Detection of Msiexec Abuse for Local, Network, and DLL Execution, Detection Strategy DET0158

Archived: 2026-04-02 11:10:01 UTC

AN0445

Detection of msiexec.exe execution where command-line arguments reference remote MSI packages, UNC paths, HTTP/HTTPS URLs, or DLLs, correlated with subsequent module loads and/or network connections to previously unseen destinations. The behavioral chain links process creation of msiexec.exe with suspicious parameters, network activity to retrieve payloads, and module loading indicative of malicious installation or DLL execution.

Log Sources

Mutable Elements

Field	Description
SuspiciousCommandlinePatterns	Patterns for identifying malicious msiexec.exe usage (e.g., UNC paths, external domains, DLL execution flags)
SuspiciousDestinationList	List of external domains or IP ranges considered suspicious for msiexec network connections
TimeWindow	Time range in seconds/minutes for correlating msiexec.exe execution with module load and network activity
LegitimateMSIHashes	Hash list of MSI packages considered known-good to reduce false positives