<https://labs.mwrinfosecurity.com/assets/resourceFiles/mwri-behavioural-ransomware-detection-2017-04-5.pdf>

2. Các thế mạnh của ransomware

Trước khi xem xét làm thế nào để bảo vệ chống lại ransomware, người ta phải hiểu được vấn đề ransomware.

Nguồn gốc của thành công của ransomware nằm trong mô hình kinh doanh có lợi nhuận cao của nó. Khoảng 3% [2] của Mỹ

Các công ty trả khoản tiền chuộc. Điều này có vẻ thấp nhưng vẫn làm cho ransomware một cách hiệu quả

Tống tiền.

Bên cạnh lợi tức đầu tư cao, ransomware là một con đường hấp dẫn cho kẻ tấn công mạng như nó là

Dường như không có lợi cho thương mại-off-thưởng cao như thường thấy trong kinh doanh độc hại khác (hoặc hợp pháp)

Thực hành. Phần thưởng cao thường có nghĩa là có nguy cơ cao và / hoặc nỗ lực cao, tuy nhiên những kẻ tấn công ransomware có

Ít có cơ hội bị bắt, và một khi ransomware được phát triển, tống tiền là tương đối dễ dàng.

Trên bình diện kỹ thuật, thành công gần đây của ransomware có thể được gán cho ba người đề xướng chính:

+ Hệ thống thanh toán vô danh và liền mạch - Các loại tiền tệ cung cấp khả năng di chuyển nhanh

Tiền bất cứ nơi nào trên thế giới với phong nha giấu tên nếu được sử dụng đúng cách. Điều này rất có lợi

Cho kẻ tấn công ransomware, có thể hoạt động trên quy mô toàn cầu trong khi vẫn tài chính

Không thể dùng được.

Khi tiền ký quỹ-tiền tệ như một hình thức trả tiền chuộc ban đầu được sử dụng khoảng bốn năm trước đây,

Nó chỉ có được thành công biên. Nạn nhân không muốn trả một khoản tiền chuộc bằng đồng tiền crypto

Vì dư luận đã không nhìn thấy các loại tiền tệ như một hệ thống tài chính hợp pháp. Tuy nhiên, với

Sự tăng lên của sự tăng trưởng và tiếp xúc với các đồng tiền tiền tệ, đã có một sự thay đổi tích cực trong công chúng

Tình cảm

Sự thay đổi trong tình cảm của công chúng đã củng cố các loại tiền tệ như là hình thức chi phối chủ đạo của tiền chuộc

Thanh toán, mà rất nhiều lợi ích ransomware kẻ tấn công.

+ Phát triển công sức thấp - Các gia đình ransomware mới và các biến thể được phát hiện hàng ngày.

Điều này một phần là vì ransomware tương đối dễ phát triển. Với sự sẵn có của tiêu chuẩn

Các thư viện mật mã, các chương trình mã hóa mã hóa sử dụng RSA và AES là một nhiệm vụ tầm thường.

Hơn nữa, thậm chí cả ransomware phát triển kém (với các thói quen mã hóa yếu), đã được

Được tìm thấy có hiệu quả trong việc tống tiền hoàn toàn bằng cách sử dụng các thủ thuật gây sợ hãi2.

Với xu hướng phát triển của Ransomware-as-a-Service (RaaS), ngay cả những kẻ tấn công không kỹ thuật cũng đang Có thể nhanh chóng tạo ra ransomware tùy biến. Với RaaS, các nhà phát triển ransomware tạo ra một

Bộ dụng cụ phát triển ransomware dễ sử dụng, mà khách hàng có thể mua và sử dụng để tạo ra

Ransomware trả tiền cho địa chỉ của họ crypto-tiền tệ.

2 Kẻ tấn công sợ hãi bao gồm đe dọa xóa các tập tin hoặc xóa khóa giải mã sau một thời gian quy định đã mất hiệu lực.

3

Labs.mwrinfosecurity.com

Tiếp tục hỗ trợ phát triển ransomware là các dự án ransomware nguồn mở như

EDA23 và Hidden Tear4. Ban đầu được dự định cho các mục đích giáo dục, ransomware mã nguồn mở

Đã được sử dụng như một khuôn mẫu để tạo ra hàng trăm biến thể ransomware khác nhau.

Chi phí phân phối hiệu quả - Các kẻ tấn công Ransomware sử dụng phân phối độc hại có trả tiền

Dịch vụ để phân phối ransomware một cách dễ dàng trên quy mô toàn cầu. Những dịch vụ phân phối này sử dụng

Một loạt các nền tảng như spam, drive-by-downloads, malvertising và khai thác bộ dụng cụ.

Trên một khoản thanh toán tải chu trình giảm giá thành công, kẻ tấn công không yêu cầu phải làm thêm

Tống tiền. Việc xác nhận thanh toán tiền chuộc và cấp chìa khóa giải mã (nếu có)

Thường tự động sử dụng phản hồi email tự động. Điều này trái ngược với mục tiêu

Các cuộc tấn công mà những kẻ tấn công phải lọc dữ liệu ra và hiểu giá trị của dữ liệu đã được

Bị đánh cắp, hoặc hiểu được tổ chức cụ thể và tìm ra cách để trích tiền từ họ.

Sự thành công liên tục của một mối đe dọa an ninh mạng đe doạ đến sự yếu kém trong việc phòng vệ trung bình hệ thống máy tính. Theo khuôn khổ an ninh mạng không dây NIST [2], cần phải có năm khía cạnh cốt lõi chiến thuật chính

Để giảm thiểu mối đe dọa: xác định, bảo vệ, phát hiện, đáp ứng và phục hồi. Bài báo này đưa ra những chi tiết cụ thể

Phát hiện ra ransomware. Để bắt đầu, chúng tôi bắt đầu với một mô tả của cơ chế phát hiện được tìm thấy

Trong máy quét virus thương mại điển hình.

3. Phát hiện phân tích dựa trên tĩnh

Phát hiện phần mềm độc hại sử dụng phân tích dựa trên tĩnh có nghĩa là phân tích mã của một ứng dụng trước

Thực hiện để xác định xem nó có khả năng hoạt động độc hại không. Nếu phân tích tĩnh tìm thấy bất kỳ độc hại

Mã, tệp thi hành sẽ bị dừng lại khi khởi chạy.

Loại phân tích tĩnh phổ biến nhất thường được sử dụng trong máy quét vi-rút thương mại là

Gọi là phân tích chữ ký. Trong phân tích chữ ký, chuỗi mã mẫu (chữ ký) được trích xuất

Từ mã của ứng dụng đích và so với một kho lưu trữ các mẫu mã độc hại đã biết.

Việc phát hiện dựa trên chữ ký dựa vào một kho lưu trữ khổng lồ của các chữ ký mã độc hại. Kho này

Cần phải được cập nhật thường xuyên để duy trì hiện tại, đó không phải là một nhiệm vụ tầm thường. Thương mại vi rút

Các máy quét thường có các nhóm các nhà nghiên cứu không gian mạng lớn tiếp tục khám phá, điều tra

Và trích chữ ký độc hại.

Hạn chế của phân tích tĩnh

Lỗ hổng cơ bản của phát hiện dựa trên chữ ký là không có khả năng phát hiện phần mềm độc hại chưa biết

Chưa được biến thành chữ ký. Một thực thi độc hại chỉ có thể phát hiện được khi nó đã được báo cáo

Độc hại và được thêm vào kho lưu trữ chữ ký độc hại. Sự phản ứng của điều này là ba lần cho

Hiệu quả phát hiện dựa trên tĩnh:

+ Không có hiệu quả chống lại sự nhầm lẫn mã - Để bỏ qua việc phát hiện dựa trên chữ ký, các nhà phát triển phần mềm độc hại

Sử dụng kỹ thuật obfuscation mã để lặp lại các phần mềm độc hại để mỗi phiên bản xuất hiện

khác nhau. Nghiêm túc, sự ngụy trang mã này không ảnh hưởng đến hành vi nguy hiểm dự định,

Chỉ ảnh hưởng đến cách nó được tĩnh nhận thức bởi một hệ thống phát hiện con người hoặc dựa trên chữ ký.

Đối với các cuộc tấn công ransomware, kỹ thuật obfuscation mã thường được sử dụng khi tạo ra

Tải trọng ở phía máy chủ dưới dạng một "nhà máy sản xuất phần mềm độc hại". Nhà máy sản xuất phần mềm độc hại là phương pháp

Tự động tạo ra các khối lượng lớn các biến thể độc hại-băm độc hại của bản gốc

Phần mềm độc hại mã sử dụng mã obfuscation. Một ví dụ về cuộc tấn công của nhà máy sản xuất phần mềm độc hại đã được nhìn thấy trong

Cerber ransomware [4], nơi mà máy chủ tấn công đã có thể tạo ra các mẫu tìm kiếm độc đáo mới

Mỗi 15 giây.

Các hình thức khác của obfuscation mã xảy ra ở phía nạn nhân của nơi mà các phần mềm độc hại giải nén một

Biến thể duy nhất của payload thực thi mỗi khi nó thực thi. Loại phần mềm độc hại này được gọi

Để tự morphing vì nó có thể nhân bản các phiên bản morphed của chính nó. Được sắp xếp theo cấp độ

Phức tạp để phát triển, tự morphing phần mềm độc hại rơi vào ba loại: oligomorphic,

Đa hình và biến chất. Tham khảo [5] để biết thêm chi tiết về kỹ thuật.

Hiện nay, sự ngớ ngẩn tự morphing hiếm khi được tìm thấy trong ransomware. Tuy nhiên, như sự phát triển

Tiếp tục ransomware, người ta có thể mong đợi một gia tăng ransomware tự morphing. Đối với một

5

Labs.mwrinfosecurity.com

Ví dụ về công thức ransomware tự sửa, tham khảo gia đình Virlock [6], tránh trật tự tĩnh

Phát hiện bằng cách sử dụng đa hình.

+ Không hiệu quả với đầu ra biến thể cao - Phân tích dựa trên chữ ký ít hiệu quả hơn đối với phần mềm độc hại

Các loại có chu kỳ phát triển nhanh và sản lượng biến thể. Đây là vấn đề cho signaturebased

Hệ thống dò tìm như ransomware tìm kiếm mới đang được phát triển xa nhanh hơn mới

Chữ ký có thể được tạo ra, thử nghiệm và bổ sung vào kho phần mềm độc hại.

+ Không hiệu quả với các cuộc tấn công được nhắm mục tiêu - Điều này đặc biệt liên quan đến trường hợp ransomware,

Nơi tấn công ransomware nhắm mục tiêu xảy ra thường xuyên hơn. Thay vì phân phối mới

Phát triển ransomware, các nhà phát triển có thể chọn để lần đầu tiên giải phóng ransomware mới trên rất

Cụ thể, các tổ chức được lựa chọn tốt. Tham khảo [3] ví dụ về một ransomware được nhắm mục tiêu

tấn công.

Do đó rõ ràng là để ngăn chặn thành công của ransomware, một sự thay đổi mô hình theo cách nó là

Phát hiện phải xảy ra. Việc phát hiện ra ransomware mới nên được xem là không chỉ khả thi mà còn là một

Yêu cầu. Để kết thúc này, chúng tôi giới thiệu phương pháp phân tích dựa trên động, một cách tiếp cận hiện đại nhằm

Để đánh giá một thực thi không phải bởi sự xuất hiện của nó, nhưng do hành động của nó.

SO SANH TINH VA DONG

4. Phát hiện phân tích động cơ (hành vi)

Phát hiện phân tích dựa trên động cho phép giám sát trực tiếp các quy trình, để xác định xem có

Đang hành xử với bất kỳ ý định độc hại. Bất kỳ quy trình hành xử độc ác nào sẽ bị gắn cờ là nguy hiểm

Và chấm dứt.

4.1 Phân tích tĩnh so với phân tích động

Có thể khái quát sự khác biệt giữa phân tích tĩnh và hành vi để phát hiện trong những điều sau

Cách: trong phân tích tĩnh, suy luận của các đặc điểm hành vi được thực hiện từ tập tin nhị phân của một không rõ

Thực thi. Hành vi inferred này sau đó được sử dụng bởi một thuật toán kết hợp đơn giản để gán một mức độ đe dọa

(Tức là an toàn hoặc độc hại). Trong phân tích hành vi, các đặc tính hành vi của thực thi được biết

Như nó đang được quan sát trong thời gian thực, và suy luận được thực hiện bởi một thuật toán quyết định quy nạp trên

mức độ nguy hiểm.

Sự khác biệt chính giữa phát hiện tĩnh và hành vi là điểm mà tại đó suy luận được thực hiện

- Phân tích tĩnh đánh giá các đặc điểm hành vi từ tệp tin nhị phân quan sát thấy, hành vi động gây ra mối đe dọa

Từ hành vi quan sát.

Đây là một sự khác biệt quan trọng vì kỹ thuật làm mờ tĩnh làm thay đổi hành vi suy luận mà không có

Thực sự ảnh hưởng đến hành vi thực sự, do đó làm cho nó dư thừa chống lại phát hiện dựa trên hành vi.

Trong phát hiện dựa trên hành vi, tất cả các tệp tin thực thi được coi là không xác định, ở đâu nó là đến tệp thực thi

Để chứng minh nó đang hành động một cách an toàn, không độc hại. Khi làm như vậy, khả năng phát hiện zero-day

(Không rõ) được cải thiện đáng kể.

4.2 Hành vi Ransomware

The fact that ransomware can be easily defined and sub-categorised within malware, implies there exists a well-defined behavioural construct in which we can predict an unknown process is ransomware. Behavioural-based analysis has been found to be highly effective for crypto ransomware detection because it exhibits core behavioural traits necessary for a data encryption attack that does not change from variant to variant or family to family. These behaviour traits can be categorised into two distinct tasks, the suspicious setup procedure and data encryption.

Thực tế là ransomware có thể dễ dàng xác định và phân loại phụ trong phần mềm độc hại, ngụ ý ở đó

Tồn tại một cấu trúc hành vi được xác định rõ ràng trong đó chúng ta có thể dự đoán một quá trình không rõ là ransomware.

Phân tích dựa trên hành vi đã được tìm thấy có hiệu quả cao đối với phát hiện ransomware crypto bởi vì

Nó thể hiện các đặc điểm hành vi cốt lõi cần thiết cho một cuộc tấn công mã hóa dữ liệu mà không thay đổi từ các biến thể Để biến thể hoặc gia đình với gia đình. Những đặc điểm hành vi này có thể được phân thành hai nhiệm vụ riêng biệt,

Thủ tục thiết lập đáng ngờ và mã hóa dữ liệu.

4.2.1 Suspicious setup behavior

Ransomware chia sẻ nhiều đặc điểm hành vi với các phần mềm độc hại khác, đặc biệt trong cách cài đặt bản thân

Trước khi phân phối tải trọng.

Hành vi chia sẻ này có thể được xem như một "công thức cho sự thành công" nói chung được theo sau là phần mềm độc hại

Nhà phát triển, có thể được phân loại thành sáu tính trạng hành vi:

Payload persistence – To ensure an attack is carried out to completion, it needs to persist across

reboots and be able to resume upon starting. Common techniques used by ransomware includes

placing a copy of its executable into the Windows startup directory, adding a registry run key

entry or setting up a scheduled task, to name a few.

+ Anti-system restore – To ensure that any malicious actions cannot be undone, malware may try

to disable system restore functionality. Ransomware for example, has been known to delete

Windows shadow copies, which prevents encrypted data from being restored to an older

unencrypted version.

+ Stealth techniques – malware will try to execute in a stealthy manner to avoid being noticed by

the user or detected by virus scanners. Common techniques include: injection into legitimate

processes, executing from the %AppData% directory and using executables named the same as

common Windows executables, to name a few.

Environment mapping – When malware is executed, it may map its system environment before

initiating its setup procedure. This is typically done to determine if it’s running on a real

computer or on a sandbox environment that could be attempting to analyse it.

Environment mapping is also used to determine security settings/policies, geographic location,

user language, file system architecture and network drives. Certain decisions about whether to

continue executing may rely on any of the environmental checks performed.

+ Network traffic – Ransomware that requires an internet connection, does so for two possible

tasks: downloading of payload related files, and/or for the communication of the encryption key.

To ensure malicious command and control servers do not easily get shut down by authorities,

malware developers use certain domain name registration tactics. Tactics include using a domain

generating algorithm to generate random domain names registered to anonymous top level

domains such as .xyz. .top and .bid.

+ Privilege elevation – Executing malicious system-related activities may require access rights

that are beyond those given to the victim’s user account. For example, ransomware may want

to overwrite the Master Boot Record, which can only be done as an Administrator. Simply

asking for administrator access may work or other privilege escalation techniques may be

used.

Labs.mwrinfosecurity.com

+ Đảm bảo tính kiên trì - Để đảm bảo cuộc tấn công được thực hiện để hoàn thành, nó cần phải tồn tại

Khởi động lại và có thể tiếp tục khi bắt đầu. Các kỹ thuật phổ biến được sử dụng bởi ransomware bao gồm

Đặt một bản sao của nó thực thi vào thư mục khởi động Windows, thêm một phím đăng ký chạy

Nhập cảnh hoặc thiết lập một nhiệm vụ theo lịch trình, để đặt tên cho một vài.

+ Khôi phục hệ thống chống lại - Để đảm bảo rằng bất kỳ hành động độc hại nào không thể hoàn tác, phần mềm độc hại có thể thử

Để vô hiệu hóa chức năng khôi phục hệ thống. Ransomware ví dụ, đã được biết là xóa

Bản sao bóng tối trong Windows, ngăn ngừa dữ liệu được mã hóa từ khôi phục đến một phiên bản cũ hơn

Phiên bản không được mã hóa.

+ Các kỹ thuật tàng hình - phần mềm độc hại sẽ cố gắng thực hiện theo cách bí mật để tránh bị chú ý bởi

Người sử dụng hoặc phát hiện bởi các máy quét vi-rút. Các kỹ thuật phổ biến bao gồm: tiêm vào hợp pháp

Xử lý, thực hiện từ thư mục% AppData% và sử dụng các tệp thực thi được đặt tên giống như

Các tệp thực thi phổ biến của Windows, để đặt tên cho một vài.

Lập bản đồ môi trường - Khi phần mềm độc hại được thực thi, nó có thể ánh xạ môi trường hệ thống của nó trước

Bắt đầu thủ tục thiết lập của nó. Điều này thường được thực hiện để xác định xem nó đang chạy trên thực tế

Máy tính hoặc trên môi trường sandbox có thể cố gắng phân tích nó.

Lập bản đồ môi trường cũng được sử dụng để xác định các thiết lập bảo mật / chính sách, vị trí địa lý,

Ngôn ngữ người dùng, kiến ​​trúc hệ thống tập tin và ổ đĩa mạng. Một số quyết định về việc liệu

Tiếp tục thực hiện có thể dựa vào bất kỳ kiểm tra môi trường được thực hiện.

+ Mạng lưới giao thông - Ransomware đòi hỏi một kết nối internet, làm như vậy cho hai có thể

Nhiệm vụ: tải các tập tin liên quan đến payload, và / hoặc cho việc truyền thông của khoá mã hóa.

Để đảm bảo các lệnh và các máy chủ điều khiển độc hại không dễ bị các cơ quan chức năng đóng cửa,

Các nhà phát triển phần mềm độc hại sử dụng chiến thuật đăng ký tên miền nhất định. Chiến thuật bao gồm việc sử dụng một miền

Tạo ra các thuật toán để tạo ra các tên miền ngẫu nhiên đăng ký cho cấp cao nhất vô danh

Các tên miền như .xyz. .top và .bid.

+ Ưu tiên quyền - Thực hiện các hoạt động liên quan đến hệ thống độc hại có thể yêu cầu quyền truy cập

Vượt quá số tiền được cung cấp cho tài khoản người dùng của nạn nhân. Ví dụ, ransomware có thể muốn

Để ghi đè lên Master Boot Record, mà chỉ có thể được thực hiện như là một Quản trị viên. Đơn giản

Yêu cầu quyền truy cập quản trị viên có thể làm việc hoặc các kỹ thuật leo thang đặc quyền khác có thể

đã sử dụng.

Điều quan trọng cần lưu ý là không phải tất cả các gia đình ransomware đều có đặc điểm hành vi từ tất cả những điều trên

Đề cập đến loại. Các gia đình ransomware được trang bị tốt và đạt được sự phân bố rộng rãi và cao

Tỷ lệ thành công như Teslacrypt, thường trình bày hầu hết các đặc điểm thiết lập được đề cập. Tuy nhiên, cũng có

Một sự phong phú của các gia đình ransomware đơn giản, ít được trang bị mà chỉ triển khai một số thiết lập

Tính cách hành vi.

Để chứng minh điểm này, hãy tham khảo bảng 1 cho thấy thành phần của các đặc tính thiết lập cho

Gia đình ransomware. Thông báo sự thay đổi trong cách thức các gia đình ransomware khác nhau thành lập. Một số gia đình trưng bày

Tất cả các tính năng của một thiết lập độc hại (Teslacrypt, CryptoWall) trong khi những người khác chỉ là một vài (Alma, Crypt2). Sự thay đổi

Trong việc thiết lập các đặc điểm hành vi trong số các gia đình ransomware có thể chứng minh thách thức đối với hành vi dựa trên

Phát hiện, đặc biệt là để phát hiện ransomware được trang bị ít trang bị đơn giản mà có hành vi thấp hồ

thiết lập.

Phân tích hành vi thiết lập của các tệp thi hành không xác định là một công cụ mạnh mẽ trong phát hiện ransomware

Có thể hỗ trợ phát hiện sớm để đảm bảo mất tập tin tối thiểu. Các máy dò giá trị ransomware dựa trên hành vi phủ nhận

Thiết lập hành vi và chỉ nhìn vào hành vi chuyển đổi dữ liệu, có thể yêu cầu mã hóa tập tin đáng kể

Để xảy ra trước khi nó có thể tự tin gắn cờ một file thực thi như ransomware.

4.2.2 Mã hóa dữ liệu

Trọng tâm của hành vi ransomware crypto là khả năng chuyển đổi khối lượng dữ liệu từ một thiết bị có thể sử dụng được

Nhà nước đến một nhà nước không sử dụng được. Thông thường, hành vi chuyển đổi dữ liệu ransomware được định nghĩa từ một tệp tin

Điều hành, đưa ra ba loại ransomware [7]:

Ransomware lớp Một mở tập tin ban đầu và trực tiếp ghi đè lên nội dung của nó với dữ liệu được mã hóa của nó.

Ransomware lớp B đầu tiên di chuyển tập tin đến một vị trí rời rạc, mã hóa tập tin như trong lớp A và sau đó

Di chuyển tệp tin về vị trí ban đầu. Lớp C đọc tệp ban đầu, mã hóa nội dung của nó, viết

Nội dung được mã hoá vào một tập tin mới, và xóa các tập tin ban đầu.

Theo các lớp ransomware nói trên, xác định ransomware bằng cách chuyển đổi dữ liệu của nó

Hành vi yêu cầu tối thiểu là khả năng theo dõi hoạt động của tệp và / hoặc khả năng xác định dữ liệu

Mã hóa. Những cách tiếp cận như vậy đối với việc phát hiện ransomware đã chứng minh hiệu quả như trong [8], theo dõi

9

Labs.mwrinfosecurity.com

Các hoạt động tập tin bằng cách sử dụng các yêu cầu I / O file, và trong [7] phát hiện tập tin khối lượng mã hóa bằng cách sử dụng thống kê

Các biện pháp như thay đổi entropy.

Các phương pháp phát hiện dựa trên hành vi chủ yếu dựa vào việc phát hiện mã hóa tập tin khối lượng có thể có hiệu quả,

Tuy nhiên có thể đi kèm với chi phí tốn nhiều tài nguyên. Xem xét ví dụ, các biện pháp mã hóa như

Entropy thay đổi đòi hỏi entropy tệp được tính cho mỗi thao tác ghi duy nhất được thi hành

Bởi một ứng dụng. Hơn nữa, các hoạt động này cần phải theo dõi các hoạt động tập tin cho từng tập tin riêng biệt qua

Tuổi thọ của một quá trình quan sát được. Cách tiếp cận như vậy có thể làm suy giảm đáng kể việc đọc và ghi đĩa

Hiệu suất và kết quả trong tải hệ thống cao.

Phân tích hành vi hoạt động của tập tin cũng có thể cung cấp thêm bằng chứng trực tiếp cho một cuộc tấn công ransomware trong

Hình thức xác định các khoản tiền chuộc được biết đến hoặc các phần mở rộng tệp ransomware được biết đến. Để tạo thuận lợi cho nạn nhân

Trả số tiền chuộc, ransomware cần phải biết rằng một vụ tấn công bằng đồng rensomware đã xảy ra và

Cung cấp hướng dẫn về cách dữ liệu của nạn nhân có thể khôi phục. Điều này thường được thực hiện bằng cách viết ra tiền chuộc

Ghi chú, thường ở nhiều vị trí trong thư mục của người dùng và nhiều định dạng.

Do đó, một cách để phát hiện ransomware là phát hiện ra các khoản tiền chuộc giảm. Cách tiếp cận như vậy đòi hỏi

Phân tích tĩnh trên các tập tin đáng ngờ để phát hiện tiền chuộc có liên quan đến nội dung. Ví dụ, người ta có thể sử dụng từ-bagof

(Chẳng hạn như các phương tiện được sử dụng trong phát hiện thư rác) để tìm mối tương quan giữa các cụm từ được tìm thấy trong

Các khoản tiền chuộc đòi tiền chuộc ("trả tiền chuộc", "mã hóa", "Bitcoin") cho những người trong một tập tin bị bỏ sót không biết.

Xác định các khoản tiền chuộc giảm xuống có thể là một kỹ thuật thành công cho một nhóm lớn các gia đình ransomware,

Tuy nhiên nó không thể chỉ dựa vào. Các nhà phát triển Ransomware có thể dễ dàng bỏ qua một hệ thống phát hiện như vậy

Bằng cách sử dụng các lựa chọn thay thế cho các khoản tiền chuộc dựa trên văn bản. Ví dụ về việc này bao gồm việc sử dụng một tệp thực thi

Hiển thị một cửa sổ hiển thị lưu ý, thay đổi nền máy tính để bàn với một bức tranh của các khoản tiền chuộc

Hoặc chèn một nhu cầu đòi tiền chuộc trong tên tệp của các tệp được mã hóa.

Các nhà phát triển Ransomware biết về các kỹ thuật phân tích chuyển đổi dữ liệu đã được biết đến

Sử dụng các thủ thuật đơn giản để che dấu sự hiện diện của mã hóa tập tin khối lượng. Những thủ thuật này bao gồm: chỉ một phần

Mã hoá các tập tin (chẳng hạn như các phần tiêu đề), hoặc saturating hệ thống với hoạt động thấp entropy ghi tập tin,

Để tạo ra một dấu chân mã hóa thấp hơn.

Ngoài hoạt động viết, di chuyển và xóa, ransomware cũng có xu hướng đổi tên

Tập tin mật mã. Thay đổi tên này thường được thực hiện để cảnh báo người dùng rằng một vụ tấn công bằng đồng rận đã xảy ra. An

Ví dụ đổi tên tập tin là gắn thêm phần mở rộng vào phần mở rộng ban đầu, chẳng hạn như

Example\_file.docx đến example\_file.docx.encrypted. Một giải pháp hiệu quả về chi phí sau đó để phát hiện ransomware

Sẽ là để phân tích các hoạt động đổi tên tập tin để xác định tên tập tin hoặc giá trị gia tăng tiền chuộc. Một

Kỹ thuật có thể làm việc trên ransomware đơn giản, nhưng sẽ không làm việc trên ransomware viết thông minh hơn

Chẳng hạn như CryptXXX ngẫu nhiên hóa tên tệp hoặc Spore giữ nguyên tên tệp gốc. Nếu như vậy

Phương pháp tiếp cận được sử dụng riêng biệt, tỷ lệ dương tính giả thường cao.

Tóm tắt, trích xuất các tính năng hành vi liên quan đến chuyển đổi dữ liệu và hoạt động tập tin có thể

Cung cấp thông tin có giá trị cần thiết để phát hiện ransomware. Tuy nhiên, nó không thể chỉ dựa vào.

4.3 Phát hiện dựa trên hành vi dựa trên máy móc

Cách tiếp cận hành vi để phát hiện ransomware đòi hỏi một thuật toán đưa ra quyết định chấp nhận một

Định lượng hành vi theo dõi của một quá trình chạy như là một đầu vào, để ra một quyết định nhị phân đơn giản - có

Nó an toàn / lành tính hoặc không có nó là ransomware.

Lĩnh vực ra quyết định mang tính thuật toán rất rộng, cho chúng ta nhiều cách tiếp cận để giải quyết phức tạp

các vấn đề. Đối với phát hiện ransomware, chúng tôi đã xác định rằng một phương pháp tiếp cận được học có máy giám sát là

Thích hợp nhất cho một vấn đề như vậy.

Theo học máy máy là tối ưu hóa mô hình dự đoán để mô tả tốt nhất bản đồ từ

Dữ liệu nhập vào nhãn mục tiêu được chỉ định, với mục tiêu cuối cùng là có thể dự đoán nhãn mục tiêu của

Dữ liệu chưa biết. Việc tối ưu hoá mô hình được gọi là mô hình lắp ráp hoặc đào tạo mô hình.

Giải thích trong bối cảnh phát hiện ransomware, học máy có giám sát là đào tạo một

Quyết định để nhận ra các đặc điểm hành vi nhất định (dữ liệu đầu vào) của các tiến trình đang chạy

Phân biệt rõ ràng giữa các ransomware và các ứng dụng lành tính không độc hại (nhãn mục tiêu).

Việc đào tạo thuật toán quyết định đòi hỏi ba thành phần quan trọng: tập dữ liệu huấn luyện có chứa

Ví dụ về ransomware đã biết (có nghĩa là) và ứng dụng lành tính được biết đến, việc thu thập

Các đặc điểm hành vi theo cách định lượng, và sơ đồ phân loại xác định việc đào tạo và

Thuật toán dự đoán.

4.3.1 Dataset construction Xây dựng bộ dữ liệu

Việc xây dựng bộ dữ liệu đào tạo được cho là quan trọng nhất, nhưng thường là một sự bỏ sót

Nhiệm vụ khi thiết kế một mô hình dự đoán. Tập dữ liệu, nếu được xây dựng đúng, phải đầy đủ

Đại diện của dân số mục tiêu để đảm bảo mô hình được đào tạo về các ví dụ được mong đợi trong

Ứng dụng trong thế giới thực. Điều này dễ nói hơn là thực hiện cho các nhiệm vụ phân loại như ransomware

Phát hiện, trong đó dân số mục tiêu bao gồm một bộ sưu tập gần như vô hạn và ngày càng tăng

Phần mềm - cả hai đều lành tính và ransomware.

Đối với một bộ sưu tập đại diện các mẫu ransomware, nó không phải là số lượng lớn mà quan trọng

Khá đa dạng - cho một mô hình dự đoán không tiếng ồn, đào tạo trên 1000 mẫu rangeromware của Locky

Nên chứng minh không hữu ích hơn là đào tạo chỉ trên một mẫu Locky. Mô hình dự báo được sử dụng trong

RansomFlare đã được đào tạo về khoảng 300 gia đình ransomware độc ​​đáo và các biến thể. Mỗi

Mẫu ransomware trong tập huấn luyện đã được phân tích cẩn thận và dán nhãn theo cách thủ công bởi gia đình và

Biến thể để đảm bảo một sự trình bày cân bằng trong lớp của ransomware. Để tăng thêm sự thay đổi trong

Tập huấn luyện, kỹ thuật tổng hợp được sử dụng để tổng hợp hành vi chuộc lại "tương lai".

Bộ dữ liệu lành mạnh là điểm tham chiếu cho những gì được coi là ransomware, và do đó là bằng nhau

Quan trọng như tập dữ liệu về ransomware. Phần lớn các file thực thi benign được sử dụng trong đào tạo của RansomFlare

Đã được thu thập từ một văn phòng thực tế của máy tính có thu thập dữ liệu về chúng. Ngoài các reallife

Ví dụ, một tập dữ liệu lành mạnh đã được thu thập bao gồm các ví dụ cụ thể lành tính

Tương tự như ransomware. Ví dụ bao gồm nén tập tin số lượng lớn bằng Winzip hoặc hình ảnh hàng loạt

Xử lý bằng Inkscape. Khi làm như vậy, nguy cơ sai tích cực được giữ ở mức tối thiểu.

4.3.2 Behaviour capturing and feature extraction (4.3.2 Thu thập hành vi và trích xuất tính năng)

4.3.3 Classification scheme Đề án phân loại

Nhiều mô hình kiến trúc học máy được giám sát chặt chẽ tồn tại: cây quyết định được tăng cường, ngây thơ

Phân loại Bayesian, mạng nơ-ron và các máy vector hỗ trợ (SVM) chỉ để đặt tên cho một vài.

Chọn một lược đồ phân loại dựa trên sự hiểu biết sâu sắc về lĩnh vực vấn đề để xác định các yêu cầu

Của người phân loại. Đối với phát hiện ransomware theo hành vi, ba yêu cầu quan trọng đã được

xác định:

+ Hoạt động theo thời gian thực - chương trình phân loại phải hoạt động theo thời gian thực, với sự liên tục

Ra quyết định trong suốt vòng đời thực thi.

+ Nguồn tài nguyên ánh sáng - Thuật toán dự đoán không được nạp tài nguyên hệ thống. Ransomware

Phát hiện là một nhiệm vụ quan trọng có thể tạo thành một phần của một hệ thống phát hiện mối đe dọa lớn hơn và do đó

Nên có một nguồn lực tài nguyên tối thiểu.

+ Dễ dàng cập nhật - Khi các gia đình ransomware mới xuất hiện, kế hoạch phân loại phải dễ dàng

Cập nhật.

Thử nghiệm thực nghiệm cho thấy một lược đồ phân loại SVM phù hợp nhất cho việc phát hiện ransomware vì nó

Đáp ứng các yêu cầu nói trên. Một SVM là một mô hình dự đoán nhị phân có hiệu suất cao sử dụng một khoảng thưa

Tập dữ liệu đào tạo (các vector hỗ trợ), cho phép tính toán theo thời gian thực ánh sáng, thời gian thực. Sức mạnh thật sự của nó

Nằm trong khả năng của nó để ngầm thực hiện một biến đổi phi tuyến tính không tuyến tính, làm cho nó thích nghi cao với một dải

Của các vấn đề phân loại khác nhau.

Vì chỉ có các vector hỗ trợ được yêu cầu bởi thuật toán dự đoán của một SVM - các vector hỗ trợ là

Các mẫu huấn luyện được sử dụng để xác định máy bay quyết định - những mẫu ransomware mới được phát hiện không cần

Nhất thiết phải được thêm vào tập huấn luyện để cập nhật mô hình. Nếu mẫu mới nằm ngoài quyết định

Máy bay, nó có thể được giả định nó sẽ không tạo thành một phần của vector hỗ trợ thiết lập và do đó mô hình không cần phải được

Đào tạo lại với mẫu mới. Đây là một lợi thế rất lớn để phát hiện ransomware nơi ransomware mới

Được phát hiện hàng ngày vì có khả năng mô hình sẽ không yêu cầu cập nhật.

5. Case study: CryptoLuck ransomware

Để làm nổi bật tầm quan trọng của phát hiện ransomware dựa trên hành vi, hãy xem xét nghiên cứu trường hợp của

CryptoLuck ransomware.

Lần đầu tiên nhìn thấy vào cuối năm 2016, gói cước CryptoLuck (một biến thể độc đáo của gia đình CryptoLocker)

Đã được phân phối bằng cách sử dụng chất làm mờ và bộ dụng cụ khai thác RIG-E. Nạn nhân bị nhiễm bệnh bằng cách ghé thăm một trang web mà

Sử dụng bộ dụng cụ khai thác RIG-E để phân phối tải trọng ransomware. Các payload CryptoLuck đã được discretely

Tải về và thực hiện trên các máy tính của người sử dụng trình duyệt web không may mắn.

CryptoLuck là một nghiên cứu trường hợp thú vị vì tải trọng có ba phần, được chứa trong một bản tự trích xuất

Lưu trữ: GoogleUpdater.exe thực thi cập nhật hợp lệ của Google, một bản đi kèm hợp pháp

Tập tin cấu hình crp.cfg, và một tập tin DLL độc hại goodate.dll.

Trong quá trình thực hiện cập nhật Google hợp pháp, tệp thi hành tải tệp tin DLAT goodate.dll

Nằm trong thư mục hiện tại. CryptoLuck đã khai thác các kỹ thuật tấn công DLL và thay thế các chính sách hợp pháp

Google DLL với DLL độc hại của riêng mình. DLL độc hại này đã được tải, sẽ giải nén và thực hiện

Tải trọng ransomware.

Bằng cách sử dụng một thực thi có chữ ký hợp pháp để giải nén ransomware, CryptoLuck đã có thể thực hiện

Không bị phát hiện từ các máy quét virus thương mại chính. Có thể lý do cho việc này là máy quét vi-rút

Đã được biết là các danh sách trắng tự động được ký và thực thi con của họ.

Sử dụng cướp DLL như là một kỹ thuật chống phát hiện không có hiệu quả đối với RansomFlare. Đó là vì

Nó được thiết kế để xử lý tất cả các thực thi không gian của người dùng (ký và không ký) như là mối đe dọa tiềm năng ransomware.

RansomFlare đã có thể gắn cờ các tệp thực thi có liên quan đến ransomware của GoogleUpdater.exe, thậm chí

Mặc dù nó không phải là một phần của bộ đào tạo ransomware (trước đây không nhìn thấy). Đó là vì

Ứng dụng có các đặc điểm hành vi cổ điển mà chỉ có thể được kết hợp với ransomware. Một số

Những đặc điểm này bao gồm:

+ Payload persistence - CryptoLuck chèn một khóa đăng ký để đảm bảo

GoogleUpdate.exe thực thi khôi phục lại khi khởi động lại hệ thống.

+ Kỹ thuật ẩn - GoogleUpdate.exe và các tệp DLL đi kèm được lưu trữ trong% AppData%

Nơi nó được thực hiện trong tàng hình. Các ransomware sử dụng DLL cướp của một ký kết

Thực thi để giả mạo như là một thực thi hợp pháp.

+ Lập bản đồ môi trường - Ransomware xác định xem nó đang chạy trong một môi trường ảo bởi

Tìm kiếm các từ khóa liên quan đến VM như vmbox, vmware và wine trong các khóa registry.

Các ransomware bản đồ ra ổ đĩa gắn kết và unmapped mạng chia sẻ ổ đĩa và cloudbased

Ổ đĩa. Chỉ các tệp cụ thể liên quan đến dữ liệu người dùng như docx, xlsx, pdf, pptx, jpeg, jpg

Trải qua quá trình chuyển đổi dữ liệu.

+ Các tệp tin được chuyển đổi dữ liệu - được nhắm mục tiêu được mã hóa bằng một thói quen mã hóa rắn: cho mỗi

Tập tin được nhắm mục tiêu, một chìa khóa AES-256 được tạo ra và được sử dụng để mã hóa tập tin. Một công cộng RSA nhúng

15

Labs.mwrinfosecurity.com

Key được sử dụng để mã hóa khoá AES mới được tạo ra và sau đó được lưu trữ trong tệp tin mật mã. Tất cả các

Các tập tin được mật mã phải trải qua sự thay đổi tên như một phần mở rộng <victim id> \_luck được nối vào

Tên.

Trong quá trình mã hóa, một khoản tiền chuộc dưới dạng một tập tin văn bản bị bỏ trong mỗi thư mục được nhắm mục tiêu

vị trí. Ghi chú về tiền chuộc này được đặt tên là @WARNING\_FILES\_ARE\_ENCRYPTED. <Victim id> .txt. Khi nào

Tất cả các tệp đều được mã hóa, nền của máy tính để bàn được đổi thành một khoản tiền chuộc và một cửa sổ là

Đưa ra với một khoản tiền chuộc. Xem Hình 2 để biết ảnh chụp màn hình của máy tính bị nhiễm CryptoLuck

Cho thấy ba hình thức của tiền chuộc ghi chú.

Cơ chế mã hóa của CryptoLuck là rắn, và như vậy, không có công cụ giải mã chưa được thực hiện

Có sẵn bởi các nhà nghiên cứu không gian mạng. Một người dùng bị nhiễm sẽ cần phải thanh toán theo yêu cầu 2.1 Bitcoins, hoặc

Phục hồi từ bản sao lưu để khôi phục lại dữ liệu của họ.