Detection of Malicious Code Execution via InstallUtil.exe, Detection Strategy DET0138

Archived: 2026-04-05 18:23:51 UTC

Analytics

- Windows

AN0388

Execution of InstallUtil.exe from .NET framework directories with arguments specifying non-standard or attacker-supplied assemblies, especially when followed by suspicious child process creation or script execution. Detection also includes correlation of newly created binaries prior to InstallUtil invocation and anomalous command-line usage compared to historical baselines.

Log Sources

Mutable Elements

Field	Description
InstallUtilPathRegex	Regex pattern for InstallUtil.exe in .NET directories; tune to exclude known good administrative scripts
AssemblyPathRegex	Patterns for identifying suspicious assemblies (e.g., in temp folders, user profiles)
ChildProcessList	List of suspicious child processes spawned from InstallUtil.exe (e.g., cmd.exe, powershell.exe, rundll32.exe)
TimeWindow	Time correlation window between file creation of assembly and its execution via InstallUtil.exe