Detection Strategy for Compile After Delivery - Source Code to Executable Transformation, Detection Strategy DET0501

Archived: 2026-04-05 15:28:14 UTC

AN1381

Detects compilation activity using csc.exe, ilasm.exe, or msbuild.exe initiated by user-space processes outside typical development environments, followed by execution or network activity from newly written binaries.

Log Sources

Mutable Elements

Field	Description
ParentProcessName	Filter for unexpected users (non-dev) launching compilers like csc.exe or msbuild.exe
OutputDirectoryPath	Adjust paths for sensitive file write zones (e.g., `C:\Users\Public\`, `%TEMP%`, or Desktop)
TimeWindow	Tune the correlation window between compilation and subsequent execution or C2

AN1382

Detects GCC or Clang invoked on suspicious file paths (e.g., /tmp/, ~/Downloads) with output to executable binaries, followed by execution or outbound traffic from these binaries.

Log Sources

Mutable Elements

Field	Description
CompilerBinaryPath	Specify path and binaries for detection (e.g., `/usr/bin/gcc`, `/opt/mingw/bin/gcc`)
FilePermissionProfile	Match uncommon chmod behavior post-compilation (e.g., +x in `/tmp` or home directories)

AN1383

Detects non-standard compilation activity via Xcode CLI tools or bundled GCC/MONO packages writing new executable files and executing them outside dev environments (e.g., user Downloads folder).

Log Sources

Mutable Elements

Field	Description
CompilerInvocationPattern	Detect calls to `xcodebuild`, `clang`, or `/Applications/Mono.app/...` from non-admin users
OutputBinaryPath	Monitor for output files in user-writable paths (e.g., `~/Library/Caches`, `~/Downloads`)
