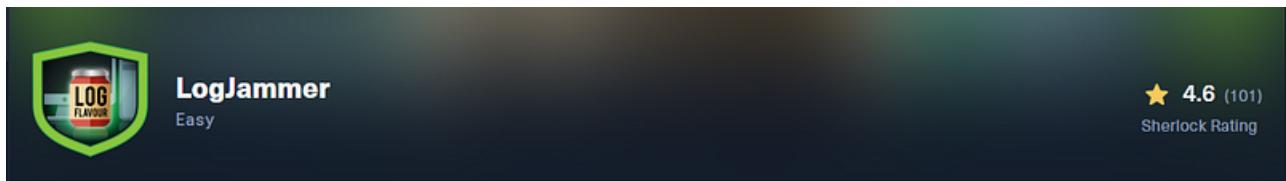


HTB Labs Sherlocks: LogJammer| DFIR Write-up



Scenario Overview

I was tasked with completing a technical assessment as a **junior DFIR consultant** for **Forela-Security**. The goal of the investigation was to analyze **Windows Event Logs** to determine whether the user **CyberJunkie** logged into the system and performed malicious actions.

The assessment focuses on identifying suspicious behavior using Windows logging artifacts.

Tool Used

Event Viewer

Event Viewer is a built-in Windows utility used to view and analyze system, security, application, and service logs. It is commonly used in DFIR investigations to reconstruct user activity, detect policy changes, and identify malicious behavior.

	Name	Date modified	Type	Size
	Powershell-Operational	22/12/2025 12:18 PM	Event Log	12,356 KB
	Security	22/12/2025 12:18 PM	Event Log	1,092 KB
	System	22/12/2025 12:18 PM	Event Log	2,116 KB
	Windows Defender-Operational	22/12/2025 12:18 PM	Event Log	1,092 KB
	Windows Firewall-Firewall	22/12/2025 12:18 PM	Event Log	1,092 KB

Task 1: First Successful Login (UTC)

Question: When did the CyberJunkie user first successfully log into the computer?

- **Event Log:** Security
- **Event ID:** 4624 (An account was successfully logged on)

To locate this:

- Navigated to **Security** logs
- Filtered for **Event ID 4624**

The screenshot shows the 'Filter Current Log' dialog box open in the Event Viewer. The 'Event logs:' dropdown is set to 'file:///C:/Users/loki/Documents/shared_files/logjammer/Event-Logs'. The 'Event ID:' field contains '4624'. The 'OK' button is highlighted. To the right is the main Event Viewer interface showing a list of events and a context menu for the selected event.

- Identified the first successful logon entry for the user *CyberJunkie*

The event timestamp was initially observed as **27/03/2023 21:37:09** (local time). Since the system operates in **UTC+7**, the time was converted back to UTC.

Answer:

The screenshot shows the Windows Event Viewer interface. The main pane displays a list of events from the 'SecurityHBT' log, with 115 events listed. One specific event is selected, which is event ID 4624, titled 'Event 4624, Microsoft Windows security auditing.' This event is categorized as a Logon event. The details pane shows the following information for this event:

Parameter	Value
Elevated Token	No
Impersonation Level	Impersonation
New Logon:	Security ID: S-1-5-21-3393683511-3463148672-371912004-1001 Account Name: CyberJunkie Account Domain: DESKTOP-887GK2L Logon ID: 0x25F9F Linked Logon ID: 0x25F28 Network Account Name: - Network Account Domain: -
Log Name	Security
Source	Microsoft Windows security
Event ID	4624
Level	Information
User	N/A
OpCode	Info
Logged	27/03/2023 10:37:09 PM
Task Category	Logon
Keywords	Audit Success
Computer	DESKTOP-887GK2L

The right-hand pane contains a context menu for the selected event, listing options like Open Saved Log..., Create Custom View..., Import Custom View..., Filter Current Log..., Properties, Find..., Save All Events As..., Delete, Rename, Refresh, Help, Event Properties, Copy, Save Selected Events..., Refresh, and Help. A message at the bottom right says 'Activate Windows Go to Settings to activate Win'.

27/03/2023 14:37:09 UTC

Task 2: Firewall Rule Added

Question: What is the name of the firewall rule added?

- Event Log:** Windows Firewall-Firewall

At **27/03/2023 22:44:43**, a firewall rule was added to the Windows Defender Firewall exception list.

The screenshot shows the Windows Event Viewer interface. The main pane displays a table of events from the 'Windows Firewall-FirewallHTBC' log, with a total of 929 events. The first few rows are Information-level events from March 27, 2023, at 10:44:43 PM and 10:37:35 PM, both related to the Windows Firewall With Advanced Security.

A specific event is selected, titled 'Event 2004, Windows Firewall With Advanced Security'. The 'General' tab is active, showing the following details:

- Added Rule:** Rule ID: {11309293-FB68-4969-93F9-7F75A9032570}
- Rule Name:** Metasploit C2 Bypass
- Origin:** Local
- Active:** Yes
- Direction:** Outbound
- Profiles:** Private, Domain, Public
- Action:** Allow
- Application Path:** Service Name: Metasploit C2 Bypass
- Protocol:** TCP
- Security Options:** None
- Edge Traversal:** None
- Modifying User:** S-1-5-21-3393683511-2463148672-371912004-1001
- Modifying Application:** C:\Windows\System32\mmc.exe

Below this, the event properties are listed:

- Log Name:** Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
- Source:** Windows Firewall With Adva
- Event ID:** 2004
- Level:** Information
- User:** LOCAL SERVICE
- OpCode:** Info
- Logged:** 27/03/2023 10:44:43 PM
- Task Category:** None
- Keywords:** (219902325552)
- Computer:** DESKTOP-887GK2L

The right-hand pane shows the 'Actions' menu for the selected event, which includes options like Open Saved Log..., Create Custom View..., Import Custom View..., Filter Current Log..., Properties, Find..., Save All Events As..., Delete, Rename, Refresh, Help, Event Properties, Copy, Save Selected Events..., Refresh, and Help.

Answer:

Metasploit C2 Bypass

Task 3: Firewall Rule Direction

Question: What is the direction of the firewall rule?

- **Event Log:** Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
- **Event ID:** 2004

Windows Firewall-FirewallIHTBC Number of events: 929

Level	Date and Time	Source	Event ID	Task Category
Information	27/03/2023 10:44:43 PM	Windows Firewall With ...	2004	None
Information	27/03/2023 10:37:35 PM	Windows Firewall With ...	2004	None
Information	27/03/2023 10:37:35 PM	Windows Firewall With ...	2004	None

Event 2004, Windows Firewall With Advanced Security

General Details

A rule has been added to the Windows Defender Firewall exception list.

Added Rule:

- Rule ID: {11309293-FB68-4969-93F9-7F75A9032570}
- Rule Name: Metasploit C2 Bypass
- Origin: Local
- Active: Yes
- Direction: Outbound
- Profiles: Private, Domain, Public
- Action: Allow
- Application Path: C:\Windows\System32\mmc.exe
- Service Name:
- Protocol: TCP
- Security Options: None
- Edge Traversal: None
- Modifying User: S-1-5-21-3393683511-2463148672-371912004-1001
- Modifying Application: C:\Windows\System32\mmc.exe

Log Name: Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
Source: Windows Firewall With Adva Logged: 27/03/2023 10:44:43 PM
Event ID: 2004 Task Category: None
Level: Information Keywords: (219902325552)
User: LOCAL SERVICE Computer: DESKTOP-887GK2L
OpCode: Info

Actions

- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Delete
- Rename
- Refresh
- Help

Event 2004, Windows Firewall With Adv... ▾

- Event Properties
- Copy
- Save Selected Events...
- Refresh
- Help

Activate Windows
Go to Settings to activate Windows.

Reviewing the same firewall event revealed the rule direction.

Answer:

Outbound

Task 4: Audit Policy Change

Question: What is the subcategory of the audit policy that was changed?

- **Event Log:** Security
- **Event ID:** 4702

Audit policy change events are recorded in the Security log. Upon inspection, the **Task Category** (subcategory) of the modified audit policy was identified.

The screenshot shows the Windows Event Viewer interface. On the left, a list of events from the 'Security' log is displayed, with event 4702 selected. The main pane shows the details of this event: 'A scheduled task was updated.' Under 'Subject', it lists security information: Security ID: SYSTEM, Account Name: DESKTOP-887GK2L\$, Account Domain: WORKGROUP, Logon ID: 0x3E7. Under 'Task Information', it shows Task Name: \Microsoft\Windows\Flighting\OneSettings\RefreshCache and Task New Content: <xml version="1.0" encoding="UTF-16"?><Task version="1.6" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"><RegistrationInfo>. Below this, event properties are listed: Log Name: Security, Source: Microsoft Windows security, Logged: 27/03/2023 10:52:20 PM, Event ID: 4702, Task Category: Other Object Access Events, Level: Information, User: N/A, Computer: DESKTOP-887GK2L, and OpCode: Info. The right pane contains a toolbar with various actions like Open Saved Log..., Create Custom View..., Import Custom View..., Filter Current Log..., Properties, Find..., Save All Events As..., View, Delete, Rename, Refresh, and Help. A message at the bottom right says 'Activate Windows Go to Settings to activate Windows.'

Answer:

Other Object Access Events

Task 5: Scheduled Task Created

Question: What is the name of the scheduled task created by CyberJunkie?

- **Event Log:** Security
- **Event ID:** 4698
- **Timestamp:** 27/03/2023 22:51:21

This event indicates the creation of a scheduled task.

Answer:

HTB-AUTOMATION

SecurityHBTC Number of events: 115

Level	Date and Time	Source	Event ID	Task Category
Information	27/03/2023 10:52:19 PM	Microsoft Windows sec...	4624	Logon
Information	27/03/2023 10:52:19 PM	Microsoft Windows sec...	4702	Other Object Access Eve...
Information	27/03/2023 10:52:12 PM	Microsoft Windows sec...	4624	Logon
Information	27/03/2023 10:52:11 PM	Microsoft Windows sec...	4624	Logon
Information	27/03/2023 10:52:09 PM	Microsoft Windows sec...	4624	Logon
Information	27/03/2023 10:51:21 PM	Microsoft Windows sec...	4698	Other Object Access Eve...

Event 4698, Microsoft Windows security auditing.

General Details

A scheduled task was created.

Subject:

```
Security ID: S-1-5-21-3393683511-3463148672-371912004-1001
Account Name: CyberJunkie
Account Domain: DESKTOP-887GK2L
Logon ID: 0x25F28
```

Task Information:

```
Task Name: \HTB-AUTOMATION
Task Content: <?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
| <RegistrationInfo>
```

Log Name: Security

Source: Microsoft Windows security Logged: 27/03/2023 10:51:21 PM

Event ID: 4698 Task Category: Other Object Access Events

Level: Information Keywords: Audit Success

User: N/A Computer: DESKTOP-887GK2L

OpCode: Info

Actions

- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- View
 - Delete
 - Rename
 - Refresh
 - Help
- Event Properties
- Copy
- Save Selected Events...
- Refresh
- Help

Activate Windows
Go to Settings to activate Windows.

SecurityHBTC Number of events: 115

Level	Date and Time	Source	Event ID	Task Category
Information	27/03/2023 10:52:19 PM	Microsoft Windows sec...	4624	Logon
Information	27/03/2023 10:52:19 PM	Microsoft Windows sec...	4702	Other Object Access Eve...
Information	27/03/2023 10:52:12 PM	Microsoft Windows sec...	4624	Logon
Information	27/03/2023 10:52:11 PM	Microsoft Windows sec...	4624	Logon
Information	27/03/2023 10:52:09 PM	Microsoft Windows sec...	4624	Logon
Information	27/03/2023 10:51:21 PM	Microsoft Windows sec...	4698	Other Object Access Eve...

Event 4698, Microsoft Windows security auditing.

General Details

```
<RunOnlyIfIdle>false</RunOnlyIfIdle>
<WakeToRun>false</WakeToRun>
<ExecutionTimeLimit>P3D</ExecutionTimeLimit>
<Priority>7</Priority>
<Settings>
<Actions Context="Author">
<Exec>
<Command>C:\Users\CyberJunkie\Desktop\Automation-HTB.ps1</Command>
<Arguments> -A cyberjunkie@hackthebox.eu</Arguments>
</Exec>
</Actions>
</Task>
```

Log Name: Security

Source: Microsoft Windows security Logged: 27/03/2023 10:51:21 PM

Event ID: 4698 Task Category: Other Object Access Events

Level: Information Keywords: Audit Success

User: N/A Computer: DESKTOP-887GK2L

OpCode: Info

Actions

- Open
- Create
- Import
- Filter
- Properties
- Find...
- Save All Events As...
- View
 - Delete
 - Rename
 - Refresh
 - Help
- Event Properties
- Copy
- Save Selected Events...
- Refresh
- Help

Activate W...

Task 6: Scheduled Task File Path

Question: What is the full path of the file scheduled for execution?

- **Event Log:** Security
- **Event ID:** 4698

Scrolling through the event details reveals the file path associated with the task.

Answer:

C:\Users\CyberJunkie\Desktop\Automation-HTB.ps1

Task 7: Command Arguments

Question: What arguments were passed to the scheduled task command?

- **Event Log:** Security
- **Event ID:** 4698

The command arguments are listed directly below the executable path in the event details.

Answer:

-A cyberjunkie@hackthebox.eu

SecurityHBTC Number of events: 115

Level	Date and Time	Source	Event ID	Task Category
(i) Information	27/03/2023 10:52:19 PM	Microsoft Windows sec...	4624	Logon
(i) Information	27/03/2023 10:52:19 PM	Microsoft Windows sec...	4702	Other Object Access Eve...
(i) Information	27/03/2023 10:52:12 PM	Microsoft Windows sec...	4624	Logon
(i) Information	27/03/2023 10:52:11 PM	Microsoft Windows sec...	4624	Logon
(i) Information	27/03/2023 10:52:09 PM	Microsoft Windows sec...	4624	Logon
(i) Information	27/03/2023 10:51:21 PM	Microsoft Windows sec...	4698	Other Object Access Eve...

Event 4698, Microsoft Windows security auditing.

General Details

```
<RunOnlyIfIdle>false</RunOnlyIfIdle>
<WakeToRun>false</WakeToRun>
<ExecutionTimeLimit>P3D</ExecutionTimeLimit>
<Priority>7</Priority>
<Settings>
<Actions Context="Author">
<Exec>
<Command>C:\Users\CyberJunkie\Desktop\Automation-HTB.ps1</Command>
<Arguments>-A cyberjunkie@hackthebox.eu</Arguments>
</Exec>
</Actions>
</Task>
```

Log Name: Security
 Source: Microsoft Windows security Logged: 27/03/2023 10:51:21 PM
 Event ID: 4698 Task Category: Other Object Access Events
 Level: Information Keywords: Audit Success
 User: N/A Computer: DESKTOP-887GK2L
 OpCode: Info

Activate W...

Task 8: Malware Identified by Antivirus

Question: Which tool was identified as malware?

- **Event Log:** Windows Defender-Operational
- **Event ID:** 1117

Windows Defender detected a malicious tool during system monitoring.

Answer:

SharpHound

Windows Defender-Operational_1 Number of events: 444

Level	Date and Time	Source	Event ID	Task Category
Information	27/03/2023 10:42:48 PM	Windows Defender	1117	None
Information	27/03/2023 10:42:48 PM	Windows Defender	1117	None
Information	27/03/2023 10:42:34 PM	Windows Defender	5007	None
Warning	27/03/2023 10:42:34 PM	Windows Defender	1116	None
Warning	27/03/2023 10:42:34 PM	Windows Defender	1116	None
Information	27/03/2023 10:41:45 PM	Windows Defender	5007	None

Event 1117, Windows Defender

General Details

Microsoft Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software. For more information please see the following:
<https://go.microsoft.com/fwlink/?linkid=37020&name=HackToolMSIL/SharpHound!MSB&threatid=2147814944&enterprise=0>

Name: HackToolMSIL/SharpHound!MSR
ID: 2147814944
Severity: High
Category: Tool
Path: containerfile_C:\Users\ CyberJunkie\Downloads\SharpHound-v1.1.0.zip; file: C:\Users\ CyberJunkie\Downloads\SharpHound-v1.1.0.zip->
SharpHound.exe; webfile_C:\Users\ CyberJunkie\Downloads\SharpHound-v1.1.0.zip[https://objects.githubusercontent.com/github-production-release-
asset-2e65be/385323486/70d776cc-8f83-44d5-b226-2dccc4f7c1e37X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=AKIAIWNIYAX4CSVEH53A4.18.2302.7F202303274.18.2302.7Fus-east-14.18.2302.7Faws4_request&X-Amz-Date=20230327114428Z&X-Amz-Signature=1989ef5ca3ee150dc1e23623434adc1e4a444ba026423c32edf5e85d881a771&X-Amz-SignedHeaders=host&actor_id=0&repo_id=385323486&response-content-disposition=attachment!0EBC4BEA-5532-4EF8-8A34-64F91CC8702E]

Log Name: Microsoft-Windows-Windows Defender/Operational
Source: Windows Defender Logged: 27/03/2023 10:42:48 PM
Event ID: 1117 Task Category: None
Level: Information Keywords:
User: SYSTEM Computer: DESKTOP-887GK2L
OpCode: Info

Actions

- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- View
- Delete
- Rename
- Refresh
- Help

Event 1117, Windows Defender

- Event Properties
- Copy
- Save Selected Events...
- Refresh
- Help

Activate Windows

Task 9: Malware File Path

Question: What is the full path of the detected malware?

- **Event Log:** Windows Defender-Operational
- **Event ID:** 1117

Answer:

C:\Users\ CyberJunkie\Downloads\SharpHound-v1.1.0.zip

Task 10: Antivirus Action Taken

Question: What action was taken by the antivirus?

- **Event Log:** Windows Defender-Operational
- **Event ID:** 1117

Answer:

Quarantine

Windows Defender-Operational_1 Number of events: 444

Level	Date and Time	Source	Event ID	Task Category
Information	27/03/2023 10:42:48 PM	Windows Defender	1117	None
Information	27/03/2023 10:42:48 PM	Windows Defender	1117	None
Information	27/03/2023 10:42:34 PM	Windows Defender	5007	None
Warning	27/03/2023 10:42:34 PM	Windows Defender	1116	None
Warning	27/03/2023 10:42:34 PM	Windows Defender	1116	None
Information	27/03/2023 10:41:45 PM	Windows Defender	5007	None

Event 1117, Windows Defender

General Details

```
BDESKTOP-887GK2L\ CyberJunkiefilename[0EBC4BEA-5532-4EFB-8A34-64F91CC8702E]\ SharpHound-v1.1.0.zip&response-content-type=application/4.18.2302.7focet-stream|pid:3532,ProcessStart:133244017530289775
Detection Origin: Internet
Detection Type: Concrete
Detection Source: Downloads and attachments
User: NT AUTHORITY\SYSTEM
Process Name: Unknown
Action: Quarantine
Action Status: No additional actions required
Error Code: 0x80508023
Error description: The program could not find the malware and other potentially unwanted software on this device.
Security intelligence Version: AV: 1.385.1261.0, AS: 1.385.1261.0, NIS: 1.385.1261.0
Engine Version: AM: 1.1.20100.6, NIS: 1.1.20100.6
```

Log Name: Microsoft-Windows-Windows Defender/Operational
Source: Windows Defender **Logged:** 27/03/2023 10:42:48 PM
Event ID: 1117 **Task Category:** None
Level: Information **Keywords:**
User: SYSTEM **Computer:** DESKTOP-887GK2L
OpCode: Info

Actions

- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- View
- Delete
- Rename
- Refresh
- Help

Event 1117, Windows Defender

- Event Properties
- Copy
- Save Selected Events...
- Refresh
- Help

Activate Windows
Go to Settings to activate Windows.

Task 11: PowerShell Command Execution

Question: What PowerShell command was executed by the user?

- **Event Log:** Powershell-Operational
- **Event ID:** 4104
- **Timestamp:** 27/03/2023 22:58:33

This event records executed PowerShell script blocks.

Answer:

```
Get-FileHash -Algorithm md5 .\Desktop\Automation-HTB.ps1
```

Powershell-Operational_1 Number of events: 578

Level	Date and Time	Source	Event ID	Task Category
Information	27/03/2023 10:58:33 PM	PowerShell (Microsoft-Win...	4103	Executing Pipeline
Verbose	27/03/2023 10:58:33 PM	PowerShell (Microsoft-Win...	4104	Execute a Remote Com...
Information	27/03/2023 10:58:33 PM	PowerShell (Microsoft-Win...	4103	Executing Pipeline
Information	27/03/2023 10:58:31 PM	PowerShell (Microsoft-Win...	4103	Executing Pipeline
Information	27/03/2023 10:58:28 PM	PowerShell (Microsoft-Win...	4103	Executing Pipeline
Information	27/03/2023 10:58:07 PM	PowerShell (Microsoft-Win...	4103	Executing Pipeline

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General Details

Creating Scriptblock text (1 of 1):
Get-FileHash -Algorithm md5 .\Desktop\Automation-HTB.ps1

ScriptBlock ID: b4fcf72f-abdc-4a84-923f-8e06a758000b
Path:

Log Name: Microsoft-Windows-PowerShell/Operational
Source: PowerShell (Microsoft-Wind Logged: 27/03/2023 10:58:33 PM
Event ID: 4104 Task Category: Execute a Remote Command
Level: Verbose Keywords: None
User: S-1-5-21-3393683511-346314 Computer: DESKTOP-887GK2L
OpCode: On create calls

Actions

- Powershell-Operational_1 ▾
 - Open Saved Log...
 - Create Custom View...
 - Import Custom View...
 - Filter Current Log...
 - Properties
 - Find...
 - Save All Events As...
- View ▾
 - Delete
 - Rename
 - Refresh
 - Help
- Event 4104, PowerShell (Microsoft-Win... ▾
 - Event Properties
 - Copy
 - Save Selected Events...
 - Refresh
 - Help

Activate Windows
Go to Settings to activate Windows.

Task 12: Cleared Event Log

Question: Which event log file was cleared?

- **Event Log:** System
- **Event ID:** 104

The log clear event specifies which log was deleted.

Answer:

Microsoft-Windows-Windows Firewall With Advanced Security/Firewall

System_1 Number of events: 2,186

Level	Date and Time	Source	Event ID	Task Category
Information	27/03/2023 11:01:56 PM	Eventlog	104	Log clear
Warning	27/03/2023 10:58:56 PM	DNS Client Events	1014 (1014)	
Information	27/03/2023 10:57:42 PM	GroupPolicy (Microsoft...)	1502	None
Information	27/03/2023 10:57:34 PM	GroupPolicy (Microsoft...)	1502	None
Information	27/03/2023 10:56:44 PM	GroupPolicy (Microsoft...)	1502	None
Information	27/03/2023 10:50:03 PM	GroupPolicy (Microsoft...)	1500	None

Event 104, Eventlog

General Details

The Microsoft-Windows-Windows Firewall With Advanced Security/Firewall log file was cleared.

Log Name: System
 Source: Eventlog
 Event ID: 104
 Level: Information
 User: S-1-5-21-3393683511-346314
 OpCode: Info
 Logged: 27/03/2023 11:01:56 PM
 Task Category: Log clear
 Keywords:
 Computer: DESKTOP-887GK2L

Activate Windows

Actions

- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- View
- Delete
- Rename
- Refresh
- Help

Event 104, Eventlog

- Event Properties
- Copy
- Save Selected Events...
- Refresh
- Help

By [Alexander Sapo](#) on [December 22, 2025](#).

[Canonical link](#)

Exported from [Medium](#) on February 7, 2026.