← Case report for event ID: 1007

ID	Alert rule	Description	Incident type	Severity level	Date and time detected
1007	Suspicious Parent Child Relationship	A suspicious process with an uncommon parent-child relationship was detected in your environment.	Process	Low	Dec 4th 2025 at 16:06

Alert details

Incident report

Edit report

Incident classification

(•) True positive ( ) False positive

Case report

Please write a detailed report on the steps taken to analyse and contain this incident, including all relevant information and the rationale for its closure.

When:
Date: 12/04/2025
Time of activity: 08:03:31

Who:
List of Affected Entities:
- Host: win-3451
- Process: taskhostw.exe
- Parent Process: svchost.exe

What (Reason for Classifying as Suspicious):
- `taskhostw.exe` was spawned by `svchost.exe`, which is an uncommon parent-child relationship.
- The command line included **KEYROAMING**, a Windows service that manages roaming cryptographic keys.
- While this can be legitimate, attackers may abuse it to access or tamper with encryption keys.

Why
Reason for Escalating the Alert:
-

Does this alert require escalation?

(•) Yes ( ) No

Complete IR:

When:
Date: 12/04/2025
Time of activity: 08:03:31

Who:
List of Affected Entities:
Host: win-3451
Process: taskhostw.exe
Parent Process: svchost.exe

What (Reason for Classifying as Suspicious):
taskhostw.exe was spawned by svchost.exe, which is an uncommon parent-child relationship.
The command line included KEYROAMING, a Windows service that manages roaming cryptographic keys.
While this can be legitimate, attackers may abuse it to access or tamper with encryption keys.

Why
Reason for Escalating the Alert:
Sensitive cryptographic key handling was invoked in an unusual way.
Uncommon parent-child relationship may indicate DLL hijacking or credential theft attempts.
Requires validation to confirm if this is normal Windows behavior or malicious activity.

How
Recommended Remediation Actions:
Verify if the KeyRoaming service was legitimately invoked during a user logon.
Check the integrity of DLLs loaded by taskhostw.exe to ensure they are not replaced.
Correlate with surrounding logs (PowerShell, login events, network connections).
Escalate to Tier 2 if linked with suspicious credential activity.
Investigate miguel.odonnell@tryhatme.com related to this action

List of Attack Indicators:
Uncommon parent-child relationship (svchost.exe → taskhostw.exe).
Invocation of KEYROAMING service outside expected logon/profile roaming events.
Sensitive cryptographic key management flagged for review.
The user miguel.odonnell@tryhatme.com is from sales and no valid purpose to execute the said parent program.