**Lab 2 - Phát hiện các tác vụ lên lịch đáng ngờ trên Windows bằng Sysmon và Splunk**

**1. Mục tiêu**

* Mục tiêu của bài lab này là phát hiện, điều tra và ứng phó với các scheduled task trái phép hoặc đáng ngờ trên máy Windows, có thể được sử dụng cho mục đích persistence, thực thi các script độc hại hoặc lateral movement. Bài lab này sử dụng Sysmon để giám sát các scheduled task và Splunk để phân tích và trực quan hóa dữ liệu.

**2. Sơ đồ mạng**

Ubuntu Server (Splunk Server): 192.168.56.105/24

Windows 10 (SplunkUniversalForwarder): 192.168.56.106/24

**3. Kiến thức nền**

* **Scheduled Tasks:** Là tính năng tích hợp sẵn trong Windows cho phép người dùng và hệ điều hành tự động thực thi các chương trình, script hoặc lệnh theo lịch định trước, chẳng hạn như khi khởi động máy, đăng nhập người dùng, hoặc lặp lại theo giờ/ngày. Kẻ tấn công thường lợi dụng cơ chế này để duy trì quyền truy cập bằng cách thiết lập các tác vụ độc hại chạy định kỳ hoặc sau khi hệ thống khởi động lại.
* **Sysmon:** Là công cụ giám sát hệ thống nâng cao do Microsoft phát hành trong bộ Sysinternals, giúp ghi lại các sự kiện bảo mật chi tiết như tạo tiến trình, thay đổi file, kết nối mạng, và đặc biệt là các hành động liên quan đến Scheduled Tasks như tạo hoặc thực thi tác vụ. Với cấu hình phù hợp, Sysmon giúp phát hiện hành vi đáng ngờ mà các log mặc định của Windows có thể bỏ sót.
* **Splunk Universal Forwarder:** Là một lightweight agent được cài trên máy Windows (hoặc các hệ điều hành khác) để thu thập log theo thời gian thực và gửi về máy chủ Splunk. Trong môi trường giám sát bảo mật, nó thường được cấu hình để gửi log của Windows Event Log, Sysmon hoặc các file log tùy chỉnh về Splunk nhằm phục vụ việc phân tích tập trung.
* **Splunk:** Là một nền tảng SIEM mạnh mẽ hỗ trợ thu thập, tìm kiếm, phân tích, cảnh báo và trực quan hóa dữ liệu log từ nhiều nguồn. Với khả năng truy vấn linh hoạt bằng SPL (Search Processing Language), Splunk giúp các analyst nhanh chóng phát hiện các hành vi đáng ngờ, như việc tạo Scheduled Task bất thường hoặc hoạt động lateral movement, từ các log được gửi về.

**4. Các bước tiến hành**

**Bước 1: Chuẩn bị môi trường**

* Tải và cài đặt máy ảo Ubuntu Server 22.04 VMware Player.
  + Ubuntu Server: <https://releases.ubuntu.com/jammy/ubuntu-22.04.5-live-server-amd64.iso>
* Thực hiện cài đặt, cấu hình Splunk Server trên Ubuntu Server và Splunk Universal Forwarder trên Windows theo hướng dẫn tại: <https://github.com/0xrajneesh/90-days-security-challenge/blob/main/Challenge%232/Lab%20Set%20up%20.md>

**Bước 2: Cài đặt Sysmon trên máy Windows**

1. **Tải Sysmon**

* Truy cập: <https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon>
* Tải file .zip về và giải nén (thường sẽ có Sysmon.exe và Sysmon64.exe)

1. **Tải file cấu hình Sysmon**

* Dùng mẫu cấu hình từ SwiftOnSecurity (rất phổ biến): <https://github.com/SwiftOnSecurity/sysmon-config>

-> Tải file sysmonconfig-export.xml.

1. **Cài đặt Sysmon**

* Mở **Command Prompt với quyền Administrator**, điều hướng đến thư mục chứa Sysmon, rồi chạy:

sysmon64.exe -i sysmonconfig-export.xml

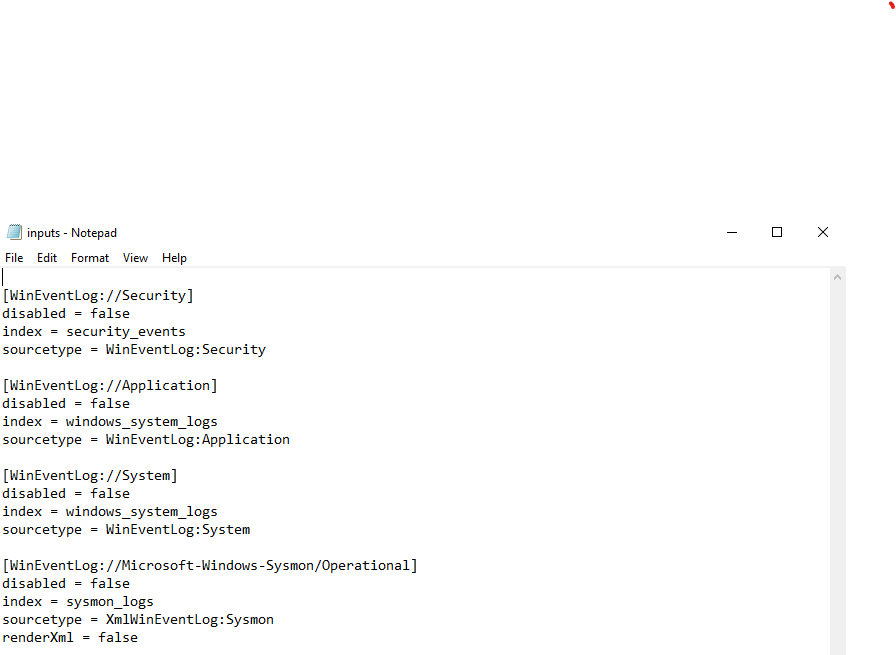
* Nếu thành công, Sysmon sẽ bắt đầu ghi lại các sự kiện vào Windows Event Log, mục **"Microsoft-Windows-Sysmon/Operational"**.
* **Kiểm tra:** Mở Event Viewer > Applications and Services Logs > Microsoft > Windows > Sysmon > Operational.

**Bước 3: Cấu hình Splunk Forwarder theo dõi và gửi log của Sysmon**

1. **Mở file inputs.conf của Splunk Forwarder**

C:\\Program Files\\SplunkUniversalForwarder\\etc\\system\\local\\inputs.conf

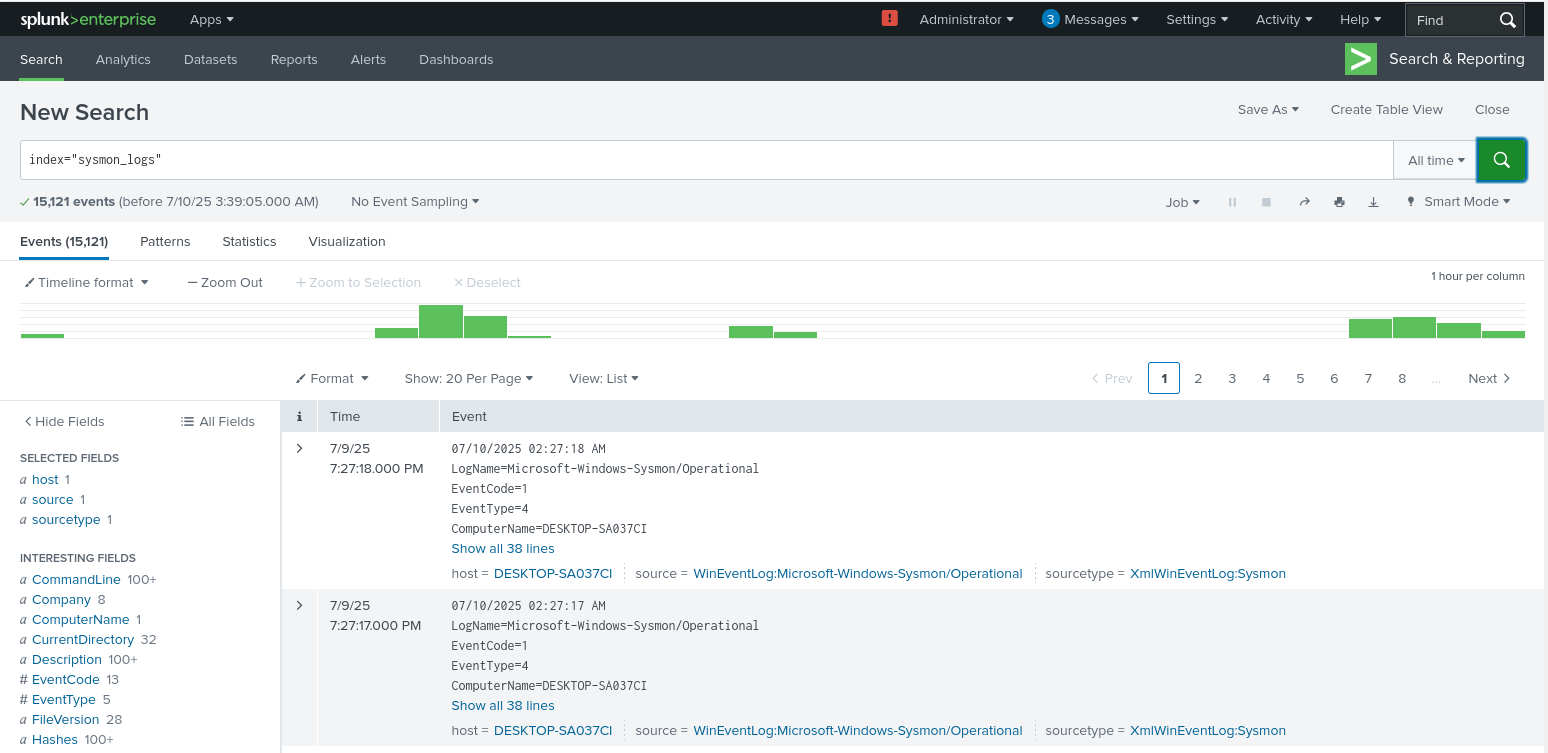
**Thêm dòng sau**



1. **Khởi động lại Splunk Forwarder**

C:\\WINDOWS\\system32>"C:\\Program Files\\SplunkUniversalForwarder\\bin\\splunk.exe" restart

1. **Kiểm tra xem Splunk nhận được log của Sysmon**



* **Lưu ý:** Nếu Splunk không nhận được log của **Sysmon** mà xem thủ công log của **Sysmon** trên máy Windows vẫn có thì khả năng là do Splunk Forwarder **không chạy bằng Local System Account** nên không đủ quyền đọc log Event Viewer ở Microsoft-Windows-Sysmon/Operational
* **Cách khắc phục:**
  + Kiểm tra lại account đang chạy Splunk Forwarder:
* Get-WmiObject win32\_service | Where-Object { $\_.Name -eq "SplunkForwarder" } | Select-Object StartName
* Nếu không thấy LocalSystem, bạn cần sửa:
  + - Nhấn Win + R, nhập: services.msc
    - Tìm dịch vụ **"SplunkForwarder"**
    - Chuột phải → Properties
    - Chuyển sang tab **Log On**
    - Chọn: Local System account
    - Khởi động lại Splunk Forwarder

**Bước 4: Mô phỏng hành vi đặt lịch tác vụ độc hại**

1. **Đặt lịch 1 tác vụ mới**

schtasks /create /tn "MaliciousTask" /tr "C:\\malware.exe" /sc once /st 12:00

1. **Thay đổi 1 tác vụ có sẵn**

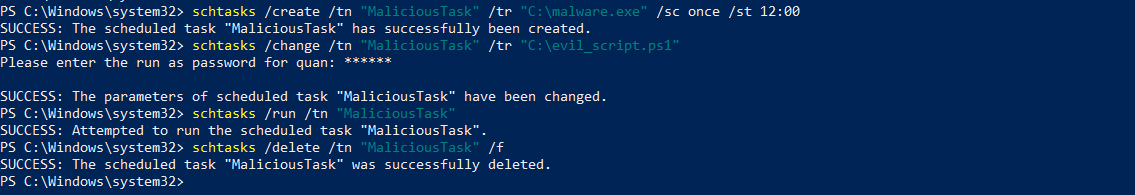
schtasks /change /tn "MaliciousTask" /tr "C:\\evil\_script.ps1"

1. **Thực thi 1 tác vụ**

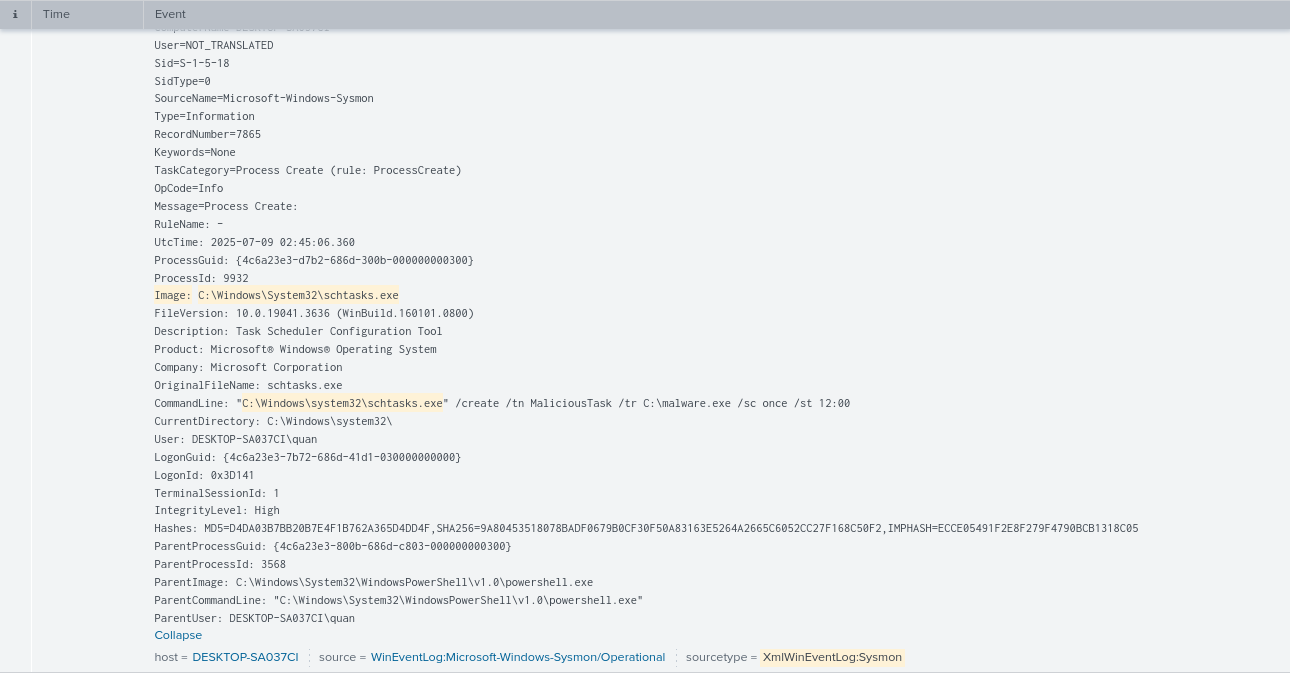
schtasks /run /tn "MaliciousTask"

1. **Xóa 1 tác vụ**

schtasks /delete /tn "MaliciousTask" /f



**Bước 5: Phân tích log trên Splunk**



**Sự kiện tạo Scheduled Task – Dấu hiệu thiết lập Persistence**

📌 **Thời gian (UTC):** 2025-07-09 02:45:06.360

📌 **Thời gian (giờ địa phương):** ~2:45:50

📌 **Hostname:** DESKTOP-SA037CI

📌 **User thực hiện:** DESKTOP-SA037CI\quan

📌 **Process thực thi:** Image: C:\\Windows\\System32\\schtasks.exe. Process ID: 9932 Process GUID: {0300}

📌 **Hành vi:**

Tiến trình schtasks.exe đã được sử dụng để tạo một scheduled task với các thông số sau:

Task Name: MaliciousTask

Action: Thực thi C:\\malware.exe

Trigger: Chạy một lần duy nhất vào lúc 12:00

Điều này đồng nghĩa với việc chương trình C:\\malware.exe sẽ tự động được khởi chạy vào thời điểm đã lên lịch.

📌 **Mô tả kỹ thuật:**

Scheduled Tasks là một cơ chế tích hợp trong Windows cho phép lên lịch chạy các chương trình hoặc script vào những thời điểm hoặc sự kiện cụ thể. Kẻ tấn công thường lợi dụng tính năng này để thiết lập persistence, đảm bảo mã độc có thể tự động thực thi sau khi hệ thống khởi động lại hoặc theo một lịch trình định sẵn. Việc tạo một task với tên gợi ý độc hại và trỏ đến một đường dẫn bất thường là dấu hiệu đáng ngờ.

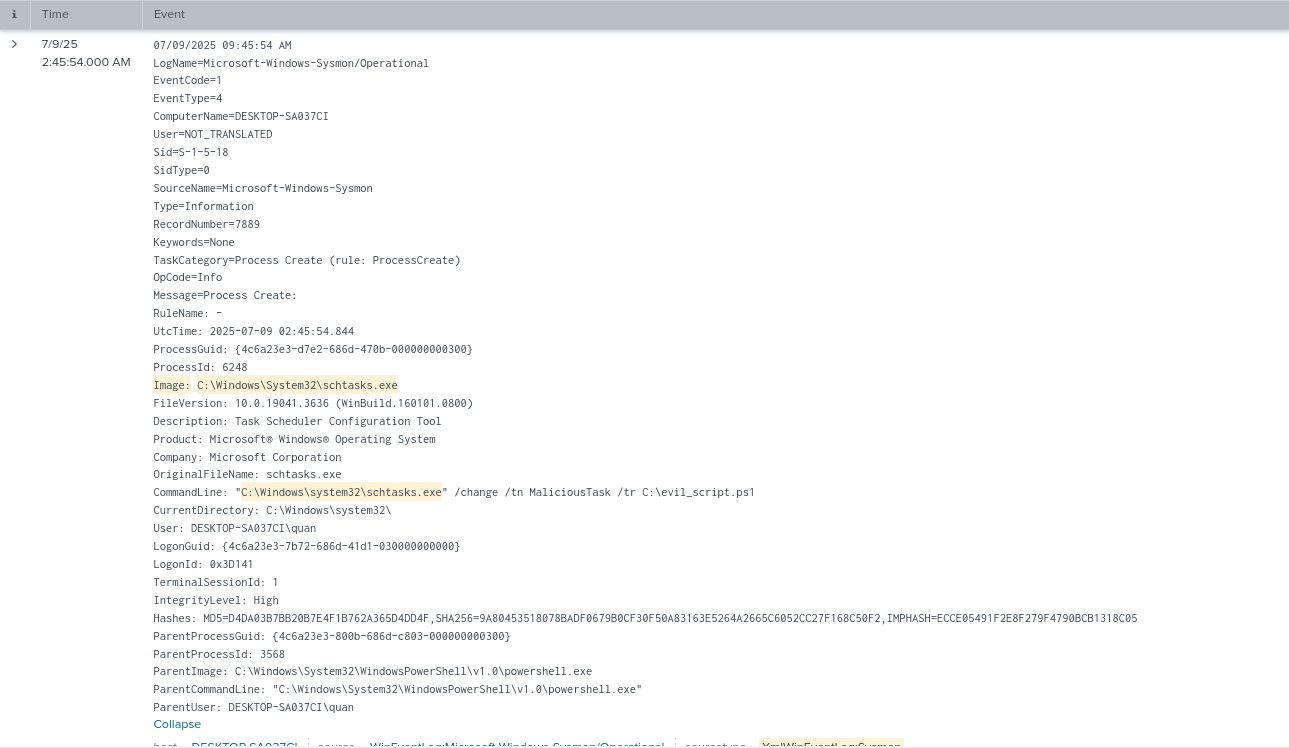
📌 **Mapping MITRE ATT&CK:**

Technique ID: T1053.005 Technique Name: Scheduled Task/Job: Scheduled Task

📌 **Mức độ nghi vấn:** Rất cao do tên task mang tính chất độc hại và đường dẫn thực thi bất thường.

📌 **Đề xuất điều tra:**

* Kiểm tra sự tồn tại và mã hash của file C:\\malware.exe.
* Phân tích hành vi của tiến trình powershell.exe (PID 1216) đã khởi tạo schtasks.exe để hiểu rõ hơn về chuỗi hành động.
* Kiểm tra cấu hình chi tiết của scheduled task "MaliciousTask" bằng lệnh schtasks /query /TN MaliciousTask /XML.
* Correlate với các sự kiện khác liên quan đến powershell.exe và schtasks.exe để xác định mục tiêu và phạm vi của hành động.
* Đánh giá tính hợp lệ của việc tạo scheduled task này trong bối cảnh hoạt động bình thường của người dùng DESKTOP-Lab\\lab .

**Sự kiện sửa đổi Scheduled Task – Tiếp tục dấu hiệu thiết lập Persistence**

📌 **Thời gian (UTC):** 2025-07-09 02:45:54.844

📌 **Thời gian (giờ địa phương):** ~09:45:354

📌 **Hostname:** DESKTOP-SA037CI

📌 **User thực hiện:** DESKTOP-SA037CI\quan

📌 **Process thực thi:**

Image: C:\\Windows\\System32\\schtasks.exe Process ID: 6248 Process GUID: {0300}

📌 **Hành vi:**

Tiến trình schtasks.exe đã được sử dụng để thay đổi (/change) task có tên "MaliciousTask". Đường dẫn thực thi của task này đã được sửa đổi thành C:\\evil\_script.ps1.

📌 **Mô tả kỹ thuật:**

Việc sửa đổi một scheduled task đã tồn tại là một kỹ thuật khác mà kẻ tấn công có thể sử dụng để thay đổi payload độc hại hoặc đảm bảo persistence. Thay vì tạo một task mới, chúng có thể nhắm mục tiêu vào một task hiện có (có thể đã được tạo bởi chúng hoặc thậm chí là một task hợp pháp bị lợi dụng) để thực thi mã độc của chúng. Việc thay đổi đường dẫn thực thi sang một script PowerShell (.ps1) là một dấu hiệu đáng lo ngại, vì PowerShell có khả năng thực hiện nhiều hành động độc hại trên hệ thống.

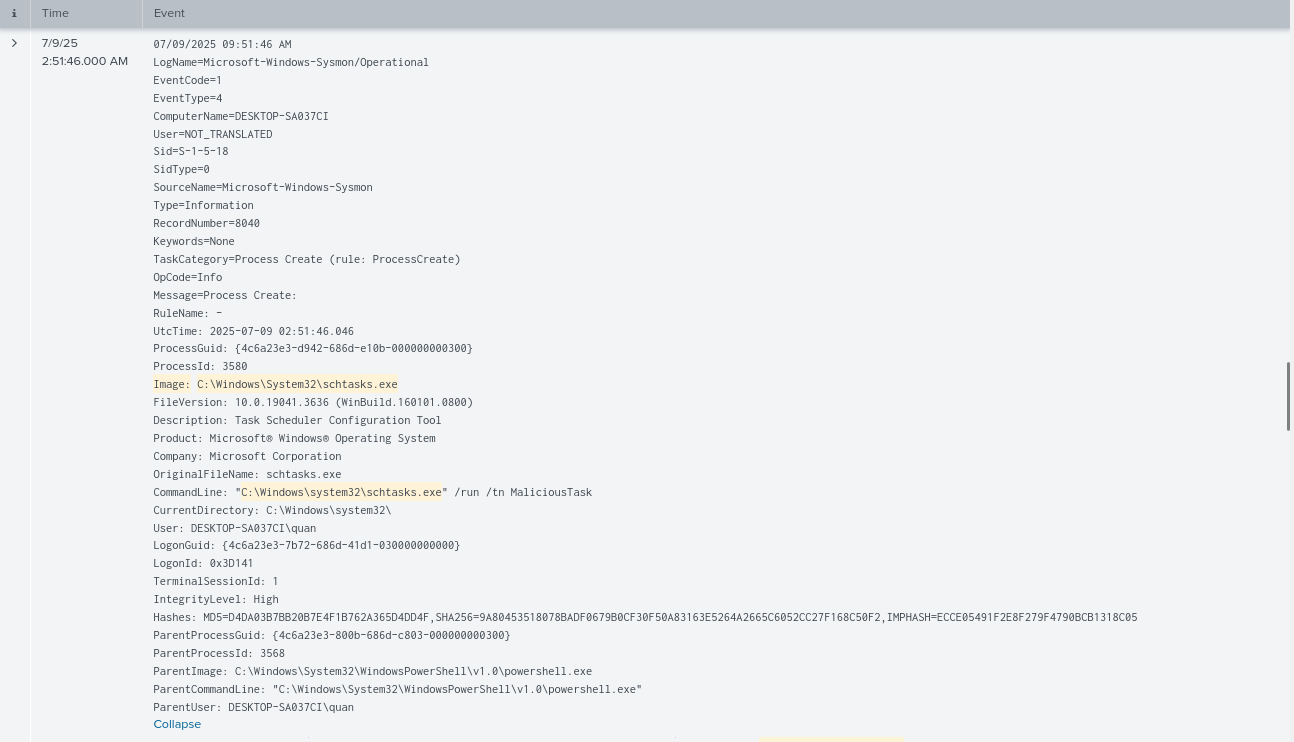
📌 **Mapping MITRE ATT&CK:**

Technique ID: T1053.005 Technique Name: Scheduled Task/Job: Scheduled Task

📌 **Mức độ nghi vấn:** Rất cao. Việc sửa đổi task "MaliciousTask" để chạy một script PowerShell có tên gợi ý độc hại ("evil\_script.ps1") cho thấy một nỗ lực tiếp tục duy trì quyền truy cập hoặc thực hiện các hành động độc hại khác.

📌 **Đề xuất điều tra:**

* Kiểm tra sự tồn tại và nội dung của file C:\\evil\_script.ps1. Phân tích script này để hiểu rõ các hành động mà nó thực hiện.
* Phân tích tiến trình cha powershell.exe (PID 2860) đã khởi tạo lệnh sửa đổi task để xác định nguồn gốc của hành động.
* So sánh các thuộc tính (thời gian tạo, người dùng) của task "MaliciousTask" trước và sau khi sửa đổi.
* Correlate sự kiện này với sự kiện tạo task ban đầu và các hoạt động khác liên quan đến tài khoản DESKTOP-Lab\\lab.
* Đánh giá xem việc sửa đổi task này có phù hợp với hoạt động bình thường của người dùng hay không.
* Thực hiện quét malware toàn diện trên hệ thống.

**Sự kiện thực thi Scheduled Task – Xác nhận hành vi độc hại**

📌 **Thời gian (UTC):** 2025-07-09 2:51:46.046

📌 **Thời gian (giờ địa phương):** ~09:51:46

📌 **Hostname:** DESKTOP-SA037CI

📌 **User thực hiện:** DESKTOP-SA037CI\quan

📌 **Process thực thi:** Image: C:\\Windows\\System32\\schtasks.exe Process ID: 3580 Process GUID: {0300}

📌 **Hành vi:**

Tiến trình schtasks.exe đã được sử dụng để thực thi (/run) ngay lập tức scheduled task có tên "MaliciousTask".

📌 **Mô tả kỹ thuật:**

Lệnh /run được sử dụng để kích hoạt một scheduled task ngay lập tức, bỏ qua lịch trình đã được thiết lập. Sự kiện này cho thấy kẻ tấn công (hoặc phần mềm độc hại) đã chủ động chạy task "MaliciousTask" sau khi tạo và sửa đổi nó. Điều này gần như chắc chắn dẫn đến việc thực thi payload độc hại đã được cấu hình trong task (hiện tại là C:\\evil\_script.ps1).

📌 **Mapping MITRE ATT&CK:**

Technique ID: T1053.005 Technique Name: Scheduled Task/Job: Scheduled Task

📌 **Mức độ nghi vấn:** Cực kỳ cao. Việc chủ động chạy task "MaliciousTask" sau khi cấu hình nó để thực thi một script đáng ngờ là một chỉ báo rõ ràng về hoạt động độc hại đang diễn ra.

📌 **Đề xuất điều tra khẩn cấp:**

* **Phân tích C:\\evil\_script.ps1 ngay lập tức:** Xác định các hành động mà script này thực hiện trên hệ thống.
* **Theo dõi các tiến trình con được tạo bởi C:\\evil\_script.ps1:** Sử dụng Sysmon Event ID 1 để theo dõi bất kỳ tiến trình nào được sinh ra từ script này.
* **Theo dõi các kết nối mạng:** Sử dụng Sysmon Event ID 3 để xem liệu script có thiết lập kết nối mạng nào không.
* **Thu thập artifacts:** Thu thập các artifacts liên quan đến việc thực thi script (ví dụ: file được tạo, registry key bị thay đổi).
* **Cô lập hệ thống (nếu cần thiết):** Để ngăn chặn sự lây lan hoặc các hành động độc hại tiếp theo.
* **Thông báo cho bộ phận ứng cứu sự cố:** Đây là một sự kiện nghiêm trọng cần được xử lý ngay lập tức.