Detection Strategy for Hidden Files and Directories, Detection Strategy DET0032

Archived: 2026-04-05 16:12:36 UTC

AN0091

Suspicious use of attrib.exe or PowerShell commands to set hidden attributes on files/directories. Defender view: processes modifying file attributes to 'hidden' or creating files with ADS (alternate data streams).

Log Sources

Mutable Elements

Field	Description
MonitoredExtensions	Filter hidden file detection by sensitive file extensions (.exe, .dll, .bat).
ADSMonitoring	Enable detection of alternate data streams depending on organizational usage.

AN0092

Creation of files or directories with a leading '.' in privileged directories (/etc, /var, /usr/bin). Defender view: monitoring auditd logs for file creations where name begins with '.' and correlated with unusual user/process context.

Log Sources

Mutable Elements

Field	Description
DirectoryScope	Restrict detection to critical directories to avoid noise from benign hidden files like .ssh or .config.

AN0093

Use of chflags hidden or SetFile -a V commands to hide files, or creation of hidden files with leading '.'. Defender view: monitoring process execution and file metadata changes setting UF_HIDDEN attribute.

Log Sources

Mutable Elements

Field	Description
HiddenAttributeScope	Restrict detection to non-standard directories where hidden flags are unexpected.

Source: https://attack.mitre.org/detectionstrategies/DET0032#AN0091