Template Injection Detection - Windows, Detection Strategy DET0566

Archived: 2026-04-05 14:02:29 UTC

AN1564

Detection of Office or document viewer processes (e.g., winword.exe) initiating network connections to remote templates or executing scripts due to manipulated template references (e.g., embedded in .docx, .rtf, or .dotm files), followed by suspicious child process creation (e.g., PowerShell).

Log Sources

Mutable Elements

Field	Description
TemplateURLPatterns	Can be tuned to flag known bad domains or external resources in template fields.
ParentProcess	May be environment-specific; typically Word, Excel, PowerPoint.
TimeWindow	Correlation window for process + network activity.
ChildProcessAnomalyThreshold	Trigger when document-spawned child process deviates from expected profile.
