SỰ PHÁT TRIỂN CỦA MALWARE TRONG 10 NĂM TRỞ LẠI ĐÂY

Ngô Hồ Anh Khôi[3], Trương Minh Cảnh[4]

Tóm tắt: *Ngày nay, công nghệ ngày càng phát triển mạnh mẽ và được sử dụng rộng rãi trên toàn cầu, do đó, việc thường xuyên xuất hiện những rủi ro là điều mà người dùng internet ngày nay không thể nào tránh khỏi. Chính vì vậy, nhiều hình thức xâm nhập đã ra đời với mục đích phá hoại hay trục lợi cá nhân được phát triển qua nhiều thế hệ máy tính. Với những phần mềm độc hại mang tính phá hoại cao hay các tập tin được ẩn những mã độc cực kỳ nguy hiểm được đính kèm cho nạn nhân được phát triển rộng trong giới tin tắc. Bài báo không đi sâu vào từng thể loại malware, mà tổng hợp nhằm khái quát hóa lại tiến trình phát triển của Malware trong chu kỳ 10 năm trở lại đây, thông qua việc tìm hiểu về đặc tính, cách lấy lan, cách hoạt động và phòng chống của từng loại.*

Từ khóa: *Malware, các loại Malware, cách thức hoạt động, hậu quả và cách phòng tránh.*

Abstract: *Today, technology is strongly developed and is globally used,so risks originated from it is unavoidable. Therefore, many infiltration forms have been created and developed to annihilate or exploit systems over generations. Malicious software, highly destructive viruses or hidden files with extremely dangerous toxic codes have been being popularized. Developers and software experts have have been trying to fix vulnerabilities of previous products. The advantages and disadvantages of anti-intrusive software to help users protect personal information or private materials leads to the need of referring to the article about Malware so that users can gain more knowledge or rectify wrong information.*

Keywords: *Malware, Malware types, how it works, consequences and how to avoid it.*

1. Giới thiệu

1.1. Lịch sử hình thành Phần mềm độc hại (Malware)

Được viết tắt từ cụm từ tiếng Anh là "Malicious Software" là một chương trình hay một tệp tin nào đó bất kỳ có thể gây hại đến người dùng máy tính mà nạn nhân không hề hay biết. Malware bao gồm các chủng loại khác nhau tương ứng với cách thức hoạt động hoặc tấn công theo một cơ chế đặc trưng của mình như virus máy tính, worms, trojan và phần mềm gián điệp (spyware),... nhưng cùng chung một mục đích là gây hại đến máy tính của người dùng. Các loại malware độc hại này có thể dễ dàng thực hiện nhiều chức năng như lấy cắp thông tin, mã hóa

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

hay trực tiếp loại bỏ các dữ liệu nhạy cảm, tự do giám sát các hoạt động của máy tính đã bị lây nhiễm mà chưa được sự cho phép của nạn nhân. (Tuấn Phong, 2019)

Với sự phổ biến và đa dạng của Virus mà lịch sử phát triển của malware được bắt nguồn từ Virus. Vì sự đa dạng của Virus cho nên kèm theo đó là một số nhận định khác nhau về lịch sử của Virus điện toán. Chúng ta hãy cùng tìm hiểu chi tiết về các loại virus qua các thời kỳ được cho là các quan điểm được thống nhất.

John Von Neuman đã phát triển nền tảng lý thuyết tự nhân bản của một chương trình cho máy tính vào năm 1949. Sau một khoảng thời gian, một chương trình mang tên "Pervading Animal" được ra đời trên các dòng máy Univax 1108 vào năm 1970 với đặc điểm khá đặc biệt là tự nó có thể nối với các phần sau của các tập tin tự hành. Vào thời gian đó vẫn chưa có khái niệm về Virus. Tiếp theo, khoảng hơn mười năm sau các virus đầu tiên được ra đời trong hệ điều hành của máy tính Apple II, tức năm 1981. Fred Cohen định nghĩa khái niệm về computer virus đầu tiên tại Đại học miền Nam California của Hoa Kỳ vào năm 1983. Basit và Amjad đã tạo ra loại virus đầu tiên cho máy tính cá nhân mang tên Virus "the Brain" vào năm 1986. Chương trình này được cài đặt sẵn và nằm trong phần khởi động của một đĩa mềm 360 Kb, với chức năng đặc biệt này nó sẽ lây nhiễm cho tất cả các ổ đĩa mềm, được nhận định là loại "stealth virus" đầu tiên. Virus "Virdem" được khám phá bởi DOS vào cuối năm 1986 với mục đích phá hoại các máy tính VAX/VMS bằng khả năng tự chép mã của mình vào các tệp tự thi hành. Virus "Lehigh" là con virus đầu tiên được biết đến với việc tấn công vào commad.com vào năm 1987. Virus "Jerusalem" là một loại virus với cấu tạo và hoạt động theo đồng hồ của máy tính đã tấn công đồng loạt vào các trường đại học và các công ty trong các quốc gia vào thứ 6 ngày 13 năm 1988.

Một sinh viên đã tốt nghiệp ngành khoa học máy tính tại Đại học Cornell là Robert Tappan Morris đã tung ra "Worms" đầu tiên và được gọi là sâu "Morris" với mục đích là chiếm cứ các máy tính của ARPANET đã làm tê liệt hàng nghìn máy tính vào tháng 11 năm 1988. Sau khi bị khởi tố và ra tòa, Morris đã bị phạt 10.000 dollar và mức án 3 năm tù với lời khai tạo ra loại virus này là vì chán đời. Với mối nguy hiểm từ virus gây ra thì Norton đã cho ra đời một chương trình thương mại chống virus đầu tiên vào năm 1990. Virus đa hình được ra đời và mang một cái tên là virus "Tequilla", được ra đời vào năm 1991 với khả năng tự thay đổi được hình thức của mình đã tạo ra nhiều khó khăn cho các chương trình chống lại virus. Lợi dụng những người thiếu hiểu biết về virus, thảm họa virus đầu tiên xuất hiện vào năm 1994 trên các email và được lan truyền khắp nơi vì các nạn nhân đã có lòng tốt truyền tải cho các người sử dụng máy tính thời bấy giờ. Virus macro đầu tiên được xuất hiện vào năm 1995, được phát hiện bởi các mã macro trong các tệp của "word office" và lây lan qua rất nhiều máy và có khả năng làm hỏng hệ điều hành chủ và được phát triển đến năm 1997 đã tấn công vào hơn 1 triệu máy và dừng khi đến năm 1999 virus "trisate" ra đời.

Virus "love bug" được ra đời vào năm 2000 với cách lây lan qua email với dòng chủ đề tràn đầy yêu thương và được nhận định là một chủng loại của macro virus. Một loại worms được lây lan với tốc độ kỷ lục vào năm 2003 mang tên virus "slammer" đã truyền cho khoảng 75 nghìn máy chỉ trong vòng 10 phút. Vào năm 2004 một hacker trẻ tuổi người Đức Sven Jaschan đã phát tán worm "sasser" với khả năng chỉ cần xem thư mà không cần ấn vào các tệp đính kèm, mặc dù không hủy hoại hoàn toàn máy tính của nạn nhân nhưng loại worm này đã làm cho máy chủ trở nên chậm đi và có khả năng tự khởi động.

1.2. Các hình thức lây nhiễm

Virus lây nhiễm theo cách cổ điển: Bằng phương pháp lây lan cổ điển của các loại virus là nhờ vào các thiết bị lưu trữ di động như các thời kỳ đầu thì người ta sử dụng đĩa mềm và các loại đĩa CD để lưu trữ các chương trình đã bị lợi dụng để phát tán các loại virus. Nhưng ngày nay, đa số không còn mấy ai sử dụng 2 loại trên thì các phương pháp được nhắm đến là các loại ổ USB, các ổ đĩa cứng di động hay các thiết bị kỹ thuật số dùng để giải trí. (Minh Nguyen, 2020)

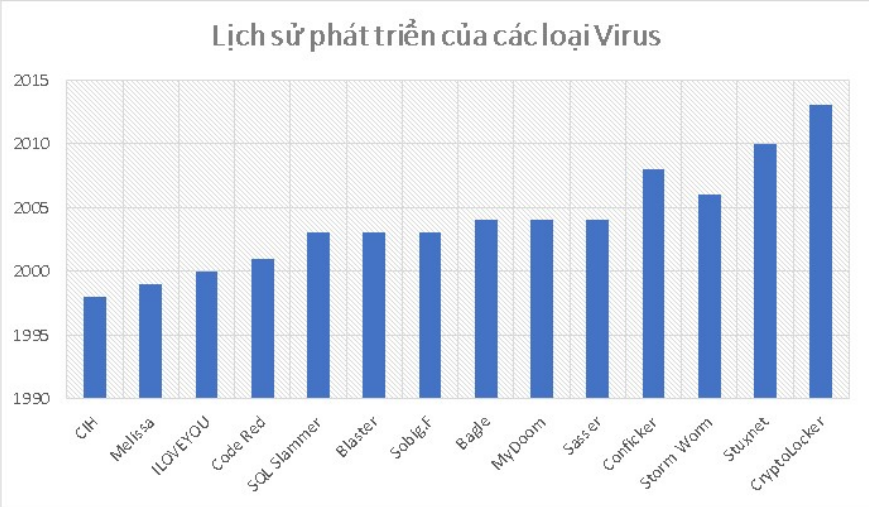
Virus lây nhiễm qua thư điện tử bao gồm 3 loại: Lây nhiễm vào các file đính kèm theo thư điện tử có nghĩa là máy tính của người dùng bị lây nhiễm virus khi người dùng tác động đến các tệp đã được ngụy trang và ẩn chứa nhiều loại virus được gửi kèm mà người dùng không hề hay biết; Lây nhiễm do mở một liên kết trong thư điện tử là một số đường dẫn được gửi kèm trong thư sẽ kích hoạt virus khi người dùng nhấn vào liên kết, trình duyệt sẽ chuyển đến một trang web khác chứa đầy những nguy hiểm không lường trước được; Lây nhiễm ngay khi mở thư điện tử là một hình thù đặc biệt nguy hiểm, với loại trá hình này sẽ khiến máy tính người dùng lập tức bị nhiễm virus trong khi chỉ click vào đọc thư. (Quang Nguyen, 2019)

Virus lây nhiễm qua mạng internet cũng bao gồm 3 dạng giống như thư điện tử như: Lây nhiễm thông qua các file tài liệu, phần mềm là một dạng lây nhiễm thuộc loại cổ điển như tải dữ liệu từ Internet thông qua các phần mềm; Lây nhiễm khi đang truy cập các trang web được cài đặt virus là khi người dùng truy cập vào một trang web đã được cài đặt virus sẵn; Lây nhiễm virus hoặc chiếm quyền điều khiển máy tính thông qua các lỗi bảo mật hệ điều hành, ứng dụng sẵn có trên hệ điều hành hoặc phần mềm của hãng thứ ba là dựa vào lỗi bảo mật của hệ điều hành để khai thác triệt để nhằm lây nhiễm virus và chiếm quyền kiểm soát. (Quang Nguyen, 2019)

2. Malware hình thành và phát triển từ năm 1940 đến năm 2010

2.1. Virus máy tính

Tồn tại chỉ là những đoạn mã chương trình được thiết kế ra nhằm mục đích xâm nhập vào máy tính để ăn cắp thông tin, xóa các dữ liệu, gửi email nặc danh và tự động nhân bản để lây lan và theo thống kê thì đa phần virus chỉ tấn công vào hệ điều hành Windows vì hệ điều hành này đang được sử dụng phổ biến trên toàn cầu. (Hoàng Tuấn, 2019)



Hình 1: Các loại virus được ra đời

Được viết dưới dạng là một routine, nó sẽ tự động sửa tham số địa chỉ của lệnh trỏ đến một địa chỉ riêng của nó và sau khi kết thúc virus sẽ chuyển đến routine được gọi trước đó và hoạt động dưới dạng mã lệnh thông qua việc lây lan với các hình thức khác nhau và càng ngày càng tinh vi hơn.

Có thể phân loại virus như sau: Qua e-mail, dựa trên sự tin tưởng của các người trong danh sách liên lạc email mà không đề phòng nên hacker tự động gửi mail hàng loạt và khi click vào tệp đính kèm, đường dẫn liên kết hay các nội dung có trong email thì ngay lập tức virus nhanh chóng lây lan theo cấp số nhân; Qua Internet, là phương pháp phổ biến nhất hiện nay khi có khả năng lây nhiễm qua các tệp tài liệu, phần mềm hay do truy cập không chủ ý vào website đã nhiễm virus. Ngoài ra virus có thể tấn công vào hệ điều hành dựa vào các lỗ hổng bảo mật. (Giang, 2018a)

Cách phòng chống virus hiệu quả là cài đặt phần mềm diệt virus. Sử dụng tường lửa bảo mật như phần mềm hay phần cứng. Cập nhật thường xuyên các bản vá lỗi hệ điều hành. Nên trang bị cho mình kiến thức về sử dụng máy tính. Nên sao lưu dữ liệu và tạo ra vài dữ liệu phục hồi cho toàn bộ hệ thống.

2.2. Worms

Được biết đến là một phần mềm có sức lây lan với tốc độ nhanh chóng, rộng và phổ biến nhất hiện nay. Khác với Virus, Worm không cần phải liên lạc với các tập tin mồi để lây nhiễm và tự động nhân bản và lây nhiễm qua môi trường Internet, P2P và các dịch vụ chia sẻ. Vào khoảng năm 1975, thuật ngữ về sâu máy tính được ra đời. Mang trong mình một chức năng đặc biệt là tự động thu thập dữ liệu và cuộc tấn công đầu tiên vào năm 1988 đã tung ra sâu đầu tiên hay sâu Morris và có khả năng làm tê liệt bất cứ thứ gì trên hệ điều hành UNIX nào đang kết nối vào Internet. (Thaipro, 2015)

Cách thức hoạt động: Dựa vào lỗ hổng trong giao thức mạng để lây lan mà không cần các tác động bên ngoài. Được biết đến là một phần mềm tồn tại độc lập sâu máy tính không cần lừa nạn nhân kích hoạt bất kỳ thứ gì. Với khả năng tự động phát tán email thông qua hệ thống mail một cách dễ dàng. Sâu máy tính thông thường chỉ là các tệp thực thi hay các tập lệnh được đính kèm theo mail. (Trinhnk, 2018)

Cách phòng chống worms hiệu quả là cài đặt phần mềm diệt virus. Sử dụng tường lửa bảo mật như phần mềm hay phần cứng. Cập nhật thường xuyên các bản vá lỗi hệ điều hành. Nên trang bị cho mình kiến thức về sử dụng máy tính. Nên sao lưu dữ liệu và tạo ra vài dữ liệu phục hồi cho toàn bộ hệ thống. Nên sử dụng các mật khẩu mang tính chất bảo mật cao.

2.3. Trojan

Hóa thân là một loại mã độc được ngụy trang khi xâm nhập vào máy tính của người dùng, sau khi tấn công thành công hệ thống máy tính của người dùng trở nên bị hỗn loạn. Tuy không tự lây lan như virus và rất dễ bị loại bỏ nhưng với bản năng tấn công theo dây chuyền rất có thể Trojan đã xâm nhập hàng loạt vào hệ thống người dùng khi được phát tán lên mạng. Được đánh giá là một loại cực kỳ nguy hiểm khi có thể hủy toàn bộ dữ liệu và ổ cứng. (Chien Tran, 2014)

Mục đích được tung ra là ăn cắp thông tin của credit card, lấy cắp toàn bộ thông tin tài khoản cá nhân, dữ liệu và thông tin tài chính. Và mục đích cuối cùng là dùng máy tính của nạn nhân để thực hiện một số tác vụ như các cuộc tấn công, quét các lỗ hổng của hệ thống và làm ngập hệ thống mạng của nạn nhân. (Aviva Zacks, 2018)

Cách thức hoạt động ẩn sâu mình bằng nhiều hình thức khác nhau từ phần mềm, hình ảnh, các link, quảng cáo hay các bài hát dưới mác an toàn và hợp pháp. Khi tấn công, các phần mềm gián điệp sẽ nhanh chóng xâm nhập vào hệ thống máy tính và chờ đợi tín hiệu của hacker và chỉ đợi khống chế toàn bộ dữ liệu cá nhân của người dùng. Không giống như virus, trojan tấn công dưới dạng một chương trình hay phần mềm khác và không tự lây lan. (Tuấn Phong, 2020b)

Cách phòng chống Trojan hiệu quả là không nên mở bất kỳ tập tin, link hay các phần mềm không an toàn. Sử dụng tường lửa bảo mật như phần mềm hay phần cứng. Cập nhật thường xuyên các bản vá lỗi hệ điều hành. Nên trang bị cho mình kiến thức về sử dụng máy tính. Nên sử dụng phần mềm diệt virus tiên tiến nhất. (Giangpth, 2018)

2.4. Phishing

Năm 1987 phương thức Phising được nhiều người biết đến với hình thức tấn công mạng mạnh mẽ. Được ra đời với ý tưởng kết hợp hai từ Fishing và Phreaking nhằm vào các mục đích lừa đảo người dùng chia sẻ các thông tin như tên đăng nhập, mật khẩu giao dịch và những thông tin nhạy cảm khác của họ dựa vào phương thức mạo danh các tổ chức lớn và có uy tín như các công ty lớn, ngân hàng và các trang web giao dịch trực tuyến. Nếu như người dùng chưa hiểu biết về kiểu tấn công mới này thì Phishing thật sự là một mối đe dọa lớn đối với người dùng. (Quách Chí Cường, 2019a)

Cách thức tấn công của Phishing được thực hiện bằng cách thông qua spam email sẽ cung cấp cho người dùng một liên kết trong email và đưa họ đến một trang web giả mạo và yêu cầu cung cấp những thông tin nhạy cảm. Lợi dụng sự tin cậy của các địa chỉ người dùng trong một email quen thuộc và yêu cầu cung cấp thông tin nhạy cảm. Gắn vào một mã độc kèm theo email hoặc các quảng cáo được gửi vào email của người dùng và dựa vào lỗ hổng đã được khai thác và ăn cắp thông tin. Web-based Delivery dựa trên việc phát tán các website lừa đảo đã được xem là một biến thể khác của Phishing. Dựa vào việc làm kiếm tiền qua các trang web, người dùng cần phải cung cấp thông tin của tài khoản ngân hàng của mình để thu phí dịch vụ. Mặc dù vậy, các hacker thường tối ưu việc giao dịch này để đưa người dùng đến một trang web giả mạo khác và số tiền mà nạn nhân kiếm được từ các trang web không còn thuộc về họ nữa. Thông qua việc tò mò của người dùng, các hacker chèn quảng cáo vào trang web và chỉ chờ đợi sập bẫy khi máy tính của nạn nhân đã bị nhiễm một loại Malware nào đó nhằm phục vụ một cuộc tấn công tiếp theo. (Nguyen Duc Minh, 2014)

Giải pháp nên dùng đối với cá nhân là nên hạn chế trả lời các email rác yêu cầu xác thực hay các thông tin cá nhân. Không click vào các link rác nếu như cảm thấy không an toàn. Nên sử dụng tường lửa và các phần mềm chống virus và phần mềm chống gián điệp. Đối với các doanh nghiệp, tổ chức có thể hướng dẫn nhân viên và thực hành các buổi tập huấn với các tình huống giả mạo nhằm mục đích xấu. Khai thác các bộ lọc SPAM để phát hiện ra virus. Thiết lập vài giải pháp chống virus, cập nhập các chữ ký thường xuyên và theo dõi tình hình kháng virus trên mọi thiết bị. Mã hóa toàn bộ thông tin quan trọng. (Quách Chí Cường, 2019a)

3. Malware phát triển từ năm 2010 cho đến nay

Dựa trên nền tảng đã có sẵn ở thế hệ trước, phần mềm độc hại được phát triển lên một tầm cao mới với nhiều biến thể được ra đời nhằm vào mục đích xấu như trước đó đã làm. Ngày nay, đa số các phần mềm độc hại chỉ được phát triển từ thế hệ trước đó và một số phần mềm độc hại khác được ra đời do nhu cầu của người dùng, đó là nguyên nhân dẫn đến việc các biến thể được hình thành và gây ra nhiều thiệt hại nặng nề. Hãy cùng tìm hiểu về các chủng loại mới và các biến thể của malware từ năm 2000 đến nay. (Tinhbigcoin, 2020)

3.1. Spyware

Một số tài liệu về Spyware được xuất hiện trên một tờ báo vào năm 1996, các thuật ngữ Spyware đã trở thành một thông cáo của báo chí trong ngành vào năm 1999 và trở thành một đề tài thu hút mạnh mẽ trên các phương tiện truyền thông lúc bấy giờ. Ứng dụng chống Spyware lần đầu tiên được phát hành vào năm 2000 và sau đó 4 năm, America Online và Liên minh an ninh mạng quốc gia đã thực hiện cuộc khảo sát và thu được sự ảnh hưởng của Spyware tới người dùng tức năm 2004 như sau: Tầm ảnh hưởng của Spyware chiếm đến 80% lên hệ thống của người dùng Internet, khoảng 93% máy tính của người dùng bị nhiễm Spyware, gần 90% người dùng máy tính đã không hề hay biết sự tồn tại của Spyware ở trên thiết bị của mình, chiếm đến 95% người dùng đã cho biết Spyware không hề được họ cài đặt vào máy tính.

Ngày nay, Spyware đã phát triển và tinh vi hơn khi đã xâm nhập vào hệ điều hành Windows do sự phổ biến của hệ điều hành này. Nhưng thực tế, hệ điều hành của Apple và các thiết bị di động hiện hành cũng đang chịu sự đe dọa tương tự khi tính phổ biến của Spyware là không thể cản phá. (Quách Chí Cường, 2019b)

Cách thức xâm nhập cũng tương tự như các loại Malware khác, Spyware phát tán dựa vào một số kỹ thuật phổ biến như: Thông qua lỗ hổng bảo mật (lỗ hổng khi tải xuống các tệp đính kèm hoặc các liên kết trong email, vào các website đã nhiễm mã độc hay click vào các banner quảng cáo); Thông qua các công cụ hỗ trợ người dùng, các hacker đã tạo ra Spyware dưới dạng hỗ trợ như các trình duyệt tăng tốc, tải xuống hay xử lý ổ đĩa vô tình đã bị lây nhiễm Spyware và đặc điểm là khi bạn đã loại khỏi hệ thống công cụ hỗ trợ, thì Spyware vẫn còn tồn tại và tiếp tục hoạt động; Thông qua các chương trình/tiện ích bổ sung thực hiện tương tự như trên, Spyware ẩn trong các file bổ sung đi kèm với phần mềm hay ứng dụng. Thông qua Trojan, Worms và Backdoor; Thông qua Spyware dành riêng cho thiết bị di động (dựa vào các ứng dụng được soạn lại bằng Malcode). (Quách Chí Cường, 2019b)

Spyware được phân loại như sau: Password Stealers được dùng để thu thập các loại mật khẩu hiện hành từ các trang web hoặc hệ thống; Banking Trojans được ra đời với mục đích thu thập các thông tin quan trọng từ các tổ chức tài chính. Infostealers được tạo ra như một ứng dụng quét Spyware trên các máy tính đã bị lây nhiễm nhằm lấy cắp thông tin cá nhân của người dùng. Keylogger là một ứng dụng được ra đời với mục đích theo dõi các thao tác trên bàn phím để thu thập thông tin từ các nguồn và chuyển về cho hacker. (Quang Nguyen, 2020)

Với mục tiêu khác với các loại Malware còn lại, Spyware ra đời chỉ nhắm vào việc thu thập dữ liệu từ người dùng với số lượng lớn. Do đó, tất cả người dùng đều rơi vào tình trạng trở thành mục tiêu của Spyware như hacker có thể spam mail để gửi các tệp thư rác độc hại hay các hình thức lừa đảo khác. Các cổng thông tin tài chính có thể bị tấn công mọi lúc hay các hình thức lừa đảo khác bằng các tài khoản ngân hàng hợp pháp. Người dùng có thể bị tống tiền dựa vào các dữ liệu cá nhân như ảnh, video. (Quách Chí Cường, 2019b)

Cách phòng chống Spyware hiệu quả là đừng bao giờ mở email từ những người nặc danh. Hãy tải các tệp từ các nguồn uy tín, đáng tin cậy. Hãy sử dụng các chương trình bảo mật mạng chất lượng. Cài đặt các phần mềm chống lại Spyware hiện đại nhất. (Quang Nguyen, 2020)

3.2. Adware

Được biết đến là biến thể khác của Spyware được nhận diện vào năm 1995 và đã được các chuyên gia bảo mật chỉ ra các đặc điểm khác biệt đó là tính nguy hiểm bị hạn chế. Sau đó, các nhà phát triển đã tự ý thay đổi kết cấu khi chưa được các đối tác đồng ý và dẫn đến sự xuất hiện đại trà khiến người dùng lo sợ vào giai đoạn 2005 - 2008. Đến thời điểm hiện tại, Adware được xem là mối đe dọa nguy hiểm xếp sau Malware và đang có sự cải tiến mới nhờ vào các kỹ thuật hỗ trợ như Trojan ẩn. (Quách Chí Cường, 2019c)

Thông qua các phần mềm miễn phí, Adware xâm nhập dựa vào các phần mềm hỗ trợ người dùng mà nhà cung cấp đưa ra với mục đích kiếm doanh thu từ quảng cáo; Hoặc xâm nhập bất hợp pháp tương tự Spyware, Adware dựa vào các lỗ hổng từ trình duyệt để tự động tải xuống vào ổ đĩa. Sau khi tấn công thành công, lập tức tiến hành thu thập toàn bộ dữ liệu, điều hướng trang web và chèn vào các quảng cáo tùy thích. (Nhật Vượng, 2018)

Mục đích chính của Adware là nhắm vào người dùng cá nhân. Khi tấn công vào máy tính thành công, nó sẽ theo sát đối tượng trên mọi thiết bị như điện thoại di động hay các máy tính và đến các trình duyệt nằm trong thiết bị.

Adware được phân loại như sau: Windows adware là các quảng cáo thường xuyên xuất hiện, tự động thay đổi giao diện trình duyệt, truy cập trang web hiển thị sai lệch, tự động chuyển hướng khi chưa yêu cầu, tốc độ truy cập bị hạn chế. Mac adware tương tự như Windows adware, nhưng được phát triển khi có thể tấn công vào macbook thay vì phiên bản cũ đã được ban hành vào năm 2012. Cuối cùng là Mobile adware là hiển thị quảng cáo pop-up đưa vào mã Javacript và tồn tại song song với các phần mềm miễn phí. (Quách Chí Cường, 2019c)

Cách phòng chống adware hiệu quả: Xem thật kỹ trước khi tải các tệp từ trình duyệt xuống, không tự tiện mở các ứng dụng từ các nguồn không an toàn. Cài đặt phần mềm bảo vệ và thường xuyên quét thiết bị để đảm bảo an toàn, sao lưu và truy cập dữ liệu thường xuyên.

3.3. Malvertising

Được biết đến là một chương trình quảng cáo độc hại và dựa vào khả năng sử dụng quảng cáo trực tuyến nhằm lây nhiễm các loại phần mềm độc hại đến máy tính người dùng. Vào năm 2008 quảng cáo độc hại lần đầu tiên được ghi nhận dựa vào nhận định mối đe dọa này ẩn náu trên một lỗ hổng trong Adobe Flash và ảnh hưởng đến một số nền tảng khác trên máy tính và được phát triển đến ngày nay. Với việc tồn tại lâu và phát triển qua các giai đoạn và ngày càng trở nên mạnh mẽ vì nó được ưu chuộng và hoạt động linh hoạt. (Bá Điền, 2018)

Mục đích được tạo ra nhằm tấn công vào các hệ thống máy tính lớn, với việc lây lan nhanh chóng mà không bị cản trở nào các hacker đã lây nhiễm cho máy tính bằng một phần mềm tống tiền mang tên là Teslacrypt. Sau khi tấn công hacker nhanh chóng mã hóa các tệp có trên máy tính và yêu cầu nạn nhân thanh toán để được giải mã.

Cách thức hoạt động: Với việc lây nhiễm với tốc độ nhanh chóng và khả năng không cần nhấp vào quảng cáo mà vẫn bị lây nhiễm. Tuy là vậy, nhưng giả thuyết đưa ra vào năm 2015 thì nguyên nhân chính lây lan là do việc cập nhật các phần mềm giả mạo đó chính là Plugin Flash của Adobe. Nó có thể lây lan qua các cảnh báo giả mạo về các phần mềm độc hại và virus độ thiệt hại theo thống kê vào năm 2015 thì ước tính mà Malvertising gây ra lên đến hàng tỷ đô la. (Trần Thùy, 2020)

Cách phòng chống malvertising hiệu quả là nên tắt Flash và Silverlight. Chặn toàn bộ các quảng cáo và tập lệnh, sử dụng phần mềm diệt virus mới nhất và an toàn nhất.

3.4. Rootkit

Được xem là một dạng phần mềm hay một bộ công cụ phần mềm bao che sự tồn tại của một phần mềm khác mà thông thường là các virus xâm nhập vào hệ thống của máy tính vào năm 2005. Với chức năng đặc biệt này rootkit được xem là phần mềm vô hại nhưng song song đó khi nó được kèm theo với các loại mã độc khác thì độ nguy hiểm lớn hơn rất nhiều. (Nguyễn Thu Hà, 2020)

Mục đích của rootkit là cho phép một người nào đó có thể duy trì lệnh và kiểm soát được máy tính mà người dùng không hề hay biết gì. Khi rootkit đã được kích hoạt, trình duyệt điều khiển của rootkit có khả năng thực hiện từ xa các file và thay đổi cấu hình hệ thống trên máy tính. Rootkit trên máy tính nạn nhân lúc này cũng có thể truy cập vào các file nhật ký đồng thời theo dõi việc sử dụng hợp pháp của nạn nhân. (Hồng Nhi, 2020)

Có thể phân loại Rootkit thành các dạng sau: Các rootkit bám dai (chứa mã độc và thực thi thường được kích hoạt mỗi lần hệ thống khởi động); Các rootkit trong bộ nhớ không có các mã độc để lưu lại trông máy và vì thế không thể tồn tại sau khi khởi động lại máy; Các rootkit ở chế độ người dùng. (Hồng Nhi, 2020)

Cách phòng chống rootkit để bảo vệ an toàn là cập nhật các hệ thống chống virus và phần mềm gián điệp, luôn luôn bật tường lửa để an toàn. Sử dụng các biện pháp xác nhận và đừng bao giờ sử dụng các phần mềm từ các nguồn không chính thống. (Nguyễn Thu Hà, 2020)

3.5. Ransomeware

Năm 2005 - 2006, Ransomeware lần đầu tiên được phát hiện tại Nga bằng những bản báo cáo của TrendMicro. Với biến thể của Trojan sau khi tấn công vào máy tính của người dùng thành công, các dữ liệu sẽ được mã hóa và nén thành các file hệ thống bằng mật khẩu và đồng thời tạo ra một file .txt với nội dung muốn lấy lại dữ liệu cá nhân của mình thì nạn nhân cần phải trả phí là 300 USD. Được phát triển sau đó, các Ransomeware đã liên tiếp tấn công đến các file văn bản và hệ thống như file doc và file exe. SMS Ransomeware là một biến thể khác được phát hiện vào năm 2011 với cách thức khác biệt đó là yêu cầu người dùng phải gọi điện hoặc nhắn tin đến số điện thoại của hacker cho đến khi hoàn thành các thủ tục chuyển tiền cho hacker. Một dạng biến thể khác là tấn công vào Master Boot Record của hệ điều hành và khi tấn công vào hệ thống và ghi đè giả mạo bằng MBR. Trong quá trình tấn công máy tính sẽ tự khởi động lại khi tấn công hoàn tất và trong lần tấn công tiếp theo các thông báo từ hacker bằng tiếng Nga sẽ được hiện lên màn hình máy tính của nạn nhân. (Bá Điền, 2019)

3.6. BackDoor

Được xem là một cổng không được thông báo rộng rãi trong một phần mềm hay hệ thống máy tính và cho phép người quản trị viên xâm nhập vào hệ thống để tìm ra nguyên nhân gây ra lỗi hoặc bảo dưỡng. Ngoài ra, đây cũng là một con đường bí mật mà các hacker và gián điệp dùng để truy cập bất hợp pháp. (Vũ An, 2020)

Backdoor thường được chia thành 2 loại: Backdoor vô hại dùng để cập nhập các phần mềm từ xa, theo dõi, tìm ra nguyên nhân lỗi và thực hiện việc bảo trì hệ thống; Backdoor có hại là một chương trình mang tính chất gián điệp và khó phát hiện. Được ra đời vào năm 1983 nhằm mục đích truy cập vào hệ thống siêu máy tính của quân đội được thiết kế mô phỏng cuộc chiến tranh hạt nhân. NSA đã cho ra đời một con chip giúp các cơ quan thực thi pháp luật thu thập và giải mã giọng nói và dữ liệu được truyền qua điện thoại và máy tính năm 1993 và các giai đoạn phát triển sau năm 2000. (Giang, 2018b)

Cách thức hoạt động của Backdoor vô hại là các thủ tục mà trong quá trình sản xuất của các nhà phát triển phần mềm và phần cứng và đôi khi phương pháp này được tạo ra chỉ nhằm vào mục đích dự phòng. Backdoor gây hại được sử dụng các phương pháp tinh vi như đính kèm link độc trong email hay ẩn nấp trong các tệp tải xuống và khả năng tự sau chép và lây lan. Với khả năng hoạt động song song cùng rootkit, sau khi xâm nhập liên khởi động rootkit và thường xuyên che giấu các hoạt động của Internet nhằm tránh tình trạng bị phát hiện. (Giang, 2018b)

Cách phòng tránh backdoor hiệu quả là nên thay đổi mật khẩu mặc định, kích hoạt loại hình xác thực cao và sử dụng nhiều mật khẩu cho từng ứng dụng. Giám sát các hoạt động mạng, nên bật tường lửa để tránh tình trạng xấu. Không nên tải các ứng dụng từ các nguồn trên các trang web. (Hồng Nguyễn, 2020)

4. Kết luận

Trên đây là một vài loại phần mềm độc hại phổ biến và đang được sử dụng rộng rãi ở thời điểm hiện tại. Ngày nay, có nhiều loại phần mềm độc hại khác nhau được cho ra đời nhằm tiếp tục phát triển ở một tầm cao mới để khẳng định khả năng của mình cho dù chỉ là một trong những kỹ thuật cũ nhưng với lớp vỏ mới. Trong một tương lai gần, chắn sẽ có nhiều phần mềm độc hại được tung ra thị trường hơn nữa nhằm vào các mục đích trục lợi cá nhân với một diện mạo mới mà không phải dựa vào các kỹ thuật cổ điển. Do đó, chúng ta cần những chuyên gia về lĩnh vực an ninh mạng với biệt tài của riêng mình là phát triển không ngừng nghĩ việc chống lại các phần mềm độc hại, là làm việc siêng suốt để không có lỗ hỏng trong việc đảm bảo an toàn, là tin tưởng cho người dùng. Chính vì vậy, một số ý tưởng tuyệt đối để bảo vệ cho người dùng là nên sử dụng một số phần mềm chống lại virut có khả năng nhận dạng và phát hiện ngay khi bắt đầu đã xác định dựa trên các hành vi của nó để biết được đây là một phần mềm độc hại chưa xác định được danh tính. Trong tương lai, sẽ có nhiều phương pháp xâm nhập khác có thể đa dạng hơn, tinh vi hơn có thể sửa được, bảo mật được cũng có thể là không thể nào sửa lỗi các phương pháp của các thập kỷ trước. Tất nhiên, các phương pháp khắc phục các lỗi kỹ thuật của các nhà phát hành cũng sẽ được đồng tạo ra nhằm bảo vệ, tạo sự an toàn cho người dùng tin tưởng.

TÀI LIỆU THAM KHẢO

[1] Tuấn Phong, 2019 a, *Malware là gì? Có những loại malware nào?*, truy cập tháng 1 năm 2020, <https://quantrimang.com/10-loai-malware-dien-hinh-58733>.

[2] Phan Khương, 2003, *20 năm lịch sử virus máy tính*, truy cập tháng 1 năm 2020, <https://vnexpress.net/20-nam-lich-su-virus-may-tinh-phan-1-1508391.html>.

[3] Quang Nguyen, 2020, *Virus máy tính là gì?* truy cập tháng 1 năm 2020, <https://quantrimang.com/virus-may-tinh-la-gi-168574>.

[4] Quang Nguyen, 2019, *Virus máy tính là gì? Cách phòng chống và ngăn chặn tác hại của nó*, truy cập tháng 1 năm 2020, <https://www.semtek.com.vn/virus-may-tinh-la-gi/>.

[5] Giang, 2018 a, *Virus máy tính là gì? Bạn có chắc mình đã hiểu đúng về virus máy tính?,* truy cập tháng 1 năm 2020, <https://bizflycloud.vn/tin-tuc/virus-la-gi-ban-co-chac-minh-da-hieu-dung-ve-virus-may-tinh-20180510163151904.htm>.

[6] Hoàng Tuấn, 2019, *Virus máy tính là gì? Cách phòng chống virus máy tính*, truy cập tháng 1 năm 2020, <https://kynguyencongnghe.com/virus-may-tinh-la-gi-cach-phong-chong-virus-may-tinh/>.

[7] Trinhnk, 2018, *Computer Worms - Sâu máy tính là gì*, truy cập tháng 1 năm 2020, <http://topthuthuat.vn/antivirus/sau-may-tinh.html>.

[8] Thaipro, 2015, *Giới thiệu về sâu máy tính*, truy cập tháng 1 năm 2020, <https://thaipro.wordpress.com/2015/12/23/gioi-thieu-ve-sau-may-tinh-phan-1/>.

[9] Chien Tran, 2014 a, *Trojan là gì? Trojan horse là gì? Những hiểu biết cần thiết*, truy cập tháng 1 năm 2020, <https://securitydaily.net/trojan-la-gi-nhung-hieu-biet-can-thiet/>.

[10] Aviva Zacks, 2018, *Trojan Horse là gì và làm thế nào để bảo vệ chống lại nó*, truy cập tháng 1 năm 2020 <https://vi.safetydetectives.com/blog/trojan-horse-la-gi-va-lam-the-nao-de-bao-ve-chong-lai-no/>.

[11] Tuấn Phong, 2020 b, *Trojan là gì? Làm sao để tránh trojan tấn công?*, truy cập tháng 1 năm 2020, <https://quantrimang.com/trojan-la-gi-lam-sao-de-tranh-trojan-tan-cong-168699>.

[12] Giangpth, 2018, *Trojan là gì? - Những điều cần biết*, truy cập tháng 1 năm 2020, <https://bizflycloud.vn/tin-tuc/trojan-nhung-dieu-can-biet-20180510170204207.htm>.

[13] Quách Chí Cường, 2019 a, *Phishing là gì ? Cách phòng tránh tấn công phishing*, truy cập tháng 1 năm 2020, <https://cuongquach.com/phishing-la-gi.html#3_Cac_kieu_tan_cong_phishing>.

[14] Tinhbigcoin, 2020, *Tấn công giả mạo (Phishing) là gì?* truy cập tháng 1 năm 2020, <https://theblock101.com/tan-cong-gia-mao-phishing-la-gi>.

[15] Quách Chí Cường, 2019 b, *Spyware là gì ? Phần mềm gián điệp là gì?*, truy cập tháng 1 năm 2020, <https://cuongquach.com/spyware-la-gi.html>.

[16] Quang Nguyen, 2020, *Spyware là gì? TOP những phần mềm diệt Spyware hiệu quả hiện nay*, truy cập tháng 1 năm 2020<https://www.semtek.com.vn/spyware-la/>.

[17] Quách Chí Cườnng, 2019 c, *Adware là gì ? Làm sao để tránh bị nhiễm Adware?*, truy cập tháng 1 năm 2020, <https://cuongquach.com/adware-la-gi.html>.

[18] Nhật Vượng, 2018, *Tất tần tật những điều bạn cần biết về adware (phần mềm quảng cáo)*, truy cập tháng 1 năm 2020, <https://quantrimang.com/lich-su-spyware-adware-va-co-che-phat-tan-17124>.

[19] Bá Điền, 2018, *Malvertising (Quảng cáo độc hại) là gì?*, truy cập tháng 1 năm 2020, <https://quantrimang.com/malvertising-quang-cao-doc-hai-la-gi-156586>.

[20] Trần Thùy, 2020, *Malvertising là gì? Những cách phòng tránh Malvertising*, truy cập tháng 1 năm 2020, <https://thuthuat.taimienphi.vn/malvertising-la-gi-nhung-cach-phong-tranh-malvertising-45653n.aspx>.

[21] Nguyễn Thu Hà, 2020, *Rootkit là gì? Có những loại rootkit nào?*, truy cập tháng 1 năm 2020, <https://quantrimang.com/rootkit-moi-nguy-hiem-tiem-tang-17800>.

[22] Hồng Nhi, 2018, *Rootkit là gì? Cách quét rootkit nhanh và hiệu quả*, truy cập tháng 1 năm 2020, <https://blog.tinohost.com/cach-quet-rootkit-nhanh-va-hieu-qua/>.

[23] Bá Điền, 2019, *Lý thuyết - Ransomware là gì?* truy cập tháng 1 năm 2020, <https://quantrimang.com/ly-thuyet-ransomware-la-gi-118309>.

[24] Vũ An, 2020, *Backdoor là gì?*, truy cập tháng 1 năm 2020, <https://quantrimang.com /backdoor-la-gi-150119>.

[25] Giang, 2018 b, *Backdoor là gì? Backdoor có lợi hay có hại?*, truy cập tháng 1 năm 2020, <https://bizflycloud.vn/tin-tuc/backdoor-la-gi-backdoor-co-loi-hay-co-hai-20180917100622221.htm>.

[26] Hồng Nguyễn, 2020, *Backdoor là gì? Làm sao để phát hiện và ngăn chặn được backdoor?*, truy cập tháng 1 năm 2020, <https://timviec365.vn/blog/backdoor-la-gi-new9007.html>.

[27] Tấn Muôn, 2018, *Các loại Malware thường thấy và cách bảo vệ máy tính khỏi bị xâm hại*, truy cập tháng 1 năm 2020, <https://www.dienmayxanh.com/kinh-nghiem-hay/malware-la-gi-co-phai-la-virus-khong-cac-loai-malw-1138301>.

[28] Nhật Linh, 2019, *9 việc cần làm khi phát hiện máy tính nhiễm malware*, truy cập tháng 1 năm 2020, <https://quantrimang.com/9-viec-can-lam-khi-phat-hien-may-tinh-nhiem-malware-105641>.

[29] Hoàng Kỷ, 2013, *7 dấu hiệu nhận biết máy tính nhiễm malware*, truy cập tháng 1 năm 2020, <https://nld.com.vn/phong-mach-pc/7-dau-hieu-nhan-biet-may-tinh-nhiem-malware-20130514023359568.htm>.

[30] Cường Mạnh, 2013, *Tìm hiểu về Malware và virus*, truy cập tháng 1 năm 2020, <https://cuumaytinh.com/tim-hieu-ve-malware-va-virus.html>.

[31] Nga bùi, 2018, *Những virus máy tính đáng sợ nhất từ trước tới nay*, truy cập tháng 1 năm 2020, <https://quantrimang.com/10-virus-may-tinh-nguy-hiem-nhat-tu-truoc-toi-nay-69255>.

[32] Vũ Thoa, 2020, *Virus tin học là gì?những thông tin quan trọng không thể bỏ qua*, truy cập tháng 1 năm 2020, <https://timviec365.vn/blog/virus-tin-hoc-la-gi-nhung-thong-tin-quan-trong-khong-the-bo-qua-new6623.html>.

[33] SEMTEK Co,.LTD, 2019, *Virus may tinh la gi? Cach phong chong va ngan chan tac hai cua no*, truy cập tháng 1 năm 2020, <https://medium.com/@semtekcorp/virus-may-tinh-la-gi-cach-phong-chong-va-ngan-chan-tac-hai-cua-no-7882b08a7e63>.

[34] Quang nguyễn, 2019, *Malware là gì? Những biện pháp phòng chống Malware hiệu quả*, truy cập tháng 1 năm 2020, <https://www.semtek.com.vn/malware-la-gi/>.

[35] Nguyễn trang, 2020, *14 phần mềm miễn phí diệt spyware hiệu quả nhất*, truy cập tháng 1 năm 2020, <https://quantrimang.com/5-phan-mem-mien-phi-diet-spyware-hieu-qua-nhat-42845>.

[36] Long vân, 2020, *Virus trojan là gì và có nguy hiểm không?*, truy cập tháng 1 năm 2020, <https://longvan.net/virus-trojan-la-gi-va-co-nguy-hiem-khong.html>.

[37] Lộc ngô, 2019, *Spyware là gì? cách phát hiện và loại bỏ phần mềm gián điệp*, truy cập tháng 1 năm 2020, <https://thuthuat.taimienphi.vn/spyware-la-gi-56079n.aspx>.

[38] Trịnh Duy Thanh, 2019, *Back door là gì? Back door có lợi hay có hại với hệ thống?*, truy cập tháng 1 năm 2020, <https://bkhost.vn/posts/backdoor-la-gi>.

[39] Minh Hằng, 2020, *Phần mềm quảng cáo (Adware) là gì? Cách hoạt động*, truy cập tháng 1 năm 2020, <https://vietnambiz.vn/phan-mem-quang-cao-adware-la-gi-cach-hoat-dong-20200603170444959.htm>.

[40] Duy Vinh, 2020, *Backdoor là gì?*, truy cập tháng 1 năm 2020 <https://thuthuat.taimienphi.vn/backdoor-la-gi-40763n.aspx>.

[41] Chiến Trần, 2018, *Phần mềm gián điệp (Spyware) là gì?*, truy cập tháng 1 năm 2020, <https://securitydaily.net/phan-mem-gian-diep-spyware-la-gi/>.

[42] Toàn Đại Toàn, 2011, *"Virus máy tính" Định nghĩa, phân loại, cách nhìn của Việt Nam và Thế Giới*, truy cập tháng 1 năm 2020, <http://www.ninhthuan.gov.vn/chinhquyen/sotttt/Pages/virus-may-tinh-%E2%80%93-Dinh-nghia,-phan-loai,-cach-nhin-cua-Viet-Nam-va-The-Gioi.aspx>.

[43] Phúc Minh, 2012, *25 loại "sâu" máy tính nổi tiếng nhất lịch sử*, truy cập tháng 1 năm 2020, <http://vneconomy.vn/cuoc-song-so/25-loai-sau-may-tinh-noi-tieng-nhat-lich-su-20120106114615627.htm>.

[44] Phúc Minh, 2012, *25 loại sâu máy tính nổi tiếng nhất lịch sử*, truy cập tháng 1 năm 2020, <http://vneconomy.vn/cuoc-song-so/25-loai-sau-may-tinh-noi-tieng-nhat-lich-su-20120106114615627.htm>.

[45] Nhật Tân, 2020, *Malware là gì? Bí kíp chặn Malware hiệu quả nhất*, truy cập tháng 1 năm 2020, <https://kowgear.com/malware-la-gi/>.

[46] Hạnh Huyền, 2019, *Malware Là Gì? Và Những Sự Thật Xung Quanh Malware*, truy cập tháng 1 năm 2020, <https://egyptsites.com/malware-la-gi-va-nhung-su-that-xung-quanh-malware/>.

[47] An nhiên, 2018, *Malware là gì?*, truy cập tháng 1 năm 2020, <https://trainghiemso.vn/malware-la-gi/>.

[48] Phạm Hải, 2019, *Phân tích phần mềm độc hại là gì? Các bước tiến hành ra sao?*, truy cập tháng 1 năm 2020, <https://quantrimang.com/phan-tich-phan-mem-doc-hai-la-gi-cac-buoc-tien-hanh-166117>.

[49] Thắng Phạm, 2020, *Top 5 phần mềm diệt Malware tốt nhất 2020*, truy cập tháng 1 năm 2020, <http://thuthuatphanmem.vn/top-5-phan-mem-diet-malware-tot-nhat/>.

[50] Thu Hương, 2008, *Những phương thức lây lan của malware và cách phòng chống*, truy cập tháng 1 năm 2020, <https://quantrimang.com/nhung-phuong-thuc-lay-lan-cua-malware-va-cach-phong-chong-50486>.