← Case report for event ID: 1002

ID	Alert rule	Description	Incident type	Severity level	Date and time detected
1002	Suspicious Parent Child Relationship	A suspicious process with an uncommon parent-child relationship was detected in your environment.	Process	Low	Dec 1st 2025 at 19:20

Alert details

datasource: sysmon

timestamp: 12/01/2025 11:18:01.544

event.code: 1

host.name: win-3451

process.name: taskhostw.exe

process.pid: 3585

process.parent.pid: 3653

process.parent.name: svchost.exe

process.command_line: taskhostw.exe KEYROAMING

process.working_directory: C:\Windows\system32\

event.action: Process Create (rule: ProcessCreate)

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: 12/01/2025
Time of Activity: 11:18:01

List of Related Entities:
Who:
- Host: win-3451
- User Context: System process (working directory: `C:\Windows\system32\`)

What:
Reason for Classifying as False Positive:
- A process `taskhostw.exe` was created with the parameter **KEYROAMING**.
- Parent process: `svchost.exe`.
- While both are legitimate Windows processes, this parent-child relationship is uncommon and flagged for review.
- The KEYROAMING parameter loads Windows' cryptographic key roaming service, which attackers could potentially abuse to access or tamper with encryption keys.

Does this alert require escalation?

(●) Yes ( ) No

Complete IR:

When
Date: 12/01/2025
Time of Activity: 11:18:01

List of Related Entities:
Who:
- Host: win-3451
- User Context: System process (working directory: C:\Windows\system32\)

What:
Reason for Classifying as False Positive:
- A process taskhostw.exe was created with the parameter KEYROAMING.
- Parent process: svchost.exe.
- While both are legitimate Windows processes, this parent-child relationship is uncommon and flagged for review.
- The KEYROAMING parameter loads Windows' cryptographic key roaming service, which attackers could potentially abuse to access or tamper with encryption keys.

Why (Reason for Escalation)
- Uncommon parent-child relationship between svchost.exe and taskhostw.exe.
- Activity involves cryptographic key management, which is sensitive and could indicate credential theft attempts.
- Requires validation to determine if this is normal system behavior or malicious DLL injection.
How (Recommended Remediation Actions)
- Verify if the KeyRoaming service was legitimately invoked by Windows at logon.
- Correlate with surrounding logs (PowerShell, network connections, other Sysmon events).
- Check integrity of the DLLs loaded by taskhostw.exe to ensure they are not replaced or tampered.
- Monitor for repeated or unusual invocations of KEYROAMING across other hosts.
- Escalate to Tier 2 if correlated with suspicious activity (credential theft, persistence).
Indicators of Attack
-svchost.exe spawning taskhostw.exe with uncommon parameters.
- Invocation of KEYROAMING service outside expected logon or profile roaming events.
- Sensitive cryptographic key handling flagged for review.