Detect Mark-of-the-Web (MOTW) Bypass via Container and Disk Image Files, Detection Strategy DET0257

Archived: 2026-04-05 15:26:08 UTC

AN0712

Detects extraction or mounting of container/archive files (e.g., .iso, .vhd, .zip) that originated from the Internet but whose contained files lack Zone.Identifier MOTW tagging. Correlates file creation metadata with subsequent execution of unsigned or untrusted binaries launched outside SmartScreen or Protected View.

Log Sources

Mutable Elements

Field	Description
WatchedExtensions	Adjust monitored file types (e.g., .iso, .vhd, .zip, .gz, .rar) based on enterprise usage
TimeWindow	Defines correlation window between extraction/mount and first execution of inner files
TrustedExtractionTools	Whitelist known enterprise archivers and deployment mechanisms to reduce false positives

---

Source: https://attack.mitre.org/detectionstrategies/DET0257