Detect Abuse of Dynamic Data Exchange (T1559.002), Detection Strategy DET0504

Archived: 2026-04-05 13:00:53 UTC

AN1393

Detects anomalous use of Dynamic Data Exchange (DDE) for code execution, such as Office applications (WINWORD.EXE, EXCEL.EXE) spawning command interpreters, or loading unusual modules through DDEAUTO/DDE formulas. Correlates suspicious parent-child process relationships, registry keys enabling DDE, and module loads inconsistent with normal Office usage.

Log Sources

Mutable Elements

Field	Description
AllowedParentChildPairs	Define legitimate parent-child relationships for Office processes to reduce false positives.
TimeWindow	Threshold for correlating Office process creation with subsequent command execution via DDE.
SuspiciousDLLList	Maintain allow/block list of DLLs that Office is expected to load.
