

# Detection of Malware Relocation via Suspicious File Movement, Detection Strategy DET0439

Archived: 2026-04-05 14:06:34 UTC

## AN1216

Detects the relocation of malicious executables via copy/move actions across suspicious folders (e.g., from Downloads to System32), followed by deletion of the original source or renaming to blend into legitimate binaries.

### Log Sources

### Mutable Elements

Field	Description
SuspiciousTargetPathRegex	Patterns like \Windows\*, \System32\*, or temp+execution directories
TimeWindow	Correlate copy+rename+delete chains within 5-minute window
FileExtensionFilter	Limit to .exe, .dll, .js, .bat unless context suggests otherwise

## AN1217

Detects binary movement or copying between untrusted and trusted paths (e.g., /tmp/ → /usr/bin/ or /etc/init.d/) that may indicate persistence attempts or cleanup of origin traces.

### Log Sources

### Mutable Elements

Field	Description
RelocationPathPatterns	Match movement into known persistence or exclusion directories
BinaryEntropyThreshold	Apply threshold to detect high-entropy relocations (e.g., packed malware)

## AN1218

Detects movement of binaries to ~/Library/ , /System/ , or app bundle locations, especially after initial execution or download from Safari or Mail.

### Log Sources

### Mutable Elements

Field	Description
TargetBundlePathPattern	Monitor relocation to .app/Contents/MacOS/ or ~/Library/Launch*
QuarantineFlagCheck	Check for disappearance of com.apple.quarantine attribute post-move

### AN1219

Detects firmware or script relocation attempts (e.g., CLI-based `copy` , `move` , or `rename` ) between temporary partitions and config startup folders on routers or switches.

### Log Sources

### Mutable Elements

Field	Description
StartupConfigPath	Targeted config folders like flash:/startup-config or nvram:
CommandPatternMatch	e.g., <code>`copy tftp flash`</code> , <code>`rename`</code> , <code>`move flash:/old.bin flash:/new.bin`</code>

---

Source: <https://attack.mitre.org/detectionstrategies/DET0439#AN1217>