Detection Strategy for Hidden Artifacts Across Platforms, Detection Strategy DET0502

Archived: 2026-04-05 13:55:34 UTC

AN1384

Abuse of file/registry attributes to hide malicious files, directories, or services. Defender view: detection of attrib.exe setting hidden/system flags, creation of Alternate Data Streams, or registry keys altering file visibility.

Log Sources

Mutable Elements

Field	Description
FileExtensions	Filter for sensitive file types likely targeted for hiding.
ADSDetection	Enable or disable detection of Alternate Data Streams depending on business use.

AN1385

Hidden file creation using leading '.' or file attribute changes with chattr (immutable/hidden flags). Defender view: detect execution of chattr, lsattr anomalies, and unusual hidden files appearing in system directories.

Log Sources

Mutable Elements

Field	Description
DirectoryScope	Restrict hidden file detection to privileged system directories.
AttributeFlags	Tune for specific chattr flags (+i immutable, +a append-only) most abused for persistence.

AN1386

Hidden files via 'chflags hidden' or Apple-specific attributes, LaunchAgents/LaunchDaemons placed in non-standard hidden directories. Defender view: detect command execution modifying file flags and unusual plist creation in hidden paths.

Log Sources

Mutable Elements

Field	Description
HiddenDirectories	List of directories monitored for hidden plist or agent placement.

AN1387

Abuse of VMFS or ESXi shell to hide datastore files, renaming/moving VMDK or VMX files into hidden directories. Defender view: anomalous ESXi shell commands or file operations obscuring VM artifacts.

Log Sources

Mutable Elements

Field	Description
VMFileScope	Restrict to VMDK, VMX, or log files critical for VM operations.

AN1388

Malicious macros or embedded objects hidden within Office documents by renaming streams or using hidden OLE objects. Defender view: detection of hidden macro streams or objects in documents correlated with anomalous execution.

Log Sources

Mutable Elements

Field	Description
MacroScope	Tune detection to specific Office apps and document types where macros are disallowed.
