Detection Strategy for Hidden File System Abuse, Detection Strategy DET0461

Archived: 2026-04-02 10:35:39 UTC

AN1271

Anomalous creation or mounting of hidden partitions or virtual file systems. Defender view: detection of registry modifications linked to non-standard file systems, suspicious disk I/O patterns, or bootkit-like behavior where hidden volumes are accessed outside normal file system APIs.

Log Sources

Mutable Elements

Field	Description
MonitoredRegistryKeys	Specify registry paths for mount points and hidden partition configs.
DiskIOThreshold	Tune thresholds for raw disk access outside expected drivers.
TimeWindow	Correlate boot-time anomalies with hidden file system mounting activity.

AN1272

Unusual mounting of loopback or pseudo file systems not aligned with legitimate administrative activity. Defender view: monitoring auditd and syslog for mount commands involving suspicious mount points, reserved blocks, or device mappings indicative of hidden partitions.

Log Sources

Mutable Elements

Field	Description
AllowedMountPoints	Whitelist standard mount points to reduce false positives.
UserContext	Flag root escalation during mount operations.

AN1273

Hidden file system use through APFS containers or custom plist configuration. Defender view: anomalous use of hdiutil or diskutil to attach hidden partitions, modification of plist entries tied to system volumes, or suspicious

raw disk access.

Log Sources

Mutable Elements

Field	Description
MonitoredPlistPaths	Adjust to target only relevant plist files linked to volume mounting.
ProcessScope	Restrict monitoring to sensitive processes like diskutil and hdiutil.

Source: https://attack.mitre.org/detectionstrategies/DET0461