hai kỹ thuật thường được sử dụng cho de phát hiện malware l dựa trên chữ ký và phát hiện dựa trên dị thường. Chống mĐộng cơ thông minh sử dụng chữ ký hoặc 'chuỗi byte' để phát hiện được biết

Phần mềm độc hại. Những chữ ký này được tạo ra bằng cách tháo rờiTập tin d một lựa chọn một số đoạn mã duy nhất.

Do đó, phát hiện dựa trên chữ ký rất hiệu quảCho phần mềm độc hại đã biết nhưng Hạn chế lớn là không có khả năng

Phát hiện các mã độc hại mới, không rõ đã dẫn đến các cuộc tấn công bằng không.

đề xuất một cách tiếp cận mới để trích xuất cấu trúcCtural và

Các tính năng hành vi

Luan van đề xuất một cách tiếp cận mới để trích xuất các tính năng hành vi thong qua viec goi cac ham API thuc thi, cac chinh sua trong regedit, cac lenh cmd, cac thu vien dll.

Chữ ký phần mềm độc hại là một dãy byte xác định duy nhất một phần mềm độc hại cụ thể (Vinod et al., 2009).Thông thường, một máy dò phần mềm độc hại sử dụng chữ ký phần mềm độc hại để xác định phần mềm độc hại như dấu vân tay. Phần lớn AVĐộng cơ được cung cấp cùng với cơ sở dữ liệu để thu thập thông tin về phần mềm độc hại hiện có để xác định sự độc hại,Tìm kiếm chữ ký mã hoặc các chuỗi byte trong khi quét hệ thống. Máy dò phần mềm độc hại quét hệ thốngỞ các vị trí khác nhau cho các chuỗi ký tự istic byte hoặc chữ ký (S ) phù hợp với một trong cơ sở dữ liệu vàTuyên bố sự tồn tại của phần mềm độc hại chặn quyền truy cập vào hệ thống. Quá trình kết hợp chữ ký được gọi làPhát hiện dựa trên chữ ký và hầu hết các công cụ AV truyền thống đều sử dụngphương pháp. Nó là một rất hiệu quả và hiệu quảĐể phát hiện phần mềm độc hại đã biết. Tuy nhiên, nhược điểm chính là không có khả năng phát hiện ra các phần mềm độc hại mới hoặc không rõMã và zero ngày tấn công. Do đó, cập nhật công cụ phát hiện hoặc phần mềm AV hàng ngày với phần mềm độc hại mới nhấtChữ ký là điều cần thiết để đánh giá hệ thống máy tính chống lại tất cả các phần mềm độc hại được biết đến. Do đó, càng nhiềuchữ ký phần mềm độc hại ( s ) được đưa vào động cơ AV, các Effe hơn ctive nó là trong việc phát hiện malware đã biết mới nhất.

Ngoai ra do viec phan tich tinh doi hoi rat nhieu cong suc cho nen thoi gian phat hien se cham hon.

Vuot qua AV:

Để tránh sự phát hiện của các động cơ AV, các phần mềm độc hại đang sử dụng các kỹ thuật obfuscating (Alazab, 2009)

Như đóng gói (Guo và cộng sự, 2008), đa hìnhIsm (Stepan, 2005) và biến chất (Bruschi et al., 2006) trong

Để biến đổi phần mềm độc hại hiện có. Biến đổi đa hình biến đổi phần mềm độc hại d-đa dạngEd malcode vào một Mới

Mã mà không ảnh hưởng đến chức năng gốc hoặc puR đặt ra để quá trình quét AV của động cơ bỏ qua Phát hiện chữ ký

Ky thuat Ofucation:

Các tác giả về phần mềm độc hại đang liên tục phát triển công nghệ mới nIques để tạo và áp dụng obfuscation Kỹ thuật

T (P) trên một chương trình phần mềm độc hại (p) để tạo ra một obfUscated chương trình ( p '), do đó mRất khó để

Kỹ sư dự bị và giải mã chữ ký thành công, thậm chí cả hai chương trình, p và p ' đang có

Cùng chức năng và triển lãm thứE cùng ảnh hưởng. Mặt khác, vì p và p ' có trình tự byte khác nhau,

Động cơ AV và các kỹ sư đảo ngược đang áp dụng kỹ thuật khử tiếng ồnEs D (p ') trên bữa ăn đã được obfuscatedRam ( p ' )

Để phân tích phần mềm độc hại và phát hiện phần mềm độc hại như thể hiện trong hình 1.

Ky thuat Packer:

Packers thường được sử dụng ngày hôm nay fHoặc mã Obfuscation hoặc nén. Người chơi đóng gói là softwLà những chương trình

Có thể được sử dụng để nén và mã hóa PE trong bộ nhớ seco ndary Và để khôi phục lại hình ảnh ban đầu thực thi

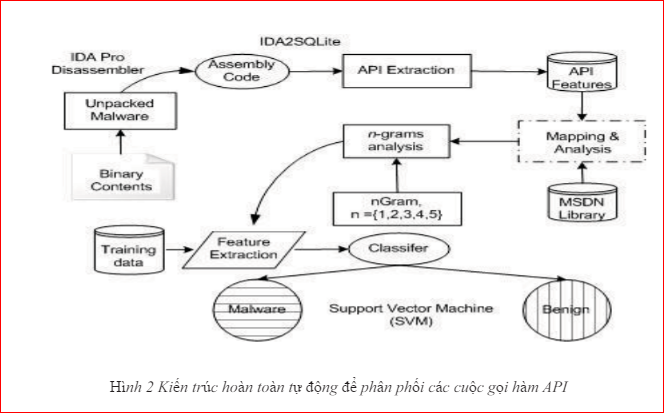
Khi nạp vào mem chínhBộ nhớ RAM. Các tác giả về phần mềm độc hại không cần phải thay đổi dòng mã lệnh để thay đổi

Chữ ký phần mềm độc hại mAinly vì, thay đổi bất kỳ chuỗi byte trong PE kết quả Một byte mới khác

Chuỗi trong PE đóng gói mới được sản xuất

Phần mềm độc hại đa hình sử dụng mã hóa và nối dữ liệu / dữ liệu đang chờ xử lý để thay đổi cơ thể củaPhần mềm độc hại, và hơn nữa, nó thay đổi thói quen giải mã từ nhiễm trùng sang nhiễm miễn làCác phím mã hóa thay đổi. Điều này đã khiến các chuyên gia AV phát triển các kỹ thuật quét khác nhau,M chuỗi matchi đơn giảnNg Đến các kỹ thuật phức tạp hơn như quét X-RAYING (Perriot & Ferrie, 2004). Năm 2006 SymAntec Internet Báo cáo về mối đe dọa bảo mật cho biết các phần mềm Malware Đa Hình dạng Phát hiện như w32.Polip và w32.Detnat rất nhiềuKhó khăn và phức tạp hơn các loại phần mềm độc hại khác (Turner, 2006).

Phần mềm độc hại biến đổi thay đổi mã chính nó mà không cần sử dụng mã hóa. Nói chung, có bốnCác kỹ thuật thường được sử dụng cho sự biến dạng phức tạp (metamorphic obfuscation). Đây là, i) Chèn Dead-mã đó là có nghĩa là làmKhông có gì chẳng hạn như một dãy NOP (không có hoạt động thực hiện), ii) Mã Tr xác định rằng thay đổiHướng dẫn như sử dụng các hướng dẫn của JMP để trình tự hướng dẫn khác với bản gốc,Iii) Đăng ký chuyển nhượng lại như thay thế push ebx witH đẩy eax để trao đổi tên đăng ký, và iv)Chỉ dẫn thay thế mà là thay thế các hướng dẫn trong hướng dẫn khác nhau với cùng một số kết quảCác tác giả sử dụng một từ điển cơ sở dữ liệu của các trình tự hướng dẫn tương đương để làm cho nó dễ dàng hơn và nhanh hơn



Malware Detection Based on Structural and Behavioural Features of API Calls (PDF Download Available). Available from: https://www.researchgate.net/publication/49285561\_Malware\_Detection\_Based\_on\_Structural\_and\_Behavioural\_Features\_of\_API\_Calls [accessed Apr 21, 2017].

*Malware Detection Based on Structural and Behavioural Features of API Calls (PDF Download Available)*. Available from: <https://www.researchgate.net/publication/49285561_Malware_Detection_Based_on_Structural_and_Behavioural_Features_of_API_Calls> [accessed Apr 21, 2017].

*Malware Detection Based on Structural and Behavioural Features of API Calls (PDF Download Available)*. Available from: <https://www.researchgate.net/publication/49285561_Malware_Detection_Based_on_Structural_and_Behavioural_Features_of_API_Calls> [accessed Apr 21, 2017].

Malware Detection Based on Structural and Behavioural Features of API Calls (PDF Download Available). Available from: https://www.researchgate.net/publication/49285561\_Malware\_Detection\_Based\_on\_Structural\_and\_Behavioural\_Features\_of\_API\_Calls [accessed Apr 21, 2017].  
*Malware Detection Based on Structural and Behavioural Features of API Calls (PDF Download Available)*. Available from: <https://www.researchgate.net/publication/49285561_Malware_Detection_Based_on_Structural_and_Behavioural_Features_of_API_Calls> [accessed Apr 21, 2017].