

Sys internal suitl

👤 Created By	
👤 Last Edited By	

[Process Monitor](#)

[Hijack Execution Flow- luồng thực thi xâm nhập](#)

[DLL Search Order Hijacking](#)

[DLL ?](#)

[DLL Hijacking là gì?](#)

[DLL Hijacking hoạt động?](#)

[Cách xác định một cuộc tấn công DLL Hijacking](#)

[Prevent](#)

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 thống, 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 đối 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 sát các tệp và hoạt động đăng ký như tên. Y/ c chế độ quản trị viên vì nó tải trình điều khiển để log lại tất cả sự kiện.

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

ProcessMon nắm bắt các hoạt động in out cụ thể:

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

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

The screenshot displays the Windows Process Monitor (ProcMon) application, which is monitoring system events. The title bar indicates it is from Sysinternals, with the URL www.sysinternals.com. The menu bar includes File, Edit, Event, Filter, Tools, Options, and Help. The toolbar contains various icons for file operations, search, and system functions.

The main window shows a list of events. The columns are Time, Process Name, PID, Operation, Path, Result, and Detail. The events are filtered to show only those performed by chrome.exe. The operations are primarily registry-related, including RegOpenKey, RegSetInfoKey, RegEnumKey, RegOpenKey, RegSetInfoKey, RegQueryValue, RegCloseKey, RegEnumKey, RegOpenKey, RegSetInfoKey, RegQueryValue, RegCloseKey, RegEnumKey, RegCloseKey, LockFile, UnlockFileSingle, ReadFile, QueryStandard..., CreateFile, and WriteFile. The paths are mostly HKLM\SOFTWARE\Microsoft\Windows... and C:\Users\Bui Dinh Cuong\AppData\Loc... The results are mostly SUCCESS, with some NAME NOT FOUND and NO MORE ENTRIES. The details provide additional information about the operations, such as Query: Handle Tag..., Desired Access: R..., KeySetInformation..., Index: 0, Name: {1..., Length: 144, and Exclusive: True, Of...

Time ...	Process Name	PID	Operation	Path	Result	Detail
5:43:3...	chrome.exe	3828	RegOpenKey	HKLM	SUCCESS	Query: Handle Tag...
5:43:3...	chrome.exe	3828	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: R...
5:43:3...	chrome.exe	3828	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	KeySetInformation...
5:43:3...	chrome.exe	3828	RegEnumKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Index: 0, Name: {1...
5:43:3...	chrome.exe	3828	RegOpenKey	HKLM	SUCCESS	Query: Handle Tag...
5:43:3...	chrome.exe	3828	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: R...
5:43:3...	chrome.exe	3828	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	KeySetInformation...
5:43:3...	chrome.exe	3828	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Length: 144
5:43:3...	chrome.exe	3828	RegOpenKey	HKLM	SUCCESS	Query: Handle Tag...
5:43:3...	chrome.exe	3828	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: R...
5:43:3...	chrome.exe	3828	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	KeySetInformation...
5:43:3...	chrome.exe	3828	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Type: REG_DWORD...
5:43:3...	chrome.exe	3828	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
5:43:3...	chrome.exe	3828	RegEnumKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Index: 1, Name: {9...
5:43:3...	chrome.exe	3828	RegOpenKey	HKLM	SUCCESS	Query: Handle Tag...
5:43:3...	chrome.exe	3828	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: R...
5:43:3...	chrome.exe	3828	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	KeySetInformation...
5:43:3...	chrome.exe	3828	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Length: 144
5:43:3...	chrome.exe	3828	RegOpenKey	HKLM	SUCCESS	Query: Handle Tag...
5:43:3...	chrome.exe	3828	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: R...
5:43:3...	chrome.exe	3828	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	KeySetInformation...
5:43:3...	chrome.exe	3828	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Type: REG_DWORD...
5:43:3...	chrome.exe	3828	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
5:43:3...	chrome.exe	3828	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
5:43:3...	chrome.exe	3828	RegEnumKey	HKLM\SOFTWARE\Microsoft\Window...	NO MORE ENTRI...	Index: 2, Length: 2...
5:43:3...	chrome.exe	3828	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
5:43:3...	chrome.exe	3828	LockFile	C:\Users\Bui Dinh Cuong\AppData\Loc...	SUCCESS	Exclusive: True, Of...
5:43:3...	chrome.exe	3828	LockFile	C:\Users\Bui Dinh Cuong\AppData\Loc...	SUCCESS	Exclusive: False, O...
5:43:3...	chrome.exe	3828	UnlockFileSingle	C:\Users\Bui Dinh Cuong\AppData\Loc...	SUCCESS	Offset: 1,073,741,8...
5:43:3...	chrome.exe	3828	LockFile	C:\Users\Bui Dinh Cuong\AppData\Loc...	SUCCESS	Exclusive: True, Of...
5:43:3...	chrome.exe	3828	UnlockFileSingle	C:\Users\Bui Dinh Cuong\AppData\Loc...	SUCCESS	Offset: 1,073,741,8...
5:43:3...	chrome.exe	3828	QueryStandard...	C:\Users\Bui Dinh Cuong\AppData\Loc...	SUCCESS	AllocationSize: 2,1...
5:43:3...	chrome.exe	3828	ReadFile	C:\Users\Bui Dinh Cuong\AppData\Loc...	SUCCESS	Offset: 0, Length: 1
5:43:3...	chrome.exe	3828	QueryStandard...	C:\Users\Bui Dinh Cuong\AppData\Loc...	SUCCESS	AllocationSize: 2,1...
5:43:3...	chrome.exe	3828	ReadFile	C:\Users\Bui Dinh Cuong\AppData\Loc...	SUCCESS	Offset: 24, Length: ...
5:43:3...	chrome.exe	3828	QueryStandard...	C:\Users\Bui Dinh Cuong\AppData\Loc...	SUCCESS	AllocationSize: 2,1...
5:43:3...	chrome.exe	3828	CreateFile	C:\Users\Bui Dinh Cuong\AppData\Loc...	NAME NOT FOUND	Desired Access: R...
5:43:3...	chrome.exe	3828	QueryStandard...	C:\Users\Bui Dinh Cuong\AppData\Loc...	SUCCESS	AllocationSize: 2,1...
5:43:3...	chrome.exe	3828	LockFile	C:\Users\Bui Dinh Cuong\AppData\Loc...	SUCCESS	Exclusive: True, Of...
5:43:3...	chrome.exe	3828	WriteFile	C:\Users\Bui Dinh Cuong\AppData\Loc...	SUCCESS	Offset: 0, Length: 5...
5:43:3...	chrome.exe	3828	WriteFile	C:\Users\Bui Dinh Cuong\AppData\Loc...	SUCCESS	Offset: 512, Length...

Showing 1,012 of 110,473 events (0.91%) Backed by virtual memory

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

- Khả năng bắt thông tin qua các tham số vào/ ra
- Quá trình lọc không làm mất dữ liệu
- Bắt các thông tin của stack trong các luồng cho từng hành động do đó dễ dàng phát hiện ra gốc của hành động
- Đưa ra các thông tin tin cậy về chi tiết sản phẩm: đường dẫn, command line, người dùng, session ID...
- Khả năng filter được thiết lập tới tất cả các trường dữ liệu

- Khả năng ghi log và capture dữ liệu rất lớn: Khoảng 10 triệu sự kiện được capture với khoảng 10 triệu GB dữ liệu
- Process Tree chỉ ra mối quan hệ giữa các tiến trình liên quan trong cùng một nhanh
- Dễ dàng xem thông tin về process thông qua tool tip
- Ghi log các theo tác, hành 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 cướp thứ tự tìm kiếm được sử dụng để load các tệp DLL. Hệ thống windows sử dụng một phương pháp chung để tìm kiếm các tệp dl cần thiết để load vào một chương trình. Hijacking dll load có thể nhằm mục đích thiết lập tình 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 mục sẽ được 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 hiện load dll trước còn được gọi là tấn công trồng nhị phân, bằng cách đặt một dll độc hại có cùng tên với dll được chỉ định không rõ ràng ở một vị trí mà windows tìm kiếm trước dll hợp lệ. Thường vị trí này là thư mục làm việc hiện tại của chương trình. Các cuộc tấn công load dll trước từ xa xảy ra khi một chương trình đặt thư mục hiện tại 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 hướng DLL, sau khi được kích hoạt có thể khiến chương trình 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 cùng sẽ phải được thực thi ở cấp cao hơn. Trong trường 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 trình trở thành nạn nhân của chiếm đoạt đường dẫn có thể hoạt động bình thường vì các dll độc hại có thể được định cấu hình để tải các dll hợp lệ mà chúng dự kiến thay thế

DLL ?

Tệp DLL hoặc tệp thư viện liên kết động 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 có thể được mở bằng ứng dụng được liên kết của họ điều này thường xảy ra khi ứng dụng khởi động

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

Các tệp DLL thường 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 trình vì vậy nhiều chương trình có thể bị bao gồm trong một cuộc tấn công chiếm quyền điều khiển dll

DLL Hijacking là gì?

Là một phương pháp tiêm mã độc vào ứng dụng bằng cách khai thác một số ứng dụng Windows tìm kiếm và tải Dynamic Link Libraries(DLL) - thư viện liên kết động

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

Bằng cách thay thế tệp DLL bắt buộc bằng một phiên bản bị nhiễm và đặt nó trong cách tham số tìm kiếm của ứng dụng, tệp bị nhiễm sẽ được gọi khi ứng dụng tải, kích hoạt các hoạt động độc hại của nó

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

Nếu các ứng dụng được tải tự động khi khởi động bị xâm 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 chiếm quyền điều khiển 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 cách khai thác thứ tự tìm kiếm DLL công khai của các ứng dụng Microsoft, thủ thuật này tương đối đơn giản để thực hiện

Thứ tự tìm kiếm DLL tiêu chuẩn của các ứng dụng Microsoft phụ thuộc vào việc tìm kiếm DLL an toàn có được bật hay không

Khi chế độ tìm kiếm DLL an toàn được bật, các ứng dụng 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 hơn 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 đó 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 dụng 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 ngờ 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 hiển thị trực tiếp các tệp dll đã được 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 dẫn 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