Detection Strategy for Hijack Execution Flow using Executable Installer File Permissions Weakness, Detection Strategy DET0038

Archived: 2026-04-05 16:35:21 UTC

AN0108

Executables written or modified in installer directories (e.g., %TEMP% subdirectories or Program Files installer paths) followed by execution under elevated context. Defender observes abnormal file replacement activity, process creation by installer processes pointing to attacker-supplied binaries, and unexpected module loads in elevated processes.

Log Sources

Mutable Elements

Field	Description
MonitoredDirectories	Specific writable directories to monitor (e.g., %TEMP%, C:\ProgramData, installer unpack paths).
HashBaseline	Known good hashes of installer binaries to detect replacement.
TimeWindow	Correlation interval between file overwrite and execution event.
UserContext	Differentiate expected admin-installer execution vs. anomalous user writes.