Detection Strategy for Indicator Removal from Tools - Post-AV Evasion Modification, Detection Strategy DET0189

Archived: 2026-04-05 14:56:49 UTC

AN0540

Detection of known tools or malware flagged by antivirus, followed by a near-term drop of a similar binary with modified signature and resumed activity (execution, C2, or persistence).

Log Sources

Mutable Elements

Field	Description
AVAlertMessage	Vendor-specific signature string or detection message that can be correlated to threat intel context.
TimeWindow	The time between AV alert and similar file/process activity (e.g., 5–30 minutes)
FilenameSimilarityThreshold	String or hash similarity thresholds between original and modified binary.

AN0541

Detection of anti-malware quarantining or flagging a tool, followed by a new binary written to disk with a similar function or name and a resumed process chain.

Log Sources

Mutable Elements

Field	Description
PathWatchlist	Tunable list of directories often abused for dropped binaries (e.g., /tmp, ~/.cache, /opt/soft/).
ProcessAncestryDepth	Limit how far up the tree to trace tool modification behavior for detection.

AN0542

Detection of XProtect or AV quarantining a known tool, followed by modification (file size, hash, string) and subsequent re-execution by the same or related user.

Log Sources

Mutable Elements

Field	Description
BinaryChangeThreshold	File hash delta or binary string diff score to tolerate renamed/mutated variants.
UserContext	User or group expected to use dev tools; reduce false positives from legitimate repacking.
