SỰ PHÁT TRIỂN CỦA TROJAN HORSE TRONG 10 NĂM TRỞ LẠI ĐÂY

Võ Văn Phúc[13], Tô Nhật Duy[14]

Tóm tắt: *Ngày nay, cùng với sự phát triển mạnh mẽ và rộng rãi của internet thì cũng là lúc các loại Virus, Trojan xuất hiện và nhanh chóng phát triển với tốc độ đáng kinh ngạc. Kỹ thuật phát triển Trojan vô cùng phong phú và đa dạng, luôn thu hút nhiều người nghiên cứu về nó. Trong bài báo này, sẽ trình bày rõ về sự phát triển lớn mạnh và nguy hiểm của Trojan trong 10 mười năm trở lại đây, ngoài ra còn giúp chúng ta hiểu sâu về các khái niệm, phương thức hoạt động và từ đó đưa ra cách phòng tránh các loại Trojan một cách phù hợp nhất.*

Từ khóa: *Trojan Horse, Virus máy tính, Malware, Backdoor, Rootkit, Exploit, DDoS Attack, Spyware, Keylogger, Ransomwar*

Abstract: *Today, along with the strong and widespread development of the internet, Viruses and Trojans appear and rapidly develop at an incredible speed. Trojan development technique is many and varied, always attracts many people to research on it. In this article, we will clearly present the growth and dangers of the Trojan in the past 10 years, in addition to help us understand the concepts, how it works of Trojan, and thereby giving the most suitable way to avoid Trojans.*

Keywords: *Trojan Horse, Malware, Backdoor, Rootkit, Exploit, DDoS Attack, Spyware, Keylogger, Ransomwar*

1. Giới Thiệu

Trong số chúng ta, còn nhiều người cho rằng Trojan là một loại Virus, nhưng trên thực tế Trojan và Virus máy tính khác nhau hoàn toàn từ cách thức hoạt động đến các phương thức lây nhiễm. Bởi vì, Virus thì có thể tự chạy và tự nhân bản còn Trojan thì không làm được như thế. Tuy nhiên, có sự giống nhau là khả năng lây nhiễm và phá hoại của Trojan cũng giống như Virus, nó tấn công mọi dữ liệu trên máy tính. Vấn nạn Trojan ngày càng tăng lên cùng với sự phát triển mạnh mẻ của nó, Trojan ẩn mình dưới nhiều phần mềm bằng nhiều cách thức khác nhau nhằm gây hại cho máy tính người dùng.

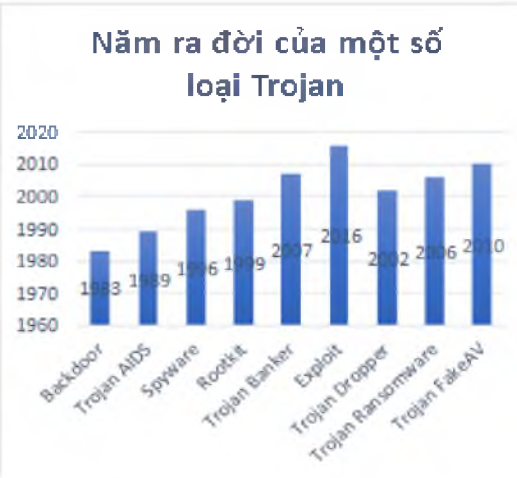
Trojan trước hết được hiểu là một chương trình độc hại cho máy tính, chúng tạo cho người dùng tin tưởng bằng sự ngụy trang với một vỏ bọc vô hại, từ đó máy tính người dùng dễ bị qua mặt và bị nhiễm Trojan. Tên "Trojan" được lấy từ điển tích con ngựa thành Troy trong thần thoại Hy Lạp. Nội dung điển tích kể về sự thông minh của người Hy Lạp khi họ không thể hạ nổi

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

thành địch, họ giả vờ tặng quân địch một chú ngựa khổng lồ và khiến cho kẻ địch lầm tưởng đó là chiến tích mà chủ quan. Sau khi chú ngựa được đem vào thành, nữa đêm đã có vô số chiến binh ẩn nấp trong thân con ngựa gỗ khổng lồ chui ra tiêu diệt quân địch một cách bất ngờ giúp quân Hy Lạp dành chiến thắng dễ dàng. Điều này cũng giống như cách thức hoạt động của Trojan. Thay vì tấn công từ cửa trước thì dễ bị phần mềm quét Virus và tường lửa máy tính phát hiện, thì tin tặc đã chèn mã độc, Virus trong các phần mềm khác. Một khi Virus hoạt động, nó sẽ lây lan rất nhanh và để lại hậu quả khó lường nếu người dùng không có biện pháp ngăn chặn kịp thời. (Tuấn Phong, 2020)

Ngoài ra, Trojan horse là một loại mã độc nhưng mã này lại có thể kiểm soát máy tính của người dùng. Mục tiêu tạo ra Trojan là để gây nhiều thiệt hại, làm hỏng hệ thống máy tính hay lấy cắp những thông tin quan trọng. (Giangpth, 2018)

Trojan hầu hết đều được thiết kế để kiểm soát, đánh cắp dữ liệu, theo dõi người dùng hoặc chèn thêm phần mềm độc hại vào máy tính của nạn nhân. Tuy được tạo ra với cùng mục đích, Trojan lại rất đa dạng về hình thức. Dưới đây là một số Trojan nổi bật hơn cả: Trojan Backdoor, Trojan Zombifying, Trojan Dialer, Trojan Data-Sending, Remote Access Trojans (RATs), Trojan Destructive, Trojan FTP, Trojan Security Software Disable, Trojan-Proxy, Trojan-Mailfinder, Trojan-SMS, Keylogger, Trojan-Ransomware, Trojan-IM, Trojan-GameThief, Trojan-FakeAV, Trojan Dropper, Trojan-Banker, Rootkit, Exploit, Trojan Downloader.



Hình 1: Năm ra đời của một số loại Trojan cơ bản

Đây là những loại Trojan cơ bản, chúng ta thường bắt gặp khi sử dụng máy tính, ngoài ra còn có khá nhiều loại Trojan như: Trojan ArcBomb, Trojan Clicker, Trojan Notifier, Trojan PSW, Trojan Infostealer, Trojan Mobile, Trojan VNC,...

Trojan ẩn mình dưới những bài hát, phần mềm, hình ảnh, link tải quảng cáo. Khi đó các phần mềm gián điệp sẽ nhanh chóng xâm nhập vào hệ thống máy tính, chờ tín hiệu của người muốn xâm nhập máy tính và sau đó khống chế toàn bộ dữ liệu cá nhân của người dùng.

Khi tấn công trực tiếp, Trojan dễ bị phần mềm antiVirus phát hiện, vì thế Trojan chọn cách tấn công phía sau một chương trình, phần mềm khác có phần mở rộng là: .exe, .com, .scr, .bat hay .pif. Trojan không tự lây lan như Virus và là một phần mềm thông thường.

Một số dấu hiệu nhận biết khi bị nhiễm Trojan như: Ổ CD-ROM tự động mở ra đóng vào, dấu hiệu lạ trên màn hình máy tính, hình nền máy tính tự động bị thay đổi, các văn bản tự động in, máy tính tự động thay đổi font chữ và các thiết lập khác, lỗi chuột máy tính như không hiển thị chuột, 2 chuột lẫn lộn nhau, nút Start không hiển thị, cửa sổ chat hiển thị mà không phải do bạn mở lên. Tất nhiên đây chỉ là một vài dấu hiệu nhận biết cho những loại Trojan đơn giản. Hiện nay Trojan không để lại bất cứ dấu hiệu nào và ở nhiều dạng khác nhau.

Cách thức Trojan gây hại lên hệ thống máy tính là: xóa hay viết lại các dữ liệu máy tính, làm hỏng các chức năng của các tệp, lây nhiễm các phần mềm ác tính khác như Virus, cài đặt mạng để máy tính có thể bị điều khiển bởi máy khác hay dùng máy nhiễm để gửi thư, đọc lên các thông tin cần thiết và gửi báo cáo đến nơi khác, ăn cắp thông tin tài khoản cá nhân như mật khẩu và số thẻ tín dụng, cài đặt lén các phần mềm chưa được cho phép đó. (Giangpth, 2018)

Trojan lây nhiễm đa dạng với nhiều hình thức khác nhau như truy cập những trang web không tin tưởng, qua các ứng dụng chat, những file hay link đính kèm trên mail, qua các thiết bị kết nối ngoài. Một số các cách để phòng tránh Trojan đó là không bao giờ mở bất kì tập tin, link hay phần mềm lạ, email thậm chí email từ địa chỉ bạn quen biết, thiết lập và chạy các chương trình bảo mật Enternet mỗi khi mở máy tính, sử dụng mậy khẩu mạnh kết hợp các chữ cái, chữ số khó đoán. Trojan phát tán khi bạn click vào những nội dung chứa phần mềm gián điệp. Tốt nhất là nên kiểm tra trước bằng những chương trình quét Virus hay dùng để kiểm tra. Luôn sử dụng những phần mềm antiVirus hay tường lửa để bảo vệ máy tính. Cập nhật đầy đủ những bản vá lỗ hổng thường xuyên với máy tính Windows, để tránh trường hợp hacker lợi dụng những lỗ hổng đó xâm nhập máy tính. Hiện nay trên thị trường có rất nhiều chương trình chống các phần mềm độc hại như: Malwarebutes, Adware AntiVirus,... (Tuấn Phong, 2020).

Nội dung chính của bài báo được chia làm 3 phần: phần thứ nhất trình bày về sự phát triển của Trojan Horse từ năm 1974 đến năm 2000, phần thứ hai trình bày về sự phát triển của Trojan Horse từ năm 2000 đến nay và phần cuối cùng là kết luận.

2. Sự phát triển của Trojan Horse từ năm 1974 đến năm 2000

2.1. Lịch sử hình thành và phát triển của Trojan

Trojan Horse lần đầu tiên xuất hiện trong báo cáo của Không quân Hoa Kỳ, trong đó có chứa các phân tích về những lỗ hổng của máy tính hồi năm 1974. Hệ thống Bulletin Board (BBS)—cho phép người dùng sử dụng đường dây điện thoại thâm nhập vào trang web—là thời điểm bắt đầu cho tiến trình khuếch tán của mã độc Trojan diễn ra trong những năm 1980. Trojan

Horse - Ngựa Gỗ Thành Troy trở nên phổ biến từ năm 1983 sau khi Ken Thompson dùng nó trong bài giảng nổi tiếng về phép thử Turing. Vì máy tính có tính năng upload, download, và chia sẻ file, tích hợp các trình add-on độc hại vào bất cứ chỗ nào một khi đã cài vào hệ điều hành. Ngày nay, có hàng nghìn phiên bản mã độc đang tồn tại. (Aviva Zacks, 2018).

Trojan có cách thức gần giống với trò chơi ANIMAL(1975) được thiết kế với tính năng tự sao chép. Với tính năng này, ANIMAL đã tự sao chép nó vào các thư mục được chia sẻ trong mạng nội bộ. Nhờ đó, trò chơi có thể lan rộng trên toàn bộ hệ thống.

AIDS Trojan - mã độc tống tiền được ra đời vào tháng 12/1989 và cũng được coi là ransomware đầu tiên - được gửi đến các thuê bao của tạp chí PC Business World và danh bạ của hội nghị về AIDS của Tổ chức Y tế Thế giới. Để giải mã dữ liệu, nạn nhân phải bỏ ra một số tiền 189 USD để gửi đến một hòm thư ở Panama.

Có thể các bạn từng đã nghe qua vụ tấn công có sức tàn phá lớn nhất trong những năm 2000 đó là cuộc tấn công bởi Trojan, Trojan tiếp tục phát triển và ngày càng tinh vi hơn. Mã độc ILOVEYOU là một mã độc điển hình- với thiệt hại ước tính lên tới 8,7 tỷ USD. Cuộc tấn công được lan truyền qua email với chủ đề "ILOVEYOU" và đi kèm với file "LOVE-LETTER-FOR-YOU.txt.vbs". Sau khi mở file này, nó sẽ tự gửi cho mọi người trong sổ địa chỉ Outlook, lúc bấy giờ nó đã trở thành một trong những Virus lây lan nhanh nhất.

Trojan tiếp tục tìm được các hướng đi mới để tạo nên sự phát triển cho mình vào thập niên thứ hai của thế kỷ 21, lợi dụng sự gia tăng chóng mặt của tiền điện tử, nhiều hacker đã tổ chức các cuộc tấn công đòi tiền chuộc. Các nhà nghiên cứu cũng chỉ ra rằng, hacker đang dần thay đổi mục tiêu tấn công nhằm nhu cầu lợi ích cho bản thân. Bởi vì, ngày càng có nhiều Trojan được thiết kế để nhằm mục tiêu riêng đến một công ty, một tổ chức nào đó. (Tuấn Phong, 2020).

2.2. Đặc điểm

Trojan horse là chương trình máy tính thường ẩn mình dưới dạng một chương trình hữu ích và có những chức năng mong muốn, hay ít nhất chúng trông như có các tính năng này. Một cách bí mật, nó lại tiến hành các thao tác khác không mong muốn. Những chức năng mong muốn chỉ là phần bề mặt giả tạo nhằm che giấu cho các thao tác này.

Ngày nay, các Trojan horse đã được thêm vào các chức năng tự phân tán. Điều này sẽ làm cho chúng ta trở nên khó phân biệt giữa khái niệm Trojan và Virus. Trong thực tế, nhiều Trojan horse chứa đựng các phần mềm gián điệp nhằm cho phép máy tính thân chủ bị điều khiển từ xa qua hệ thống mạng. Khác nhau cơ bản với Virus máy tính là Trojan Horse về mặt kỹ thuật chỉ là một phần mềm thông thường và không có tự lan truyền. Các chương trình này chỉ lừa người dùng để tiến hành thực hiện một số các thao tác khác mà thân chủ sẽ không tự nguyện cho phép tiến hành. (Maiphuongdc, 2014).

2.3. Trojan Backdoor

2.3.1. Khái niệm

Backdoor là một cách tấn công để xâm nhập vào các thiết bị, phần mềm. Sau khi Backdoor được cài đặt, một cổng dịch vụ sẽ tự động mở ra, cho phép người tạo Backdoor kết nối từ xa tới thiết bị, từ đó thiết bị sẽ nhận và thực hiện lệnh được đưa ra. Ngoài ra backdoor là chương trình gián điệp được tích hợp vào nhân của phần mềm với nhiều mục đích khác nhau. Chương trình này có thể xuất hiện ở mọi thiết bị từ điện thoại, laptop cho tới router mạng, miễn là những nơi đó có sự tồn tại của ứng dụng/phần mềm.

2.3.2. Lịch sử của Backdoor

Lần đầu tiên cộng đồng tranh luận về Backdoor là vào những năm 80 của thế kỷ 20. Trong bộ phim khoa học viễn tưởng WarGames (1983), nhân vật chính là một hacker tuổi teen do Matthew Broderick thủ vai đã sử dụng Backdoor để truy cập vào siêu máy tính được quân đội thiết kế để mô phỏng cuộc chiến tranh hạt nhân.

Năm 1993, NSA đã phát triển một con chip mã hóa có tích hợp Backdoor nhằm giúp các cơ quan thực thi pháp luật thu thập và giải mã giọng nói, cũng như dữ liệu được truyền qua điện thoại và máy tính. Chip Backdoor chúng khó gỡ bỏ - trừ khi bạn tách hẳn chúng ra. (Quách Chí Cường, 2019).

Có khá nhiều cuộc tấn công về Backdoor trong vài thập kỷ qua trên thế giới. Trong đó không thể không nhắc đến cuộc tấn công backdoor Back Orifice xảy ra vào năm 1999 do một nhóm hacker tự xưng là Cult of the Dead Cow thực hiện. Back Orifice kích hoạt điều khiển từ xa trên máy tính Windows thông qua lỗ hổng trên hệ điều hành. (Duy Vinh, 2018)

Sony BMG bắt đầu tham gia cuộc chơi vào năm 2005. Hãng này đã phát hành hàng triệu đĩa CD ca nhạc với bộ rootkit kèm theo để theo dõi thói quen nghe nhạc của khách hàng. Hậu quả là, Sony BMG đã trả hàng triệu đô để giải quyết các vụ kiện liên quan đến rootkit và thu hồi số đĩa CD đã phát hành trên. (Quách Chí Cường, 2019).

Vào năm 2013, tờ Der Spiegel uy tín của Đức đưa tin đơn vị Tailor Access Operations (TAO) của NASA duy trì backdoor để cấy vào tường lửa, các bộ định tuyến (router) và các thiết bị khác được sử dụng trên thế giới. Ngoài ra NASA cũng bị cáo buộc tích hợp backdoor trong các thành phần như ổ cứng và và cáp USB. (Duy Vinh, 2018).

Năm 2014, Backdoor trên Samsung đã được các nhà phát triển Android của Google phát hiện, bao gồm cả loạt điện thoại Galaxy. Tuy nhiên, Backdoor này là một tính năng và không có rủi ro bảo mật.

Apple, Google và Facebook kiên quyết không tạo Backdoor cho các sản phẩm của họ dù bị sức ép từ phía chính trị. Áp lực càng lớn sau vụ tấn công khủng bố San Bernardino năm 2015,

khi FBI đã thu hồi được một chiếc iPhone thuộc sở hữu của một trong những kẻ nổ súng. Tuy nhiên, Apple một lần nữa từ chối yêu cầu mở Backdoor từ phía FBI. Thế cục căng thẳng này duy trì đến khi FBI rút lại yêu cầu vì họ đã hack được chiếc iPhone đời cũ kém bảo mật này. Backdoor cũng nhộn nhịp vào năm 2017 - 2018. Các hãng lớn được ghi nhận là nạn nhân của loại mã độc này bao gồm WordPress, Joomla, Drupal, NotPetya - đủ để biết nó nguy hiểm đến mức nào.

2.3.3. Phương thức lây nhiễm và hoạt động của Backdoor

Backdoor gây hại cực kỳ tinh vi, sử dụng nhiều chiêu trò để xâm nhập vào thiết bị, chẳng hạn như đính kèm link trong email hoặc ẩn mình trong các file tải xuống. Một ví dụ phổ biến nhất về con đường xâm nhập của Backdoor độc hại đó là khi bạn tải một phần mềm vi phạm bản quyền (ví dụ bản crack của Adobe Photoshop), mã độc đã theo đó mở một Backdoor trên thiết bị của bạn và tùy ý làm mọi điều nó muốn mà chẳng sợ bị phát hiện.

Trong quá trình sản xuất của các nhà phát triển phần cứng, phần mềm backdoor vô hại được xem như một thủ tục. Đôi khi Backdoor này được tạo ra chỉ nhằm mục đích dự phòng. Đó cũng chính là lý do Apple, Facebook và Google đã từ chối lời yêu cầu của Five Eyes (Hiệp ước chia sẻ thông tin tình báo của 5 nước Hoa Kỳ, Anh, Canada, Úc và New Zealand) về việc mở Backdoor trong dịch vụ của họ.

Thông qua Backdoor, hacker có thể khai thác thông tin người dùng (thông tin cá nhân, sở thích truy cập Internet, tài khoản, mật khẩu, mã số thẻ hoặc phức tạp hơn, chúng sẽ dùng Backdoor làm bàn đạp để đưa các phần mềm độc hại khác vào (như Ramsomware, Spyware, Cryptojacking,...).

2.3.4. Biện pháp ngăn chặn Backdoor

Sau đây sẽ là một số biện pháp ngăn chặn Backdoor để không gây hại cho máy tính: Thay đổi mật khẩu mặc định, sử dụng mật khẩu khác nhau cho từng ứng dụng và thiết bị, kích thước xác thực đa yếu tố; Thường xuyên cập nhật các thông tin mới nhất về Backdoor và an ninh mạng để phòng tránh kịp thời. (Hồng Nguyễn, 2020); Giám sát các hoạt động mạng và sử dụng tường lửa để theo dõi hoạt động từ các ứng dụng đã cài đặt; Cẩn thận trong việc cài đặt ứng dụng và plugin, đó là hai nguồn phổ biến nhất mà Backdoor có thể trà trộm vào; Không dùng các phần mềm không đáng tin cậy bởi đôi khi các ứng dụng tin tưởng vẫn có nguy cơ dính Trojan; Cập nhật hệ điều hành thường xuyên và kịp thời ngay khi có phiên bản update mới; Sử dụng các phần mềm diệt Virus uy tín, chất lượng như: Kaspersky Internet Security, Mcafee Total Security, Norton Internet Security,... sau khi cài đặt, hãy update chúng thường xuyên. Tóm lại Backdoor cho phép hacker truy cập hệ thống máy tính của nạn nhân từ xa. (Trịnh Duy Thanh, 2019)

2.4. Spyware

2.4.1. Khái niệm

Spyware là thuật ngữ thường được sử dụng để chỉ các phần mềm thực hiện hành vi nhất định như quảng cáo, thu thập thông tin người dùng hoặc thay đổi cấu hình máy tính của bạn.

Ngoài ra spyware là phần mềm chuyên thu thập các thông tin từ các máy chủ qua mạng Internet mà không có sự nhận biết và cho phép của chủ máy. Spyware được cài đặt một cách bí mật của các phần mềm miễn phí (freeware) và phần mềm chia sẻ (shareware) mà người ta có thể tải về từ Internet. Spyware điều phối các hoạt động của máy chủ trên Internet và chuyển các dữ liệu thông tin đến một máy khác. (Nguyễn Hữu Duy Khang, 2019).

2.4.2. Lịch sử ra đời của Spyware

Năm 1996, các tài liệu về Spyware lần đầu tiên xuất hiện trong một tờ báo. Năm 1999, thuật ngữ Spyware trong báo chí trong ngành và trở thành đề tài thu hút mạnh mẽ trên các phương tiện truyền thông đại chúng. Tháng 6/2000, ứng dụng chống Spyware đầu tiên được phát hành.

Tháng 10/2004, America Online và Liên minh an ninh mạng quốc gia đã thực hiện cuộc khảo sát và thu về kết quả như sau: 80% hệ thống của người dùng Internet bị ảnh hưởng bởi Spyware; 93% máy tính bị nhiễm Spyware; 89% người dùng máy tính không biết đến sự tồn tại Spyware trên thiết bị của mình; 95% người dùng cho biết họ chưa bao giờ cho phép Spyware cài đặt vào thiết bị.

Các nguyên do đầu tiên là từ các cá nhân chế tạo phần mềm miễn phí có mục đích. Do đó, một cách để kiếm thêm thu nhập là thu thập thông tin từ người đã tải về các phần mềm. Cách thu thập ban đầu chỉ là dựa vào sự điền vào các mẫu đăng ký (register). Cách thức đọc thông tin được chuyển sang dạng cài lén phần mềm phụ để tự nó đọc thông tin của chủ và gửi thẳng về cho nơi mà phần mềm gián điệp này được chỉ thị. Thứ hai là các phần mềm này chuyển sang dạng có ác tính: tìm cách đọc tất cả những thông tin bí mật của máy chủ từ mật mã truy cập, các số thẻ tín dụng cho đến giành luôn quyền điều khiển bàn phím. Vào năm 1995 “spyware" xuất hiện đầu tiên trên USENET. Các phần mềm chống gián điệp (antispyware) cũng ra đời vào đầu năm 2000. (Quách Chí Cường, 2019a).

2.4.3. Cách xâm nhập của Spyware

Spyware lây nhiễm dưới rất nhiều dạng Trojan, Virus, worm, exploit và các hình thức khác thông qua một số kỹ thuật phổ biến sau:

Thông qua lỗ hổng bảo mật: Spyware thường xâm nhập thông qua các lỗ hổng bảo mật khi bạn tải xuống, mở các liên kết hoặc tệp đính kèm lạ trong email, truy cập vào các website độc hại và nhấn vào banner quảng cáo, nhấp vào một số tùy chọn trong cửa sổ bật lên hoặc là mở các phần mềm giao dịch, tài liệu, file nhạc,... có chứa Spyware.

Thông qua các công cụ hữu ích: Hacker thường tạo ra Spyware dưới dạng các công cụ hữu ích để tải xuống. Đó có thể là một trình tăng tốc Internet hay là trình quản lý tải xuống, trình dọn dẹp ổ đĩa hoặc một dịch vụ tìm kiếm web thay thế.

Thông qua các chương trình tiện ích bổ sung: Spyware có thể ẩn trong các chương trình bổ sung đi kèm với ứng dụng phần mềm. (Quách Chí Cường, 2019a).

2.4.4. Biện pháp phòng tránh Spyware

Sau đây sẽ là một số biện pháp ngăn chặn Spyware để bảo vệ máy tính đó là: Không mở email từ người gửi không xác định; Chỉ tải xuống các tệp từ nguồn đáng tin cậy; Chỉ tải xuống các tệp từ nguồn đáng tin cậy; Kiểm tra kỹ trước khi nhấp vào các liên kết để đảm bảo bạn được chuyển đến đúng trang web; Sử dụng một chương trình bảo mật mạng uy tín; Cài đặt phần mềm chặn Spyware hiện đại để bảo vệ máy tính trước khi hacker kích hoạt chúng; Kích hoạt tính năng ngăn chặn việc phân phối Spyware trên máy tính. (Quách Chí Cường, 2019a).

Cách hay nhất để phòng chống Spyware là sử dụng một hệ điều hành không phải là Windows (như OS X, Linux,...) vì có rất ít Spyware được viết cho những hệ điều hành này. Hơn nữa, rất nhiều Spyware được cài đặt dùng ActiveX trong Internet Explorer (IE), cho nên nếu một người dùng một trình duyệt khác như Firefox, Opera, thì họ sẽ bị ít spyware hơn. Tóm lại, Spyware theo dõi mọi thao tác của người dùng, kể cả khi họ đang truy cập vào các tài khoản trực tuyến như mạng xã hội, thẻ tín dụng. (Wikipedia, 2018).

2.5. Các trình download Trojan

Các phần mềm độc hại sau khi xâm nhập sẽ tải và cài đặt các ứng dụng độc hại khác. Trojan này nhằm mục tiêu đến máy tính người dùng đã bị nhiễm, tải xuống và cài đặt các biến thể của chương trình độc hại, bao gồm Trojan và phần mềm quảng cáo (adware).

Sự phát triển của các trình download Trojan khá gần đây, chỉ trong vài năm qua. Phiên bản Trojan này được thiết kế để lây nhiễm vào máy tính mục tiêu theo cách tương tự như các loại Virus Trojan khác. Công việc duy nhất mà trình tải xuống Trojan thực hiện trên máy tính bị nhiễm là tải thêm phần mềm độc hại về máy tính vào máy tính bị nhiễm. Một số trình tải xuống Trojan cũng có thể được sử dụng để cấp quyền truy cập từ xa vào máy mục tiêu cho một máy chủ hoặc cá nhân từ xa như một phần công việc của họ. (Tech-FAQ, 2012).

2.6. Trojan Dialer

2.6.1. Khái niệm

Trojan Dialer là chương trình làm thay đổi cấu hình modem để thiết bị quay số tới một số nào đó nhằm làm tăng hóa đơn tiền điện thoại. Loại Trojan này có vẻ đã lỗi thời, vì ngày nay chúng ta không quay số gọi điện nữa. (Hồng Nhi, 2018b)

2.6.2. Cách thức hoạt động của Trojan Dialer

Sau đây là cách thức hoạt động của Trojan Dialer: Sử dụng máy tính bị xâm nhập để kết nối với các số điện thoại giá cao; Quảng cáo các trang web có khả năng không an toàn hoặc các nội dung tương tự khác; Gây ra sửa đổi hệ thống và thay đổi cài đặt quay số và mạng cần thiết; Thay đổi cài đặt của trình duyệt web; Tạo nhiều liên kết có thể dẫn mọi người đến các trang web có khả năng không an toàn; Không cung cấp tính năng loại bỏ. (Ugnius Kiguolis, 2017)

2.7. Remote Access Trojan (RAT)

RATs đóng vai trò như một server trên máy tính của bạn và tạo điều kiện cho hacker kết nối với máy tính của bạn và thực hiện các lệnh khác nhau. Sử dụng Trojan loại này khá đơn giản, chúng thường gồm 2 file server và client, mỗi khi tải chúng về bạn chỉ cần đọc mục Help của chúng là đã có thể biết cách sử dụng. Các tính năng của Trojan loại này càng ngày càng cao hơn, ví dụ như Trojan girl-friend có thể ngăn không cho nạn nhân tắt máy tính, hiển thị text lên màn hình, biểu diễn âm thanh, hình ảnh, download, upload file từ server, thậm chí là chát cùng với nạn nhân ...

Cách thức làm việc của Trojan RAT: thường ẩn trong các chương trình lớn, vì vậy mỗi khi bạn chạy các chương trình này, Trojan sẽ tự động được kích hoạt. Mỗi RAT thường chạy server dưới một cổng riêng biệt, cổng này cho phép hacker xâm nhập vào máy của bạn. Các Trojan khi đã xâm nhập vào trong máy tính thường tạo ra 1 file thực thi nào đó hoặc ghi thêm dòng lệnh tự kích hoạt vào trong file win.ini, có thể bạn biết được file đó là Trojan nhưng cũng không thể vô hiệu hóa nổi nó bằng những cách thông thường. Thường thì bạn không thể xoá nó đi và cũng không thể vào trong registry để xoá vì chúng thường làm mất chức năng edit registry của hệ điều hành. Người ta có thể sử dụng RAT để điều khiển, quản lí từ xa máy tính của chính bản thân họ, chúng ta sẽ không biết trước được RAT sẽ gây ra những hậu quả như thế nào. Remote Access Trojan (RAT): chạy vô hình trên máy tính nạn nhân và cho phép hacker truy cập và kiểm soát máy tính bị nhiễm từ xa.

2.8. Trojan Destructivethe

Destructive Trojan: là một loại Virus được thiết kế để phá hủy hoặc xóa các tập tin. Chúng có nhiều tính năng đặc trưng của Virus hơn so với các loại Trojans khác. Destructive Trojan có thể không được phát hiện bởi phần mềm chống Virus. Một khi Destructive Trojan truyền nhiễm vào một hệ thống máy tính, nó sẽ tự động xóa các tập tin, thư mục và các mục registry, dẫn đến lỗi hệ điều hành.

2.9. DDoS Attack Trojan

DDoS Attack Trojan: được thiết kế để tiến hành tấn công DDoS từ máy tính bị nhiễm vào một địa chỉ được xác định trước. Để thực hiện tấn công DDoS thành công, hacker thường lây phát tán và lây nhiễm loại Trojan này vào một số máy tính trước. Sau đó, tất cả các máy tính bị nhiễm sẽ tấn công máy tính có IP xác định trước. (Kaspersky, 2020).

2.10. Trojan Proxy

Trojan proxy là một loại Virus chiếm quyền điều khiển và biến máy tính chủ thành một máy chủ proxy, là một phần của mạng botnet, từ đó những kẻ tấn công sẽ thực hiện một số thao tác làm hư hỏng máy tính. Trojan proxy là che giấu kẻ tấn công, khiến việc truy tìm nguồn gốc thực sự của một cuộc tấn công trở nên khó khăn hơn vì các cuộc tấn công sẽ giống như chúng đến từ ngẫu nhiên và đa phần là do các bot proxy. (Techopedia, 2014)

Proxy Trojan: loại Trojan này tạo ra các máy chủ proxy từ các máy tính bị nhiễm để thực hiện các cuộc tấn công. Trojan này cung cấp cho kẻ tấn công rất nhiều cơ hội để tiến hành các hoạt động xấu như: hack thẻ tín dụng và nhiều hoạt động bất hợp pháp khác vì nó che dấu địa điểm thực sự của kẻ tấn công. Bên cạnh đó, nó có thể thu thập thông tin từ máy chủ và gửi nó cho kẻ tấn công.

2.11. FTP Trojan

Trojan FTP là một loại Trojan đặc biệt cho phép kẻ tấn công truy cập vào máy bằng giao thức FTP. Nói chung, Trojan này là một loại Virus xâm nhập vào hệ thống theo cách không bị phát hiện và truy cập vào tất cả dữ liệu bí mật, do đó gây ra rắc rối bằng cách xâm nhập hoặc để lộ dữ liệu. Nó cho phép tất cả mọi người kết nối thông qua cổng 21 trên máy tính đến máy tính nhiễm Trojan mà không cần mật khẩu và sẽ có toàn quyền tải bất kì dữ liệu nào xuống. (Bùi Thị Lụa, 2013).

Mục đích chính của phần mềm độc hại là mở cổng 21 trên máy tính bị nhiễm. Sau khi mở, bất kỳ ai cũng có thể kết nối với máy tính bằng giao thức FTP. Đối với các phiên bản nâng cao hơn, tính năng bảo vệ bằng mật khẩu Trojans được kích hoạt để chỉ hacker mới có thể truy cập vào máy bị nhiễm. FTP Trojan: tự tạo thành FTP server để kẻ tấn công có thể khai thác lỗi. (Tech-FAQ, 2012).

3. Sự phát triển của Trojan horse từ năm 2000 đến nay

3.1. Rootkit

3.1.1. Khái niệm

Rootkit là bộ công cụ phần mềm giúp che giấu sự tồn tại của một phần mềm khác mà thường là Virus xâm nhập vào hệ thống máy tính. Hacker dùng rootkit sau khi chiếm được quyền truy cập vào hệ thống máy tính. Nó sẽ che dấu dữ liệu hệ thống, tập tin hoặc tiến trình đang chạy, từ đó chúng ta không thể biết được hacker đã xâm nhập được vào hệ thống máy tính.

3.1.2. Lịch sử phát triển của Rootkit

Rootkit lần đầu tiên được công khai dựa trên Windows là vào năm 1999 bởi Grep Hoglund một chuyên gia về bảo mật và là người lập trình website rootkit.com. Rootkit đã tồn tại hàng chục năm lần đầu tiên phát triển trên hệ điều hành Unix (Linux) và sau đó là Windows.

Sysinternal phát hiện Sony Rootkit đã khiến rootkit được quan tâm một cách đặc biệt và nhiều người tìm hiểu hoạt động của nó. Ngày 31/10/2005 sự kiện Sony Rootkit xảy ra đã đưa ra rootkit thành trung tâm chú ý. Sau sự kiện này, Sony đã phải tiến hành gỡ bỏ rootkit trên các đĩa CD và tốn khoản bồi thường lớn.

Bằng cách sử dụng rootkit và khả năng lén lút của nó, những hacker mới đã tìm ra cách mới và hiệu quả để tấn công. Các chương trình che giấu và rootkit cho thấy một nguy cơ cận kề về an ninh mạng. Thực tế, ngày 6/12/2005 tạp chí eweek đã công bố rằng có tới 20% malware bị phát hiện trên Windows XP SP2 là các rootkit trong số các malware là 14% trong khi tại điểm của sự kiện Sony Rootkit con số đó là 8%.

3.1.3. Đặc điểm của Rootkit

Đặc điểm chính của rootkit là có khả năng che dấu nên nếu dùng các chương trình từ hệ thống như: "Registry Editor", "Find Files", "Task Manager" thì không thể phát hiện. Thậm chí dù có phát hiện ra rootkit đi nữa thì xóa nó đi cũng không là một cách dễ dàng. Không thể sử dụng các công cụ bình thường mà phải dùng các chương trình anti rootkit đặc biệt. Rootkit thường hoạt động ở 2 mức thứ nhất là mức ứng dụng (User-mode), thứ hai là mức nhân hệ điều hành (Kernel-mode) nên phát hiện được chúng vô cùng khó khăn.

3.1.4. Tác hại của Rootkit

Rootkit thường được dùng để che dấu các công cụ tạo các "cửa sau" giúp hacker truy cập vào hệ thống dễ dàng hơn ở lần sau. Nó che dấu mọi loại công cụ khác có thể dùng để xâm nhập vào hệ thống. Người quản lý hệ thống khi bị xâm nhập vẫn không hay biếtm, hay hậu quả có thể mang lại cho chủ sơ hữu các thông tin, dữ liệu là vô cùng lớn, thậm chí trong thời gian dài. Cách tốt nhất để tránh bị nhiễm Rootkit chính là thuê máy chủ ảo để lưu trữ từ những nhà cung cấp dịch vụ chuyên nghiệp để chạy các chương trình cũng như lưu trữ dữ liệu quan trọng. Long Vân (2014).

Rootkit là phần mềm độc hại rất khó bị phát hiện. Rootkit che giấu đi tất cả mọi thứ. Chúng ẩn mình trên máy tính của bạn và cũng ẩn hoạt động độc hại trên PC của bạn. Hồng Nhi (2018).

3.1.5. Cách phòng tránh rootkit

Rootkit là mối đe dọa cho máy tính khi rootkit đã được cài vào hệ thống tức là hệ thống đã bị xâm nhập từ trước. Cách tốt nhất để phòng chống rootkit là ngăn chặn khả năng cài đặt chúng bằng chiến lược phòng thủ nhiều lớp. Cụ thể là: Cập nhật hệ thống chống antiVirus và phần mềm gián điệp; Triển khai hệ thống tường lửa mạng và host-based; Cập nhật các bản vá cho hệ điều hành và ứng dụng; Xiết chặt hệ điều hành; Sử dụng phương pháp xác thực mạnh; Không bao giờ sử dụng phần mềm từ những nguồn không tin cậy.

3.2. Trojan Banker

3.2.1. Khái niệm

Banker Trojan là một chương trình máy tính độc hại được thiết kế để truy cập vào thông tin bí mật được lưu trữ hoặc xử lý thông qua hệ thống ngân hàng trực tuyến. Banker Trojan là một dạng của con ngựa Trojan và có thể xuất hiện như một phần mềm hợp pháp cho đến khi nó được cài đặt trên một thiết bị điện tử.

Trojan Banker có hướng truy cập từ các trang web tài chính ngân hàng đến một trang web khác. Khi phần mềm được thực thi, nó sẽ tự sao chép vào máy tính chủ, tạo các thư mục và thiết lập các mục Registry mỗi khi khởi động hệ thống. (Will Kenton, 2018)

3.2.2. Lịch sử của Trojan Banker

Tiny Banker lần đầu tiên được phát hiện vào năm 2012, khi nó được phát hiện đã lây nhiễm cho hàng nghìn máy tính ở Thổ Nhĩ Kỳ. Sau khi được phát hiện, mã nguồn ban đầu của phần mềm độc hại đã bị rò rỉ trực tuyến và bắt đầu trải qua các bản sửa đổi riêng lẻ, khiến quá trình phát hiện khó khăn hơn đối với các tổ chức. Tuy nhiên, Tinba được phát hiện có kích thước nhỏ khiến phần mềm độc hại khó bị phát hiện hơn. Với chỉ 20KB, Tinba nhỏ hơn nhiều so với bất kỳ loại Trojan nào đã biết. Để tham khảo, kích thước tệp trung bình của một trang web trên máy tính để bàn là khoảng 1.966 KB. (Wikipedia, 2020).

Trojan Banker đầu tiên là Zeus/Zbot, xuất hiện vào năm 2007. Nó nhanh chóng trở nên phổ biến và cho phép các nhóm tội phạm mạng đánh cắp hàng trăm triệu đô la. Năm 2011 chứng kiến sự phát hành của mã nguồn. Điều này cho phép một nhánh và sự xuất hiện của phần mềm độc hại dựa trên Zbot (như Spyeye hoặc Citadel).

Zeus đã cho Citadel và sau đó cho Atmos. Vào tháng 4 năm 2016, Atmos nhắm mục tiêu các ngân hàng Pháp: Điều tương tự cũng xảy ra với Gozi Trojan xuất hiện vào năm 2007, mà vào năm 2009 đã cho Trojan Banker Ursnif và Vawtrak. (Malekal.com, 2019).

3.2.3. Biện pháp khắc phục Trojan Banker

Malwarebytes có thể phát hiện và loại bỏ Trojan Banker mà không cần người dùng tương tác thêm: Tải Malwarebytes xuống máy tính để bàn của bạn; Bấm đúp vào MBSetup.exe và làm theo lời nhắc để cài đặt chương trình; Khi quá trình cài đặt Malwarebytes dành cho Windows của bạn hoàn tất, chương trình sẽ mở ra màn hình Chào mừng đến với Malwarebytes; Bấm vào nút Bắt đầu; Nhấp vào Quét để bắt đầu Quét mối đe dọa; Nhấp vào Kiểm dịch để loại bỏ các mối đe dọa được tìm thấy; Khởi động lại hệ thống nếu được nhắc để hoàn tất quá trình gỡ bỏ.

3.3. Exploit

3.3.1. Khái niệm

Thuật ngữ Exploit dùng để chỉ các cuộc tấn công vào một hệ thống máy tính nào đó. Đặc điểm của kiểu tấn công máy tính này là những kẻ xâm nhập sẽ tận dụng triệt để một lỗi hoặc lỗ hổng hệ thống cụ thể mà những kẻ này phát hiện ra được. Chaupm (2018)

3.3.2. Lịch sử của Exploit

Dữ liệu của 1 tỷ người dùng bị rò rỉ đó là vụ hack xảy ra nhiều năm trước đó được Yahoo tuyên bố vào năm 2006. Những kẻ tấn công đã truy cập tấn công vào tài khoản email của người dùng vì mật khẩu được bảo vệ bởi MD5, một thuật toán hash yếu và lỗi thời.

Một trong những cuộc tấn công khai thác lỗ hổng nổi tiếng nhất trong những năm gần đây là EternalBlue, tấn công vào một lỗ hổng được vá trong giao thức Windows Server Message Block. Cuộc tấn công này được công bố bởi nhóm Shadow Brokers và sau đó được tiếp tục sử dụng trong các cuộc tấn công ransomware WannaCry và NotPetya.

Một bản vá đã được phát hành vào đầu năm 2017 công ty báo cáo tín dụng Equachus đã gặp phải một cuộc tấn công vi phạm dữ liệu nghiêm trọng, sau khi những kẻ tấn công khai thác lỗ hổng trong framework Apache Struts, được sử dụng trong một ứng dụng web của công ty, nhưng Equachus đã không cập nhật ứng dụng web của mình cho đến khi phát hiện ra kẻ tấn công. (Dương Nguyễn, 2019).

3.3.3. Các loại tấn công

Tấn công exploit có thể được phân loại theo một số cách khác nhau, tùy thuộc vào cách tấn công exploit hoạt động và loại tấn công nào được sử dụng. Zero-day là kiểu tấn công quen thuộc nhất, tấn công lỗ hổng zero-day. Lỗ hổng zero-day xảy ra khi một phần mềm - thường là ứng dụng hoặc hệ điều hành - mang lỗ hổng bảo mật quan trọng mà nhà cung cấp không biết. Lỗ hổng bảo mật này chỉ thực sự được chú ý đến khi hacker tấn công và bị phát hiện, và từ đó xuất hiện thuật ngữ zero-day. (Chaupm, 2018).

3.3.4. Phương thức hoạt động của Exploit

Phương pháp phổ biến nhất là khai thác từ các trang web độc hại. Nạn nhân có thể vô tình truy cập một trang web như vậy hoặc họ có thể bị lừa nhấp vào liên kết đến trang web độc hại trong email phishing hoặc quảng cáo độc hại.

Phần mềm độc hại có thể được sử dụng cho những cuộc tấn công vào các trình duyệt khác nhau xuất hiện những lỗ hổng, từ một trang web độc hại hoặc từ một trang web đã bị hack. Các trang web độc hại được sử dụng để khai thác lỗ hổng máy tính được trang bị bằng bộ công cụ hoặc phần mềm.

Khai thác lỗ hổng tự động, chẳng hạn như bởi các trang web độc hại, thường bao gồm hai thành phần chính: Exploit code và shell code. Exploit code là phần mềm cố gắng khai thác lỗ hổng đã biết. Shell code là payload của phần mềm được thiết kế để chạy khi hệ thống đích bị xâm phạm. Cái tên shell code xuất phát từ thực tế là một số các payload này có thể mở shell để chạy những lệnh chống lại hệ thống đích. (Dương Nguyễn, 2019).

3.4. Keylogger

3.4.1. Khái niệm

Keylogger thường là một phần mềm nhỏ gọn nhưng nguy hiểm thậm chí là một thiết bị phần cứng với khả năng ghi lại mọi phím bấm mà người dùng đã nhấn trên bàn phím. Tổng hợp kết quả của các tổ hợp phím này, kẻ cài đặt keylogger có thể thu được tin nhắn cá nhân, nội dung email, số thẻ tín dụng và dĩ nhiên nguy hiểm nhất là mọi loại mật khẩu của người dùng.

3.4.2. Cách thức hoạt động của Keylogger

Keylogger thuộc dạng phần mềm thường chạy ngầm trên máy tính, ghi lại tất cả các phím bấm mà người dùng nhập vào. Để tránh việc gửi dữ liệu thường xuyên khiến cho người dùng chú ý, các gói phần mềm này được tạo ra với mục đích gửi đi những dữ liệu có hữu dụng.

Để tăng tính hiệu quả, keylogger cũng thường được kết hợp với một số loại phần mềm theo dõi khác, nhờ vậy kẻ xâm nhập có thể phân biệt được các thông tin mà người dùng nhập vào khi chat chit vô nghĩa với các thông tin nhập vào khi đang đăng nhập vào tài khoản ngân hàng trực tuyến.

Kẻ cài đặt keylogger thường sẽ phải sử dụng công cụ để quét qua toàn bộ file log ghi lại tất cả những gì người dùng đã nhập vào trong suốt thời gian bị theo dõi, từ đó lọc ra cả những thông tin như nội dung tìm kiếm Google, comment trong một topic...

Hiện nay, phần mềm Keylogger không chỉ sử dụng trong tổ chức công nghệ thông tin nhằm hỗ trợ công việc khắc phục sự cố kỹ thuật mạng. Hacker mũ đen có mưu đồ xấu cài đặt nhằm ăn cắp mật khẩu đăng nhập vào mạng xã hội, tài khoản ngân hàng online, các thông tin bí mật.... (Hoàng Bách, 2018)

3.4.3. Cách phòng chống Keylogger

Cách phòng tránh hiệu quả nhất là diệt trừ toàn bộ các chương trình đang theo dõi bàn phím. Một số chương trình như là Keylogger Killer của Totto quét các process tìm các chương trình theo dõi cùng lúc quá nhiều ứng dụng. Thế nhưng một số chương trình tốt (như các chương trình giúp gõ bàn phím Unikey, Vietkey) cũng dùng cách này nên có thể gây diệt lầm.

Nhưng điểm gây khó khăn nhất của cách dùng này là đa số các chương trình sử dụng tốt đều phải trả tiền (ví dụ như Spyware Doctor của Pctools, McAfee, Antispyware của McAfee, Bitdefender...). Đây cũng là một số cách phòng tránh keylogger: Đổi trật tự gõ phím;

Copy chuỗi ký tự; Dùng phần mềm diệt Virus; Cài đặt thêm tường lửa trong hệ điều hành, trình duyệt để giúp keylogger không thể cài đặt và xâm nhập được trên máy tính của bạn; Dùng bàn phím ảo. (Hoàng Bách, 2018)

3.5. Trojan Dropper

3.5.1. Khái niệm

Dropper là một phần mềm hay chương trình thiết kế chủ yếu để chuyển một payload đến hệ thống mục tiêu. Mục tiêu chính của Dropper là cài đặt mã malware vào máy tính mục tiêu, tránh khỏi cảnh báo và phát hiện. Nó sử dụng rất nhiều phương pháp để lan truyền và cài đặt malware.

3.5.2. Lịch sử của Trojan Dropper

Dropper xuất hiện từ ý tưởng về các tệp phần mềm độc hại có thể tải xuống các mô-đun bổ sung (tức là Agobot, được phát hành vào năm 2002).Một ví dụ thú vị về trình tải xuống hiện đại là OnionDuke (được phát hiện vào năm 2014), được thực hiện bởi các nút Tor bị nhiễm. Khi người dùng tải xuống phần mềm thông qua proxy Tor bị nhiễm độc, OnionDuke sẽ đóng gói tệp gốc và thêm một phần mềm độc hại vào đó. (Malwarebyte, 2016)

3.5.3. Phương thức lây nhiễm

Người dùng bị nhiễm do sử dụng một số tài nguyên trực tuyến chưa được xác thực. Hậu quả của các hoạt động như: Nhấp vào các liên kết độc hại hoặc truy cập các trang web mờ ám; Tải xuống các chương trình miễn phí không xác định; Mở tệp đính kèm được gửi bằng thư rác; Cắm ổ bị nhiễm; Sử dụng proxy bị nhiễm (như trong trường hợp của OnionDuke). (Malwarebyte, 2016)

Những chương trình này được tin tặc tạo ra để tránh sự phát hiện và ngăn chặn của các phần mềm diệt Virus.Từ đó, Trojan sẽ hoạt động ngầm trong máy tính của nạn nhân và bị điều khiển bởi hacker. (SecurityBox, 2018)

3.5.4. Biện pháp khắc phục

Trong những trường hợp như vậy, để thoát khỏi trình tải xuống, cần phải tìm và xóa các khóa đã tạo và tệp ẩn. Những gì còn lại là thực hiện các bước thích hợp để vô hiệu hóa. Mức độ khó khăn của việc làm sạch hệ thống khác nhau vì tải trọng có thể thuộc nhiều loại khác nhau. Cách phổ biến nhất là sử dụng các công cụ chống phần mềm độc hại tự động, chất lượng tốt và quét toàn bộ hệ thống. Malwarebyte (2016)

3.6. Trojan FakeAV

FakeAV là phần mềm diệt Virus, nhưng bản chất Trojan-FakeAV lại đòi tiền từ người dùng nếu muốn diệt Virus hoặc loại bỏ lỗ hổng trong thiết bị của mình.

Bùng nổ phần mềm diệt Virus giả mạo - Fake AV năm 2010 đã chứng kiến sự bùng nổ lượng máy tính bị nhiễm Virus giả mạo phần mềm diệt Virus, lên đến 2,2 triệu lượt, gấp 8,5 lần so với con số 258 000 của năm 2009. Phần mềm giả mạo liên kết người dùng tới các website giả mạo quét Virus trực tuyến, nhằm cài đặt mã độc lên máy tính là đặc điểm chung của các FakeAV. Nguyên nhân chính khiến rất nhiều người sử dụng tại Việt Nam đã nhiễm loại Virus này là do thói quen dùng phần mềm không có bản quyền.

Giả mạo file dữ liệu, xu hướng mới của Virus hơn 1,4 triệu lượt máy tính đã bị nhiễm dòng Virus giả mạo thư mục, giả mạo file ảnh, file word, file excel... Bằng cách sử dụng icon để ngụy trang, file thực thi của Virus trông có vẻ giống hệt một thọ mục hay một file dữ liệu dạng ảnh, file word, file excel... (Trần Thị Hằng, 2016)

3.7. Trojan IM

Các chương trình Trojan-IM được tạo ra với mục đích đánh cắp thông tin đăng nhập và mật khẩu của người dùng thông qua các ứng dụng tin nhắn tức thời như ICQ, MSN Messenger, AOL Instant Messenger, Yahoo, Skype và nhiều hơn nữa. (SecurityBox, 2018)

Trojan này nhắm mục tiêu đến các tin nhắn, đánh cắp thông tin đăng nhập và mật khẩu của người dùng trên nền tảng IM. Trojan không chỉ ảnh hưởng đến các thiết bị như máy tính hay laptop mà còn ảnh hưởng đến cả các thiết bị di động bao gồm điện thoại di động và máy tính bảng. Ngoài ra các ứng dụng này cũng có thể đánh cắp thông tin trên thiết bị nạn nhân và kiếm lợi nhuận bằng cách gửi tin nhắn SMS tới số điện thoại có phí bảo hiểm. (Trọng Tâm, 2018)

3.8. Trojan Ransomware

3.8.1. Khái niệm

Ransomware Trojan là một loại phần mềm được thiết kế ra để tống tiền nạn nhân. Thông thường, Ransomware sẽ yêu cầu một khoản thanh toán để hoàn tác các thay đổi mà Virus Trojan đã thực hiện đối với máy tính của nạn nhân.

3.8.2. Nguồn gốc của Ransomware

Ransomware có thể xâm nhập vào máy tính của người sử dụng khi: tìm và dùng các phần mềm crack, bấm vào quảng cáo, truy cập web đen đổi trụy, truy cập website giả mạo, tải và cài đặt phần mềm không rõ nguồn gốc, file đính kèm qua email spam..... (Techopedia, 2014)

3.8.3. Lịch sử hình thành và phát triển Ransomware

Lần đầu tiên, Ransomware được phát hiện vào khoảng giữa năm 2005 - 2006 tại Nga. Những bản báo cáo đầu tiên của TrendMicro là năm 2006, với biến thể TROJ_CRYZIP.A - 1 dạng Trojan sau khi xâm nhập vào máy tính của người dùng, sẽ lập tức mã hóa, nén các file hệ thống bằng mật khẩu, đồng thời tạo ra các file *.txt với nội dung yêu cầu nạn nhân trả phí 300$ để lấy lại dữ liệu cá nhân. Dần dần phát triển theo thời gian, các Ransomware tấn công tiếp đến các file văn bản và hệ thống như *.DOC, *.XL, *.DLL, *.EXE...

Năm 2011 một dạng khác của Ransomware là SMS Ransomware đã được phát hiện. Cách thức của SMS Ransomware đó là người dùng phải gửi tin nhắn hoặc gọi điện thoại đến số điện thoại của hacker, cho đến khi thực hiện xong thủ tục chuyển tiền cho hacker.

TrendMicro đã ghi nhận được rất nhiều vụ tấn công xảy ra khắp Châu Âu vào đầu năm 2012. 1 biến thể Ransomware khác đã từng lây lan rất mạnh ở 2 khu vực chính là Pháp và Nhật, cùng với cách thức hoạt động của Ransomware nguyên bản. (TOP9XY, 2015), (RANSOMWARE Techopedia, 2014)

3.8.4. Cách thức hoạt động của Ransomware

Khi đã xâm nhập và kích hoạt trong máy tính của người dùng, Ransomware sẽ đồng thời thực hiện các tác vụ như sau: khóa màn hình máy tính, mã hóa bất kỳ file tài liệu nào mà nó tìm được, tất nhiên là sẽ có mật khẩu bảo vệ.

Nếu trường hợp 1 xảy ra, người dùng sẽ không thể thực hiện được bất kỳ thao tác nào trên máy tính. Còn trường hợp thứ 2 thì Ransomware sẽ mã hóa toàn bộ các file văn bản (thường là file Office như *.doc, *.xls... file email và file *.pdf), những file này sẽ bị đổi đuôi thành những định dạng nhất định nào đó, có mật khẩu bảo vệ, bạn không thể thực hiện bất kỳ thao tác nào như copy, paste, đổi tên, đổi đuôi hoặc xóa. Ransomware hoặc gọi là Scareware có cách thức hoạt động tương tự như những phần mềm bảo mật giả mạo - FakeAV (1 loại Malware). (Techopedia, 2014)

3.9. Trojan SMS

SMS Trojan là một loại mã độc dành riêng cho điện thoại di động với mục đích là đăng ký nạn nhân vào các số nhắn tin có mức phí bảo hiểm. Vì loại dịch vụ này thường thông báo cho người dùng rằng anh ta đã được đăng ký thành công, một số Trojan thuộc loại này lọc SMS từ các số điện thoại Premium đó để người dùng vẫn không biết về sự lây nhiễm.

Có thể thấy người dùng khởi động ứng dụng độc hại và một tin nhắn SMS đã được gửi. Do đó, một cuộc tấn công bởi loại phần mềm độc hại này, được thiết kế dành riêng để nhắm mục tiêu thiết bị di động, tạo ra lợi nhuận cho kẻ tấn công. (welivesecurity.com, 2011)

3.10. So sánh sự khác nhau giữa Trojan Horse, Virus và Worm

Virus: có thể tự cài đặt chính nó vào trong các file chạy chương trình. Điều này có nghĩa là máy tính của bạn có thể chứa Virus nhưng chưa chắc đã bị ảnh hưởng, trừ khi bạn cho chạy chương trình đó. Virus đươc phán tán qua việc chia sẻ các file hay gửi mail có đính kèm Virus.Virus không sự tác động của con người thì không lây lan được. Một số Virus gây ra có tác tụng gây phiền nhiễu cũng có thể gây ra các việc làm hỏng phần cứng, phần mềm, hoặc các tập tin làm việc của chúng ta thường tất cả các Virus đươc gắn vào tập tin thực thi .exe.

Worm: lợi dụng các tính năng truyền file hay thông tin trên hệ thống để di chuyển. Sự nguy hiểm của worm là từ trong hệ thống của bạn, nó có thể tự gửi chính nó đến hàng chục,

hàng trăm, thậm chí hàng ngàn máy khác và cứ thế nhân lên, làm cho các máy chủ web, máy chủ mạng, và cả máy tính bị tràn bộ nhớ đến mức không thể hoạt động nữa. Đối tượng dễ bị worm tấn công: đơn vị cho thuê máy chủ, các server game, các server ngân hàng, server tòa soạn báo điện tử,...

Trojan: Trojan xuất hiện lúc đầu như là một phần mềm có ích, nhưng nó sẽ ngay lập tức trở nên nguy hiểm ngay khi bạn cái nó hay chạy nó lần đầu tiên trên máy tính. Ví dụ: trang download.com.vn, bạn cài phần mềm trên đó là dính quảng cáo. Khi Trojan đươc phán tán đến máy khác, thông thường bên nhận sẽ chạy nó vì người dùng sẽ thấy nó như là một phần mềm hay file đáng tin cậy và được gửi từ một nguồn đáng tin cậy. Khi Trojan được kích hoạt trên máy tính của bạn thì hậu quả mà nó gây ra có thể sẽ khác nhau. Giúp cho kẻ lạ có thể thâm nhập vào hệ thống mở cổng và làm hư hại hay lấy cắp thông tin. Không giống như Virus và worm, Trojan không phán tán bằng cách làm cho các file khác nhiễm cũng như không tự nó nhân bản lên được. (VDO Data, 2019).

4. Kết luận

Tóm lại, bài báo này đã trình bày về lịch sử phát triển của Trojan Horse trong giai đoạn từ năm 1974 đến năm 2000 và từ năm 2000 đến nay. Bài báo cũng đã tổng hợp khá đầy đủ và sâu sắc về Trojan Horse và đầy đủ nhất cho đến nay. Tuy nhiên, còn một số loại Trojan mà bài báo vẫn chưa đề cập vì rất ít tài liệu viết về loại Trojan đó. Qua bài báo này đã giúp được cho mọi người nắm rõ hơn và đầy đủ hơn về Trojan Horse. Chúng tôi hy vọng sẽ có cơ hội đào sâu hơn để cho bài viết được hoàn chỉnh hơn trong tương lai. Bài viết kế tiếp sẽ đi sâu về những phương pháp ngăn chặn hiệu quả và các kỹ thuật code mã Trojan.

TÀI LIỆU THAM KHẢO

[1] Quách Chí Cường (2019). "Backdoor là gì? Cách phát hiện và phòng tránh Backdoor", xem 19/01/2021, <https://cuongquach.com/backdoor-la-gi.html>.

[2] Trịnh Duy Thanh (2019). "Back door là gì? Back door có lợi hay có hại với hệ thống?", xem 19/01/2021, <https://bkhost.vn/posts/backdoor-la-gi>.

[3] Hồng Nguyễn (2020). "Backdoor là gì? Làm sao để phát hiện và ngăn chặn được Backdoor?", xem 19/01/2021,<https://timviec365.vn/blog/backdoor-la-gi-new9007.html>.

[4] Duy Vinh (2018). "Backdoor là gì?", xem 19/01/2021, <https://thuthuat.taimienphi.vn/backdoor-la-gi-40763n.aspx>.

[5] Giang(2018). "Trojan Horse là gì? Tác hại và ví dụ", ngày 19/01/2021, <https://bizflycloud.vn/tin-tuc/web-service-la-gi-loi-ich-va-vi-du-20180908095107017.htm>.

[6] Nguyễn Hữu Duy Khang (2019)., xem 19/01/2021, <http://duykhang9a12.simplesite.com/444084685>.

[7] Wikipedia (2018), "Phần mềm gián điệp", xem 19/01/2021,

[8] <https://vi.wikipedia.org/wiki/Ph%E1%BA%A7n_m%E1%BB%81m_gi%C3%A1n_%C4%91i%E1%BB%87p>.

[9] Quách Chí Cường (2019a). "Spyware là gì ? Phần mềm gián điệp là gì ?", xem 19/01/2021, <https://cuongquach.com/spyware-la-gi.html>.

[10] Tố Uyên(2012). "Tiểu luận tìm hiểu về Trojan Horse", ngày 20/01/2021, <https://ebookxanh.com/tai-lieu/tieu-luan-tim-hieu-cong-nghe-web-service-680921.html>.

[11] Long Vân (2014). "Rootkit là gì? Đặc điểm của Rootkit?", xem 19/01/2021, <https://longvan.net/rootkit-la-gi-dac-diem-cua-rootkit.html>.

[12] Hồng Nhi (2018). "Rootkit là gì? Cách quét rootkit nhanh và hiệu quả", xem 19/01/2021, <https://blog.tinohost.com/cach-quet-rootkit-nhanh-va-hieu-qua/>.

[13] Lê Tuyết Mai(2012). "Luận văn: Một số biện pháp phòng tránh Trojan Horse", ngày 23/01/2021,<https://ebookxanh.com/tai-lieu/luan-van-he-thong-quan-ly-dang-ky-thue-su-dung-web-service-685940.html>.

[14] GP Coder (2019). "Tìm hiểu về Trojan", ngày 19/01/2021, <https://gpcoder.com/5572-tim-hieu-ve-web-service/>.

[15] Hoàng Quang Thụy (2016). "Tấn công rootkit trong Oracle", xem 19/01/2021, <https://123doc.net/document/3624515-tan-cong-rootkit-trong-oracle-at8a-hvktmm.htm>.

[16] Hacker/Malware (2008). "Những điều cần biết về rootkit", xem 19/01/2021, <http://m.antoanthongtin.vn/hacker-malware/nhung-dieu-can-biet-ve-rootkit-100074>.

[17] Will Kenton (2018). "Trojan Banker", xem 19/01/2021, <https://www.investopedia.com/terms/b/banker-Trojan.asp>.

[18] Education(2019). "Đề tài: Tìm hiểu về các loại Trojan", ngày 20/01/2021, <https://www.slideshare.net/trongthuy3/luan-van-tim-hieu-ve-web-service-va-ung-dung-hay-9d>.

[19] Malwarebytes (2020). "Trojan Banker", xem 19/01/2021, <https://blog.malwarebytes.com/detections/Trojan-banker/>.

[20] Wikipedia (2020). "Trojan Banker", xem 19/01/2021, <https://en.wikipedia.org/wiki/Tiny_Banker_Trojan>.

[21] NguyenThiHue (2015). "Tìm hiểu ban đầu về Trojan horse", ngày 19/01/2021, <https://viblo.asia/p/tim-hieu-ban-dau-ve-web-service-jdWrvwQ5Mw38>.

[22] Malekal.com (2019). "Trojan Banker: botnet chuyên đánh cắp tài khoản ngân hàng", xem 19/01/2021, <https://www.malekal.com/Trojan-banker-botnet-vol-compte-bancaire/>.

[23] Techopedia (2014). "Proxy Trojan", xem 19/01/2021, <https://www.techopedia.com/definition/4070/proxy-Trojan>.

[24] Giangpth (2018). "Trojan là gì? - Những điều cần biết", xem 19/01/2021, <https://bizflycloud.vn/tin-tuc/Trojan-nhung-dieu-can-biet-20180510170204207.htm>.

[25] Aviva Zacks (2018). "Trojan Horse là gì và Làm Thế Nào Để Bảo Vệ Chống Lại Nó", xem 19/01/2021, <https://vi.safetydetectives.com/blog/Trojan-horse-la-gi-va-lam-the-nao-de-bao-ve-chong-lai-no/>.

[26] Trung Quan Tri Vien (2019). "Web Service là gì? Tìm hiểu về web service", ngày 19/01/2021, <https://ghouse.com.vn/web-service-la-gi-tim-hieu-ve-web-service>.

[27] Tuấn Phong (2020). 'Trojan là gì? Làm sao để tránh Trojan tấn công?", xem 19/01/2021, <https://quantrimang.com/Trojan-la-gi-lam-sao-de-tranh-Trojan-tan-cong-168699>.

[28] Chaupm (2018). "Exploit là gì? Tấn công Exploit xảy ra như thế nào?", xem 19/01/2021,<https://bizflycloud.vn/tin-tuc/exploit-la-gi 20181123162650 94.htm>.

[29] Dương Nguyễn (2019). "Exploit là gì?", xem 19/01/2021, <https://quantrimang.com/computer-exploit-la-gi-163081>.

[30] SecurityBox (2018). "13 LOẠI VIRUS TROJAN GÂY HẠI MÁY TÍNH CỦA BẠN", xem 19/01/2021, <https://securitybox.vn/5024/11-loai-Virus-Trojan-gay-hai-may-tinh/>.

[31] Trọng Tâm (2018). "Trojan là gì? có nguy hiểm như Virus?", xem 19/01/2021, <https://thuthuat.taimienphi.vn/Trojan-la-gi-48560n.aspx>.

[32] Lan Lan(2012). "Nghiên cứu Trojan và ứng dụng trong thương mại điện tử" ngày 20/01/2021, <https://tailieu.vn/doc/luan-van-nghien-cuu-web-service-va-ung-dung-trong-thuong-mai-dien-tu-1230443.html>.

[33] Wikipedia (2019). "Keylogger", xem 19/01/2021, <https://vi.wikipedia.org/wiki/Keylogger>.

[34] Hoàng Bách (2018). "Keylogger là gì? tác hại và cách phòng tránh", xem 19/01/2021, <https://thuthuat.taimienphi.vn/keylogger-la-gi-36786n.aspx>.

[35] Malwarebyte (2016). "Trojan Dropper", xem 19/01/2021, <https://blog.malwarebytes.com/threats/Trojan-dropper/>.

[36] Kteam (2018). "Nguy cơ Malware - Cách lan truyền Malware và khái niệm Trojan", xem 19/01/2021, <https://www.howkteam.vn/course/51-phan-tich-lo-hong-bao-mat-vulnerability-analysis/ 71-nguy-co-malware--cach-lan-truyen-malware-va-khai-niem-Trojan-3815>.

[37] Rdom rname (2020). "What is Trojan Virus?", xem 19/01/2021, <https://curbjumperstreeteats.com/Virus-Trojan-la-gi-dinh-nghia>.

[38] Hoang Thi Kim Thuy(2012). "Luận văn: Trojan Horse và nguyên nhân gây hại", ngày 20/01/2021, <https://ebookxanh.com/tai-lieu/luan-van-web-services-va-tich-hop-ung-dung-685091.html>.

[39] Trần Thị Hằng (2016). xem 19/01/2021, <https://lib.hpu.edu.vn/bitstream/handle/123456789/25237/1_TranThiHang_CHCNTTK1.pdf?sequence=>.

[40] TOP9XY(2015). "RANSOMWARE", xem 19/01/2021, <https://it.die.vn/r/ransomware/>.

[41] Bùi Thị Lụa (2013). "Tìm hiểu về Virus Trojan Horse", xem 19/01/2021, <https://www.slideshare.net/saophaiyeuai/Virus-Trojan>.

[42] Kaspersky (2020). "Virus Trojan là gì?", xem 19/01/2021, <https://www.kaspersky.com/resource-center/threats/Trojans>.

[43] Tố Uyên(2012). "Tiểu luận tìm hiểu công nghệ Trojan", ngày 20/01/2021, <https://ebookxanh.com/tai-lieu/tieu-luan-tim-hieu-cong-nghe-web-service-680921.html>.

[44] Hồng Nhi (2018b). "Virus và Malwarw là gì? Tầm quan trọng của chương trình diệt Virus trên cloud hosting", xem 19/01/2021, <https://blog.tinohost.com/Virus-va-malware-la-gi/> Xem 23/09/2020.

[45] VDO Data (2019). "Sự khác nhau giữa Virus,Worm và Trojan Horse", xem 19/01/2021, <https://vdodata.vn/su-khac-nhau-giua-Virusworm-va-Trojan-horse/>.

[46] Database Answers(2002). "History of Web Service", ngày 19/01/2021, <http://www.databaseanswers.org/web_services_history.htm>.

[47] Maiphuongdc (2014). "Trojan Horse: con ngựa thành Troia phần mềm ác tính", xem 19/01/2021, <http://doc.edu.vn/tai-lieu/Trojan-horse-con-ngua-thanh-troia-phan-mem-ac-tinh-57724/>.

[48] welivesecurity.com(2011)., xem 19/01/2021, <https://www.welivesecurity.com/wp-content/uploads/2013/02/SMS_Trojan_Whitepaper.pd>.

[49] Hoàng Phương(2016). "Tìm hiểu về Trojan Horse", ngày 19/01/2021, <https://viblo.asia/p/tim-hieu-ve-webservice-ZnbRlD0QR2Xo>.

[50] Tech-FAQ (2012). "Virus Trojan", xem 19/01/2021, <https://www.tech-faq.com/Trojan-Virus.html>.

[51] Ugnius Kiguolis (2017)., xem 19/01/2021, <https://www.2-spyware.com/dialers-removal>.