Detection Strategy for Hijack Execution Flow through the AppDomainManager on Windows., Detection Strategy DET0517

Archived: 2026-04-05 18:36:15 UTC

AN1433

Detection focuses on unauthorized manipulation of .NET AppDomainManager behavior. Defenders may observe suspicious creation of new AppDomains within trusted processes, anomalous loading of assemblies via non-standard configuration files, or registry/environment variable changes redirecting AppDomainManager to malicious assemblies. Correlated events include config file tampering, new process creation of .NET host processes (e.g., w3wp.exe, powershell.exe) with modified runtime parameters, and module loads of unusual or unsigned .NET DLLs.

Log Sources

Mutable Elements

Field	Description
TargetProcesses	List of monitored .NET host processes (e.g., powershell.exe, w3wp.exe, svchost.exe).
AssemblyWhitelist	Known benign .NET assemblies expected to load via AppDomainManager.
ConfigFilePaths	Directory paths where configuration tampering should be monitored (application directories, system32, program files).
TimeWindow	Correlation period between file modification of config/environment settings and subsequent anomalous module load.