Sys internal suitl

Created By	
Last Edited By	

Process Monitor

Đây là công cụ giám sát và theo dõi gianh cho hđh Windows bằng cách ghi lại các hành động liên quan tới file hệ thông, registry, process/ thread trong real time.

Đây là công cụ hữu ích hỗ trợ quá trình phát hiện Malware, phần mềm độc hại hoặc muốn theo dõi hành vi của bất kỳ một chương trình nào đang tác động tới hệ thống. ProcessMon cung cấp các cơ chế lọc cho phép tập trung vào việc theo dõi các đôi tượng cụ thể theo nhiều tiêu chí khác nhau

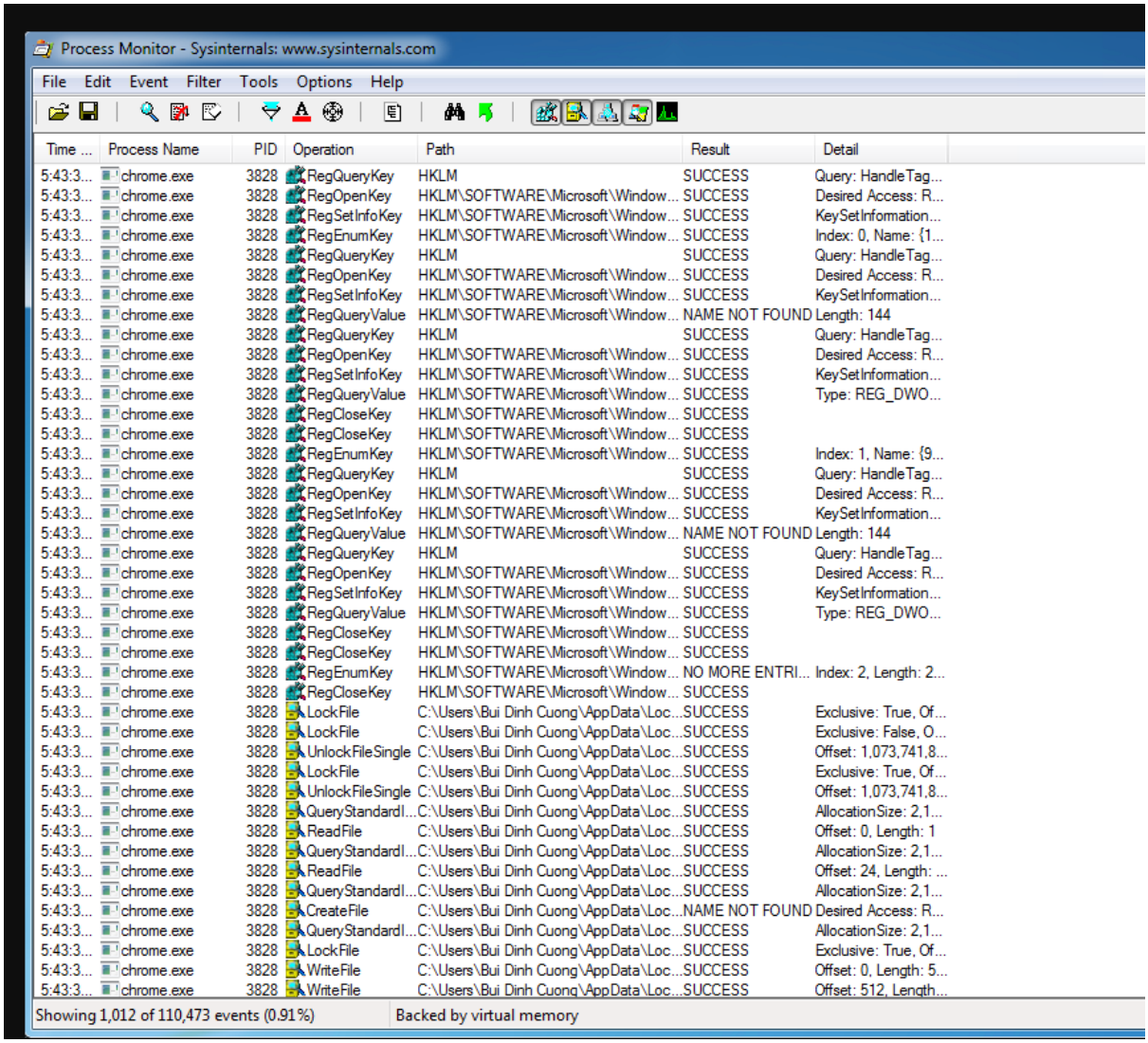
Được tạo bằng cách kết hợp hai tiện ích Filemon và Regmon, được sử dụng để giám sat các tệp và hoạt động đăng ký như tên. Y/ c chế độ quản trị viên vì nó tải trinh điêu khiển để log lại tất cả sự kiên.

ProcessMon log được nhiều thứ n không thu thập được việc di chuyển chuốt và nó không biết liệu trình điều khiển có hoạt đông tối ưu không, không theo dõi quá trình nào đang mở và lãng phí CPU

ProcessMon nắm bắt các hoạt đông in out cụ thể:

- Đăng ký:
- Hệ thống tập tin: tạo tệp, ghi, xóa…
- mạng: nguồn đich lưu lượng tcp/ udp (không hiển thị dữ liệu)
- Quá trinh: la các sự kiện cho quy trinh và luồng

- hồ sơ: log lai để check lượng thời gian của bộ xử lý được sư dụng bở mỗi quy trình và việc sử dung bộ nhớ



ProcessMon có tinh năng giám sát và khả năng lọc tốt:

- Khả năng bắt thông tin qua các tham số vào/ ra
- Quá trinh lọc không làm mât dữ liệu
- Bắt các thong tin của stack trong các luồng cho từng hành đông do đó dễ dàng phat hiện ra gốc của hanh động
- Đưa ra các thông tin tin cậy về chi tiết sản phẩm: đương dẫn, command line, người dung, session ID…
- Khả năng filter được thiết lập tới tất cả cac trường dữ liệu

- Khả năng ghi log và capture dữ liệu rất lớn: Khoảng 10 triêu sự kiện được capture với khoang 10 triệu GB dữ liệu
- Process Tree chỉ ra mối quan hệ giữa các tiến trinh liên quan trong cung một nhanh
- Dễ dàng xem thông tin vê process thông qua tool tip
- Ghi log các theo tác, hanh động theo thời gian boot

Hijack Execution Flow- luồng thực thi xâm nhập

DLL Search Order Hijacking

Adversaries có thể thực hiện các malicious payloads bằng cách cuơp thứ tự tìm kiêm được sử dụng để load các tệp DLL. Hệ thông windows sử dụng một phương pháp chung để tìm kiếm các tập dl cần thiết để load vào một chương trình. Hijacking dll load có thể nhằm mục đich thiết lâp tinh bền bỉ cũng như nâng cao đặc quyền và trốn tránh các hạn chế đối với việc thực thi tệp

Có nhiều cách để chiếm đoạn load dll

- có thể đặt các tệp thư viện liên kết động trojan (dll) trong một thư muc sẽ đuợc tìm kiếm trước vị trí của một thư viện hợp pháp sẽ được một chương trình y/ c, khiến Windows load thư viện độc hại của chúng khi nó được gọi bởi chương trình nan nhân. attacker có thể thực hiên load dll trước còn được gọi là tấn công trồng nhị phân, băng cách đặt một dll độc hại có cùng tên với dll duợc chỉ định không rõ ràng ở một vị trí mà windows tìm kiếm trước dll hơp lệ. Thươờg vị trí nay là thư muụ làm việc hiện tại của chương trinh. Các cuộc tấn công load dll truớc từ xa xảy ra khi môt chương trình đặt thư muc hiện tai của nó thành một remote location, VD như web share trước khi load dll
- Adversaries cũng có thể trực tiếp sửa đổi thứ tự tìm kiếm thông qua chuyển hương DLL, sau khi được kích hoạt có thể khiến chương tình load một dll khác
- Nếu chương trình yếu trong thứ tự tìm kiếm được định cấu hình để chạy ở cấp đặc quyền cao hơn thì dll do Adversaries kiểm soát được tải cung sẽ phải được thực thi ở cấp cao hơn. Trong trương hợp này, kỹ thuật này có thể được sử

dụng để chuyển đặc quyền từ user sang admin tùy thuộc vào chương trình. Các chương trinh trở thành nạn nhân của chiếm đọat đương dẫn có thể hoạt đông bình thương vì các dll độc hại có thể được định cấu hình đê tải các dll hợp lệ mà chúng dự kiến thay thế

DLL ?

Tệp DLL hoặc tệp thư viện liên kết đông chứa các tài nguyên mà ứng dụng cần để chạy thành công. Chúng có thể bao gồm hình ảnh và thư viện các hàm thực thi

Người dùng cuối không thể mở tệp dll chúng chỉ co thể được mở bằng ứng dung được liên kết cua họ điều này thường xảy xa khi ứng dụng khơi động

Hệ thống Windows yêu cầu tệp DLL để hiêu cach sử dụng tài nguyên của chúng, host computer mem và dung lượng ổ cưng hiệu quả nhất

Các tệp DLL thương kết thúc bằng phần mở rộng .dll nhưng một số có thể là .drv, .drov or .exe

Một tệp dll duy nhất có thể chạy nhiều chương trinh vì vậy nhiều chương triìh có thể bị bao gồm trong một cuộc tấn công chiếm quyền điều khiên dll

DLL Hijacking là gì?

Là một phương pháp tiêm mã độc vào ưng dụng băng cách khai thác một sô ứng dung Windows tìm kiếm và tải Dynamic Link Lirbraries(DLL) - thư viện liên kết đông

Chỉ hệ điều hành của Microsoft mới dễ bị xâm nhập DLL

Bằng cach thay thế tệp DLL bắt buộc bằng một phiên bản bị nhiễm và đăt nó trong cách tham số tìm kiếm cuủ ưng dụng, tệp bị nhiễm sẽ đươc gọi khi ứng dụng tải, kich hoạt các hoat động độc hại của nó

Để xâm nhập DLL thành công, nan nhân cần tải tệp DLL bị nhiễm từ cùng thư mục với ứng dụng được nhắm mục tiêu

Nếu cac ứng dụng được tải tự động khi khởi động bị xam nhập với tệp DLL bị nhiễm độc, → hacker sẽ được cấp quyền truy cập vào máy tính bị nhiễm bất cứ khi nào load

DLL chiêm quyền điều khiên không phải là một phương pháp tấn công mạng tốt.

DLL Hijacking hoạt động?

Để một cuộc tấn công chiếm quyền điều khiển DLL thành công, ứng dụng Windows cần được lừa để mở một tệp dll bị nhiễm thay vì dll hợp lệ

Bằng cach khai thác thứ tự tìm kiếm DLL công khai của các ứng duụg Microsoft, thủ thuật này tương đối đơn giản để thực hiện

Thứ tự tìm kiếm DLL tiêu chuân của các ứng dụng Microsoft phụ thuộc vào viêc tìm kiêm DLL an toàn có đc bật hay không

Khi chế độ tìm kiếm DLL an toàn được bật, các ứng udnjg sẽ tìm kiếm các tệp DLL cần thiết theo thứ tự:

1. Thư mục mà ứng dụng được tải từ đó
2. Thư mục hệ thống
3. Thư mục hệ thống 16 bit
4. Thư mục Windows
5. Thư mục hiện tại
6. Các thư mục được liệt kê trong biến môi trường Path

Khi chế độ tìm kiếm DLL an toàn tắt, thứ tự tìm kiếm sẽ:

1. Thư mục mà ứng dụng được tải từ đó
2. Thư mục hiện tại
3. Thư mục hệ thống
4. Thư mục 16 bit
5. Thư mục Windows
6. Thư mục được liệt kê trong biến môi trường Path

Khi tính năng tìm kiếm an toàn tắt thư mục hiện tại của người dùng sẽ được nâng cao thơn trong thứ tự tìm kiếm

Các ứng dụng windows sẽ mặc định cho bất kỳ một trong các giao thức tìm kiếm kiếm DLL ở trên nếu một ứng dụng không chỉ định đường dẫn đầy đủ của các dll được liên kết

VD: nếu ứng dụng Win yêu cầu tệp dll nằm trong thư mục hệ thống C:\windows\system32 nhưng không có hướng dẫn nào trong mã của nó có thể tìm kiếm ở vị trí rõ ràng này, ứng dụng sẽ hoạt động thông qua lệnh tìm kiếm dll để định vị tệp

Bất kể có bật tìm kiếm an toàn hay không, thư mục mà từ đố ứng dụng được khởi chạy là vị trí đầu tiên được tìm kiếm

Nếu hacker gửi tệp dll bị nhiễm vào vị trí này ứng dung sẽ mở tệp đó thay vì tệp gốc vì vị trí của nó đã được tìm kiếm trước thư mục hệ thống

→ chiếm quyền điều khiển tìm kiếm DLL

Để khởi chạy xâm nhập dll hacker chỉ cần gửi một payload dll vào thư mục của một ứng dụng được nhắm mục tiêu (social engineering, phishing, supply chain attacks)

Để ngăn bị phát hiện , các tệp dll bị nhiễm bắt chước digital singnature của ứng dụng được nhắm mục tiêu. → xác minh rằng một tệp là authentic có thể cho phép chuyển các tệp dll độc hại cho các đối tác của nhà cung cấp trong một cuộc tấn công chuỗi cung ứng

Tệp dll độc hại gây ra vi phạm dữ liệu của

Cách xác định một cuộc tấn công DLL Hijacking

sử dụng Procmon của windows

Procmon hiển thị tất cả các hệ thống tệp đang được tải trong thời gian thực. Bằng cách áp dụng các bộ lọc phù hợp, có thể xác định xem có tệp dll khả nghi nào đang được tải thay vì tệp gốc hay không

B1: Cài Procmon

B2: Tìm kiếm ứng dụng bị nghi nờ là mục tiêu trong cuộc tấn công chiếm quyền điều khiển dll

B3: Áp dụng filter để chỉ hiển thị các tệp dll

B4: Áp dụng filter cho thư mục: name not found

Vì chiếm quyền điều khiển DLL chủ yếu xảy ra khi tệp dll nghi ngờ được load thay vì bản xác thực trong thư mục hệ thống, nên áp dụng filter hiern thị trực tiếp các tệp dll đã bược tải bên ngoài hệ thống

Procmon gắn cờ các tệp này là FILE NOT FOUND

Prevent

Các nhà phát triển cần tuân theo secure coding practices và chỉ định vị trí chính xác của tất cả các tệp dll được liên kết để ngăn windows mặc định theo giao thức đường dẫ tìm kiếm dll của nó

Không bao giờ có thể đảm bảo việc tuân thủ các thực hành mã hóa an toàn vì vậy các tổ chức nên triển khai các biện pháp bảo vệ bổ sung:

1. Luôn cập antivirus
2. đào tạo
3. Giải pháp quản lý rủi ro