Detect Persistence via Malicious Office Add-ins, Detection Strategy DET0050

Archived: 2026-04-05 14:11:35 UTC

AN0137

An adversary writes or drops a malicious Office Add-in (e.g., WLL, XLL, COM) to a trusted directory or modifies registry keys to load malicious add-ins on Office application launch. Upon user opening Word or Excel, the add-in is automatically loaded, triggering execution of the payload, often spawning scripting engines or anomalous child processes.

Log Sources

Mutable Elements

Field	Description
AddInExtension	Malicious add-ins may have varying extensions (.wll, .xll, .dll, .vsto)
TrustedPath	Office trusted add-in paths may differ across enterprise configurations
RegistryPath	Registry keys used to load add-ins may be version- and app-specific
ChildProcessName	Office processes spawning mshta.exe, powershell.exe, or rundll32.exe are abnormal
TimeWindow	Add-in loading may occur only during Office launch windows

AN0138

Malicious Office add-ins loaded via VSTO, COM, or VBA auto-load paths. Upon launch of Word/Excel/Outlook, the add-in executes code without user action. Add-in resides in trusted directory or registered via Office COM/VBE subsystem. Behavior includes unsigned add-in execution, anomalous load context, or add-in spawning interpreter process.

Log Sources

Data Component	Name	Channel
Application Log Content (DC0038)	WinEventLog:Application	Office Add-in load errors, abnormal loading context, or unsigned add-in warnings

Data Component	Name	Channel
Command Execution (DC0064)	WinEventLog:Microsoft-Office/OutlookAddinMonitor	Outlook loading add-in via unexpected load path or non-default profile context

Mutable Elements

Field	Description
UnsignedAddInBehavior	Admins may allow or block unsigned add-ins depending on GPO configuration
OfficeProductVersion	Different Office versions store trusted paths and add-in configs in version-specific locations
AddInTrigger	Some add-ins only load on specific actions (new document, open file, etc.)
