Detection Strategy for IFEO Injection on Windows, Detection Strategy DET0422

Archived: 2026-04-05 16:20:06 UTC

AN1186

Registry key modifications under IFEO paths (e.g., Debugger value set under Image File Execution Options), especially for security-related or accessibility binaries, followed by anomalous process execution with debugger flags or SYSTEM-level access at login. Detectable by correlating registry modifications, process creation, and parent-child anomalies with unusual command-line usage or access tokens.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Time delta for correlating registry modification and debugger-triggered execution
TargetBinary	Specific executables that trigger defenders’ alerts when IFEO values are set
ParentProcessAnomaly	Tunable logic for detecting parent-child anomalies (e.g., non-standard parent processes)
TokenElevationContext	May require tuning based on normal SYSTEM or admin process elevation patterns

---

Source: https://attack.mitre.org/detectionstrategies/DET0422#AN1186