← Case report for event ID: 1006

ID	Alert rule	Description	Incident type	Severity level	Date and time detected
1006	Suspicious Parent Child Relationship	A suspicious process with an uncommon parent-child relationship was detected in your environment.	Process	Low	Dec 4th 2025 at 16:05

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: 08:02:41

Who:
List of Affected Entities:
- Host: win-3450
- Process: rdpclip.exe
- Parent Process: svchost.exe

What
Reason for Classifying as Suspicious:
- `rdpclip.exe` was spawned by `svchost.exe`, which is an uncommon parent-child relationship.
- Normally, `rdpclip.exe` is started during Remote Desktop sessions by the session manager, not directly by `svchost.exe`.

Why
Reason for Escalating the Alert:
- Unusual parent-child relationship may indicate process injection or abuse of legitimate Windows services

Does this alert require escalation?

(•) Yes ( ) No

Complete IR:

When:
Date: 12/04/2025
Time of activity: 08:02:41

Who:
List of Affected Entities:
Host: win-3450
Process: rdpclip.exe
Parent Process: svchost.exe

What
Reason for Classifying as Suspicious:
rdpclip.exe was spawned by svchost.exe, which is an uncommon parent-child relationship.
Normally, rdpclip.exe is started during Remote Desktop sessions by the session manager, not directly by svchost.exe.

Why
Reason for Escalating the Alert:
Unusual parent-child relationship may indicate process injection or abuse of legitimate Windows services.
Activity involves Remote Desktop clipboard, which attackers can exploit for data transfer or persistence.

How
Recommended Remediation Actions:
Verify if an active RDP session was occurring at the time of the alert.
Check integrity of rdpclip.exe to confirm it is the legitimate Windows binary.
Correlate with other logs (network connections, PowerShell, login events).
Escalate to Tier 2 if linked with suspicious activity or unauthorized RDP usage.

List of Attack Indicators:
Uncommon parent-child relationship (svchost.exe → rdpclip.exe).
Remote Desktop clipboard process invoked outside expected context.