy chủ của Storm đã ngừng hoạt động vào năm 2008 và ngày nay mạng botnet được cho là

ít nhiều không hoạt động. Nói tóm lại tùy vào từng thời điểm cụ thể mà các cuộc tấn công Botnet mang lại những hậu quả và tác hại khác nhau. (Enright, B., Voelker, G., Savage, S., Kanich, C. , Levchenko, K. 2008).

5. Kết luận

Tóm lại, Botnet là một mạng lưới hệ thống máy tính bị chi phối, điều khiển bởi một ai đó, một máy tính từ xa khác. Bonet là một phần mềm vô cùng độc hại cho máy, hầu hết thì các máy hiện nay đều bị nhiễm Botnet nào đó mà các bạn không thể biết đã bị nhiễm từ bao giờ. Một khi bị nhiễm, máy sẽ bị điều khiển mọi hoạt động trên máy bởi một Botmaster. Điều này sẽ gây cản trở hoạt đông, giảm năng suất hiệu quả giải quyết công việc của người dùng. Việc máy bạn bị nhiễm Botnet tương tự như việc bị lây nhiễm Malware, việc chiếm đoạt lấy những thông tin người dùng để phục vụ cho mục đích riêng của hacker. Bài báo này đã tổng hợp một số thông tin về cách tấn công Botnet cũng như cách phòng ngừa Botnet, hy vọng rằng những thông tin này sẽ hữu ích cho tất cả mọi người đang sử dụng mạng Internet hiện nay.

TÀI LIỆU THAM KHẢO

[1] Citron DK(2006). Số liên lạc tối thiểu trong một thế giới không biên giới: thoại qua Internet giao thức và sự bùng nổ sắp tới của lý thuyết quyền tài phán cá nhân, Luật UC Davis Ôn tập. 20/1/2021,
<https://nhandan.com.vn/thong-tin-so/Internet-day-2020-in-dam-dau-chan-so-cua-viet-nam-trong-khong-gian-mang-628364/>

[2] Susan CH(2002). Truyền thông qua trung gian máy tính trên Internet. Đại học Indiana, Đánh giá hàng năm về Khoa học Thông tin và Công nghệ.20/1/2021,
<https://thongtinduhoc.org/truong/dai-hoc-indiana-tai-bloomington-inindiana-university-bloomingtona-tieu-bang-indiana-my-421.html>

[3] Bu Z, Bueno P, Kashyap R(2010). Kỷ nguyên mới của Botnet.20/1/2021,
<Available:https://www.mcafee.com/in/resources/white-papers/wp-new-era-of botnet.pdf>

[4] Mansfield-Devine S(2014). Hacking trên một quy mô công nghiệp. An ninh mạng. 20/1/2021,
<https://nhandan.com.vn/thong-tin-so/toan-canh-an-ninh-mang-viet-nam-nam-2020-ton-that-hon-1-ty-usd-do-virus-may-tinh-632235/>

[5] Dell Secure Works(19/2/2016). Đơn vị Chống Đe doạ.Tin tức về mối đe dọa.20/1/2021,
<http://cand.com.vn/Giai-dap-phap-luat/Ban-ve-toi-de-doa-giet-nguoi-theo-quy-dinh-cua-phap-luat-hien-hanh-546205/>

[6] Weyers B(25/10/2016). Ảnh hưởng của Internet đối với Suy nghĩ. Văn học AP. Nd.20/1/2021,
<https://binhthuan.gov.vn/mDefault.aspx?sid=1328&pageid=3641&catid=65573&id=570294&catname=thong-tin-tuyen-truyen&title=mang-xa-hoi-doi-voi-loi-song-cua-thanh-thieu-nien-viet-nam-hien-nay-doc-va-suy-ngam>

[7] Warmer M(2011). Phát hiện dựa trên web kênh lệnh & điều khiển.19/1/2021,
<http://www.cit.ctu.edu.vn/thongtinkh/Tap%20chi%20SoDacBiet(HTCNTT2013)_Full.pdf>

[8] Anomali(2019). APT28 Tiến trình hoạt động độc hại,20/1/2021,
< https://www.bbc.com/vietnamese/world-55733867>

[9] Boshmaf, Y., I. Muslukhov, K. Beznosov, và M. Ripeanu(2013). Thiết kế và phân tích một Botnet xã hội,21/1/2021,
<https://vietnetco.vn/botnet-la-gi-giai-phap-phong-ve-botnet-fortiguard/4999.html>

[10] Chen, W., và cộng sự(2017). CloudBot: Botnet di động tiên tiến sử dụng công nghệ đám mây phổ biến.20/1/2021,
<https://synologyvietnam.vn/dien-toan-dam-may-danh-cho-doanh-nghiep-o-viet-nam/>

[11] Feily, M., A. Shahrestani và S. Ramadass(2009). Khảo sát về Botnet và Phát hiện Botnet. 20/1/2021,
<http://www.itk.ilstu.edu/faculty/ytang/botnet/3%202009-A%20Survey%20of%20Botnet%20and%20Botnet%20Detection.pd>

[12] Hyslip, T. và J. Pittman(2015). Một cuộc khảo sát về các kỹ thuật phát hiện Botnet bằng cơ sở hạ tầng lệnh và điều khiển.20/1/2021,
<http://antoanthongtin.gov.vn/gp-attm/hai-phuong-phap-phat-hien-botnet-truc-tuyen-moi-101775>

[13] Kudo, T., và cộng sự(2018). Mô hình ngẫu nhiên của các Botnet tự phát triển với khả năng phát hiện lỗ hổng.20/1/2021,
<http://antoanthongtin.gov.vn/gp-attm/hai-phuong-phap-phat-hien-botnet-truc-tuyen-moi-101775>

[14] Wang, P., et al(2007). Một Botnet Peer-to-Peer lai tiên tiến.20/1/2021,
<http://www.eecs.ucf.edu/~czou/research/P2PBotnetsbookChapter.p>

[15] Yuan, Z., Lu, Y., Wang, Z., Xue, Y.(2014) 'DroidSec: deep learning trong phát hiện phần mềm độc hại android', được trình bày tại ACM SIGCOMM Computer Communication Review. 20/1/2021,
<http://www.antoanthongtin.vn/gp-atm/phat-hien-ma-doc-iot-botnet-dua-tren-do-thi-psi-voi-mo-hinh-skip-gram-105864>

[16] Saxe, J., Berlin, K(2015). 'Phát hiện phần mềm độc hại dựa trên mạng nơ-ron sâu bằng cách sử dụng hai Tạp chí Khoa học và Công nghệ về An toàn Thông tin. 20/1/2021,
<http://tapchikhcn.udn.vn/OrtherFile/2017_8_21_14_29_796tapchikcnso5(114)%20q.2%20(ngay16.08)%20.pdf>

[17] M. Sanchez(2017). "Giải thích 10 mối đe dọa bảo mật phổ biến nhất". 20/1/2021,
<https://www.who.int/vietnam/vi/news/feature-stories/detail/ten-threats-to-global-health-in-2019>

[18] Us.norton.com(năm 2017). "Bots và botnet — mối đe dọa ngày càng tăng". 20/1/2021,
<https://quantrimang.com/tim-hieu-ve-nhung-moi-de-doa-an-rootkit-va-botnet-35106>

[19] B. Cusack và S. Almutairi(12/2014). Lắng nghe các kênh truyền thông botnet để bảo vệ hệ thống thông tin, trong Kỷ yếu của Hội nghị Pháp y Kỹ thuật số Australia. 20/1/2021,
<B.Cusack và S. Almutairi(12/2014). Lắng nghe các kênh truyền thông botnet để bảo vệ hệ thống thông tin, trong Kỷ yếu của Hội nghị Pháp y Kỹ thuật số Australia>

[20] Linari, A., Buckley, O., Duce, D., Mitchell, F., Morris, S(2010). Một phương pháp luận để phát hiện và xác định đặc điểm bất thường và mạng botnet từ nhật ký ứng dụng. 20/1/2021,
< https://vi.wikipedia.org/wiki/Botnet>

[21] G. Kirubavathi và R. Anitha(2016). Phát hiện botnet thông qua khai thác các đặc điểm của luồng lưu lượng. Máy tính & Kỹ thuật Điện. 20/1/2021,
<https://www.microsoft.com/vivn/windows/windows10specification>

[22] D. Zhao, I. Traore, B. Sayed và cộng sự(2013). Phát hiện botnet dựa trên phân tích hành vi lưu lượng và khoảng thời gian lưu lượng. Máy tính & Bảo mật. 20/1/2021,
<https://ehealth.gov.vn/?action=News&newsId=46923>

[23] C Y. Huang(2013). Phát hiện máy chủ bot hiệu quả dựa trên các mô hình Lỗi mạng. Mạng Máy tính. 20/1/2021,
<https://tintuc.wecvietnam.org/>

[24] G. Zhao, K. Xu, L. Xu và B. Wu(2015). Phát hiện nhiễm phần mềm độc hại APT dựa trên phân tích lưu lượng và DNS độc hại. 20/1/2021,
<https://ehealth.gov.vn/?action=News&newsId=53618>

[25] R. Abdullah, M. Faizal, và Z. Noh(2014). Theo dõi các hành vi của mạng botnet P2P thông qua phương pháp phân tích kết hợp. 20/1/2021,
<https://files.ais.gov.vn/portal/attt/source_files/2017/09/18/08433279_DuthaoDeAnPhongChongPMDH_17-09-18.pdf>

[26] Ferguson, R. Trend Micro(2010). Biên niên sử Botnet - Biên niên sử
<https://www.trendmicro.co.uk/media/wp/botnetchronicleswhitepaenpdf>

[27] Caballero, J., Grier, C., Paxson, V., Song, D(2010). Insights từ bên trong: Một cái nhìn về quản lý Botnet từ sự xâm nhập. 20/1/2021,
<https://123doc.net/document/4361643-theo-doi-va-giam-sat-mang-bang-botnet-tracking.htm>

[28] B., Sharma, V.,Ni viện, C., Kang, B., Dagon, D(2007). Botnet ngang hàng: Tổng quan và Nghiên cứu điển Grizzard, J. 20/1/2021,
<https://www.trendmicro.co.uk/media/wp/botnetchronicleswhitnpd>

[29] Krebs, B. Krebs(2010). Trung tâm cuộc gọi cho tội phạm máy tính. về An ninh.20/1/2021,
<http://krebsonsecurity.com/2010/04/call-centers-for-computer-criminals/.>, xem 17/9/2021

[30] CyberInsecure(2008). Bộ công cụ và dịch vụ Botnet được cung cấp cho người không phải là công nghệ. 20/1/2021,
<http://cyberinsecure.com/botnet-kit-and-service-offered-to-non-techies>

[31] Hao S., Feamster, N(2008). Ước tính Quần thể Botnet từ Lưu lượng Tấn công.20/1/2021/
<http://www.cit.ctu.edu.vn/thongtinkh/Tap%20chi%20SoDacBietTCNTT2013)_Full.pdf>

[32] Nguyễn Trọng Hưng, Hoàng Xuân Dậu, Vũ Xuân Hạnh(12/2018). "Phát hiện Botnet dựa trên phân loại tên miền sử dụng các kỹ thuật học máy," Tạp chí Thông tin và Truyền thông. 20/1/2021,
<https://quantrimang.com/botnet-hoat-dong-nhu-the-nao-36773>

[33] Zhichun Li, Anup Goyal và YanChen(2007). Phân tích lưu lượng truy cập quét Botnet dựa trên Honeynet. 20/1/2021,
<https://www.researchgate.net/publication/333679588_SoIS-2018-Phat_hien_botnet_dua_tren_hoc_may>

[34] Enright, B., Voelker, G., Savage, S., Kanich, C. , Levchenko, K(2008). Storm: Khi các nhà nghiên cứu va chạm. 20/1/2021,
<http://www.cit.ctu.edu.vn/thongtinkh/Tap%20chi%20SoDacBiet(HTCNTT2013)_Full.pdf>

[35] Dittrich, D., Dietrich, S. Stevens CS(2008). Kỹ thuật khám phá mạng botnet P2P. Báo cáo kỹ thuật 2008-4. 20/1/2021,
<http://www.antoanthongtin.vn/gp-atm/phat-hien-ma-doc-iot-botnet-dua-tren-do-thi-psi-voi-mo-hinh-skip-gram-105864>

[36] Krebs, B. Krebs về An ninh(2010). Mariposa 'Các tác giả botnet có thể tránh được thời gian ngồi tù',

<http://krebsonsecurity.com/2010/03/mariposa-botnet-authors-may-avoid-jail-time>, 20/1/2021

[37] Fossi, M., Egan, G., Haley, K., và cộng sự(2011). "Xu hướng Báo cáo Đe dọa An ninh Internet Symantec," Báo cáo Đe dọa An ninh Internet Symantec
<https://www.microsoft.com/vivn/windows/windows10specification>

[38] K. Alieyan, A. Almomani, A. Manasrah và, M.M. Kadhum(2017). "Một cuộc khảo sát phát hiện botnet dựa trên DNS," .20/1/2021,
<https://www.trendmicro.co.uk/media/wp/botnetchronicleswhitepaenpdf>

[39] Wang, P., et al. (2007). Một Botnet Peer-to-Peer lai tiên tiến.20/1/2021,
<http://congvinhlinh.ictquangtri.vn/vanhoaxahoi/modid/405/itemid/>

[40] Rege, A. (2014). Xu hướng chiến tranh thông tin kỹ thuật số ở Âu-Á. Tạp chí An ninh 4.20/1/2021,
<https://ehealth.gov.vn/?action=News&newsId=53618>

[41] Karim, Ahmad. (2014). Kỹ thuật phát hiện botnet: xem xét, xu hướng trong tương lai và các vấn đề. Tạp chí Khoa học-Đại học Chiết Giang .20/1/2021,
<https://www.duhoctrungquoc.vn/university/hocvientruyenthongchiet-giang-hang-chau-trung-quoc.html>

[42] Công cụ tấn công từ chối dịch vụ phân tán "Stacheldraht".1999.20/1/2021,
< https://kontum.gov.vn/pages/detail/6678/Thong-tin-can-biet.html>

[43] Dietrich, S., Long, N(2020). Phân tích về công cụ từ chối dịch vụ phân tán "Shaft". 20/1/2021,
<https://www.trendmicro.co.uk/media/wp/botnetchronicleswhitnpd>

[44] Các vấn đề pháp lý trong Giảm thiểu Botnet. Báo cáo ENISA, sẽ xuất hiện, 2011.20/1/2021,
<https://ssd.eff.org/vi/glossary/t%E1%BA%A5nc%C3%B4ngt%E1-ch%E1%BB%91i-d%E1%BB%8Bch-v%E1%BB%A5ph%C3%A2n-t%C3%A1n>

[45] Báo cáo phần mềm độc hại năm 2007: Tác động kinh tế của vi rút, phần mềm gián điệp, phần mềm quảng cáo, Botnet và Mã độc hại khác; 2007.20/1/2021,
<https://www.digistar.vn/tan-cong-tu-choi-dich-vu-dos-va-ddos-phan1/>

[46] A Survey, D. Seenivasan, K. Shanthi(2020). Các hạng mục của Botnet.20/1/2021,
<http://cyberinsecure.com/botnet-kit-and-service-offered-to-non-techies>

[47] Siciliano(2011) R7 động lực của Hacker.20/1/2021,
<https://tintuc.wecvietnam.org/>

[48] 10 Câu hỏi Khó về Giảm thiểu Botnet. Báo cáo ENISA; 2011.20/1/2021,
<http://cyberinsecure.com/botnet-kit-and-service-offered-to-non-techies>

[49] Cantón, D., (2015). Phát hiện botnet thông qua các phương pháp tiếp cận dựa trên DNS. 20/1/2021,
<https://www.bbc.com/vietnamese/world-55733867>

[50] Shipp, A. (2010). RSA Bài học trong Botnet: Hậu quả của việc gỡ bỏ ISP.20/1/2021,
https://nhandan.com.vn/thong-tin-so/Internet-day-2020-in-dam-dau-chan-so-cua-viet-nam-trong-khong-gian-mang-628364/